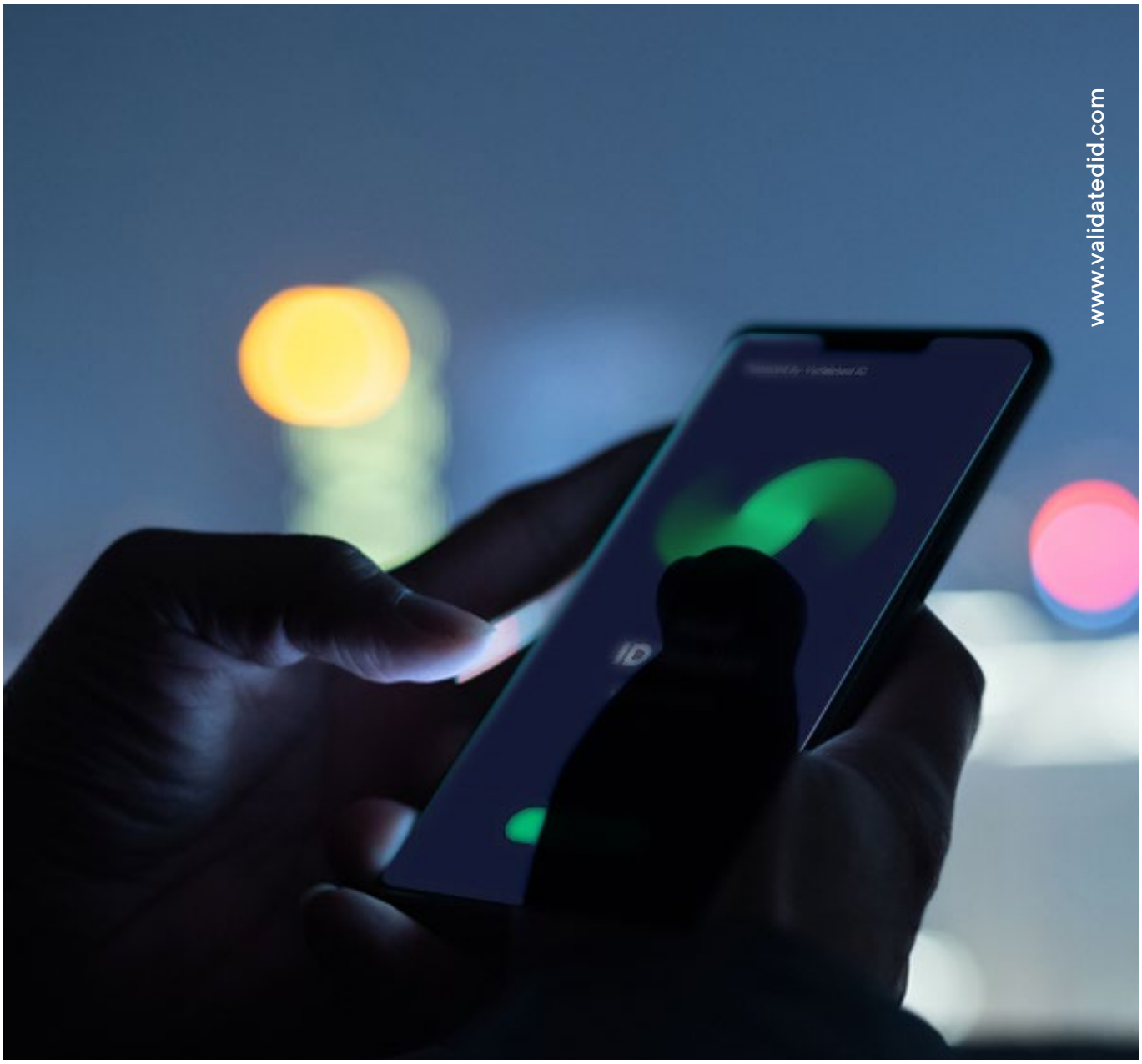
Validated ID

Always be yourself

The evolution of the sovereign self identity



Introduction

Ivan Basart, CTO of Validated ID

The history of the concept of Self-Sovereign Identity (SSI) is relatively short. At first, decentralized identity was a topic of concern only to highly specialized professionals. This group was concerned about privacy issues related to centralized digital identities. This led to forms of identity management based on cryptography.

It gained attention because of a surge in data breaches. These breaches exposed millions of people's data, stolen from large companies such as Yahoo, Equifax, eBay, Uber, and others.

Blockchain technology followed, with its ability to create systems that are more secure and fraud-proof than those created before. This led to the push for decentralization of identity.

