Funded by the European Union

DIVINE - Grant Agreement 101060884 HORIZON-CL6-2021-GOVERNANCE-01-20

DIVINE - DemonstratIng the Value of agri data sharIng for boostiNg data Economy in agriculture

Deliverable D6.4

Title: Development & integration of agri data sharing governance models, policies and regulations - Release 2

Dissemination Level:	**Public**
Nature of the Deliverable:	**DEM, Report**
Date:	**31/07/2024**
Distribution:	
Editor:	**Delia Milazzo (ENG)**
Contributors:	**Sergio Comella (ENG), Alessandra Diana (FE), Concetta Cardillo (CREA), (KGZS)**
Reviewers:	**Stavros Xynogalas (ICCS), Kevin McDonnell (UCD), Soumya Kanti Datti (DIGI)**

European Union
European Regional Development Fund

Disclaimer

Revision History

Date	Rev.	Description	Partner
01/07/2024	1	Draft TOC	ENG
07/07/2024	2	TOC validation and contribution allocated	ENG, FE, CREA, KGZS
20/07/2024	3	Partners Contribution	ALL
22/07/2024	4	Internal Review	UCD, DIGI, ICCS
25/07/2024	5	Final Version after review	ENG

Summary

1 Introduction

1.1 Purpose

The primary purpose of this document is to outline the functionalities and benefits of the software tool that allows responsible parties, pilots and stakeholders, to add new policies or governance models into the DIVINE Ecosystem. This capability ensures that the agricultural data governance framework remains flexible and responsive to emerging needs and technological advancements.

Key functions of this document include:

1. Policy Recommendations: It allows to provide a set of validated recommendations for data sharing policies tailored to the agricultural sector, guiding stakeholders in effective data management.
2. Evaluation and Monitoring Framework: It details the framework used to evaluate the effectiveness of these policies and monitor their impact, fostering a culture of continuous improvement.
3. Software Functionality: It describes the core features of the software tool, which facilitates the integration of new policies and governance models. This user-friendly tool ensures that policymakers can efficiently manage the evolving policy landscape.

By integrating these elements, this document supports the development of robust agricultural data governance, promoting transparency, efficiency, and innovation in the sector by engaging ADSE participants.

1.2 Scope and Audience

The Development & Integration of Agricultural Data Sharing Governance Models, Policies and Regulations aims to provide software that would allow responsible parties (policy makers) to add new policies or new governance models in ADSE systems. This will allow users to add new policies and governance models as documents in the system.

The aim of this document is to present the functionalities of a software tool designed to integrate new policies and governance models into the agricultural data sharing framework. It aims to provide validated policy recommendations tailored to the agricultural sector, detail an evaluation and monitoring framework, and describe the key features of the software tool. This document supports the development of robust agricultural data governance and promotes transparency, efficiency and innovation in the sector. It is aimed at stakeholders involved in agricultural data management, in particular policy makers, developers and users of agricultural data.

1.3 Document Structure

The document is structured to provide an overview of the ADSE repository of agricultural data sharing governance models, policies and regulations. It begins with an introduction that outlines the purpose and scope, followed by sections of detail including understanding agri-data sharing governance policies, software overview and features, and testing and validation. Each section is divided into subsections covering definitions, essential components, policy creation processes and

compliance with EU regulations. The document also includes practical user guidelines for accessing and managing the software system, ensuring a thorough understanding of its features and benefits.

2 Understanding Policies in Agri Data-Sharing Governance

2.1 Definition and Characteristics

2.1.1 Data Governance Models

Data governance is the process of managing the availability, usability, integrity and security of the data in enterprise systems, based on internal standards and policies that also control data usage[1].

A data governance framework can enhance the value of organizational data by improving data accuracy, which influences both simple decisions and complex automation initiatives. Key benefits include:

1. **Driving Scale and Data Literacy:** Limiting data access can hinder innovation and create dependencies on experts. Data governance promotes a shared understanding of data across systems through standardized definitions and metadata, enabling self-service solutions and federated data access.
2. **Ensuring Security, Privacy, and Compliance**: Data governance policies help meet regulatory requirements, like GDPR, preventing costly fines and data misuse by setting protective guardrails.
3. **Maintaining High-Quality Data:** Ensuring data integrity, accuracy, completeness, and consistency helps organizations optimize performance.
4. **Promoting Data Analytics:** High-quality data supports advanced analytics and data science initiatives, fostering stakeholder trust[2].

Data governance models vary depending on the primary objectives, scope, and specific needs of the project. Fundamentally, data governance is based on a comprehensive Data Strategy that aligns with the project's goals, ensuring that data management practices support the desired outcomes.

In the case of DIVINE, developing the AgriDataSharing Platform was driven by several key necessities:

1. **Easy Data Access**: Ensuring that data is readily accessible to authorized users is essential. This facilitates efficient decision-making and allows stakeholders to leverage data effectively for various agricultural applications.
2. **Farmer Control Over Data:** It is crucial to empower farmers with control over their own data. This not only respects their ownership but also builds trust in the platform by providing them with autonomy over how their data is used and shared.
3. **Rapid Data Sharing:** The platform needs to enable swift data sharing among stakeholders. Quick access to relevant data can enhance collaboration and responsiveness, particularly in time-sensitive agricultural operations.

[1] https://www.techtarget.com/searchdatamanagement/definition/data-governance
[2] https://www.ibm.com/topics/data-governance

4. **Transparent Policies and Clear Data Processing:** Transparency in data governance policies and clear procedures for data processing are vital. This ensures that all stakeholders understand how data is managed, processed, and utilized, fostering confidence in the system's integrity.
5. **Appropriate Data Storage**: Ensuring that data is stored appropriately is critical for maintaining data integrity, security, and compliance. The platform must have robust storage solutions that protect data while allowing for efficient retrieval and use.

2.2 Essential Component - Data Governance Models

As mentioned above, Governance models can vary greatly based on the main scope and strategy we want to achieve.

In Data Governance, the model is often composed as it follows:

6. **SoTA of the current regulatory Requirements**. This involves a comprehensive review of current regulatory requirements at regional, national, or global levels, depending on the model's scope. Understanding these regulations is crucial to ensure that the final model complies with all relevant rules, thereby avoiding potential fines and legal issues. This step establishes the foundational compliance framework for the governance model.
7. **SoTA and through analysis of the Data Model** that is planned to be used and developed in the project. This step involves a detailed examination of the data model intended for use and development within the project. By narrowing down the specific requirements for the model, this analysis aids in crafting pragmatic and tailored policies that are both effective and relevant to the project's needs. It ensures that the data model aligns with the overall data governance strategy.
8. **Policy and Recommendations Creation:** Based on the insights gained from the regulatory requirements and data model analysis, this step involves developing a comprehensive set of policies and recommendations. These guidelines form the core of the data governance framework, addressing how data should be managed, protected, and utilized.
9. **Definition and refining of policies**: to ensure a smooth data flow and enhance the value chain, it is essential to define and continually refine the data governance policies. Policies must be well-suited to the specific context and interact seamlessly to create value and facilitate processes. This involves regular updates and adjustments to the policies to keep pace with evolving data practices and regulatory landscapes.

