Self-sovereign identities and the underlying technologies: a critical analysis

yann cantais - mathieu degre

June 2022

Contents

1 Introduction

1.1

For more than 20 years, a desire to provide qualitative electronic identities to citizens of different countries has been developing. Pushing this phenomenon even further, the interconnected world in which we live has led us to think about the standardization of these electronic means of identification, for example with the proposal of the new EIDAS2 regulation, which plans to provide European citizens with a digital identity that is recognized everywhere in the European Union.

This desire to manage citizens' identities has been brought about by the multiplication of different applications and the increasing omnipresence of the use of the Internet in our lives. Some initiatives have already been put in place, but to date, there is no sufficiently effective solution that preserves the confidentiality of data and gives users control without a centralized entity that covers territories in several countries or states.

The users of the various services that exist are more and more attentive to how their data is managed. It is therefore a major challenge to be able to implement a solution that preserves confidentiality and where identifying information is not stored by a third-party entity without really knowing who will or will not have access to this information.

Thus, it is not surprising that decentralization technologies such as blockchain and distributed ledgers are at the center of attention to achieve a solution. These solutions are the best hope for solving the identity management problem by meeting all the desired criteria.

Behind this rhetoric, it is worth analyzing why the self-sovereign identity technology is the most prominent now to address the problem of digital identity. Is it really the best solution? What are the limits of this technology and are there other more suitable solutions? These are the questions we will address in this report.

1.2 Definitions

To better understand the concepts discussed in this report, here are some definitions.

A digital identity is every electronic information that is associated with someone, some organization or some electronic device. These identity systems are used both for authentication and authorization.

Self-Sovereign identity is a specific approach to digital identity that allows people to have a better control of their digital identities and on how it is used by services. Self-Sovereign identity addresses the difficulty to trust organizations or individuals during an interaction. One party in an interaction will present credentials to the other parties, and those relying parties can verify that the credentials did indeed come from a trusted issuer.

To be self-sovereign, it is usually established that users control the credentials they hold. Their consent is always required to give or use these credentials to other individuals or services. It reduces the possibility for these credentials and data to be shared without their approval. In a self-sovereign identity system, users have unique identifiers called decentralized identifiers. Most of these systems are decentralized and rely on crypto wallets. The credentials are verified using cryptography with public keys anchored on a distributed ledger. This is the opposite of centralized identity with identity provided by some outside entity.

As it is explained in [Baa16], Self sovereign identity or Sovereignty provides ten principles :

1. "Existence: Entities must have an independent existence and cannot only exist digitally."
2. "Control: Entities must be able to control their identities, they should always be able to refer, update or hide it."
3. "Access: Entities should have direct access to their own identity and all related data. All data must be visible and accessible without gatekeepers."
4. "Transparency: The system and its logic must be transparent in how they function, how they are managed and how they are kept up to date."
5. "Persistence: Identities must be long-lived, at least for as long the user desires but it should not contradict a "right to be forgotten"."
6. "Portability: All information about identities must be transportable. The identity must not be held by a singular third party."
7. "Interoperability: Identities should be as widely usable as possible."
8. "Consent: Entities must agree to the use of their identities and the sharing of all related data."
9. "Minimization: Disclosure of claims must be minimized."
10. "Protection: The right of entities must be protected, when there is a conflict between the needs of the network and the right of entities, the priority should be the latter."

2 Self-sovereign identity, a scalable, cross-border implementation

2.1 The European project Eidas2

With the digitization of most aspects of society, the issue of digital identity has never been more important. It has always been a major issue. How to transfer and prove one's physical identity through the virtual world?

The development of digital identities in Europe over the last 20 years has been funded by the European Commission. This combined research has formed the pillar of the Eidas regulation. Some countries have even adopted the electronic identity card for example. Despite these initiatives, digital identities today are most often in the form of a login and password. The development of digital identity still faces major challenges.

The real challenge is to put in place an ecosystem using this technology that is adopted by users and services alike and that can stimulate this use of digital identity, while at the same time establishing it in a sustainable manner over time. To be adopted, digital identification systems must be accepted by a maximum number of applications and services in order to have a sufficiently large ecosystem to attract users. Indeed, studies show that for the user, it is not the confidentiality of the data or the security of the data that is important first but the ease of use of a technology that makes it used. Moreover, users often do not prefer a system where they have to pay. This poses a problem and hinders the development of sovereignty technologies because it is difficult to find a sustainable economic model for identity providers [Coma].

The reglementation eIDAS has been updated and says now that by 2023, every state of the European Union shall provide a Digital Identity Wallet to every citizen who wants one. This aims at building a EU Digital Identity Wallet which will be cross-border and who will offer many benefits to citizens, states and enterprises.

