vicomtech

MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Identity Provider based on Self-Sovereign Identities and Blockchain Technology

Authors: Daniel Paredes, José Álvaro Fernández, Lucía Muñoz

Presenter: Daniel Paredes García, VICOMTECH

dparedes@vicomtech.org

IARIA

Short Bio

EDUCATION

- Bachelor's Degree in Industrial Engineering with a specialization in Automation at the University of Seville.
- Master's Degree in Industrial Engineering at the University of Seville.

ROLE

- Working at Vicomtech since 2022 as a Research Assistant, within the Department of Digital Security.

SPECIALIZATION

- Identity management
- Data Spaces
- Spiking Neural Networks (SSN)

vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

01

INTRODUCTION AND OBJECTIVES

02

DIGITAL IDENTITIES

03

ARCHITECTURE

04

CONCLUSION AND FUTURE WORK

1. Introduction and Objectives

- DIVINE is an European Project related to agri-food sector.

- Owners provide specialized agricultural applications. Four main DIVINE pilot projects agri-food services.

- Identity Management System (IdM) for a Data Space ecosystem.
  - Compliant with eIDAS2
  - Compliant with GDPR

vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

01

INTRODUCTION AND OBJECTIVES

02

DIGITAL IDENTITIES

03

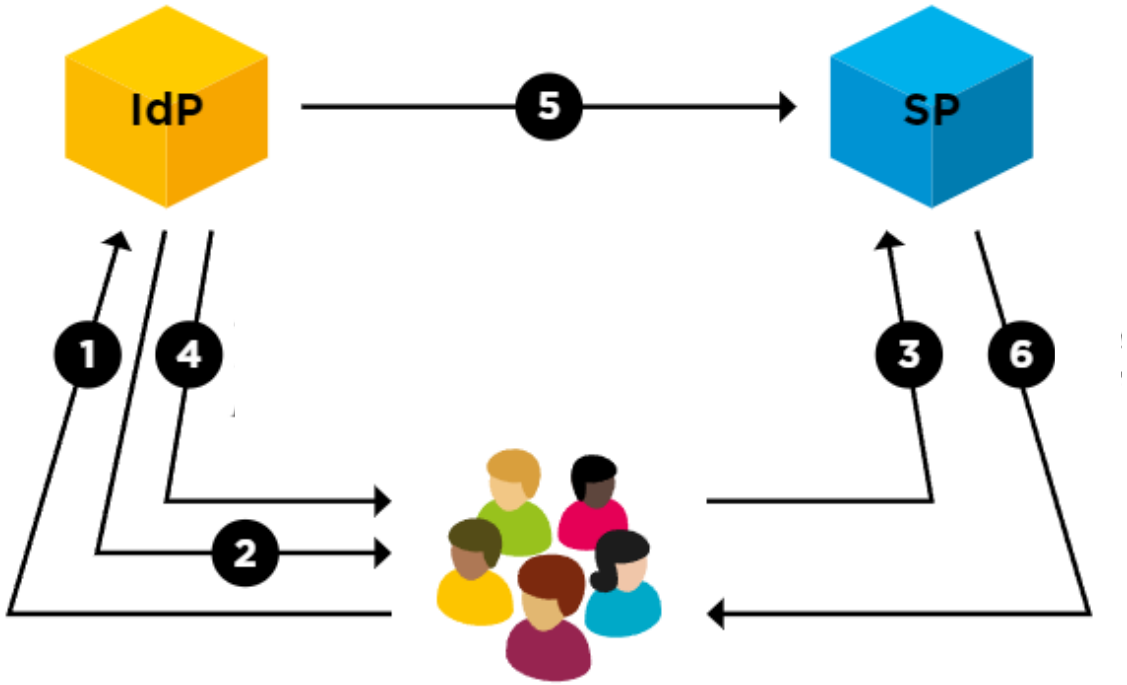
ARCHITECTURE

04

CONCLUSION AND FUTURE WORK

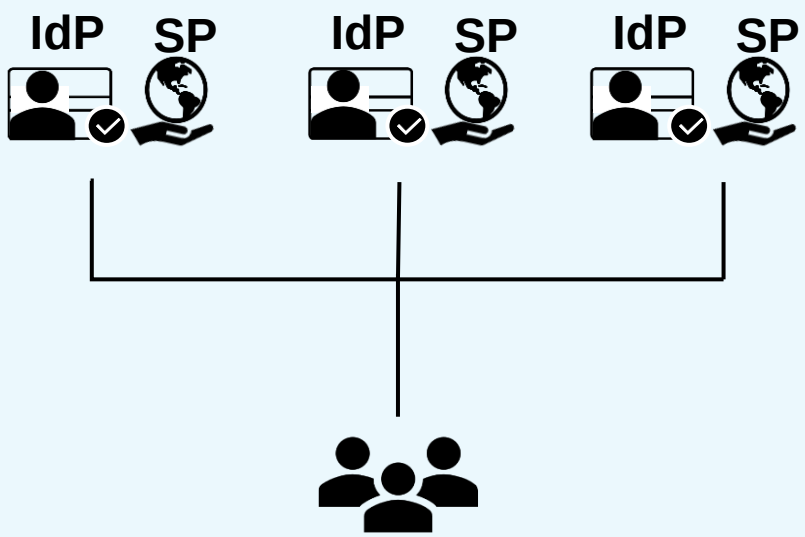
2. Digital Identities

- Online representations of individuals used for identification and authentication purposes
- **Identity Provider** → Authenticates users and provides identity information to other systems
- **Service Provider** → Provides services to users (apps), relying on identity information from identity providers.



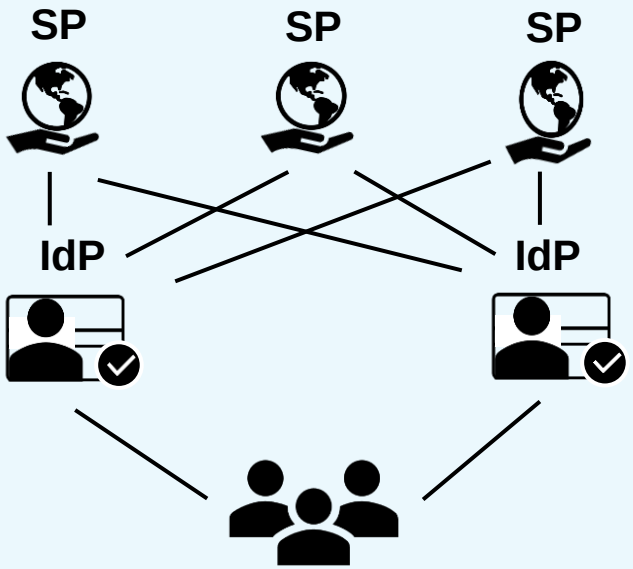
2. Digital Identities

CENTRALIZED SYSTEM



- Each SP has its own IdP to manage and verify user identities.
- Different usernames and passwords for each service.

