Identity Provider based on Self-Sovereign Identities and Blockchain Technology

Daniel Paredes-García, José Álvaro Fernández-Carrasco, Lucía Muñoz-Solanas
Department of Cybersecurity
Vicomtech, Basque Research and Technology Alliance (BRTA)
Donostia/San Sebastián, Spain
e-mail: {dparedes | jafernandez, | lmunoz}@vicomtech.org

***Abstract*—The paper presents a work in progress on the improvements made to CredSSI, an identity management system based on Self-Sovereign Identities (SSI), developed as part of a European initiative for a data space in the agri-food sector. Enhancements include the development of a digital wallet for secure and efficient user credential management, the incorporation of a Police Enforcement Point Proxy to streamline user request handling by service providers, and the implementation of a traceability module that uses blockchain technology to log and secure system events. These improvements enhance security, privacy, and operational efficiency in digital identity management through the Self-Sovereign Identities approach.**

Keywords-SSI; blockchain; identity wallet; verifiable credential.

I. Introduction

Protecting personal data is essential for cybersecurity in the digital age. Users need to trust that their data stays secure and private online, making identity management crucial for safe and efficient service access.

Traditional identity management methods, like centralized or federated systems, focus on the organizations managing user identities. This can lead to potential privacy vulnerabilities and data protection law breaches. As an alternative, a new model of identity management is emerging, with the user at the center. This is called Self-Sovereign Identity (SSI) [1][2], providing the user with full control over their information. This reduces reliance on centralized authorities and enhances privacy and security using cryptographic and blockchain techniques. This technology provides an extra layer of protection and trust, which means that recorded transactions cannot be altered or erased. In addition, its transparency facilitates tracking of all transactions. Because of these advantages, SSI is increasingly becoming a solution for identity management across various sectors, including the agri-food industry [3]. This industry is transitioning digitally to enhance efficiency, traceability, and sustainability through data and identity management processes with secure, reliable, and user-centric solutions to ensure secure access and facilitate interactions within complex data systems.

As part of the European DIVINE project [4], an advanced identity management system based on SSI is being developed for a Data Space related to the agri-food sector. This project addresses critical needs in agriculture, where secure, efficient data sharing supports both sustainability and digital transformation goals. Each of the DIVINE pilots demonstrates unique use cases that benefit from the SSI system by enabling safe data exchange and reliable user interaction across various agricultural services. This work builds upon previous studies [5], by implementing enhanced features such as a traceability module, which provides a robust, immutable record of system events, and a digital wallet for secure credential management. Additionally, a Police Enforcement Point Proxy (PEP-Proxy) has been activated to streamline requests, improving both security and user experience.

This paper will study the design, implementation, and benefits, showing how it addresses challenges related to data security, access control, identity management and its traceability, thereby supporting the sector's digital transformation.

The rest of the paper is organized as follows: Section 2 outlines the key background concepts essential for understanding digital identities, with a particular focus on SSI. Section 3 presents an analysis of the related work on SSI and applications already being implemented. Section 4 presents the use case architecture, detailing the main components involved in the SSI model. Section 5 focuses on an explanation of the process used to verify the system's functionality. Section 6 focuses on the results obtained, and comparisons with other models, in addition to the initial version. Finally, Section 7 presents the conclusions drawn from the work and future lines of improvement.

II. Preliminaries

The landscape of identity management has undergone significant transformation over the years. Initially, centralized systems were prevalent, wherein a single entity had full control over user information for authentication purposes. One notable drawback of this model was the inconvenience for users of having to remember passwords for each identity manager, as well as the need to have databases where user information was stored, with the danger that this could be stolen by hackers.

To resolve this issue, the federated system was introduced, enabling the sharing and reuse of credentials across different organizations [6], thus reducing the number of accounts for the user. Nevertheless, both centralized and federated models harbored serious security concerns due to potential vulnerabilities leading to user information exposure.