Many other questions arise as well. What about privacy? Should people be forced to identify themselves on the Internet? What about freedom of expression? Will user data be secure and protected?

2.2 The use cases

The main objective of the EUDI Wallet is to provide a secure, practical and easy authentication to a private space that would contain and centralize a maximum of personal data. The data stocked in the wallet aims to be shared with external entities with proof of ownership provided by the wallet. This general kind of definition can be broken down into a few key points [Comb]:

- First, the authentication. The European Union doesn't plan for now to use a centralized way of authenticating. Instead, it's the member states that have to provide a secured and relatively simple way of identifying. Security is, of course, one of the main priorities at this point, because having everything centralized means that an identity usurpation or, even worse, a security breach that would leak multiple identifiers, could have catastrophic consequences for the parties involved.

- However, despite this state-centered authentication system, the wallet aims to be international, and so all of these state-internal systems have to communicate with each other, if requested.

- The main documents that should be included in the wallet include, in February 2022:

  - The diplomas and certifications relative to education. This would be mainly useful abroad to check the validity of international diplomas instead of spending time-consuming resources.
  - The health-centered documents: Sharing medical files between hospitals, or any health institutions, is really long nowadays and can take years. The risk of losing valuable documents is important, and even more so in a subject as important as health. The Wallet would provide a way to fix a part of these problems by acting as a trusted intermediary.
  - Mobility: The Wallet would facilitate the share of mobility-related documents across borders, which would help exchanges.
  - Secured authentication to other services: The Wallet would act as a trusted authentication supplier to connect to other services that require such connections. This would function like, for example, the service France Connect works in France.
  - Finance: The wallet could allow trusted and highly-secured payments between entities. The exact use case for this very subcase is yet to be determined.

Let's detail who will be actors of this ecosystem, and how they will interact with each other, as of the February 2022 revision.

- The end users of Wallets will be all the users that will use the wallet to prove, or receive proof of identity, or any similar services. Typically, the citizens of the member states. This initiative would obviously not be mandatory for the citizens, but the state members will have to provide the opportunity of using it or not.

- The Wallet Issuers will be all the ones that would be allowed to deliver a wallet to the end user: in this case, the member states and every organization appointed by a State Member.

- The Providers of Person Identification Data (PID) would be the one tasked with verifying a user's identity through a PID, and connecting it to its wallet. It must also provide an explicit way for the Wallet to check and validate its verification and not to rely on a single actor verifying the identity. This role can be combined with the Wallet Issuer
- The Providers of Registries of Trusted Sources will be tasked to mark the other actors as legitimate. For example, if a member state entrusts a third-party to be a Wallet Issuer, it will be necessary that the member state provides a certified registry of such Issuers. Different registries for different roles could be provided by different providers if required. Such actors would have the responsibility of maintaining such registries, assuring they are up-to-date and accessible.
- Qualified Electronic Attestation of Attribute Providers would be dealt by Qualified Trusted Service Provided for their respective Service. One example of such a certificate would be a qualified certificate of nationality. They must provide ways to check the validity of their certificates, and can't store any knowledge about what the certificate will be used for. On the same pattern, Non-Qualified EAA Providers would be dealt by TSP for their respective Services. The rules for the interactions between TSPs and Wallets are yet to be determined, but would likely depend on the TSP. If necessary, they can publish a catalogue (Catalogue of Attributes and Schemes for the Attestations of Attributes providers) publicly available that will help the other entities to interact with them.
- It is required that the Wallet allows the user to append its signature via the Wallet. This can be accomplished by two means: either the Wallet itself contains a qualified signature/seal creation device (QSCD), or it relies on an external QSCD. If this option is chosen, it will require a Qualified and Non-qualified Certificates for Electronic Signature/Seal Providers (again, dealt by a QTSP)
- The policy concerning other Providers of Trust Services is yet to be determined, but should follow the same guidelines as the previously mentioned services.
- The Authentic Sources would be every entity trusted or forced by law to store information about an individual, like address, age or education qualifications. They will need to provide interfaces to QEAA Providers to allow them to check the validity of such information.
- This would require the consent of the person in question to allow QEEAP to use their data.
- Relying Parties would be the ones that use the Wallet to act as a trusted authentication intermediary. In order to do so, it will be necessary to install gateways to allow such services to use some information from the Wallet to perform the authentication.