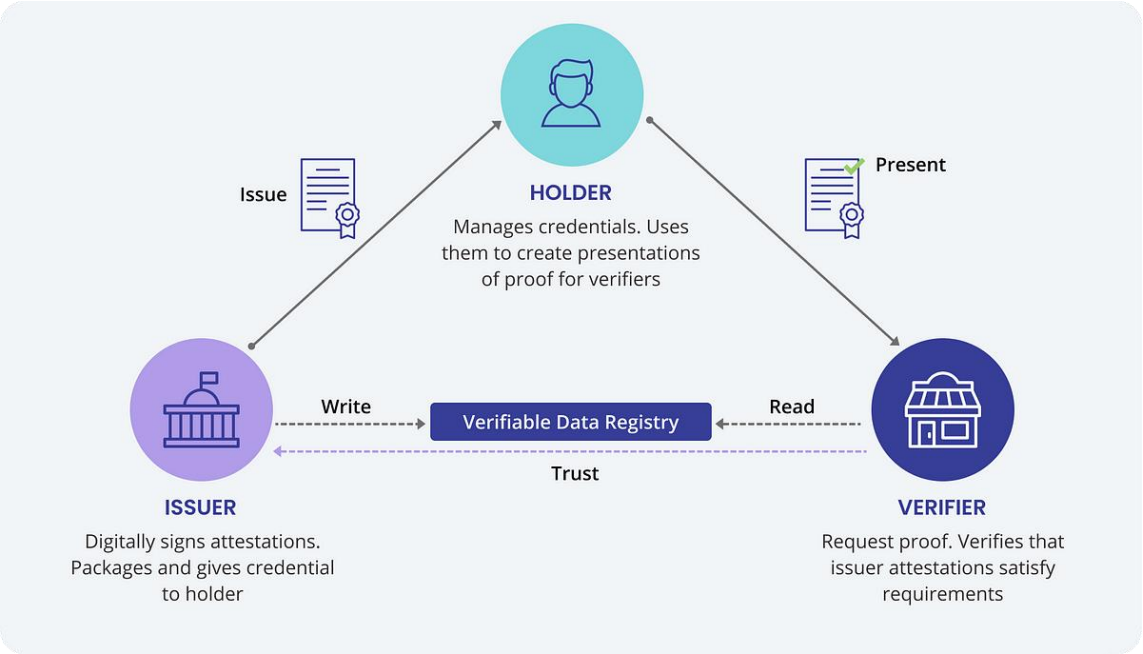
FEDERATED SYSTEM

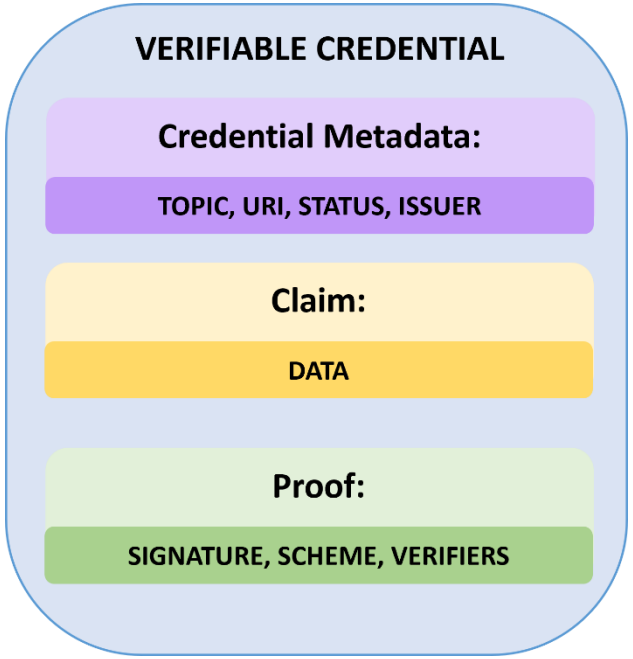


- IdP and SP are separate entities that communicate with each other.
- Logging in with your credentials on various services.

Self Sovereign Identities

- User at the core → The user is the only owner of his Identity
- **Wallets** → Verifiable Credentials (VCs) and claims
- 3 actors → **Holder, Issuer, Verifier**
- Verifiable Data Registry → **Blockchain** Technology