In response to these challenges, the SSI model has emerged as a solution, seeking to decentralize user information management and empower individuals as the rightful owners of their own information. The SSI system is structured around a standard, Verifiable Credentials (VCs), and four principal actors: Holder, Issuer, Verifier, and a Verifiable Data Registry (VDR). VCs serve as digital counterparts to traditional physical credentials, comprising metadata for subject and issuing authority identification, claims encompassing specific individual traits, and cryptographic proofs for credential verification by

 ISBN: 978-1-68558-323-1

the issuing authority. In addition, the main actors participating in the SSI model are:

- **Holder**: The individuals or entities that own and control their VCs. The Holder stores, manages and shares its VCs.
- **Issuer**: Trusted entities, e.g., universities, governments, etc., that validate and sign the VCs of holders.
- **Verifier**: The service provider or entity with whom the holder shares their credentials. This entity verifies the authenticity of the credential presented.
- **VDR** [7]: Acts as a secure database for managing and verifying digital identities. The VDR does not store credential information. Instead, it stores the issuers' public keys, credential schemas and other crucial data for verifiers to assess their authenticity, often using blockchain technology for immutability and security. This system allows verifiers to trust the information without needing direct issuer-verifier communication, since the issuer registers the validity of the credential in it by signing it and the verifier can consult in the VDR that the credential is valid.

III. Related work

SSI represents an innovative solution to the constraints associated with traditional identity management systems. As digitalization advances, there is an escalating demand for identity systems that empower users with enhanced, secure control over their data. In recent years, new European initiatives have emerged to advance the SSI methodology, such as the European Blockchain Services Infrastructure (EBSI) [8]. This initiative uses blockchain to create reliable cross-border services for public administrations, businesses, and citizens, with a decentralized, tamper-proof structure.

With all this, significant work is being done in the field of SSI, as well as with the use of blockchain technology to create decentralized and secure structures. In this aspect, Cocco et al. [9] preset a solution with an SSI system that seeks to guarantee the quality of the products marketed and compliance with standards and regulations through the use of food certifications. In [10], Stockburger et al. propose a theoretical design of an SSI-based identity manager with blockchain for a transportation system in Europe, allowing students to obtain discounts using VCs from their universities. It ensures secure and decentralised verification.

Due to the great advantages seen in studies on the SSI model, it has started to be implemented in different commercial solutions. For example, Shobanadevi et al. [11] have developed ShoCard, a digital authentication platform that uses the Bitcoin blockchain to allow secure identification for both users and businesses. This technology enables quick and reliable identity verification and transactions, as identities are stored on the Bitcoin blockchain, and users manage their private keys on their mobile devices. However, it is worth noting that this solution does not adhere to Web3 standards and is not open source. Another commercial solution is proposed by Lundkvist et al. [12], called uPort, which is a mobile application allowing users to transfer their information using Decentralised Identifiers (DIDs) and VCs on the Ethereum blockchain.

This paper utilizes a model based on SSI in the agri-food sector as part of the DIVINE project on Data Spaces. This model uses a system of roles and permissions, represented by VCs, to enable users to access resources from various services within the agri-food sector. It represents an advance over [5], as it introduces new features such as event traceability registration and the implementation of a digital wallet for users, where they can securely and compactly store all their VCs. Furthermore, to the best of our knowledge, it is the first solution that uses SSI for this use case.

IV. Architecture

The SSI method has been used to manage identities, in order to give users greater control over their information and ensure its integrity. Once registered in the system, users (Holders) will obtain a digital identity based on VC. These credentials will represent roles within specific applications or services. The service provider will act as the "Issuer", signing the credentials that assign roles to users. An identity provider will perform the role of Verifier, validating the authenticity of the VCs in each request made.

The system presented in this paper builds on the development from [5] to create a fully functional SSI-based Identity Management (IdM) system.