- Conformity Assessment Bodies would be the organizations, appointed by Member States, that will be tasked with verifying the authenticity and the validity of newly provided Wallets, and also to give to TSPs the Qualified attribute if deserved. They will check regularly if the requirements for the Qualified status of such services are still respected.
- Supervisory Bodies will be tasked with handling Non-Qualified TSPs
- Device Manufacturers and Related Entities are all the entities that will provide, in devices where the Wallet will be present, interfaces to other services, like an Internet Connection, a microphone, or a Wi-Fi interface, or any services similar, like storage. They will be required to follow strict rules mainly concerning the cryptographic security of the data they're handling.

2.3 The Functional Requirements

After seeing how actors will interact between each other in the larger ecosystem, let's have a look at what are the minimum functionalities or properties that Wallets must have before being published.

As we've seen, the core utility of wallets is their ability to store PIDs and QEEAs or EEAs. As such, it is either necessary to store such important information locally to avoid comprimmission and by ease of access, or at the very least to store locally pointers to where the information is located. It must also be able to request PIDs and (Q)EAA online through an interface that shall be, like all the other interfaces in the Wallet, accessible and intuitive.

The use of efficient, secure and strong cryptographic functions is a must-have for Wallets. It would be better if such functions would be stored locally but it's also possible to have them stored elsewhere with locally stored secure means of recovering them. These functions shall be used every time sensitive information is being passed or exchanged through the Wallet. This include, but is not limited to, online authentication, request of PID and (Q)EAA, or access to local datas.

To maximise security, it's necessary to implement mutual authentication between Wallets and Third Parties. Wallets must be able to identify and verify the integrity of every third party it's interacting with, including TSPs, Wallets Issuers and relying Parties. To harmonise and facilitate those operations, mainly at an european scale, it will be important to define clear protocols to follow. In general rule, interoperability between member states is a global requirements for Wallets.

The Wallet must allow users to authenticate by sharing PIDs to third parties services. This authentication and share of data must be controlled by the user,

cryptographically secured, follow a common protocol every time to ensure interoperability, and should follow the principle of 'the need to know' and share only the information required to the authentication.

The user interface should be as clear and accessible as possible. In particular, in case of interactions with third parties, it should be very clear to see which are those third parties, what data they are requiring and why, what information will be transmitted and what are the rights under GDPR. This would apply for every operation: for signing, for example, it should be also very clear to see which document is being signed, who is requiring it.
It should also be very clear to see the logs of what interactions happened with this Wallet, to allow users to better check if they might have been compromised. This interface shall be accessible only through a two-factors authentication process to improve security. It's required for functioning wallets to be able to create either a signature or a seal, either directly or with the help of an external QSCD as we've seen in the ecosystem.
It's also required that interfaces with different actors like member state institutions should be put in place, as we can see in the following schema:

3 Analysis of existing technologies

3.1 Approaches to decentralized management

It's important to understand the difference between traditional identity management systems and blockchain-based systems like SSI. In traditional systems, the registration and the connection are separated, and each service provides its own interface separately. Even in the case of the use of a trusted intermediary, like for example FranceConnect in France or, to a lesser extends, a password manager, there is still the need to use an authentication and a registration form to connect to such service. On the other hand, with blockchain related identity management systems, the user uses its own identity to connect to a service. This shifts the authentication from a service-oriented view to a user-oriented one. The identity, the credentials used by the user are issued by trusted credential issuers. The user is the master of the information it wishes to share by external services.

The blockchain is used here as a secure and trusted bulletin board to share Public Key, in order to create cryptographically secured communications, either through a Diffie-Hellman Key Exchange or through or more classic asymmetric information exchange. As the blockchain is a Distributed Ledger Technology, a technology where there is no centralisation of the data and where each node updates itself to have access to all of the information in the network, this share of public keys system is called a decentralized Public Key Infrastructure [Tom]. A Self-sovereignty Identity system uses such technology, with a maximum focus on the liberty of data management by the user, as we saw before. It uses a

bottom-up approach where no central authority could have a control over what the user could ask, by contrast with a top-down classic approach. However, despite these rather strict conditions imposed on a SSI system, because of the recent popularity of the subject, the term SSI is being used for systems that don't fully comply with the above rules [Baa].

This explains why a majority of existing or in-development sovereignty systems are based on blockchains in a decentralized approach to keep the property of credentials for their owners only.