01

INTRODUCTION AND OBJECTIVES

02

DIGITAL IDENTITIES

03

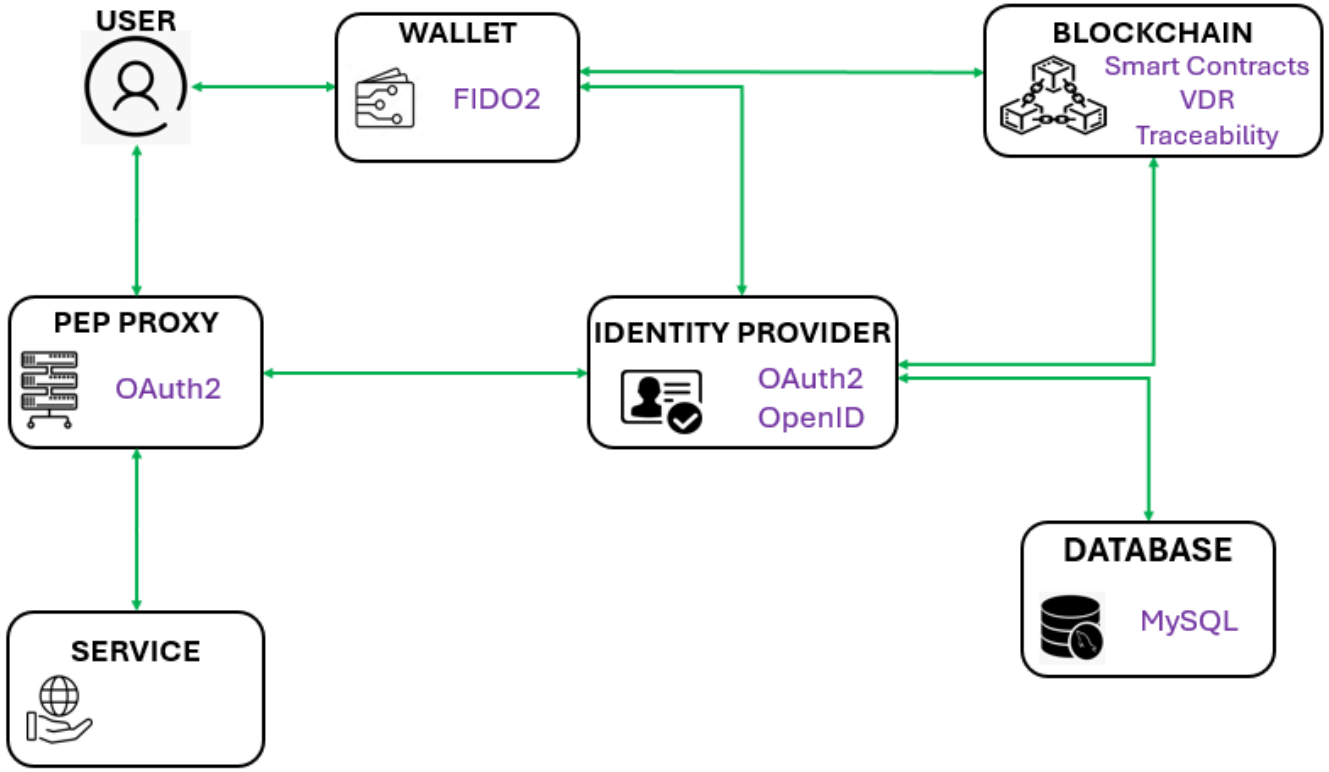
ARCHITECTURE

04

CONCLUSION AND FUTURE WORK

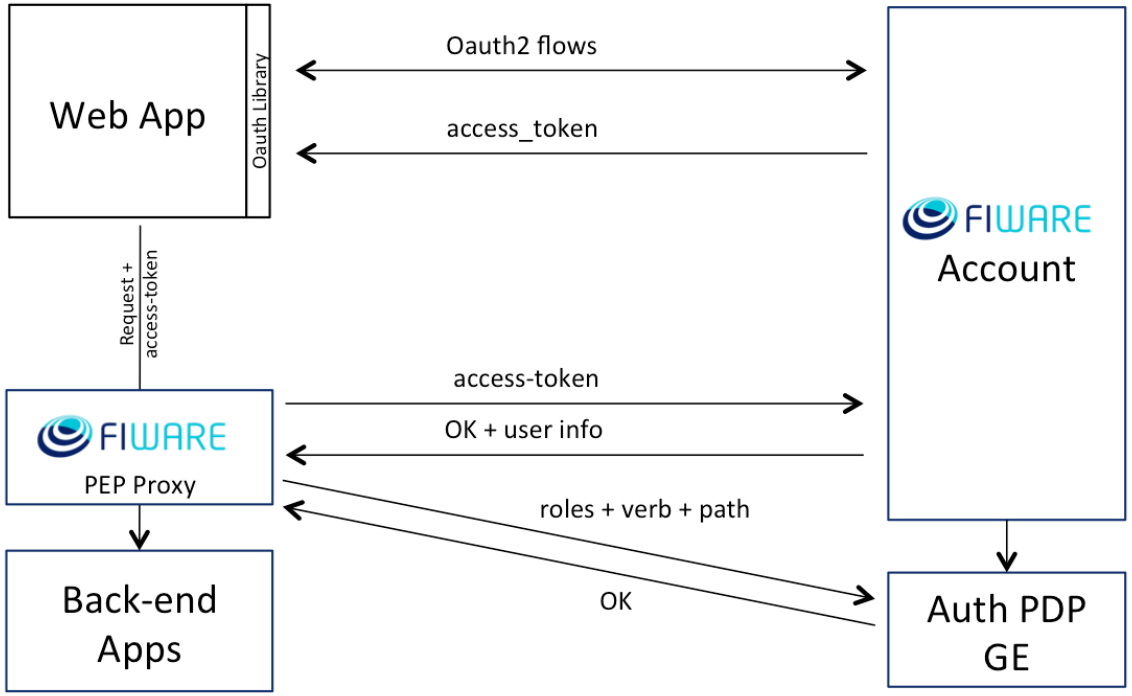
3. Architecture

- Identity Management for an Agri Data Space
- eIDAS2 compliant → SSI
- Authentication and Authorization of Users
- Five Modules