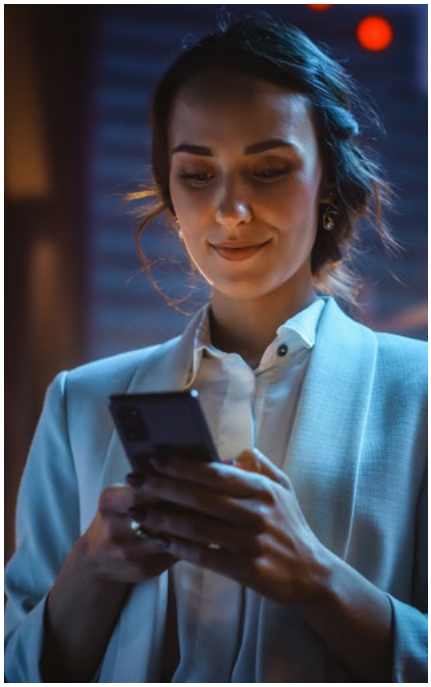
Public concern about privacy and security reached such a level that governments began to regulate this area with laws such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA).

It is surprising that regulators have made self-sovereign identity the basis for the updated identity regulation in Europe (eIDAS 2.0). In this section we will review the evolution of the identity world in recent years to understand the current moment.

The seven laws of identity

The history of self-sovereign identity began with The Seven Laws of Identity, written in 2005 by Kim Cameron, a systems architect at Microsoft.

Kim was a guru on this subject and sadly passed away a few months ago. He has always been considered one of the key figures in **the evolution of decentralized identity**[1]. The theory of identity laws describes what a modern, flexible and secure identity model should look like. They are as follows:



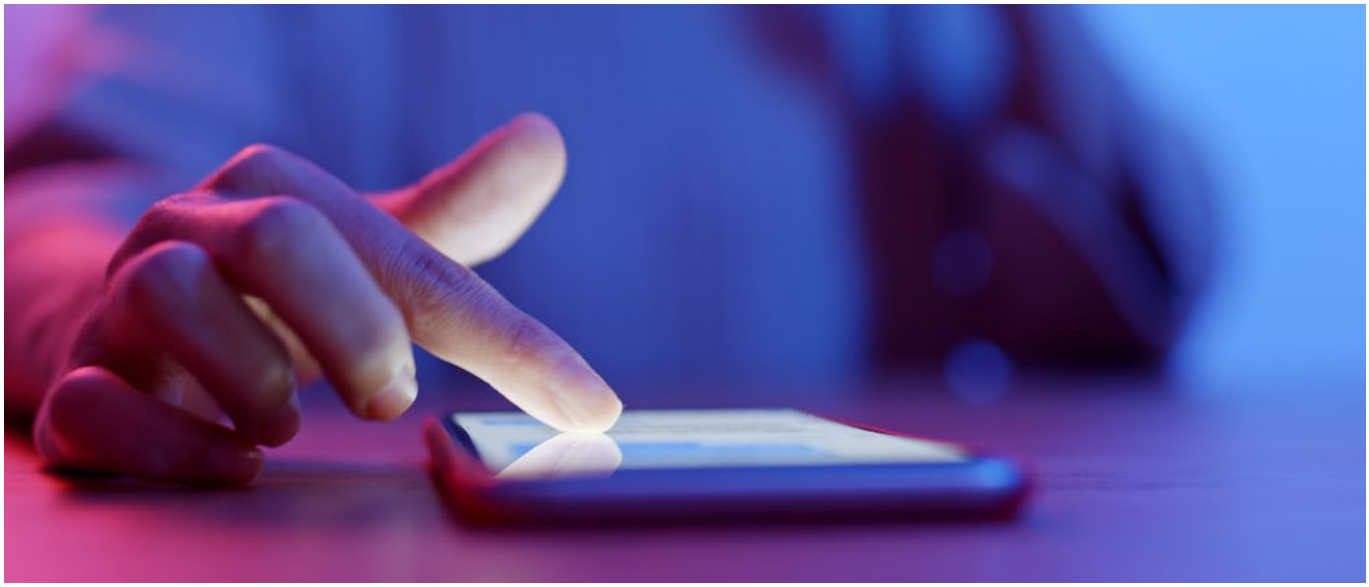
1. **User control and consent:** digital identity systems should disclose information identifying a user only with the user's consent.
2. **Limited access, for limited use:** the solution that displays as little information as possible and effectively limits its use is the most stable in the long term.
3. **The Law of Fewest Parties:** digital identity systems should be designed so that disclosure of information is limited to parties that have a necessary and justifiable identity relationship.
4. **The law of Directed Identity:** A universal identity metasystem must support omnidirectional identifiers for use by public entities and unidirectional identifiers for private entities. Thus facilitating discovery, but preventing unnecessary "launching" of correlation.
5. **Pluralism of operators and technologies:** a universal system (or metasystem) must channel and enable the interaction of multiple technologies and multiple identity providers.
6. **Human integration:** the next-generation identity system must profoundly change the human user experience to be sufficiently predictable and unambiguous to enable them to make informed decisions.
7. **Consistent experience in different contexts**: a unified metasystem should provide a simple and consistent user experience while allowing for the separation of contexts across multiple operators and technologies.