It will now be helpful to talk about two very important concepts in blockchain-based identity systems: Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs). These two concepts are currently investigated by the World Wide Web Consortia (W3C), which shows the ongoing efforts to standardize these concepts. Verifiable Credentials are objects that contain information about its issuer. It has been provided by a trusted service, and signed by a cryptographically secure algorithm like ECDSA. The object must also contain metadata that contains every useful information like the issuer, the algorithm used to sign, ... Also, it must have an intern method to remove itself, but without leaking any private information about the user, and so must balance effectiveness and privacy. This problem is still ongoing today, and no consensus has yet been achieved on the solution. For example, in Ethereum-based IdM systems, currently, there is a blockchained-connected registry that users can access to directly remove the information. This of course isn't a really practical solution when privacy is at the core of the technology, and even IdM is currently trying to shift this method towards something closer to what W3C recommends, which is to only use the blockchain to associate authentication method and identifier. To put it in a nutshell, Verifiable Credentials are credentials signed cryptographically, which aims to be passed to a third-party issuer which can easily verify the authenticity of the information thanks to cryptographic methods.

Those private keys and credentials, which are vital for a user in order to connect with VCs, are usually stocked in Wallets, which are usually located on smartphones, although they can be located in other devices like desktops or cloud services. If the Wallet is provided by a third party, it's called a custodial wallet. This one specifically can be used to recover keys or credentials if the main wallet has been lost or damaged. Finally, hardware wallets like hard drives, or paper wallets (e.g. private keys directly printed on paper) can be used to store backup wallets. It goes without saying that this last option should only be used if no other backup options are available.

Decentralized identifiers are publicly (or at least locally) available identifiers, used for authentication. They're associated with a Public Key, and the proof of ownership is given by a proof of possession of the private key associated with the public key. For example, this can be done like this:

- User A wants to connect to User B with DID A
- User B sends a verification string to User A
- User A signs / encrypts the string with the private key and send it to User B
- User B uses the public key associated with DID A to decrypt the string. If this deciphered string correspond to the same one it sent, then User A proved that it owns the private key of DID A

A specification of this standard has already been released by W3C [W3C]. It contains all the information required to manage such entities. Notably, one tool that is associated with DIDs is the DID resolver, which takes a DID object and produces a DID document, which is a set of datas describing the DID, like public keys. Universal DID Resolvers are currently being worked on.

3.2 Comparing existing systems

3.2.1 The premise of self sovereign identity : onename.io

Onename.io was created in order to simplify bitcoin transactions between users [one]. Instead of using long adresses and qr codes, it aims at using verified names in order to make a transaction.

It is not common when it comes to blockchain that people have to identify themselves through social media. One also needs a wallet app compatible with onename.io. Onename takes advantage of Bitcoin's distributed ledger, the blockchain, which is used to record and verify bitcoin transactions.

Sign-up is fairly simple: people just select a name and confirm their identity by registering on a social media app such as Twitter or Facebook. Once they are confirmed, they can send and receive bitcoin just by typing usernames into compatible wallets. It is also a way to certify the social networks acounts that people own in order to access them with a private key. The usernames are registered in an open namespace. Users data is integrated directly on the blockchain and it cannot be modified or censored by anyone. For now, this technology is far from secure in term of the first authentication process but it would be possible to rely on concrete credentials to become a trusted digital identity.

3.2.2 The case of Estonia

Being at the cutting edge of digital management and digitalisation, Estonia was without surprises the first European state to put in place SSI systems nationwide. There are currently two main systems.

The first one is called e-Residency, and its aim is to facilitate business in Estonia from abroad. Indeed, it's possible for any citizen to apply for e-Residency, as long as they're willing to create a business in Estonia. People who are accepted in this program get access to a Wallet with a digital identity issued by the state, which ensures, for now, its sovereignty. Then, the owners of those wallets are able to use their identity to sign, encrypt and decrypt documents, access trusted services, and other advantages related to business that are related to business but not really with SSI. This service inspires enough confidence abroad to make some external entities trying to include themselves in the ecosystem, like for example Ethereum: it's now possible to sign Ethereum transactions with the e-Residency.

The second one, called e-Identity [eEs], is offered to every Estonian citizen, regardless of where they live. They have the same services as e-Residents, like signing, encrypting and decrypting documents [dev], but are also able to vote, check medical bills or pay taxes through trusted services managed by the government. The cryptography behind the security of these two systems is based on Elliptic Curve Cryptography, and to be more precise here 384-bit ECC public keys (Secp384r1), which ensures both a high quality of security and a high speed for every operations.

3.2.3 The Belgium case

Belgium has a robust identity system and offers its citizens the possibility to benefit from digital identity cards, called eID. About 59 in a 100 Belgian citizens interact digitally with the government. The Belgian public sector is dynamic in terms of identity system governance.