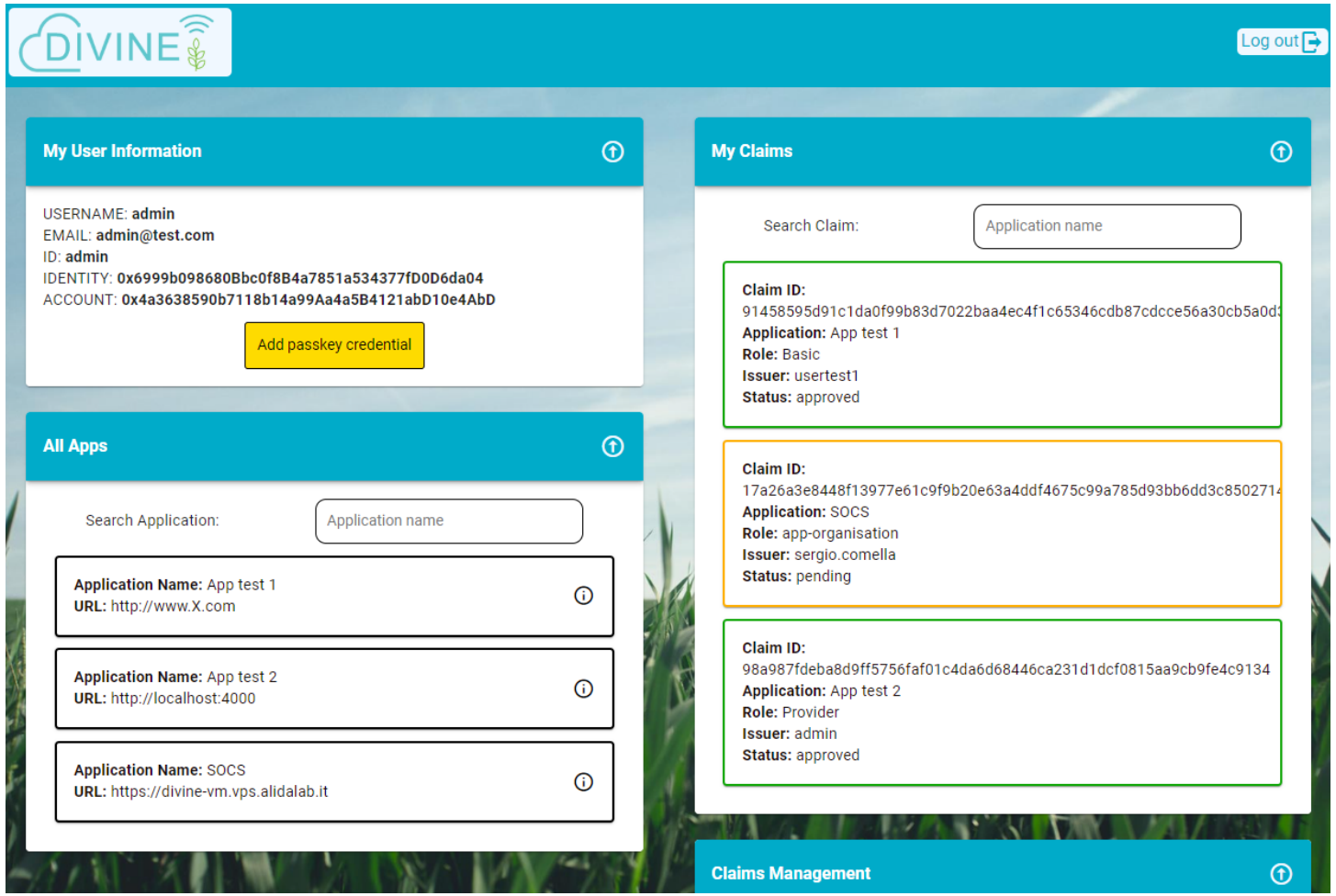
Identity Management

- Identity Provider (FIWARE)
- Manage identities, roles and permissions within the applications
- OAuth2.0 and OpenID Connect
- PEP-Proxy



Wallet

- Designed for holders to manage their credentials
- Allows viewing of available services
- Request and view credentials



Blockchain tool