[1] https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

There were several initiatives to create an internet identity model at that time. The most relevant was OpenID, which we know as the "Login with Facebook and Google" models we have today. On the one hand, these models lack privacy, and on the other hand, they lack identity verification, which affects both users and companies.

At the same time, we have an official model based on eIDAS (the European Union's Electronic Identity Act). Unlike the previous model, this one has a strong identity, but is mainly used by a minority of citizens due to its great complexity.

Principles of self-sovereign identity



It is essential to give credit to the pioneers of the concept of self-sovereign or decentralized identity and mention that this term was already conceptualized in 2011 by Devon Leffretto and used in the VRM list.

Later on, the explosion of Blockchain technology would generate a strong impact on the digital identity sector and this concept would be brought to life again by Christopher Allen, in 2016, in his article **The Road to Self Sovereign Identity**[2]. In this article, Christopher Allen explains the principles that should guide any self-sovereign identity:

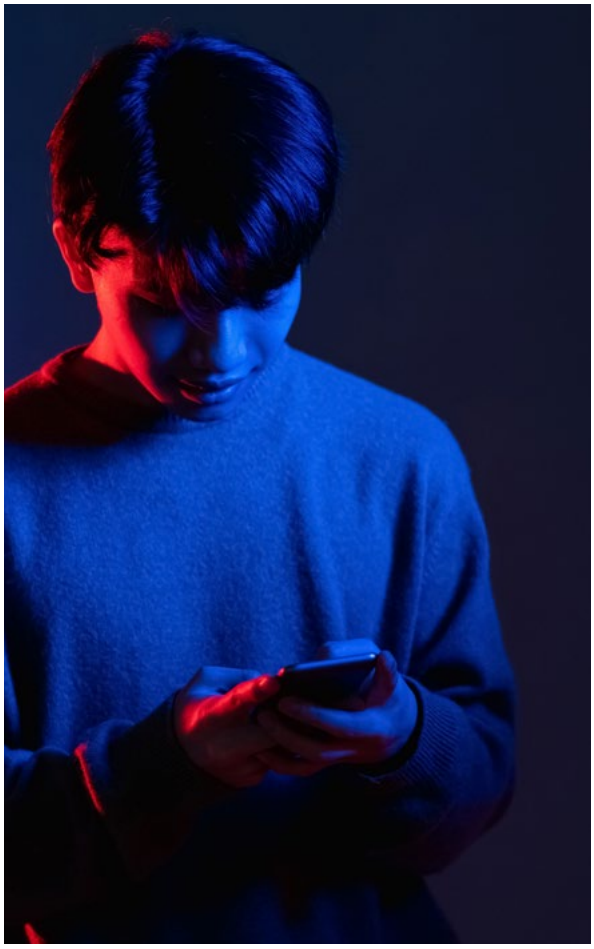
1. **Existence:** the user must have an independent existence. Any self-sovereign identity is ultimately based on the concept of the self at the heart of identity, which, inevitably, can never exist as such in digital format. Self-sovereign identity simply makes public and accessible some aspects of the self that already exists.

2. **Control:** the user must control his identity. Although the user's identity is subject to processing by algorithms that validate it, the user must be the ultimate authority of their own identity. You should always be able to view, update or even hide it.

3. **Access:** the user must be able to access his own data. There can be no hidden data or information inaccessible to the identity owner. However, this does not imply that the user can change all aspects and statements associated with their identity. To protect the sovereignty of other users, an individual should only have access to their own identity and not to those of others.

4. **Transparency:** algorithms and systems must be transparent. The systems that manage and operate the identity network must be open, both in terms of their operation and management. Algorithms must be free, open-source, architecture-independent and accessible for consultation.

5. **Persistence:** identities must be long-term. Ideally, they should last forever, or at least as long as the user wants. This cannot contradict the "right to be forgotten": the user must be able to delete an identity if they wish to do so. This requires a strong separation between an identity and its parts.