This eID is a digital proof of identity containing a chip that allows several things. First of all, it allows you to identify yourself to prove your identity, for example in the street with your smartphone. It is also possible to connect and authenticate oneself online to prove one's identity to public services. Another feature is to sign electronically as an adult. An electronic signature has the same legal value as a handwritten signature. There are currently three types of proof of identity:

- The electronic identity card for Belgians over 12 years old
- The Kids-ID, for Belgians under 12 years old
- The electronic card for foreigners

This eID system is now compliant with the eIDAS regulation and ISO-7816 certification. The security and confidentiality of users' personal data are ensured at a high level. This is especially true for fingerprint information. Users who use self sovereign identity properties consent to the use of their data by public sector organizations.

Several initiatives are being developed in Belgium to meet the needs of self sovereign identity. The "MonDossier" project allows citizens to see the data that the state has on them. This data is centralized by the Belgian National Register1, a central institution for identity management in Belgium. It is likely that citizens will be able to extend their means of identification in the "MonDossier" application.

Another app, itsme, developed in 2017 by a consortium of Belgian banks and cellular connection providers allows you to identify yourself securely. This allows you to log in, confirm transactions, and sign documents. On this application, it is possible to identify yourself with the eID or else with your bank card and is used by 1.8 million Belgian citizens.

It is interesting to note that itmse is a private sector initiative, operated in agreement with the state. Absolutely all means of identification, itsme included, must be controlled and approved by the federal public authentication service. Here, the government has allowed flexibility in the choice of technology, provided that the governance framework is respected. The self-sovereignty of itsme is ensured by an active consent step that users give to each transaction, specifying what information is allowed to be shared and with whom. The itsme system involves many private partners. To solve the problems of exchange between the public and private sector, it is envisaged to implement a system providing a centralized identity and other decentralized attributes. There could be several attributes contained in the databases of different entities. The digital identity will allow access or not and will administer consent between the parties as explained in the text [MTC21].

As one of the experts states in the text [MTC21], itsme is a very centralized wallet limited to identity authentication. Another important point is that every transaction can potentially be monitored. This turnkey solution produced by the private sector creates a huge dependency of the government on the private sector.

3.2.4 The German and Spanish collaboration

In 2021, the Spanish and German governments signed a joint declaration attesting to an agreement between the two countries to cooperate in the field of digital identity, including cross-border sovereign self-identity [bun]. This agreement foresees a pilot project in the near future to contribute to the development of the European digital identity announced in the proposal of the eIDAS Commission. This agreement aims to explore the possible options to establish a large-scale digital identity system, open to all their citizens, decentralized, secure and reliable. This system will be based on state-issued credentials. This collaboration is open to other member states that wish to participate.

Spain's Secretary of State for Digitalization and Artificial Intelligence, Carme Artigas, said: "People should be empowered in relation to their data and identity. The collaboration we are starting today with Germany on a self-sufficient digital identity is a step on the European path to data sovereignty."

German Minister of State for Digitalization Dorothee Bär said, "The German government recognizes that digital identity is a fundamental element for successful digitalization. We have already launched a national digital identity ecosystem based on ISS, which now involves more than 60 stakeholders from the private and public sectors, as well as a real-life use case - digital check-in at a hotel. In the coming months, we plan to implement several more national use cases to expand this ecosystem. We are excited to take the next natural step through our partnership with Spain to show the potential of decentralized user-centric identities to all of Europe."

The goal of this collaboration is also to show other countries the potential of digital identity at the national and European level, providing a secure and user-friendly identity for citizens. This extends offline rights to the online space.

3.2.5 The Sovrin Network

The Sovrin Network is an open-source management system that offers decentralized self-sovereign identity for users, organizations and devices. This network is built on Hyperledger Indy, an open-source distributed ledger meant for decentralized identity. It provides a strong security system and let users full control on their identity and data.
One can not operate nodes if he does not fulfill some requirements. Indeed, the Sovrin Network is not based on a public permissioned ledger. There are institutions that are trusted and that are called Stewards that have the permission and duty to operate nodes and participate to the consensus process. Common users can transfer their credentials, control their data and sign transactions for exemple, all of it in a secure way.

Additional libraries As it is said in [NJ21b], two main Hyperledger libraries are used : Aries and Ursa. Hyperledger Aries is used to provide verifiable digital credentials. Hyperledger Ursa provides a shared cryptographic library.

A digital identity is created through a standard called Decentralized IDentifier. The credentials linked to an identity are securely stored and controlled due to the Zero Knowledge Proofs, which is a cryptographic method for creaitng anonymous credentials. Users can create several identities that are separated for privacy reasons. Each identity has its pair of private and public keys.
Users determines what type of attributes they want to associate with their identity. They store their credentials by themselves on storages they own. They have full control on their data. The Sovrin Nework offers a social recovery method,

where Recovery Key Trustees trusted by the identity owner store recovery data on behalf of the identity owner in the trustees' own agents. The key distribution, verification, and recovery is based on the Decentralized Key Management System (DKMS) standard. This allows the management of cryptographic keys without a central authority.