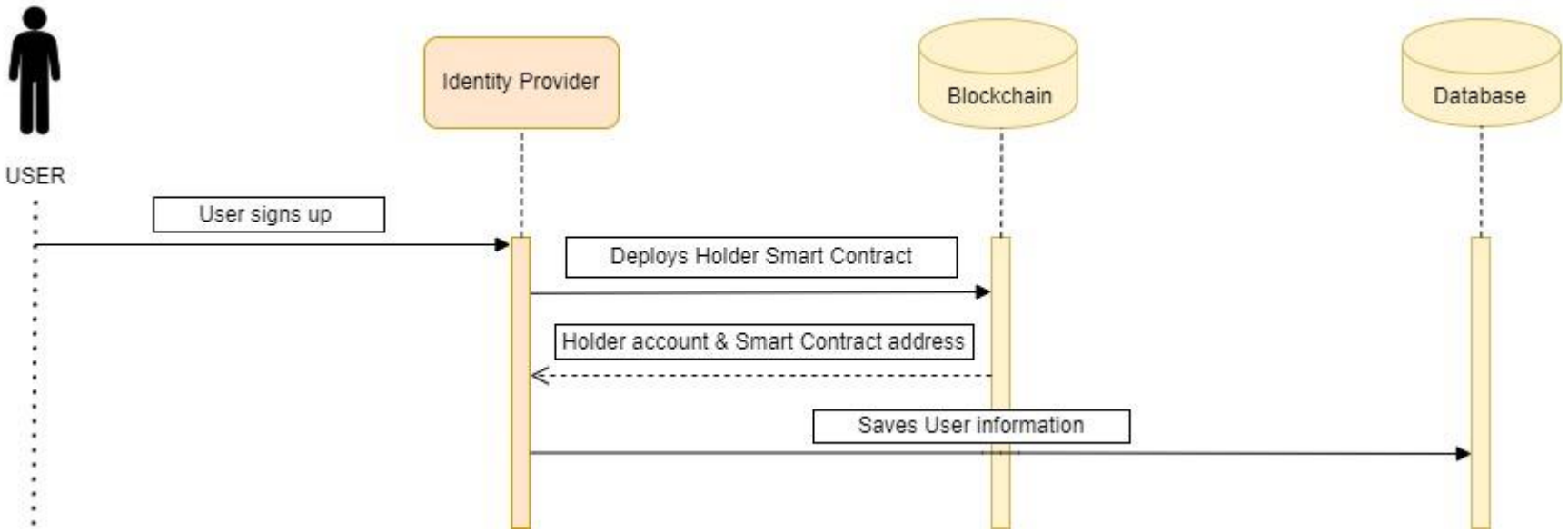
- A private Ethereum network with three nodes has been deployed to develop the VDR.
- Custom Smart Contracts in Solidity developed for each participant in the SSI ecosystem.
- Based on the Ethereum standards ERC-735 and ERC-734.
- Another Smart Contract has been created for the Traceability Module.

