Self-sovereign Identity Model in a Higher Education Institution

Facundo N. Montero[1], Hugo Ramon[2] [0000-0003-1577-3092], Adrián Pousa[3] [0000-0001-8072-6626],

[1] Prosecretaria TIC (PRO TIC), Universidad Nacional del Noroeste de la Provincia de Buenos Aires (UNNOBA)
facundomontero@unnoba.edu.ar

[2] Instituto de Investigación y Transferencia en Tecnología (ITT), Comisión de Investigaciones Científicas (CIC), Escuela de Tecnología (ET), Universidad Nacional del Noroeste de la Provincia de Buenos Aires (UNNOBA)
hugo.ramon@itt.unnoba.edu.ar

[3] Instituto de Investigación en Informática-LIDI (III-LIDI), Comisión de Investigaciones Científicas (CIC), Escuela de Tecnología (ET), Universidad Nacional de la Plata (UNLP)
apousa@lidi.info.unlp.edu.ar

Abstract. Self-Sovereign Identity (SSI) arises as a response to the need of users to have control and autonomy over their identity in the digital environment. In this new paradigm, users manage and safeguard their credentials in personal repositories, eliminating dependence on centralized databases of service providers.

The development of IAS-based solutions is growing. It is seen as a key technology to unify personal identity control promoting security, privacy, and transparency by allowing individuals to decide how and when to share their personal information in a decentralized environment.

The proposed work will address the technological and non-technological requirements to implement effective SSI solutions. The state of the art will be analyzed, highlighting government initiatives.

In addition, specific tools such as Hyperledger Indy and Aries will be explored and used to develop a prototype IAS solution in a controlled environment. This prototype will serve as an initial experience using IAS within academia, with the expectation of fostering future Research, Development, and Innovation (R&D&I) projects.

Keywords: Self-Sovereign Identity, Decentralized Identifiers, blockchain., HEI

1 Introduction

Initially, the Internet was designed without a universal user identification system, which led each website to solve this problem independently. Today, there are multiple identification solutions, each with advantages and disadvantages. With the growth of the Internet, individuals must manage numerous credentials to access different services, which can include multiple credentials with different levels of access.

In response to these challenges, the concept of Self-Sovereign Identity emerges, an innovation that seeks to empower individuals by giving them direct control over their digital identity and associated data. This paradigm promises to mitigate the risks of centralization and offer a more secure and transparent solution for identity management in digital environments.

The development of this paper sought to investigate the current status of technologies and projects in the field of Self-Sovereign Identity, as well as to present an initial prototype within the scope of a Higher Education Institution (HEI). This work not only sought to evaluate the technical feasibility of these solutions but also to anticipate future directions in research, development, and innovation in this emerging and crucial field for online security and privacy.

The rest of the paper is organized as follows: Section 2 defines Self-Sovereign Identity. Section 3 describes the experimental work. Finally, Sections 4 and 5 present conclusions and future work, respectively.

2 Self-Sovereign Identity

Self-Sovereign Identity (SSI) is a revolutionary concept for building the Internet that focuses on users' privacy and control over their data. It proposes a new paradigm of decentralized identity where users can manage their identities autonomously. This is achieved through the development of open standards and protocols such as DIDComm [1], and by making use of blockchain technology [2] to store validation records in a secure and immutable way.

SSI allows users to request and receive credentials from entities such as governments, educational institutions or companies, store them securely and share only the necessary information without revealing sensitive data. Christopher Allen defines it as:

> *... the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; it can't be locked down to one site or locale [3].*

In technical terms, the development of SSI requires new standards and communication protocols that extend the OSI model, creating an independent layer for digital identity management. Some key developments include immutable data structures such as blockchain, Decentralised Identifiers (DIDs) [4] that are not controlled by a central authority, and Verifiable Credentials backed by cryptographic validations on blockchain chains.

In addition, SSI leverages technologies such as smartphones and virtual wallets to securely store and manage Verifiable Credentials, empowering individuals with full control over their digital identity in a decentralized and secure environment.

For the adoption of SSI, not only are technological advances necessary, but also regulations and guidelines for governments to adopt and legislate based on them. Highlights the efforts of the European Commission which published the European electronic IDentification, Authentication and Trust Services (eIDAS) regulation [5], compatible with the Self-Sovereign Identity paradigm, in search of facilitating secure cross-border transactions by establishing a framework for digital identity and authentication, offering trust in electronic interactions and promoting seamless digital services within the European Union, and the European Digital Identity (EUDI) regulation [6] that allows the creation of a universal, reliable and secure European digital identity wallet.

3 Experimental Work

As an experimental work, we worked on the implementation of an initial prototype of Self-Sovereign Identity within the Prosecretaría TICs of the Universidad Nacional del Noroeste de la Provincia de Buenos Aires (UNNOBA), this is framed in a use case in which the university issues credentials containing academic and identification data to its students and a test in which they must perform a presentation containing partial information of their credentials. In addition, a zero-knowledge test evaluates whether a given attribute of the credential fulfills an arithmetic condition, allowing the credential holder to validate his or her identity without revealing unnecessary information. For this, it was necessary to deploy a credential issuing agent for the university and develop a controller for simple management of the same, designed for administrative users with a non-technical profile, in addition to publishing in a blockchain the scheme and definition of credentials to be used on which to base the generation of credentials.