As described in [NJ21b], the Sovrin Network is decomposed into 4 different layers :

- THE LEDGER LAYER : It runs on a blockchain with the Hyperledger Indy Ledger. It is a public ledger which means that anyone can write or read in it. However, all the operations are performed in accordance with the Sovrin Governance Framework.
  This management is not expensive. Transactions on the ledger are validated by known entities under proof of authority. The fact that it is not expensive make it possible to provide identity for all.
  The network does not store any personal identifying informations on the ledger. There are only credentials definitions, decentralized identifiers schema definitions and revocation registeries that are written on it. There are several ledgers : the config ledger, node ledger, domain/main ledger, and payment ledger. Only the domain ledger and payment ledger accept publicly available transaction types.
  The Sovrin Network rely on server nodes that are located around the world. These nodes are hosted and administred by trusted entities called the Stewards that validate the transactions. Each node contains a copy of the ledger, a record of the informations that are needed to verify credentials issued within the network. As a node can be a validator or an observer, it can act only one at a time.

- THE AGENT LAYER : An agent is a program made for an entity to interact with others. They share digital ids with each other and do not need to access the blockchain. The communication rely on signed and encrypted messages, based on a protocol defined in the Hyperledger Aries project. Every user have one agent per device they use, the edge agent, that operate locally and one agent in the cloud, the cloud agent that route requests to and from the edge agent.

- THE CREDENTIAL EXCHANGE LAYER : This layer involves the three key roles of issuer, holder and verifier. This layer establish how the the credentials are issued to the credential holder. It addresses how the credential verifier requests information from the credential holder and how the credential holder presents a proof of information from their credentials that can be trust by the verifier. A credential definition is used to define the credentials. It links the public DID of the issuer, the schema for the credential, and a revocation registry for the credential that are all stored on a distributed ledger.

- THE GOVERNANCE LAYER : No central authority controls the network, that is the definition of a decentralized system. However, this network is governed through the Sovrin Network Framework. It is required to provide trust to the network and to certify data security, privacy, protection and portability. Furthermore, it prevents censorship and ensures individual sovereignty.

3.2.6 The digital identity wallet from Thales

The development of the Thales portfolio is still in its infancy. However, it will provide the ability to have online identification and to perform electronic signatures [Tha]. For the time being, the wallet is not intended to be the digital equivalent of a physical card and will probably not replace the ID card in everyday life. However, for online transactions, including utility applications, the wallet is intended to provide an acceptable proof of identity.

EDIW will be accepted for authentication of individuals for public services upon launch. Launch. It is also expected that private services in the transportation, energy, banking and other sectors will accept EDIW. Smaller businesses - such as gyms and car rental companies - are expected to begin accepting it soon after implementation. In the public domain, it will also allow for the storage and delivery of driver's licenses, prescriptions, and medical records. It is also planned to replace passports and identity cards within the European Union, providing digital travel documents. It will be possible to pay with it and to certify your qualifications or diplomas.

In a second phase, when the use of this wallet will have developed, other uses will be added. We can then think of use cases such as providing a European health insurance card or documents to change your address, or to apply for scholarships and download degree certificates. In the private sphere, the wallet will be used for identity verification, age verification, service subscriptions, hotel check-in and flight check-out.

In a third phase, the development of 5G will allow the wallet to integrate iot services. An example of this would be to be able to store your car keys on your wallet.

A very important point of the wallet is that private sector companies will not be able to monetize user data. These companies will also have to provide a level of security and privacy equivalent to that of government providers.

In order to publicize this wallet and push its use, the very large online platforms would be forced to accept its use. After 18 months, if uptake of the wallet is too slow, further efforts could be made.

This Thales wallet is specifically designed to meet the Eidas2 proposal. Thus, it is essential that common practices are developed and that the different systems are compatible. The toolkit for a "European Digital Identity Framework" will be developed through cooperation between the Member States, the Commission and private sector operators. This toolkit will have to define everything that states need to put in place the technical architecture to deliver the portfolio. It will contain a set of common standards and technical references, practices and guidelines.

Many of these practices will be derived from European and international standards. A lot of work will remain on the security of the portfolio. The technical specifications for this Thales project are being finalized and should be released during 2022. Testing will follow and member states are expected to implement their plans in 2023.