6. **Portability:** identity-related information and services should be easily portable. According to Allen, information and services must be easily portable and cannot be in the exclusive hands of a centralized third-party entity. Even when the third entity works for the benefit of the user, the Single Point Of Failure (SPOF) problem still exists. Portability ensures that a user's identity can be transferred and stored in multiple locations, at their own discretion.

7. **Interoperability:** the identity can be used as broadly as possible. Identities have only marginal value if they only work in niche environments. The purpose of a digital identity system is to make information available worldwide without allowing the user to lose control of their identity.

8. **Consent:** the user must consent to the use of their identity. It is vital to have the user's consent before sharing personal information. Although other users, such as the company you work for, your health insurance provider, or a friend, may submit data, the user always has to give consent for this data to be valid.

9. **Minimization:** disclosure of proprietary data should be kept to a minimum. When sharing user data, the disclosure of information should include as little information as possible to complete the transaction. For example, if you require a minimum age for a transaction, you cannot require that they provide the exact date of their birth. Instead, you can require that they meet the condition. According to Allen, by applying selective disclosure, scoping tests and other zero-knowledge techniques, developers can facilitate minimization to better support privacy. Fundamentally, active minimization allows for greater privacy protection in interactions between users and systems.

10. **Protection:** users' rights must be respected. Allen argues that when there is a conflict between the needs of the identity network and the rights of users, the network must err in favor of preserving the freedoms and rights of individuals. To ensure this, identity authentication must occur through independent, censorship-resistant and decentralised executed algorithms.

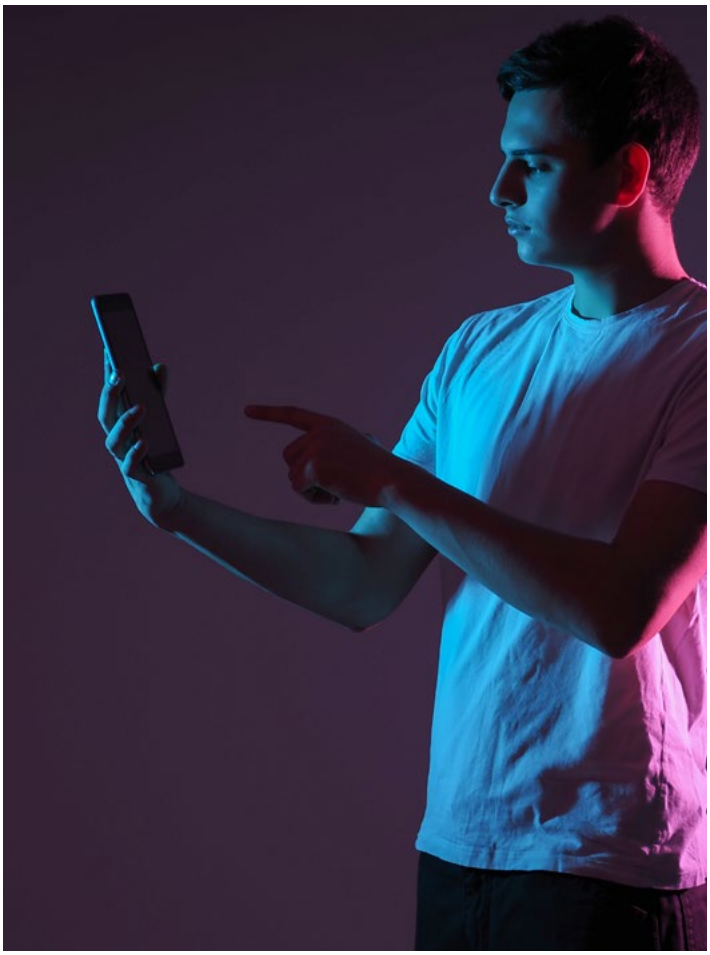
[2] http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Pretty good privacy