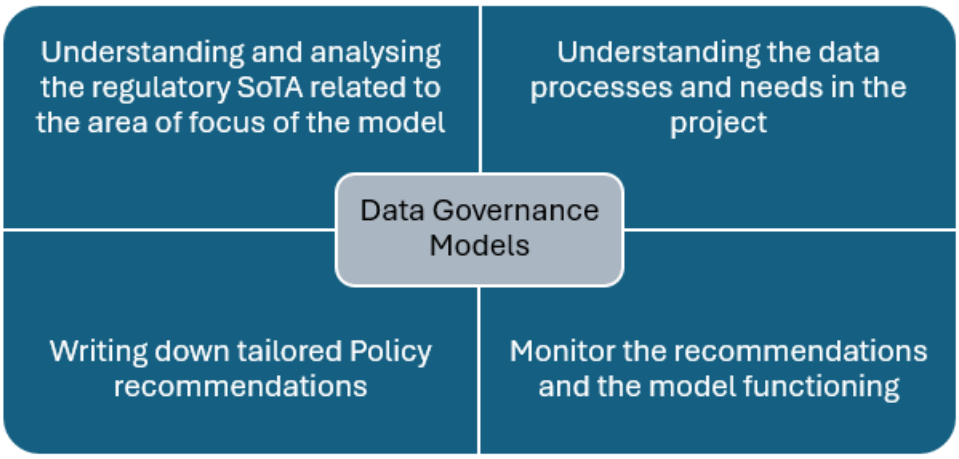


Figure 1. Data Governance Models Components

2.3 Policy Creation Process

Policy recommendations to facilitate the adoption of IoT solutions in agriculture are a set of policy proposals based on the analysis of collected needs of the agricultural sector, fully in line with what the EIP-Agri also highlighted: enhancement of digital infrastructures, facilitation of access to open data, clear rules on data ownership and usage of shared data, data protection policy, reusability of components, standardization, support to the adoption of these solutions. The EU on digital policy tries to provide answers to these barriers, with the 2020 EU Digital Strategy or ensure the successful development and use of IoT solutions, the agricultural sector needs to be prepared for adopting new techniques.

In many instances, IoT promises great potential to meet the demands being placed on farmers, but in other instances, they may be difficult to implement on the farm because of restrictions, policy, affordability, accessibility, and usability. Therefore, policymakers must be aware of the benefits that IoT solutions can bring, but also, be proactive to bring about changes that will support farmers in the transition towards greater technologization. Technology has the potential to help to realize the objectives of the Green Deal and the Farm-to-Fork Strategy to reduce impacts on the environment without jeopardizing food production. Overall, the EU' approach to digitalization aims to: a) strengthen the EU's digital capabilities (achievement of technological sovereignty) in the fields of IT, data, security and accountability, Artificial Intelligence, robotics; b) ensure the widest possible dissemination that maximizes the benefits for all citizens, businesses, including SMEs, in all regions, in all sectors by pursuing respect for fundamental rights; c)lead the development of next generation technology.

The European Data Governance Act is a key pillar of the "European strategy for data" (European Commission, 19.2.2020). The aim is to create a single European data space, – a single market for data, where personal as well as non-personal data, including sensitive business data, are secure, and businesses also have easy access to an almost infinite amount of high-quality industrial data,

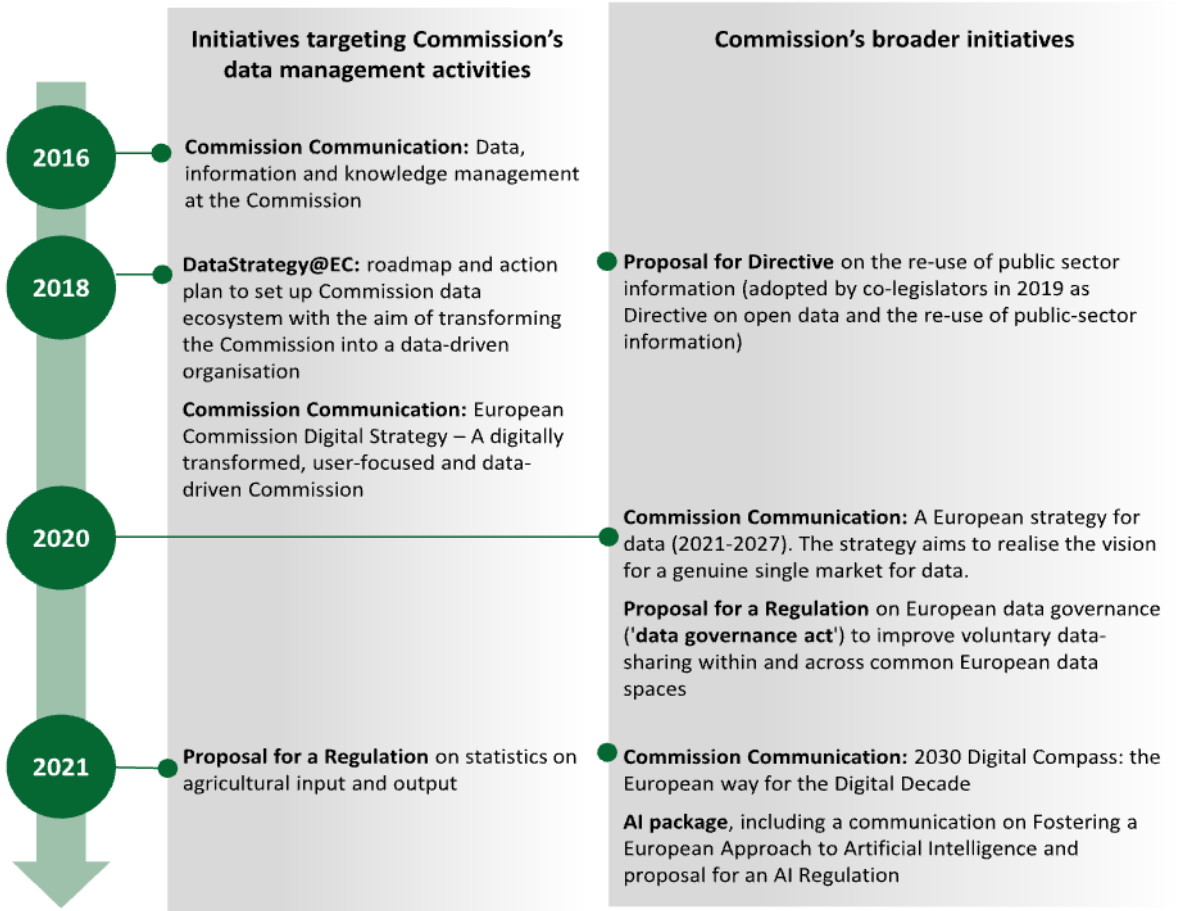
boosting growth and creating value, while minimising the human carbon and environmental footprint.