- **Identity Provider (IdP)**: Keyrock [13], FIWARE's identity management component that supports protocols such as OAuth 2.0 and OpenID Connect, and facilitates role-based access control. This component acts as a Verifier within our SSI system.
- **PEP-Proxy**: Derived from FIWARE's Wilma [14], which manages access to resources and services by acting as an intermediary with the user. This component collects calls made to the service and queries the IdP to determine if the user has the appropriate permissions.
- **Blockchain tool**: A private network with three nodes has been deployed, based on Ethereum's ERC735 [15] and ERC734 [16] standards, implementing Smart Contracts (SCs) for SSI. In this network, each component of the ecosystem (holder, issuer and verifier) has its own contract. The network uses a Proof of Work (PoW) consensus mechanism to develop the VDR for the SSI environment. Modifications have been made to the original standards to create SCs suitable for use within CredSSI, including a new contract specifically designed to oversee the functions of the verifier.

Using the existing blockchain, the system now includes a new contract that adds the Traceability module. This module allows for a detailed logging of user interactions with the IdP and Identity Wallet, securely and immutably storing each action on the blockchain. With a specific SC on the Ethereum platform, it ensures an unalterable record of all events, facilitating thorough investigations.

Finally, an additional element to the system is being developed, which is the Identity Wallet. The Identity Wallet is a digital tool accessible via mobile applications and web services, designed for users to securely manage their digital

identities and credentials. It supports operations such as adding, modifying, deleting, and presenting credentials. This component has been included to make it easier for users to interact with their credentials, providing greater accessibility to their various VCs. Another interesting aspect of the wallet is that fingerprint access through the FIDO2 protocol is enabled for logging in.

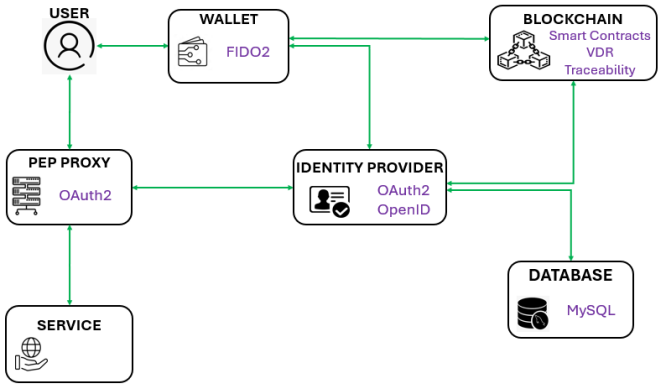

Figure 1. Model Architecture.

In Figure 1, the communication between the different elements that make up our SSI system are shown, where the blockchain includes the three mentioned elements.

The system's structure is demonstrated in four main DIVINE pilot projects, which showcase the agri-food services supported by our SSI-based model.

- **ITC - Inovacijsko Tehnoloski Grozd Murska Sobota (Innovation and Technology Cluster of Murska Sobota)**. This pilot, in Slovenia, focuses on sustainable food production, enabling Slovenian farmers and advisors to access benchmarking data.
- **University College Dublin**. This pilot runs a crop yield prediction model in which farmers share anonymized yield metrics and data related to climate, soil, and disease.
- **Neuropublic Ae Pliroforikis and Epikoinonion (Neuropublic Information and Communications Incorporated)**. In this pilot, Greek farmers share weather data and agricultural calendars, enabling data-driven decisions to optimize production
- **Dynamic and Security Computations SL**. This pilot, in Spain, focuses on traditional olive and almond plantations, facilitating a secure exchange of environmental data and agricultural calendars, thus supporting sustainable farming practices.

These pilot projects demonstrate the system's ability to provide flexible and secure management of access to a variety of agri-food applications. Each pilot benefits from the credential-based role and permission structure provided by the SSI model, allowing users to access services while enabling service providers to control access.

V. Functional Analysis

To ensure the Identity Management System runs smoothly and securely, it is important to understand how each part works within the SSI framework. The process below outlines the steps to follow from account creation to resource access:

1) The user creates an account in Keyrock (Holder).
2) The service owner registers the service in Keyrock (Issuer).
3) The service owner defines the roles and permissions.
4) The user requests a role (VC).
5) The service owner approves this request (signs the VC).
6) The user accesses the service with his VC.
7) The user requests a resource.