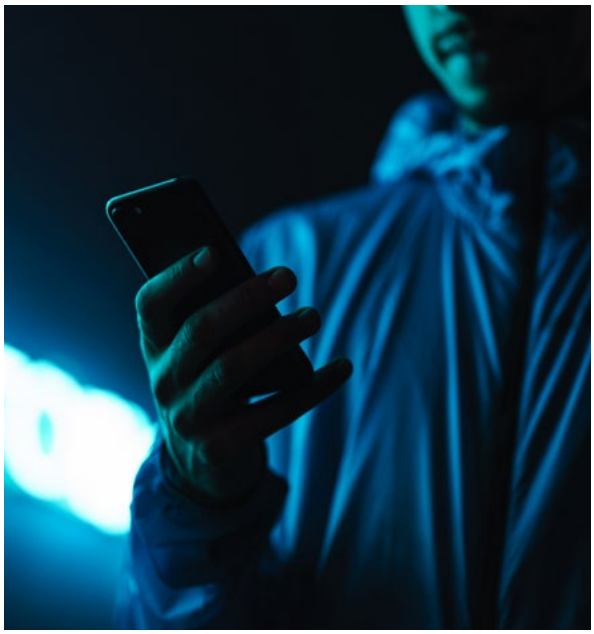
In 1991, Phil Zimmermann's Pretty Good Privacy (PGP) program was one of the first implementations of a public key-based encryption scheme. It was spearheaded by Christopher Allen.

To send encrypted messages, PGP required users to exchange cryptographic keys before communicating. Using PGP, users exchange their public keys by distributing them to friends and associates, who in turn pass them on to their friends and associates and so on. This process eliminated the need for a third party to exchange information. This process gradually builds a network of trust that can be used to securely distribute keys. The more people who sign a person's key, the greater the likelihood that the key is secure. This concept is called the Web Of Trust.

PGP became so popular that parties were held to meet people and exchange keys. This system, prior to the massive use of the Internet, was not very scalable. However, it laid the foundation for the concept of the decentralized trust model.



Rebooting web of trust: the first initiative to organize the industry



Christopher Allen decided to organize a series of events called **RWOT**[3] (Rebooting Web Of Trust) with the aim of building the next generation of identity systems based on the concept of a decentralized web of trust. To this end, the idea was to create a series of whitepapers as a result of the conversations at these events. In the first event, held in November 2015, the first paper was titled **"Rebranding the Web of Trust"**[4], which redefined the term and created a new model for trust with a more modern definition.

Originally, these events were attended mostly by Blockchain professionals. As an anecdote, the first RWOT events were attended by Vitalik Buterin, the creator of Ethereum, a celebrity in the Blockchain world. Among his contributions was the **"Decentralized Public Key Infrastructure"**[5] paper.

The RWOT is a conference that takes place in different parts of the world, usually every six months. It brings together engineers, but also philosophers, lawyers and a wide variety of profiles to discuss all kinds of topics related to identity, from technical protocols to diversity and sustainability issues. A list of all the whitepapers published can be accessed at this link: **https://www.weboftrust.info/papers.html**[6]

[3] https://www.weboftrust.info

[4] https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/rebranding-web-of-trust.pdf

[5] https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf

[6] https://www.weboftrust.info/papers.html

DIF: the great think tank of the SSI WORLD

In addition to the RWOT, the IIW (Identity Internet Workshop) was the main forum for the identity industry. This organization focuses on user-based identity. In October 2005, **the first workshop**[7] was held with the aim of having a forum in which issues of governance, architecture, etc., could be discussed for Internet identity
services and their underlying philosophies.

As a result of these events, the need arose to organize the various industry thinkers on SSI issues. Thus, both the RWOT and IIW served as the basis for creating the DIF (Decentralized Identity Foundation) in 2017.

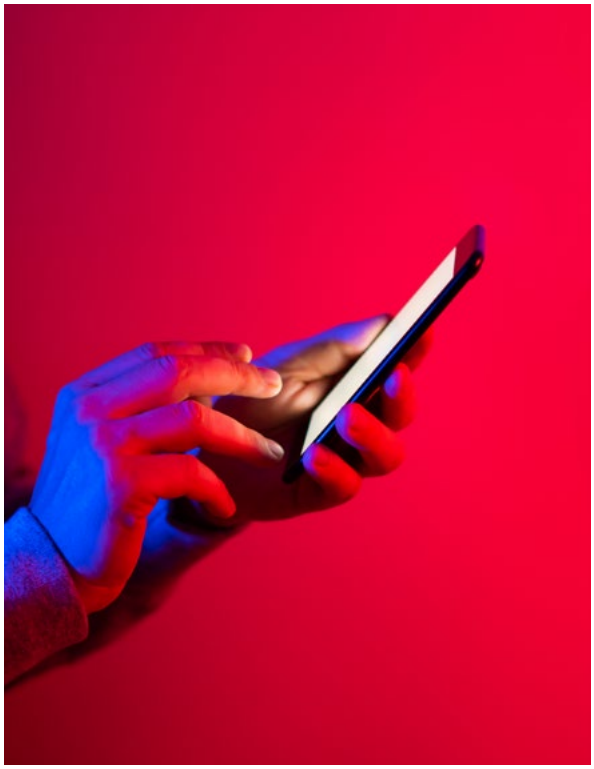
Since its creation, it has been one of the most relevant think tanks in the world of SSI. Hundreds of companies participate, such as Microsoft, Hyperledger, Accenture, Sovrin, among others.