3.3 Comparison

It is clear that the onename.io is not a self sovereign solution as it rely on social medias to realize an identification. The first rule of Sovereignty [Baa16] is not respected here. Anybody can create a fake account with a false name and therefore, link it to a bitcoin address. On an other hand, the other solutions seem to rely on strong ways of authentication. In all the country having a digital identity solution, the government seems to take the authentication process seriously in order to get a eID.

Onename.io and the Sovrin Network are cross-border networks. Thales's will is to create a solution to deploy in all Europe but it is not yet created. It is interesting to see that each country has its own policy. Estonia for exemple, has opened it border to let foreigners be part of their program e-Residency whereas the other countries, Belgium, Spain and Germany have managed solutions only for their own citizens. The Sovrin Network offers the possibility of digital identity in several countries as it is public and everyone has access to it. It is then written in [NJ21a] that this network offers a sovereign identity but is subjected to the place where the user is living. Some laws may make variations between levels of sovereignty in different countries. This is beyond the control of Sovrin which does not work with governments. The digital Identity allet from Thales answers the call for a system deployed in all Europe and shall give the same sovereignty to every user it gets as governments laws will be tailored by the European Union to harmonize this technology across Europe.

Estonian and Belgian governments are using enterprises from the private sector to put their eIdentity system in place. It tackles the issue of the power that these private corporations will get. Thales is also a private corporation that could become very powerful if it manages to deploy its solution across all Europe. We can wonder if the solution will indeed be decentralized with no

governance at all from these corporations or if they will take advantage from digital identity. As Speaking of governance, Sovrin is public but it functions with Stewards, that are authorized members to validate transactions. How can Governments be sure that they will control the systems and be the only governance if they delegate to private entities is a true concern.

The Sovrin Network's architecture seems very trustable, with a very strong security system and a governance that manage the nodes on the network and prevents people to lose their identity. Thales seems to want to deploy a solution that looks like Sovrin but aims to work with the countries of the European Union in order to build an ecosystem that will work the same way cross-border. Despite, the variety of existing systems across Europe can be a problem in building an homogeneous ecosystem. For exemple, Belgium policy is strongly focused on centralization as the EUID would be decentralized. It may be a problem to find common ground for different countries and different cultures.

4 Critique of decentralized management

4.1 A new technology still in development

Sovereignty technologies have been in the spotlight for a short time. As a result, developers are rapidly deploying SSI solutions using for example already existing systems like Hyperledger Indy. Because of this rapid development, versions can become unstable and are frequently changed. Some security flaws could therefore appear in these solutions. It is therefore risky to develop a system now, on an industrial scale, as it may require costly modifications as different technologies and standards are implemented and adjusted.

Until now, user data is monetized, and this monetization allows services like facebook or google to be profitable. With a system of self-sovereignty and control of the data by the users, it is obvious that the goal is not to have this monetization anymore. However, the development and maintenance of digital wallets will inevitably entail a cost. Users are certainly not willing to pay. A new economic system must therefore be established, which has yet to be determined.

4.2 A non-liability

One of the goals of privacy protection is non-liability. No one (neither the issuer of the securities nor the auditors) should be able to monitor the use of the securities by their ownership. A securities auditor should not need to contact the securities issuer to verify that the security has not been revoked.

An important problem is that non-liability conflicts with transparency. It is indeed, in theory, impossible to monitor the use of credentials. This implies a security gap because even the owner of the credentials cannot verify their use. If a wallet is compromised and an intruder uses the credentials, the owner

cannot realize the fraudulent use of their identity. The lack of transparency is therefore very dangerous and can lead to identity forgery without the intruder being bothered.

4.3 A difficult identification

Self sovereignty, by its name, implies that users manage their digital identities without relying on a third party. The confidentiality and security of their information relies on one or more private keys. In case of loss of this key, with a decentralized blockchain system, it becomes very complicated to recover it. It is obviously necessary for third parties to intervene in case of key loss. Finding the balance between confidentiality and ease of use is therefore a necessary and difficult task.

In addition, these third party entities, for example, empowered to manage and retrieve your key, will need to be administered by governance bodies to ensure that the third party entities meet all necessary standards. Credential portability is a new concept. Governance is also needed to ensure regulation.

4.4 The need of a Governance

One question that arises is that of trust in the entity issuing the identity documents. How do we know that it is the official body, that it is the right entity? If anyone can issue a certificate of competence or official character in the name of an entity, how can we be sure that the certificate issued is indeed issued by the official entity and that it is not a third party? We can take the example of certified accounts on instagram. Instagram is the sovereign entity that validates the certification of such or such account. This entity alone can decide who is certified or not. In a decentralized system, the authority of Instagram no longer exists. So, how can you be sure that an instagram account of a well-known brand is really who it claims to be? The account in question can be created by someone else.