Regarding what has been developed in [5], the first three steps correspond to the first two diagrams, which remain unchanged. On the other hand, steps 4 and 5 correspond to the third diagram, although with the new presence of the Identity Wallet, this sequence changes to the following (see Figure 2):

1) The user accesses his Wallet with his Keyrock credentials.
2) The user creates a credential with a role in a service.
3) The issuer receives the signing request for this credential.
4) The service owner signs the user's credential and registers the signature proof in the VDR.
5) The user receives the signed VC.

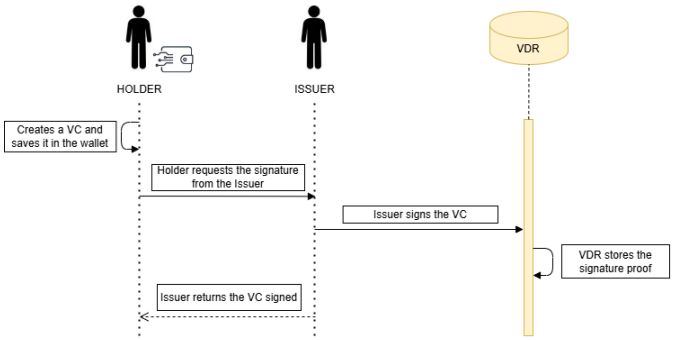

Figure 2. VC signature by the Issuer.

When the user has the signed VC, he can access the service (see Figure 3). He must first authenticate (which aligns with step 6), using the following sequence:

1) The user attempts to access the service.
2) The service redirects him to Keyrock, where he enters his username, password and Claim ID from his signed VC.
3) The IdP checks the credentials in the MYSQL database, while the validity of the claim is checked in the VDR, acting as a Verifier.
4) If the received information is correct, it allows the user to access the service by providing an access token.

After authentication, the user can request resources using his token, which contains information about the user, such as roles or permissions (see Figure 4). This token will be checked each time a request is made, resulting in an authorization process (which corresponds to step 7). The steps to request a resource are as follows:

1) The user requests a resource to the proxy with his token.
2) The proxy asks Keyrock to verify the validity of the token for that request.

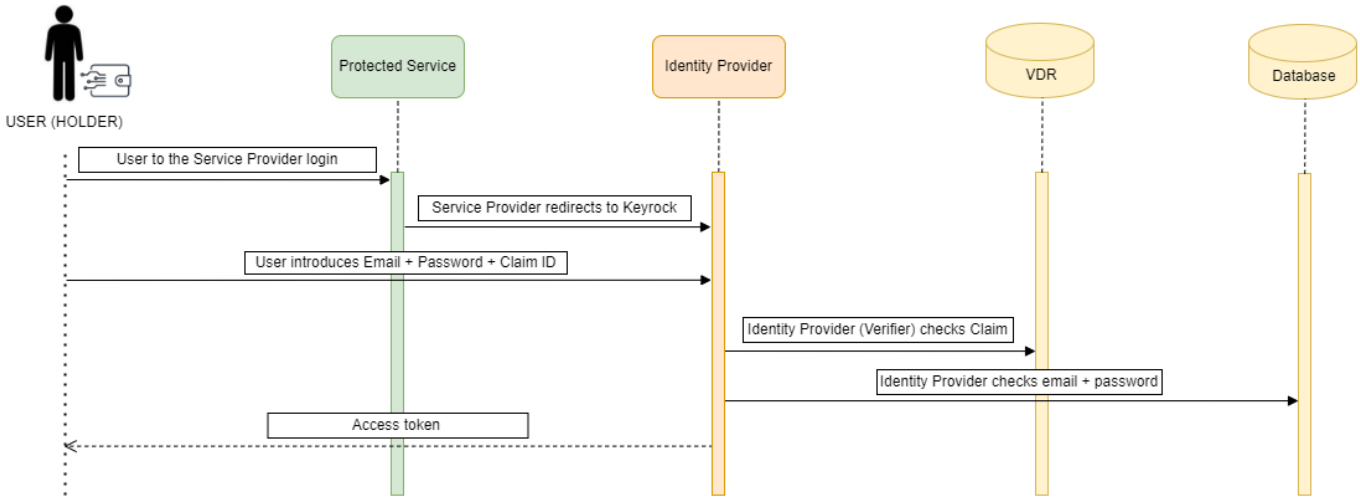

Figure 3. Authentication service.