To establish a market for data and facilitate data exchange between companies—has not been reached to date the EU Data Strategy occurred. The framework communication acts a 5-years policy road map dealing with initiatives in every sector: • Connectivity. • The relationship between citizens and public administrations. • New measures for the business system. • The digital skills of all Europeans. The Strategy for Data proposes, among the other things, the creation of a European cloud to compete internationally on big data, while the White Paper indicates tools designed to make Artificial Intelligence accessible to industries, included SMEs and public administration. The Digital Strategy is based on three main pillars: technology that works for the people; a fair and competitive digital economy; an open, democratic and sustainable society. Under this perspective, the key points of the Digital Strategy for agriculture:

- A Common European Data Space on agriculture will be created to respond to the specific needs of the agricultural sector (precisely in the context of the Digital Europe program) and considering the creation of a federated distributed system of existing data platforms providing for a basic agreement on a set of interoperability mechanisms, avoiding possible blocking in existing platform architectures. A common agricultural data space based on existing data sharing approaches could lead to a neutral platform for sharing and pooling agricultural data, including private and public data.
- High data potential to increase the competitiveness of the entire agri-food sector, ensuring greater efficiency in the use of resources while reducing risks in agricultural production and in farmers' income; key role of data in improving the information made available to consumers by enabling the traceability and use of digital labels.
- Need to reduce the gap between urban and rural access to opportunities and services, including ensuring high-speed broadband access for all rural areas.
- Importance of promoting the development of digital skills to support farmers and rural communities in the digital transition.
- Need for a robust legal framework that safeguards farmers' right to data sovereignty and prevents distortion of competition, while not constraining the development of a data-driven economy.
- The Farm to Fork Strategy (15) presented by the European Commission in May 2020 places research, innovation and digitization at the center of the process that will have to accompany European agriculture to sustainability: in terms of funding and investments in research activities, there are 10 billion foreseen within the new Framework Program for R&I (Horizon Europe) on food, bioeconomy, natural resources, agriculture, fisheries, aquaculture and environment, use of digital technologies (e.g. data, Artificial Intelligence, IoT, robotics) and agro-ecological approaches.
- Specifically, Digital plays an important chapter within the F2F strategy. In short, it is envisaged: (i) the enhancement in the use of satellite images and Artificial Intelligence (AI) for the purpose of optimizing agricultural practices, traceability and controls, and (ii) guaranteeing access to fast broadband Internet in rural areas - target of 100% access by 2025; particular attention will be paid to education and training.

The "EU Code of conduct on agricultural data sharing by contractual agreement"is a clear example of a relevant and concrete initiative led by the key players of the agri-food sector, which embodies and includes the expectations of different stakeholders involved. It represents basically a joint effort from signatory organisations to shed greater light on contractual relations and provide guidance on the use of agricultural data. The Code of Conduct stresses that attention should be paid to: which data could be shared (and by who, what level of aggregation, what quality). • reflection on the inclusion of different levels of access by different stakeholders. • Data needs to be categorised according to different criteria, which are as follows: o Reusability, level of aggregation, quality o Purpose o Sensitivity (confidential, sensitive, private or public). For example, field weather data and satellite data are already public. Field boundaries and historic crops may be considered as semi-public o period for use (e.g. some information on harvest could be considered sensitive to avoid speculation, but after a while could be considered public and therefore shared).

The European Commission has issued several documents emphasising the need to improve and maximise the use of data for better policy-making, or impacting data sharing or tools in the EU (e.g. some information on harvest could be considered sensitive to avoid speculation, but after a while could be considered public and therefore shared). 3



[3]ECA, based on C(2016) 6626, DataStrategy@EC, C(2018) 7118, COM(2021) 37, COM (2018) 234/Directive (EU) 2019/1024, COM(2020) 66, COM(2020) 767, COM(2021) 118, COM(2021) 205 and COM(2021) 206

2.4 Differences from Guidelines and Procedures

Policy relates to a decision of the governing body of an organisation. A policy is typically an internal organisational decision that aids how it functions. A policy is a formal statement of a principle that should be followed by its intended audience. Each policy should address an important issue concerning the achievement of the overall purpose of the organisation. So a policy on health and safety in the workplace addresses the relevance of safety to the enterprise and to whom the principles apply.

A procedure provides detailed mandatory steps (sometimes in the form of a checklist) someone needs to follow to achieve a recurring task or comply with a policy. These procedures can include step by step instructions or statements telling you where something needs to go. A procedure informs employees how to carry out or implement a policy. Procedures usually contain written instructions in logical numbered steps.

2.5 Compliance with EU Regulations

2.5.1 GDPR Policies

The main regulation to account for when processing personal data consists in the General Data Protection Regulation (GDPR). Adopted in May 2016, its main goal is to *harmonize the protection of fundamental rights and freedoms of natural persons, laying down rules aiming at protecting the processing and the flow of personal data [Art. 1], handled both through automated and manual means [Art. 2]*.

Including this regulation and the policies deriving from it in DIVINE is fundamental. Non-compliance could lead to several negative outcomes, including losing the trust of farmers and incurring costs from fines due to unlawful data handling.

The main policies extracted from the adopted text include:

1. Lawful and Transparent Processing:
2. In the context of the creation of a data sharing platform as DIVINE, explicit consent to handle and process specific data (health, sex life, orientation, ethnicity, religious beliefs), needs to be given by farmers.
3. DIVINE will collect these data only for specific, legitimate purposes (Contract performance, legal obligations, vital interests, public interest), and the farmers need to be aware of it. Moreover, DIVINE needs to make sure the farmer:
4. Knows his rights;
5. Knows the data storage duration;
6. Knows and is able to access, rectify, erase, and restrict processing these data.
7. The data needs to be stored in a safe, secure and confidential environment.
8. Fair Processing:
9. In addition to the measure above-mentioned, DIVINE needs to make sure that these actions taken by data subjects are free of charge.

10. Make data easily portable.
11. Store the data only as long as necessary.
12. Data Protection Measures:
13. DIVINE, or any other data sharing platform, will implement risk-avoidance measures to prevent accidental or unlawful destruction, alteration, or access to data.
14. Notify data subjects of any personal data breaches.