SOLIDITY

ethereum

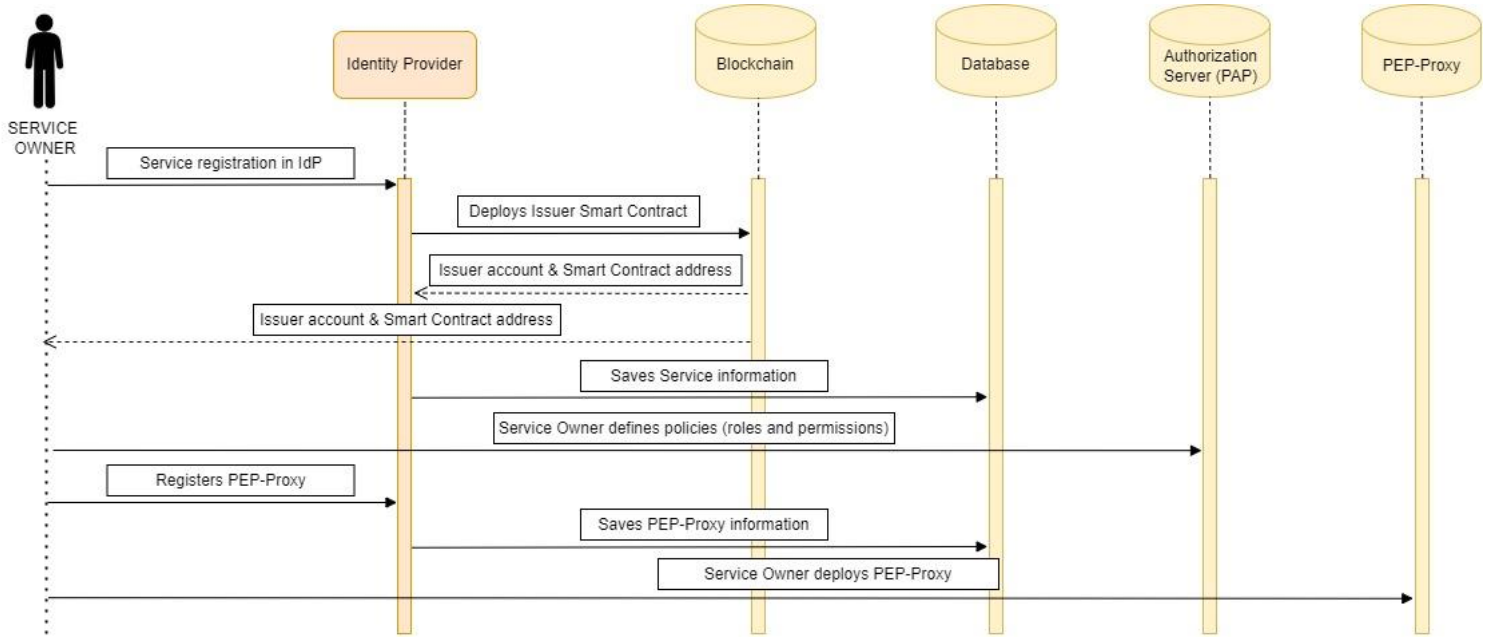
Create user

1. The user signs-up in Keyrock.
2. Keyrock deploys a Holder Identity for the User in the Blockchain.
3. Blockchain returns the holder's account and SC address.
4. Keyrock stores the user information in the MySQL database.