The tools used for this development were:

- Hyperledger Indy [7], a blockchain implementation project specifically designed for decentralized for identity solutions, is maintained by the Linux Foundation. Notably, the Verifiable Organizations Network (VON) implementation by the government of the Canadian province of British Columbia worked on its test blockchain running in the https://test.bcovrin.vonx.io/ domain.

- Hyperledger Aries [8], another Linux Foundation project, for the deployment of the agent used by the university to issue Verifiable Credentials. Aries offers a set of tools and libraries that allow the development of agents in different programming languages with support for multiple blockchains, credential types, and protocols. In particular, in this work, we used the one developed in Python, called Aries Cloud Agent Python, known as ACA-Py [9]. In addition, a web driver was developed to interact with the agent, oriented to the use case, allowing the management of credential issuance by non-technical users.

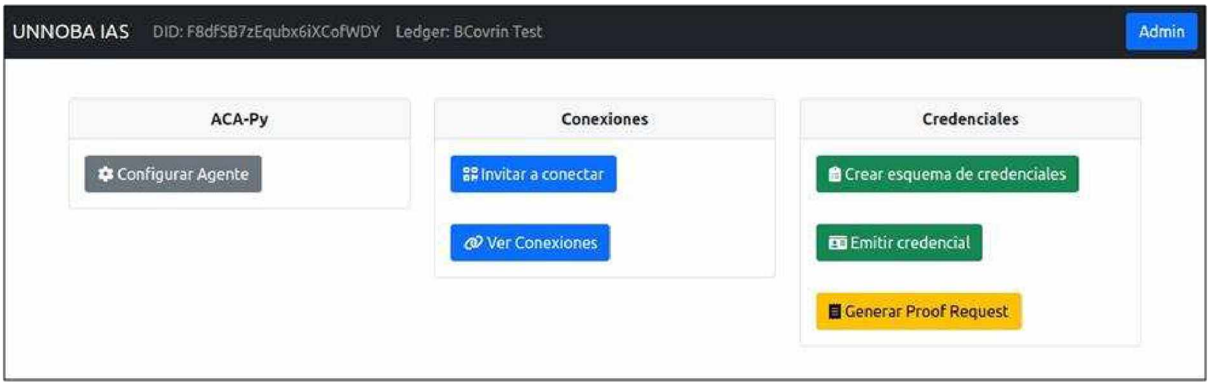

Fig.1 - Controller developed to communicate with the agent

- Lissi ID-Wallet [10], an application of the German company Lissi GmbH, for the use of a digital wallet to store Verifiable Credentials. It is also characterized as an EUDI-Wallet as it complies with the requirements of the European eIDAS regulation.

Once the resources with which to work had been deployed, the credential scheme was defined based on the use case, the generation of Verifiable Credentials, and the creation of Verifiable Presentations. During these steps, particular characteristics and limitations found in the tools used were detailed.

4 Conclusions

It analyzes the state of the art of various public and private initiatives that promote the use of this technology to address and provide solutions to different social problems.

The key technological components for its implementation are detailed, such as distributed log technologies (DLT), in particular blockchain, distributed identifier standards, verifiable credentials, digital wallets, and agents. These components are currently under continuous development and standardization.

Experimental work was carried out using tools such as Indy and Aries from the Hyperledger project to make an initial prototype at UNNOBA, where a credential issuing agent was deployed, a controller was developed, credentials were issued to virtual wallets, and validated against the information in the blockchain. During all these steps we tried to show the degree of maturity of the tools used for its deployment, most of which are considered still in the early stages as they are not in stable versions, we detailed problems and limitations encountered and possible future changes in both the tools and protocols used.

5 Future Work

Based on the work carried out in this paper, the following lines of research are considered of interest given the global boom in this technology:

- Develop trust frameworks for its implementation with legal validity according to the laws and regulations in force.
- Develop mechanisms for interoperability of DIDs between different blockchains.
- A solution to overcome the current mechanisms of revocation of Verifiable Credentials.
- Comparison of use and interaction capacity between different communication protocols such as DIDComm and OpenID.
- Analyze the various accessibility considerations required to ensure this technology is usable and available to all users.

References

[1] DIDComm Working Group (2023). DIDComm Messaging v2.x Editor's Draft. Decentralized Identity Foundation. https://identity.foundation/didcomm-messaging/spec/
[2] EU Blockchain (2018). EU Blockchain. Comisión Europea. https://www.eublockchainforum.eu/
[3] Christopher Allen (2016). The Path to Self-Sovereign Identity. Life With Alacrity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html
[4] M. Sporny, A. Guy, M. Sabadello, D. Reed. (Julio 2022). Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations. W3C. https://www.w3.org/TR/2022/REC-did-core-20220719
[5] European Commission (2014). eIDAS Regulation. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
[6] European Commission (2021). EUID Regulation. https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation
[7] Hyperledger Indy (2023). Hyperledger Indy. https://hyperledger-indy.readthedocs.io/en/latest/index.html
[8] Hyperledger Aries (2023). Hyperledger Aries. https://www.hyperledger.org/projects/aries
[9] Hyperledger Aries (2024). Aries Cloud Agent Python. https://aca-py.org/v0.12.1/
[10] Lissi GmbH (2023). Lissi ID-Wallet . https://www.lissi.id/for-users