3 Software Overview and Features

3.1 General Description

To address the objective of this deliverable, we are utilizing NextCloud, a robust, open-source software suite designed to provide secure, scalable, and user-friendly cloud storage and file-sharing solutions. NextCloud allows organizations to manage, share, and synchronize files seamlessly across various devices while maintaining strict control over data privacy and security. In the context of agricultural data, NextCloud serves as an invaluable tool for distributing policies, guidelines, and datasets efficiently among stakeholders, ensuring that critical information is accessible and up-to-date.

3.2 Key Functionalities

NextCloud provides a comprehensive solution for managing and sharing agricultural data policies, with a range of features that enhance security, collaboration and customisation. Below is a list of key features that make NextCloud an ideal platform for the distribution of agricultural policies and guidelines.

1. **Secure file sharing and storage**: NextCloud ensures that agricultural data policies are stored securely using advanced encryption techniques, ensuring that only authorised personnel have access to sensitive documents and maintaining the integrity and confidentiality of the information.
2. **Collaboration and accessibility**: it facilitates collaboration between stakeholders by enabling real-time editing and sharing of documents. Users can access policies from any device with an Internet connection, ensuring that critical information is always at their fingertips.
3. **Granular permission controls**: With this platform, administrators can set precise permissions for each user or group, defining who can view, edit or share specific documents. This ensures appropriate data sharing and protection of sensitive information.
4. **Scalability**: it is designed to scale as an organisation's needs grow. Whether you need to share small amounts of data or manage large datasets and policies, NextCloud can handle increasing loads without compromising performance.
5. **Version Control**: NextCloud's version control feature allows users to track changes made to documents over time. This is particularly useful for agricultural policies, allowing stakeholders to reference previous versions and understand the evolution of policies.
6. **Customisable and extensible**: it offers a high degree of customisation through its extensive application ecosystem. Organisations can tailor the platform to their specific needs by integrating additional functionality such as calendar management and task tracking.
7. **End-to-end encryption**: NextCloud provides end-to-end encryption to ensure that data remains secure in transit. This is particularly important when sensitive agricultural policies are shared across different networks.

With NextCloud, organizations can maintain control over their data while facilitating effective communication and compliance, making it a valuable asset in the agricultural sector.

3.3 System Architecture

The system architecture is designed to ensure high performance, security and scalability. Built on a robust LAMP (Linux, Apache, MySQL/MariaDB, PHP) stack, it leverages the flexibility and reliability of open-source technologies to deliver seamless cloud storage and file sharing solutions. The platform supports a federated cloud architecture, allowing multiple instances to connect and share data securely. Integration with IDM Keyrock, a powerful identity management (IDM) system, enhances security by providing centralised authentication and authorisation services. This federation with IDM Keyrock ensures that user identities are managed consistently across the network, facilitating secure access and collaboration while maintaining strict privacy and security standards. In addition, the use of the DIVINE library adds advanced functionality to the platform, further improving the efficiency and security of data management and sharing.

3.4 User Guidelines

DIVINE Library offers a comprehensive set of features designed to improve user productivity and collaboration within organisations. Users can seamlessly store, synchronise and share files across devices, ensuring access to documents, images and other data from anywhere. Its robust file management capabilities include version control, allowing users to track changes and revert to previous versions when needed.

It integrates powerful collaboration tools such as real-time document editing, commenting and task management to facilitate efficient teamwork. Enhanced security features, including encryption and advanced access control mechanisms, protect sensitive data from unauthorised access. In addition, Nextcloud supports seamless integration with various third-party applications and services, enhancing its versatility and usability across different workflows. With features designed for scalability and customisation, it enables organisations to tailor their cloud solutions to specific needs, whether for small teams or large enterprises, ensuring flexibility and efficiency in data management and collaboration.

After authentication, the user is given access to their own dashboard, Figure 2, which can be customised in many ways.

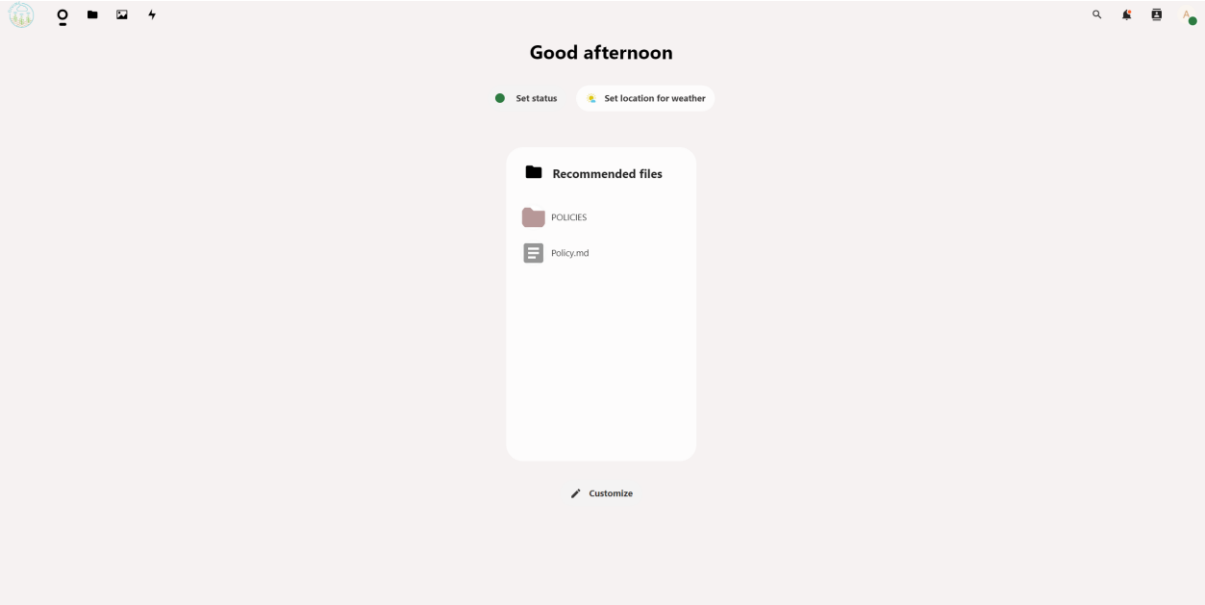


Figure 2. DIVINE Library Dashboard

In the navbar, user access to the files where it is possible to put files and create directories, Figure 3:

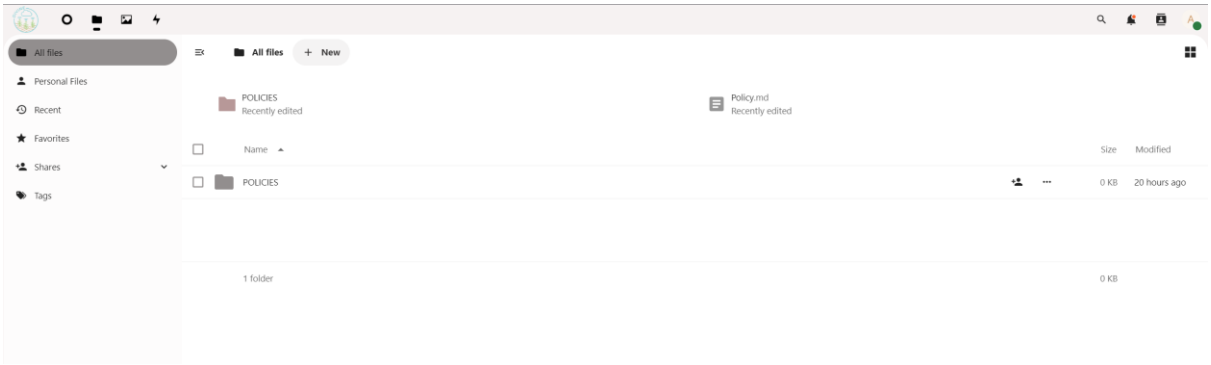


Figure 3. Files management

Once some files are created or some directories are created, user is able to share them with the share button, Figure 4. Of course, user can share via link or grant access via email.

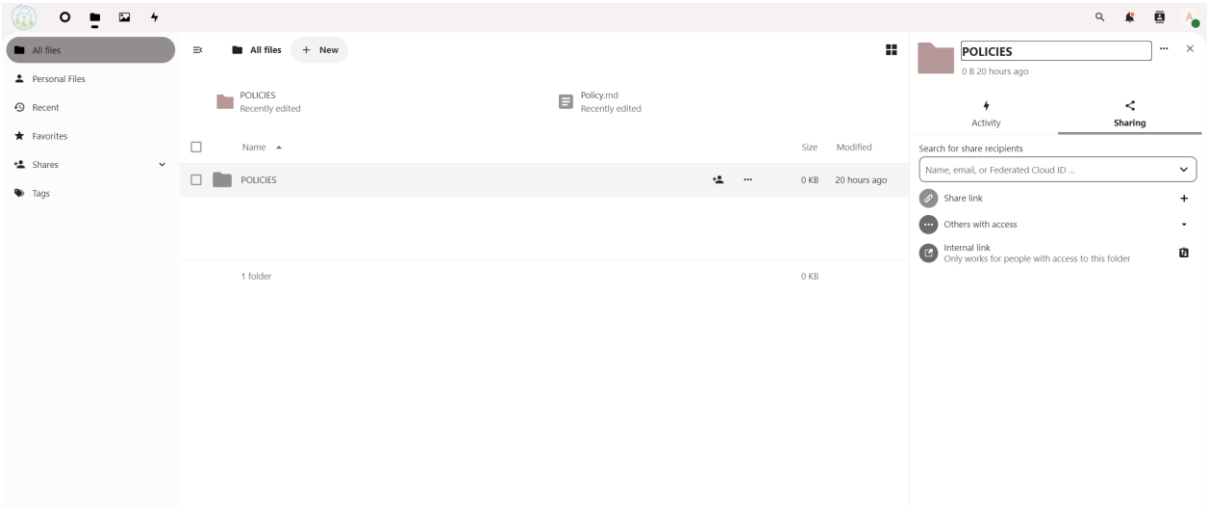


Figure 4. Share functionality

3.4.1 Accessing the System

The Identity Management System (IdM) for DIVINE is based on Self-Sovereign Identities (SSI). SSI represents a paradigm where privacy and security are fundamental, empowering individuals to control their digital identities.

In a foundational SSI model, four primary entities assume vital roles: Holder, Issuer, Verifier and Verifiable Data Registry. The Holder denotes the individual user who possesses Verifiable Credentials (VCs) that form the basis of their identity, with the primary responsibility of storing and presenting these credentials when necessary. The Issuer serves as a trusted entity or individual authorized to issue and sign (validate) the holder's credentials, thereby ensuring the authenticity and validity of the contained information. Lastly, the Verifier represents the entity or individual to whom the holder intends to provide their credentials. To ascertain the authenticity of the holder's identity or claims, the verifier must validate these credentials. The Verifiable Data Registry (VDR) constitutes an additional infrastructure supporting this process, enabling individuals to establish ownership, control, and portability of their digital identities. A VDR, functioning as a system or database such as a blockchain, facilitates the registration and storage of public keys of issuers, credential schemes, and other crucial data required to verify the authenticity of credentials. Unlike traditional Distributed Ledger Technologies (DLTs), the VDR does not store the credentials themselves; instead, it holds the information necessary for verifiers to reliably assess their validity. Blockchain technology, a widely adopted form of VDR, ensures secure and immutable record-keeping through a chain of cryptographically linked blocks. This capability enables the tracking of modifications in digital credentials, which is indispensable for security and identity verification.

The IdM implemented in DIVINE comprises a comprehensive suite of modules designed to manage access and permissions within data spaces effectively: Personal Wallet to store and manage Verifiable Credentials (VCs) securely, a private Ethereum network to deploy the Smart Contracts for Holder, Issuer and Verifier and serve as a Verifiable Data Registry, the Identity Provider (IdP) implemented with Keyrock (powered by FIWARE), an Authorization module to manage policies and granting permissions to the users, a PEP-Proxy for each service to protect them by enforcing access control policies, and a Traceability module to record events within the system, enhancing

transparency and accountability. The IdM leverages protocols, Figure 5, and technologies such as FIDO2, OAuth2, and OpenID to ensure robust security and interoperability.