3) Keyrock checks its database to determine if the user has the permissions to request that resource and confirm it to the proxy.
4) Once the validity is confirmed, the proxy requests the resource from the service.
5) The service provider returns the requested resource to the proxy, and the proxy delivers it to the user.

All events will be recorded in the blockchain by the Traceability module to ensure a correct forensic analysis and avoid malicious interactions by third parties. This module collects all the movements carried out by Issuer, Holder and Verifier, to record all the activities carried out in the ecosystem. The storage of this information is done by deploying a new SC that exclusively collects all the events carried out, the information collected being the following:

- Type of event produced.
- User that triggers the event
- Timestamp.
- Extra description of the event produced.

This information is collected every time a participant carries out an event both in the identity manager and in the Wallet of each of them, with the exception of read-only events.

VI. Discussion And Evaluation

After developing the implemented system, it becomes that an SSI system based on roles and permissions through VCs represents an advancement over traditional identity management systems, as it grants control of information to the users, allowing them to share their information with the entities they choose. Compared to its predecessor [5], it also constitutes an improvement by completing the process of resource acquisition through user authentication and authorization, as well as enhancing robustness by developing a traceability module that records events, providing greater transparency and improving the security of the developed system. Additionally, the introduction of the digital Wallet for users allows them greater control over their credentials, enabling them to manage these as they see fit, whether adding, reading, or deleting them from their Wallet.

This project is a work in progress, which means it is not fully completed, allowing for continuous improvement. Nonetheless, this tool is operational within the European project DIVINE, where project partners are starting to use this tool.

VII. Conclusion and Future Work

Developing an SSI identity management system in an agri-food environment such as the European project DIVINE represents a step forward in the methodologies used, as it allows users to have full control of their information, being able to manage their own VCs themselves through their digital Wallet thanks to blockchain technology, which provides greater robustness and trust. Likewise, the use of blockchain together with a system based on roles and permissions allows the owners of the services to have control over who can access their resources, as they are in charge of assigning these roles and permissions, through the signature of the users' VCs, making this model a decentralised system but also maintaining control by the providers. At the same time, thanks to the incorporation of a traceability module, it is possible to record the events that occur during the course of the resource request, making this system even more secure and robust and improving on its predecessor, CredSSI [5]. Even so, this project is still active, so that further improvements are possible, such as:

- Standardisation of VCs, as they do not explicitly follow W3C standards.
- Gathering feedback from users, as it is in a current state of deployment where few users are using it regularly, which makes it difficult to identify areas for improvement.
- Adding new functionalities to the system, such as the inclusion of new authorization servers for more elaborate permissions management; or the inclusion of new forms of authentication in the Wallet, such as voice biometrics.