Through its Working Groups, which are divided into functional areas, **DIF**[8] promotes the development of the identity industry. Working Groups cover topics ranging from conceptual to technical issues, which are then addressed by the corresponding standardization committees.

[7] https://identitywoman.net/announcing-the-internet-identity-workshop-iiw2005/

[8] https://identity.foundation

INATBA: the european association for blockchain ISSUES



INATBA[9] (International Association of Trusted Blockchain Applications), a blockchain alliance created by the European Union in 2019, will address blockchain-related issues. The aim of the association is to promote the use of Blockchain technology, bringing together public and private sector entities, as well as policy makers, international organizations, regulators, civil society and standard-setting bodies from across Europe.

Currently, there are more than 100 members, such as Accenture, Everis, Fujitsu, IBM, Deutsche Telekom, Telefónica, BBVA, IOTA, Ripple, Sovrin or ConsenSys.

They have a specific **working group**[10] that deals with issues related to the identity sector. A whitepaper worth mentioning is **"Decentralised Identity: What's at Stake?"**[11] published in November 2020.

You can also consult **the response**[12] that INATBA prepared to the public consultation on the draft eIDAS 2 regulation, which includes a proposal for improvements.

[9] https://inatba.org

[10] https://inatba.org/identity-working-group/

[11] https://inatba.org/wp-content/uploads/2020/11/2020-11-INATBA-Decentralised-Identity-001.pdf

[12] https://inatba.org/wp-content/uploads/2021/10/INATBA-Response-to-the-EU-Commission-Open-Public-Consultation-response-on-the-eIDAS-Regulatory-Framework-1.pdf

Sovrin: the first large SSI network

sovrin

As concepts, protocols, and international standards were being developed, several initiatives and projects centered around SSI emerged.

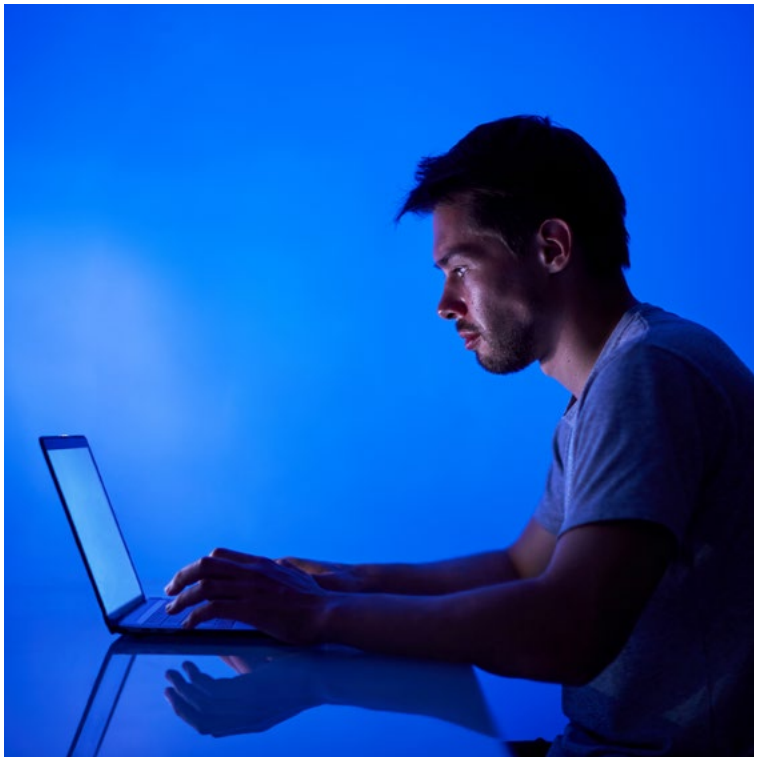
Sovrin[13] is a distributed, public, permissioned identity network. Sovrin was the first major SSI network for identity and has had a major influence on the current model. Several Stewards (stakeholders who maintain the network nodes) participate in the network. In Spain, the only Sovrin node is hosted by Validated ID.

In 2020, as a result of collaboration between companies in international forums, **Trust Over**[14] IP (ToIP) was born. During 2019, the idea was hatched due to the convergence of multiple efforts in the areas of digital identity, verifiable credentials, blockchain technology, and secure communications. These efforts saw the need to converge and create an interoperable architecture for decentralized digital trust. More than 300 member organizations and individuals are part of the ToIP Foundation, such as Accenture, Avast, British Columbia, IBM, MasterCard, among others.