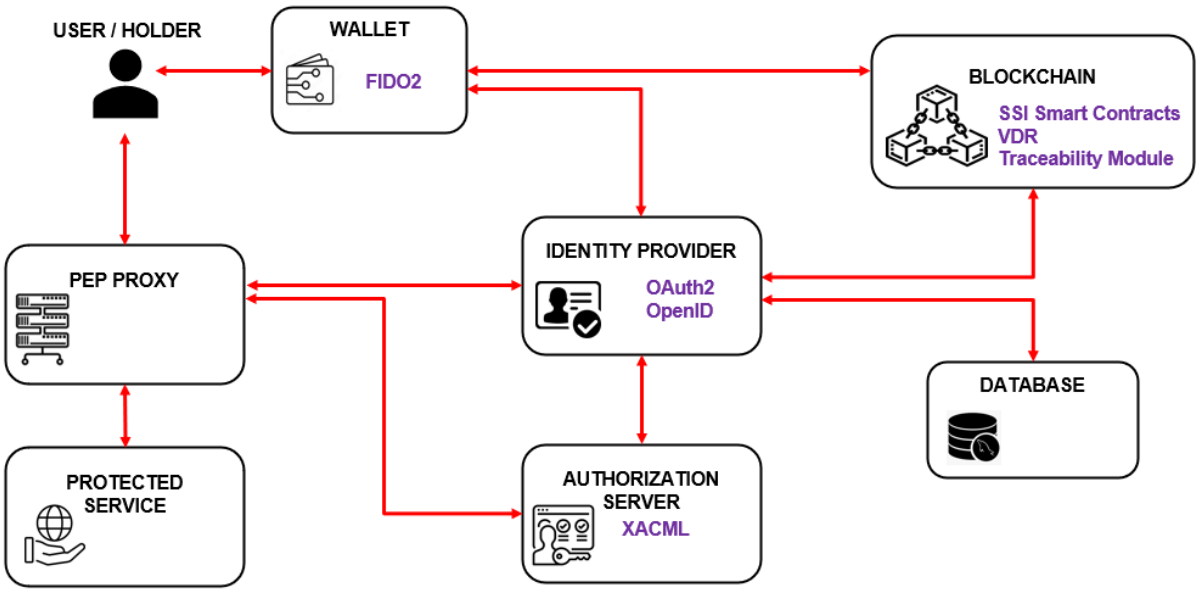


Figure 5. IDM Protocol

The goal is to facilitate application developers and dataset owners in registering their services on a trusted platform, thus enabling them to assign roles and permissions to users.

Upon registration on the CredSSI platform, users will be equipped with a digital identity ("Holder") based on Verifiable Credentials, which can be managed through a personal wallet to add, modify, delete, present, and read VCs. The aim is for these Verifiable Credentials to denote roles within a specific application or pre-registered service. Consequently, the application owner would assume the role of "Issuer" and could sign a claim for the user, designating the role the user holds within the application. Moreover, a role encompasses a set of permissions and available calls. In this way, the IdP (Keyrock) would serve as a "Verifier" each time a user initiates an HTTP request to a service, validating the authenticity of the Verifiable Credential and ensuring that it is signed by the corresponding issuer (the service owner or trusted issuer). Finally, the modules dedicated to managing the authorization (PEP-Proxy and Authorization Server) will check that the role of the user who is making the request has the necessary permissions to make the request.

3.4.2 User Roles and Permissions

The registration and role management processes are crucial in ensuring the security and efficiency of user interactions. This section provides a comprehensive outline of the procedures involved in these processes, including user registration, application registration, role requests, role assignments, and claim revocation. Each of these processes utilizes blockchain technology to ensure transparency, security, and immutability, creating a strong and reliable environment for all users and applications.

3.4.2.1 User sign-up

Users must acquire a Holder Smart Contract to efficiently manage their VCs. This will enable users to perform a range of credential management activities. To do so, the following actions are performed:

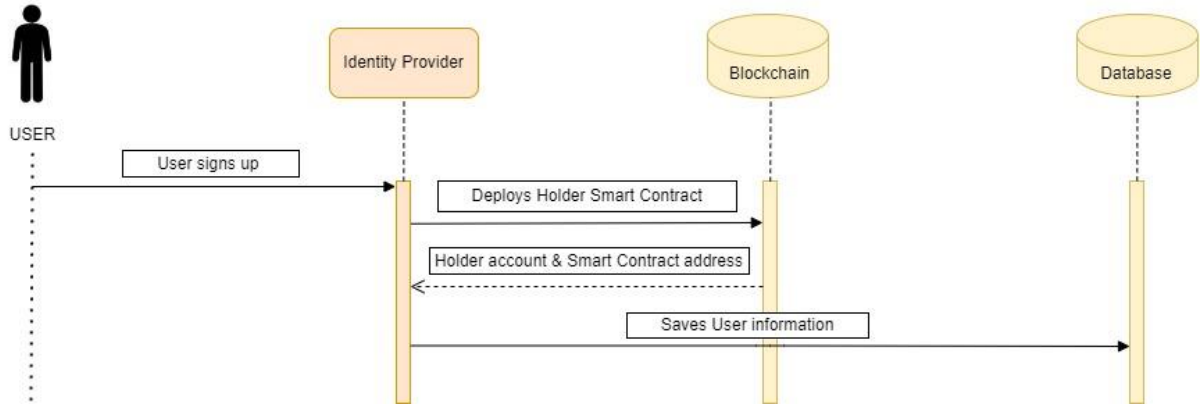


Figure 6. User sign-up

3.4.2.2 Service registration

Upon the creation of the user account, the subsequent requirement is for the service owner to register the service, thereby facilitating access for various users. For this purpose:

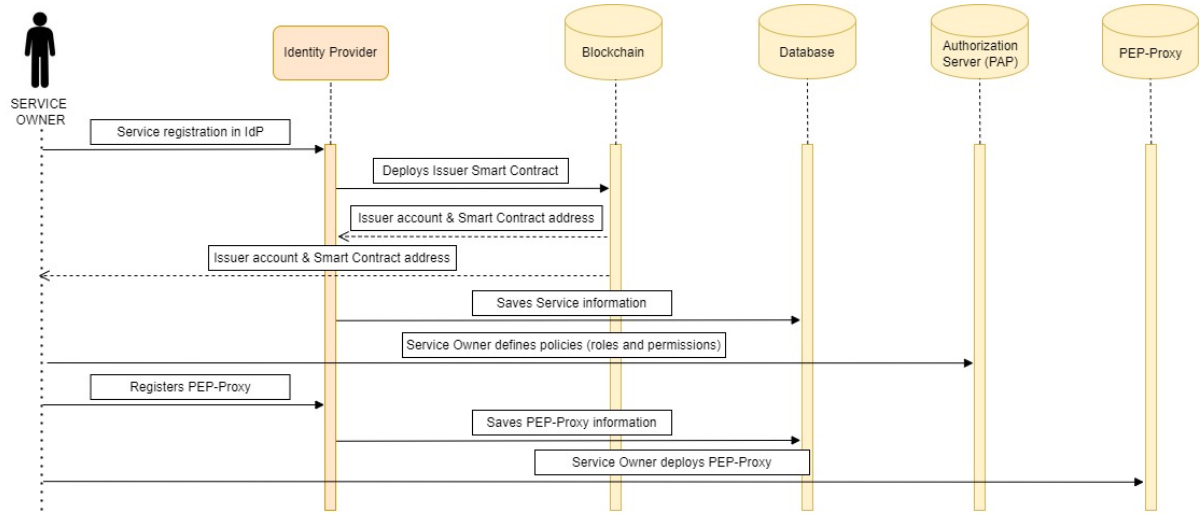


Figure 7. Service Registration

3.4.2.3 Request a signed VC

When a service is registered in Keyrock, the user can generate a Verifiable Credential and request that it be signed by the owner of the service. It is necessary to have a signed credential for the service in question, as it must be presented in the authentication process for the service. To achieve this, the user must perform the following sequence of actions:

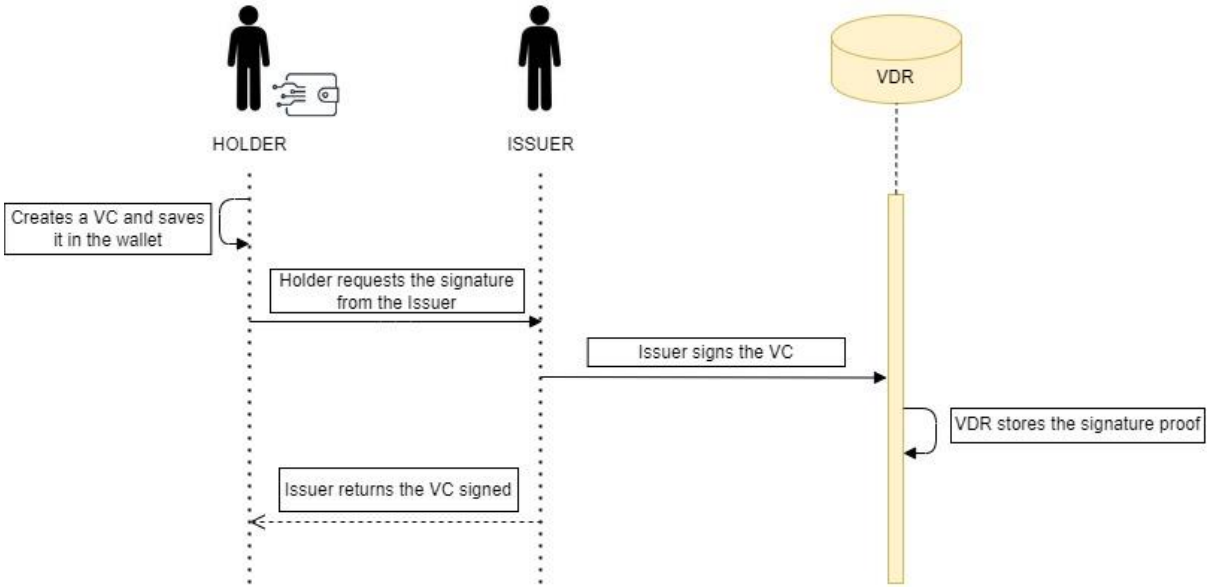


Figure 8. Request a signed VC

3.4.2.4 Authentication process

The steps for authentication are as follows:

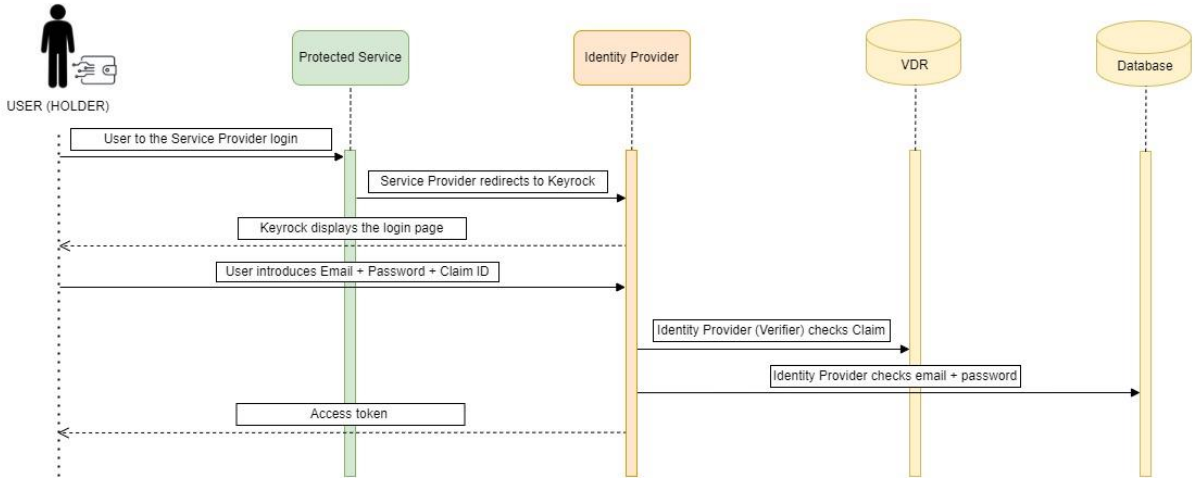


Figure 9. Authentication Process

3.4.2.5 Authorization process

Upon successful authentication, individuals can use their access token to request specific resources. The access token will contain user-specific details, including the user's identifier, roles, and permissions. If a user's role does not permit specific requests, those requests may be denied. Consequently, there is a defined process from the initial user request for a resource to the eventual receipt or denial of the requested resource. The sequential steps involved in this process are as follows:

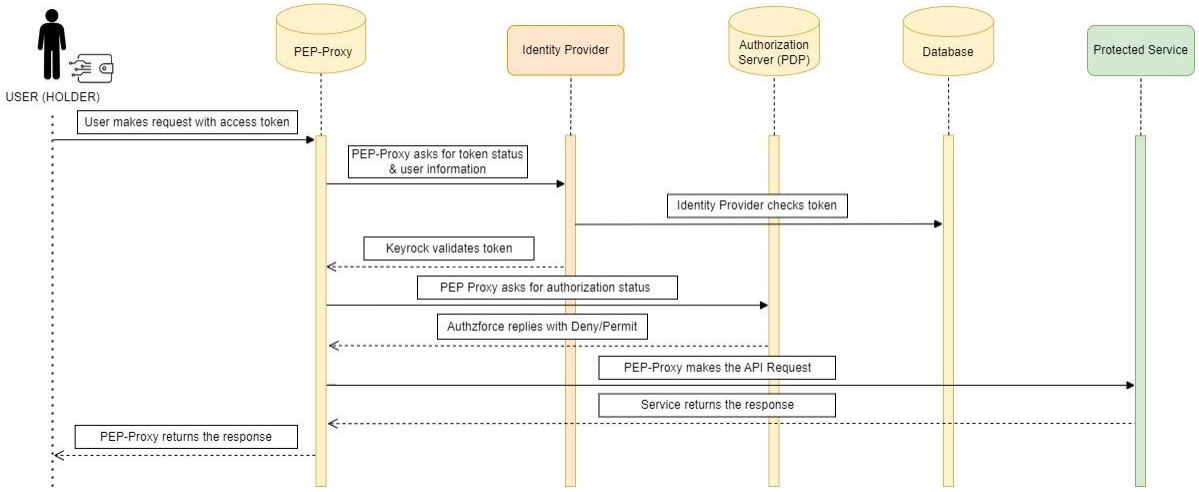


Figure 10. Authorization process

3.4.3 Adding and Editing Policies

The owner of a service, once he has registered the service in Keyrock, is free to create roles within his application. A role is a set of permissions and policies, so that if a user is assigned a certain role, he or she will be able to perform the actions allowed for that role.