Thus, certificates must retain their value. Self sovereignty must therefore guarantee that a public key issued is really issued by the entity that claims to have issued it. At present, setting up a system where the community agrees on what is trustworthy is possible, however, it is not clear that the dedicated cost and speed of consensus can compete with the ease of creating fake accounts at zero cost.

A viable and widely applicable system of self sovereignty would have to include centralized governance of some aspects of the system to address this problem. This however goes against one of the main arguments in favor of self sovereignty, decentralization. Users are still obliged to trust certain entities, namely the developers of the ISS system such as those in charge of portfolios for example, who

have significant power. This goal can be achieved by open source development of applications. It is therefore quite complicated to set up a system and to find the balance between a decentralized and centralized system.

5 Conclusion

Even if SSI brings novelty and innovation in the field of digital identity management, it's not a complete and total revolution: old problems like how to deal with trust anchors still exist and remain. Moreover, if the security and transparency provided by this service are obvious advantages that come out of the SSI system, they also imply a difficulty to detect illegitimate connection from a legitimate account, for example through an identifiers leak, and so even for the legitimate owner of the compromised account. Coupled with the fact that SSI systems will most likely require external cloud services to function, and so to have trust in, it seems clear that this technology has flaws. This could make it complex to find trust services / providers that would agree to be integrated in the ecosystem. This 'lack of trust' may be emphasised by the fact that SSI models are currently looking for new trust frameworks (like SOVRIN) to be based on, instead of already established and trusted ones. Maybe it would be a better idea to try to integrate SSI networks in such frameworks, which would help tackling the sustainability problem that currently has no real answers for such systems.
Despite all of these flaws, SSI certainly brings something new to the table and could be used to tackle otherwise impossible problems. Lots of important international actors like governments or even multinationals are currently showing lots of interest in this technology. One of the main points that could lead to its success would be the fact the Distributed Ledger Technology used by SSI, by being distributed, doesn't rely on a platform. For business, it means that a company that would be interested in investing in or through it wouldn't be forced to finance an external operator by doing so.

6 Bibliography

References

[Baa16] D.S. Baars. *Towards self-sovereign identity using blockchain technology*. Oct. 2016. URL: http://essay.utwente.nl/71274/.

[MTC21] Stanislav Mahula, Evrim Tan, and Joep Crompvoets. "With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case". In: *DG.O2021: The 22nd Annual International Conference on Digital Government Research*. 2021, pp. 495–504. DOI: 10.1145/3463677.

[NJ21a] Nitin Naik and Paul Jenkins. "Does Sovrin Network Offer Sovereign Identity?" In: *2021 IEEE International Symposium on Systems Engineering (ISSE)*. 2021, pp. 1–6. DOI: 10.1109/ISSE51541.2021.9582472.

[NJ21b] Nitin Naik and Paul Jenkins. "Sovrin Network for Decentralized Digital Identity: Analysing a Self-Sovereign Identity System Based on Distributed Ledger Technology". In: *2021 IEEE International Symposium on Systems Engineering (ISSE)*. 2021, pp. 1–7. DOI: 10.1109/ISSE51541.2021.9582551.

[Baa] Djuri Baars. *Towards Self-Sovereign Identity using Blockchain Technology*. https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf.

[bun] bundesregierung. *Germany and Spain and join forces on the development of a cross-border, decentralised digital identity ecosystem*. https://www.bundesregierung.de/breg-de/aktuelles/germany-and-spain-and-join-forces-on-the-development-of-a-cross-border-decentralised-digital-identity-ecosystem-1947302.

[Coma] European Commission. *Commission proposes a trusted and secure Digital Identity for all Europeans*. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663.

[Comb] European Commission. *European Digital Identity Architecture and Reference Framework*. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline.

[dev] devpost. *Ethstonia Identity*. https://devpost.com/software/ethstonia-identity.

[eEs] eEstonia. *e-Identity*. https://e-estonia.com/solutions/e-identity/id-card/. Accessed: 2015-05-13.

[one] onename.io. *Onename launches blockchain identity product passcard*. https://bitcoinmagazine.com/business/onename-launches-blockchain-identity-product-passcard-1431548450. Accessed: 2015-05-13.

[Tha] Thales. *White Paper Wallet Thales*. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/documents/what-is-EU-ID-wallet.

[Tom] Ken Timsit Tom Lyons Ludovic Courcelas. *Blockchain and digital identity*. https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf.

[W3C] W3C. *Decentralized Identifiers (DIDs) v1.0*. https://www.w3.org/TR/did-core/.