[13] https://sovrin.org

[14] https://trustoverip.org/about/about/

ALASTRIA: the great national INITIATIVE



In Spain, the main network in the decentralized identity sector is Alastria. Founded in 2017, it billed itself as "the world's first regulated national blockchain-based network. Backed by major Spanish entities such as BBVA, Banco Santander, Iberdrola, Repsol, among many others, it was created with the aim of accelerating the creation of digital ecosystems by providing a common collaborative platform.

The initiative extends beyond identity, even though identity plays an instrumental role. Based on Ethereum technology, this is the first initiative to concentrate specifically on legal issues.

ALASTRIA

Europe and eIDAS bridge

All the above players, except perhaps Alastria, are far removed from the regulatory world. Even though there are many credential wallets under development and that several companies like us are looking forward to this outstanding paradigm, the reality is that the legal framework is still immature. Currently we have eIDAS, which focuses mainly on PKIs and traditional certificates.

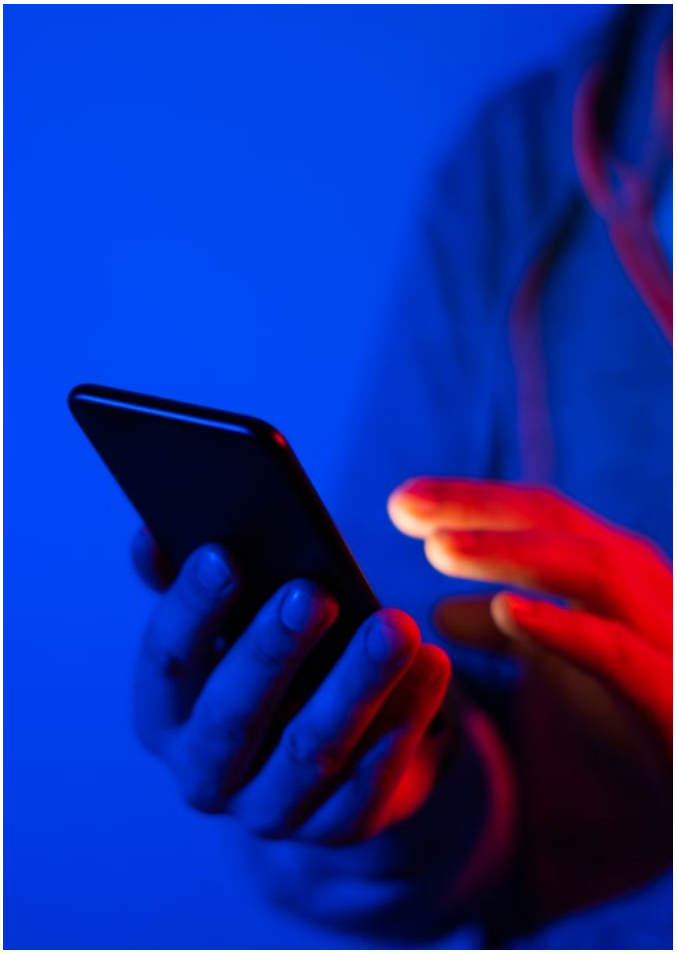
In June 2021, the European Commission approved a new draft of this regulation. This draft states that the upcoming identities of European citizens will be based on SSI principles and supported by identity wallets. However, these regulations have yet to be formally approved and developed, i.e. there is still no established trust framework. Therefore, the eIDAS Bridge project has emerged as an intermediate step.

The eIDAS Bridge project is an initiative of the European Commission (EC) within the ISA2 program. The EC developed eIDAS Bridge to promote eIDAS as a trusted framework for the SSI ecosystem.

Later, **eSSIF Lab**[15], another EU-funded project aimed at providing an interoperable ecosystem, launched eIDAS Bridge. The main objective of this pilot program is to provide an eIDAS Bridge implementation and test interoperability between different vendor implementations.

Validated ID's technical deliverables involve using linked keys of qualified certificates in SSI operations. They can be consulted at the following link: **https://joinup.ec.europa.eu/collection/ssi-eidas-bridge**[16]

The legal deliverables, prepared by Nacho Alamillo, expose the parts of the current regulation that need to be modified to accommodate this new identity model. This will be resolved by eIDAS 2.0.