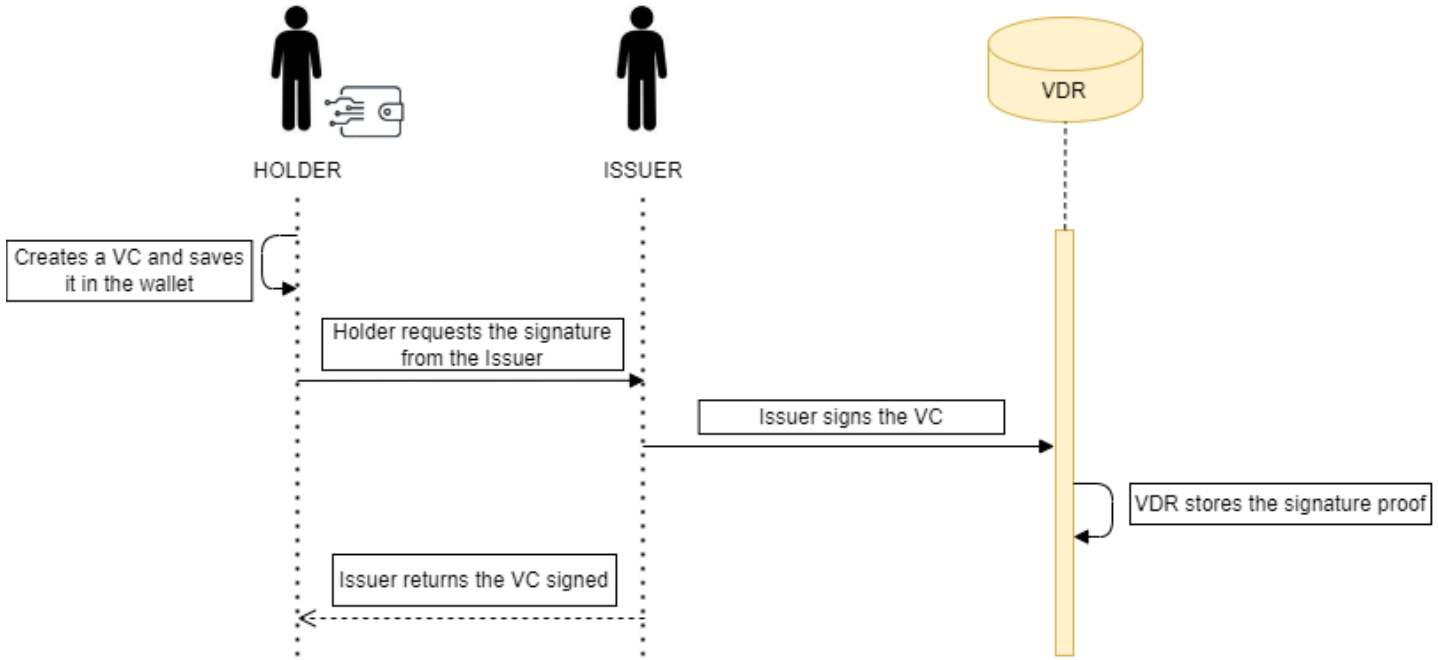
Register Service

1. The user register the service in Keyrock (url, callback-url, roles…).
2. Keyrock deploys, on the blockchain, an issuer's account for the owner of the service.
3. Keyrock stores the relevant application information in the MySQL database.
4. The issuer registers the roles in Keyrock, with their permissions.
5. Keyrock saves the role associated and the permissions with the application in the MySQL database.
6. The owner of the service deploys a Wilma PEP-Proxy.