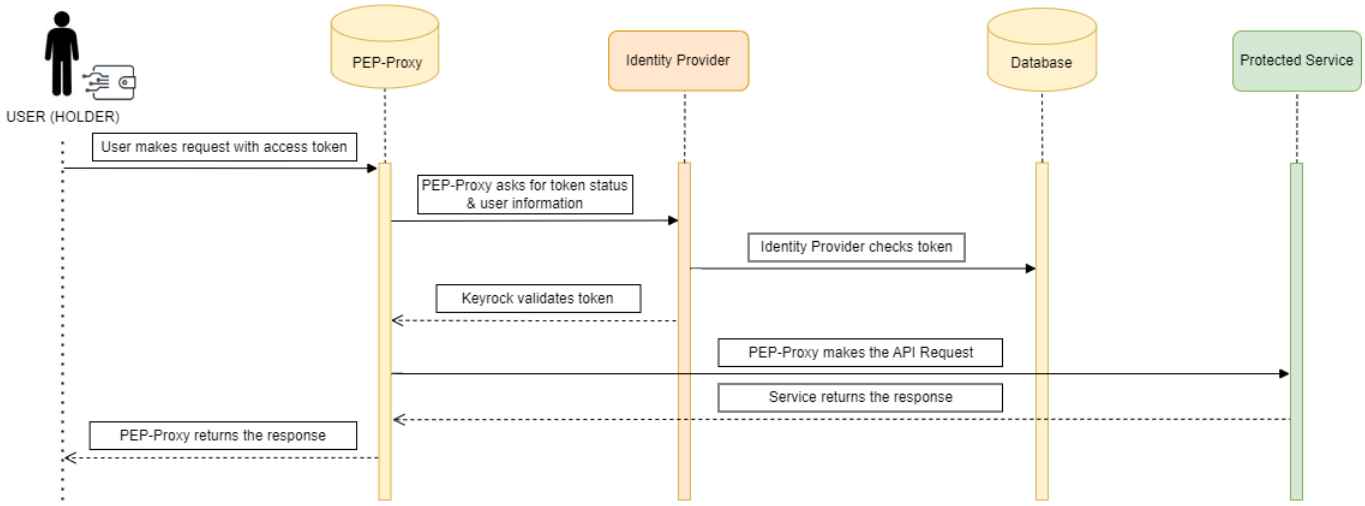

Figure 4. Authorization service.

ACKNOWLEDGMENT

This work has been partially supported by:

- The European Union's Horizon 2020 Research and Innovation Program under the project DIVINE (Grant Agreement No. 101060884).
- The Basque Country Government under the ELKARTEK program, project SONETO (KK-2023/00038).

REFERENCES

[1] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity", *Computer Science Review*, vol. 30, pp. 80–86, 2018.

[2] A. Preukschat and D. Reed, *Self-sovereign identity*. Manning Publications, 2021.

[3] G. Pe'er *et al.*, "Action needed for the eu common agricultural policy to address sustainability challenges", *People and nature*, vol. 2, no. 2, pp. 305–316, 2020.

[4] DIVINE Project Consortium, "Divine - demonstrating value of agri-data sharing for boosting data economy in agriculture", 2024, https://divine-project.eu/ [retrieved: October, 2024].

[5] J. Á. F. Carrasco, L. Muñoz-Solanas, L. S. Gil, and D. Paredes-García, "Credssi: Enhancing security and privacy with self-sovereign identities approach", in *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, IEEE, 2024, pp. 745–750.

[9] L. Cocco, R. Tonelli, and M. Marchesi, "Blockchain and self sovereign identity to support quality in the food supply chain", *Future Internet*, vol. 13, no. 12, p. 301, 2021.

[10] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation", *Blockchain: Research and Applications*, vol. 2, no. 2, p. 100 014, 2021.

[6] S. S. Shim, G. Bhalla, and V. Pendyala, "Federated identity management", *Computer*, vol. 38, no. 12, pp. 120–122, 2005.

[7] W3C, "Verifiable credentials data model v2.0", https://www.w3.org/TR/vc-data-model-2.0/ [retrieved: October, 2024].

[8] European Commission, "European blockchain services infrastructure (ebsi)", https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home [retrieved: October, 2024].

[11] A. Shobanadevi *et al.*, "Novel identity management system using smart blockchain technology", *International Journal of System Assurance Engineering and Management*, vol. 13, no. Suppl 1, pp. 496–505, 2022.

[12] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, "Uport: A platform for self-sovereign identity", *URL: https://whitepaper. uport. me/uPort_ whitepaper_DRAFT20170221. pdf*, vol. 128, p. 214, 2017.

[13] FIWARE, "Identity manager - keyrock", https://fiware-idm.readthedocs.io/en/latest/ [retrieved: October, 2024].

[14] FIWARE, "PEP Proxy - Wilma", https://fiware-pep-proxy.readthedocs.io/en/latest [retrieved: October, 2024].

[15] Ethereum Improvement Proposals, "EIP-735: Self-sovereign identity", 2018, https://github.com/ethereum/EIPs/issues/735 [retrieved: October, 2024].

[16] Ethereum Improvement Proposals, "EIP-725: Ethereum identity", 2018, https://github.com/ethereum/EIPs/issues/734 [retrieved: October, 2024].