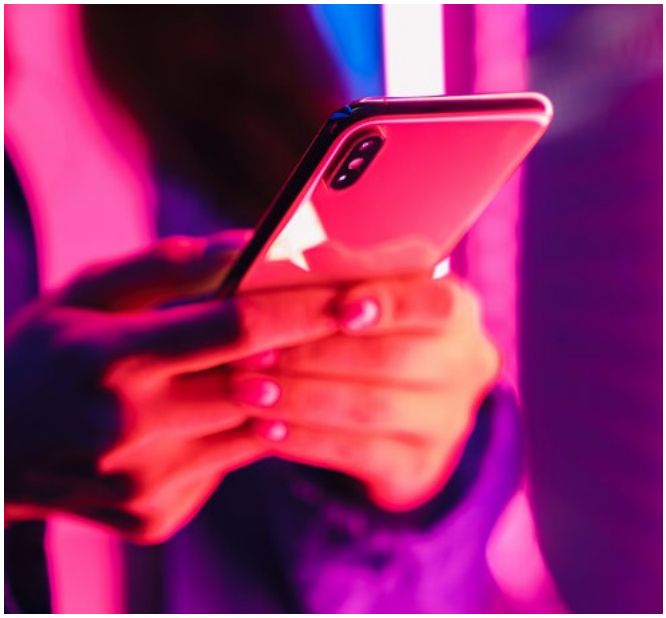


eIDAS

[15] https://essif-lab.eu

[16] https://joinup.ec.europa.eu/collection/ssi-eidas-bridge

EBSI: the great european project



The European Blockchain Services Infrastructure **(EBSI)**[17] is a joint initiative of the European Commission and the European Blockchain Partnership. This project was launched in 2020 to accelerate the creation of cross-border services for public administrations and their ecosystems to verify information and make services more reliable.

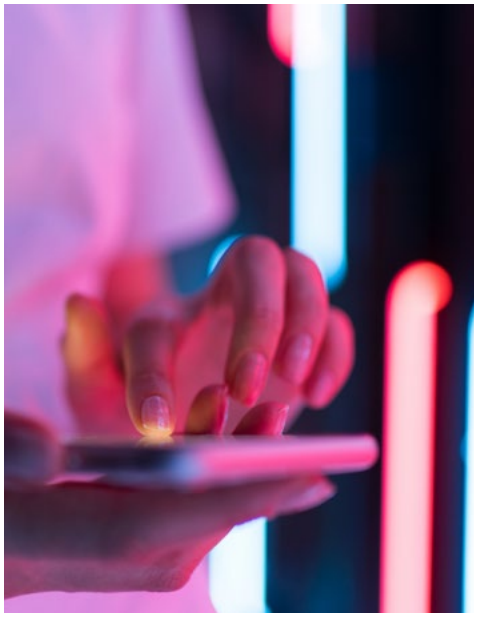
A pilot program was developed under the EBSI Early Adopters program to test the interoperability of solutions in a real multi-university environment in order to enable the exchange of verifiable credentials between key players in the ecosystem.

Since 2020, EBSI has deployed a network of distributed nodes across Europe, supporting applications focused on selected use cases. The project has become the reference for SSI in Europe.

EBSI and eIDAS 2 were created independently and managed by different groups, although it seems that they are in a period of convergence.

[17] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

eIDAS 2.0: the final horizon of SSI



The eIDAS Regulation on electronic identification and trust services for electronic transactions in the internal market was published in July 2014. This European initiative was a key milestone in the regulation of identification in electronic transactions. This regulation was aimed at increasing trust in electronic transactions to promote online commerce and was based on certificates, seals, and electronic signatures of documents (trust services).

The first eIDAS regulation serves as an international benchmark that sets the regulatory foundations that have been replicated in regulations in countries outside of the European Union. Despite its high level of acceptance in terms of trust services, almost a decade later, the adoption of electronic identification systems in public administrations is still very low.

Therefore, **a new proposal**[18] to amend the eIDAS Regulation (known as eIDAS 2) is published in June 2021. This regulation aims to provide European citizens with a digital identity for the entire EU territory. This will enable them to share personal information in a wide variety of contexts, including the private environment.

EIDAS 2 is based on SSI technology concepts. With its origins in the alternative world of blockchain, it is surprising that the revised European identity regulation is based on the decentralized identity technology.

The next major milestone is the Toolbox, a set of common protocols and tools. This is being worked on by both the EC and the member states and is scheduled for its first version to be released in September.

[18] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

Validated ID

Always be yourself

Barcelona
C/ Aragó 179, 4° piso
08011 Barcelona
Tel: +34 900 828 948

Madrid
Paseo de las Delicias, 30 planta 7
28045 Madrid
Tel: +34 900 828 948

info@validatedid.com
validatedid.com