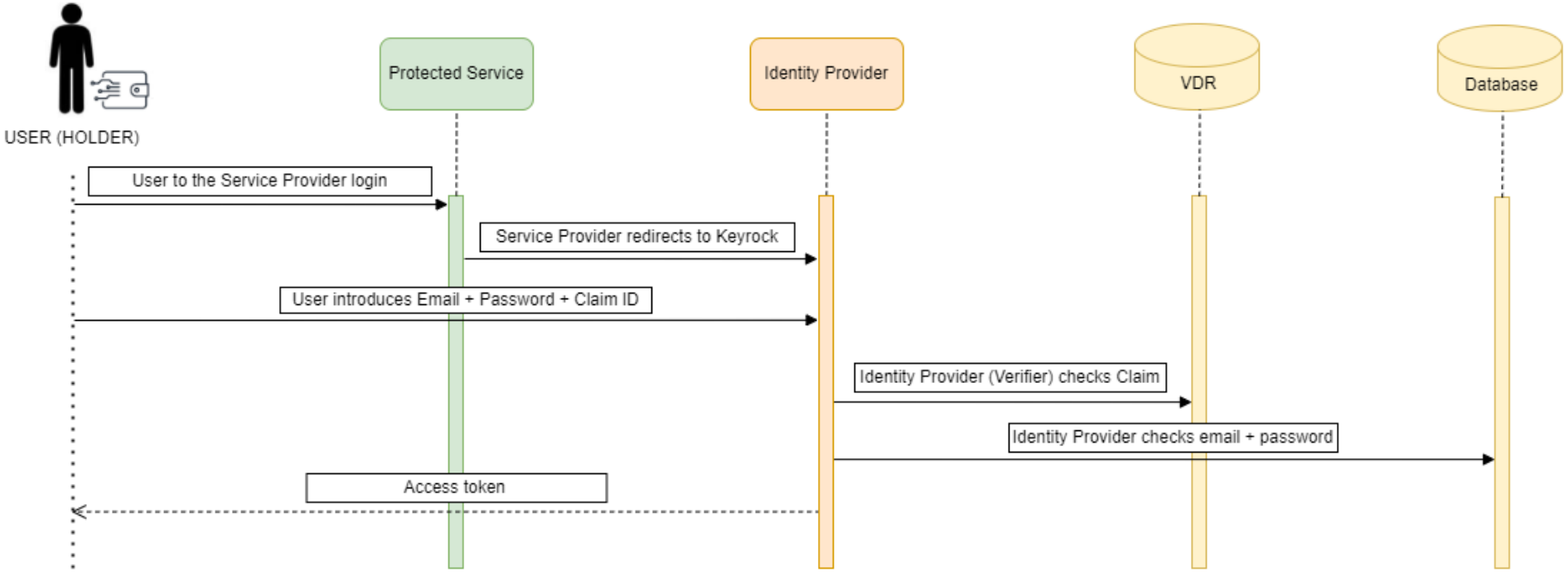
Verifiable Credentials Management

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.



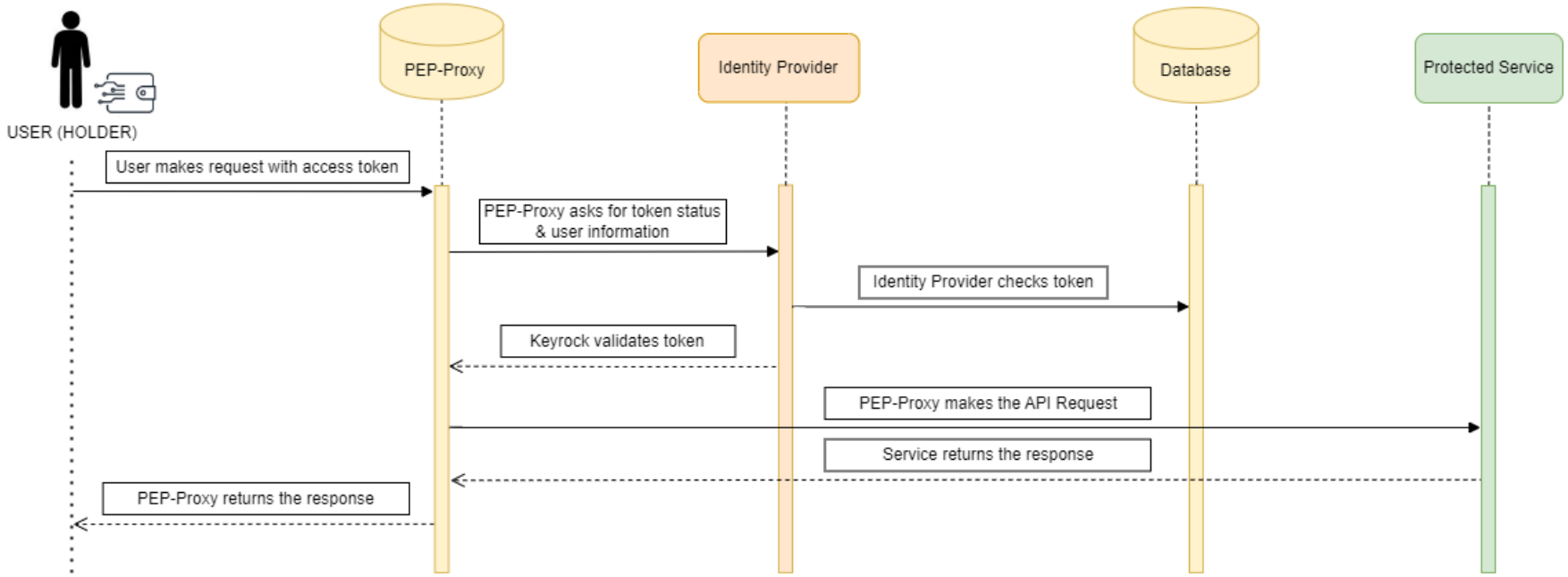
Authentication process

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. It allows the user to access the service by providing an access token.



Authorization process

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.
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.



vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

01

INTRODUCTION AND OBJECTIVES

02

PROPUESTA ORIGINAL

03

ARCHITECTURE

04

CONCLUSION AND FUTURE WORK

4. Conclusion and Future Work

vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

CONCLUSION

- This tool implements an identity management model based on SSI
- It is being used as a complete user Authentication and Authorization system in DIVINE
- Robustness and security of the system thanks to the traceability module

FUTURE WORK

- Standardization of VC to align it with the European Blockchain Services Infrastructure (EBSI)
- Add authorization servers for more elaborate permissions management

vicomtech

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

Thank you!

"Identity Provider based on Self-Sovereign Identities and Blockchain Technology"

dparedes@vicomtech.org

www.vicomtech.org