Roles and permissions can be added and edited in the Keyrock interface itself if the permissions to be implemented are relatively simple. For complex permissions such as limiting calls from certain IPs, imposing time restrictions on calls or restrictions on the call body, the AuthzForce module should be used.

Then, as explained above, to grant a role to a specific user, this user must have a VC in his wallet representing this role and the owner of the service must sign this credential acting as Issuer. To sign the credentials and grant roles, the Keyrock interface records user role requests, so that service owners can easily accept or deny the requests.

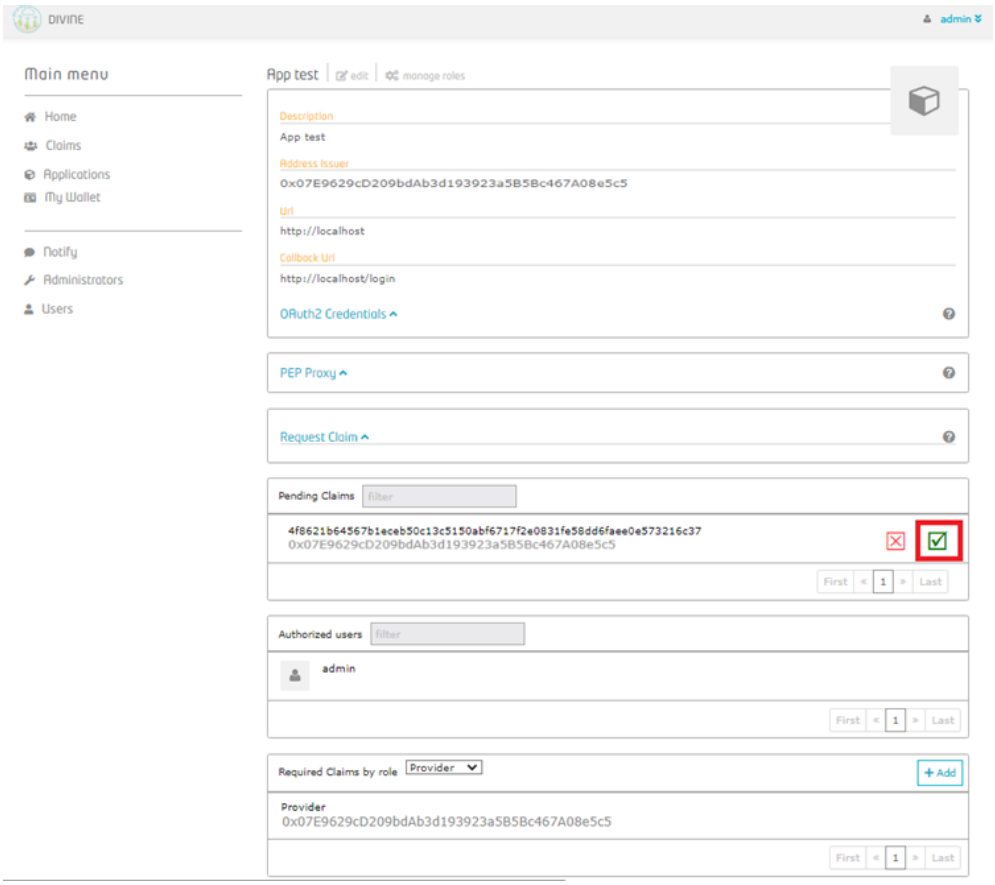


Figure 11. Adding and Editing Roles/Policies

3.4.4 Versioning and History

The activities page on the Application provides a comprehensive overview of recent modifications and interactions within the DIVINE Library. It tracks changes such as file creations, deletions, modifications, and shares, as well as collaborative interactions like comments and tag applications. This feature ensures users are promptly informed about updates and actions performed on their files and folders, thereby enhancing transparency and facilitating efficient collaboration. The Activities page allows filtering by various criteria, making it easy to monitor specific types of changes and maintain an organized workflow.

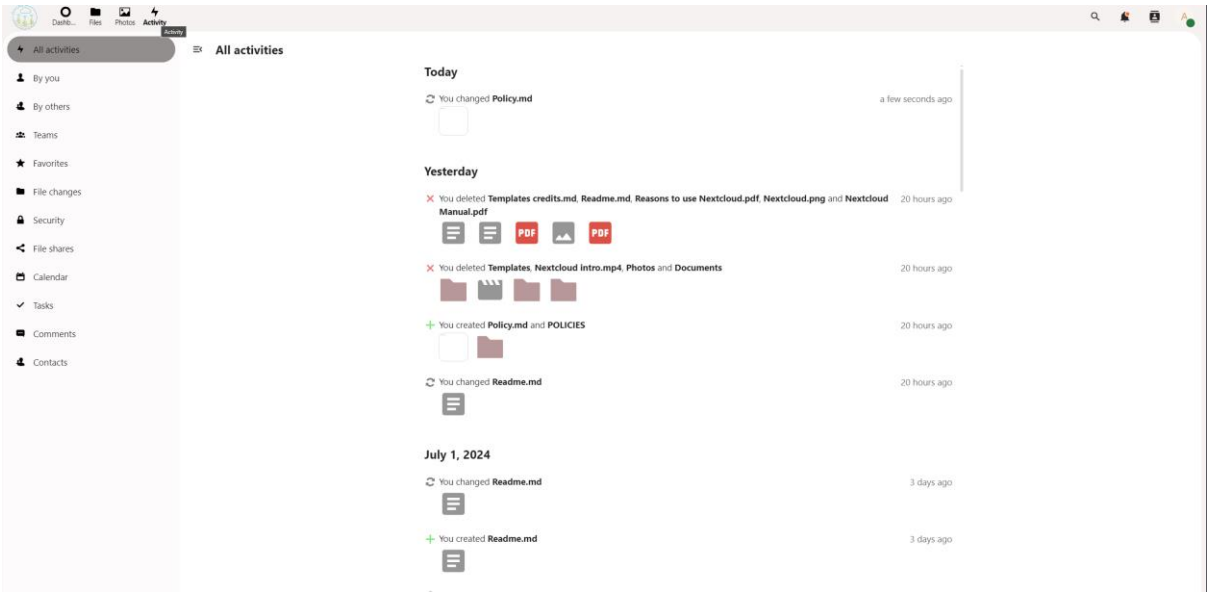


Figure 12. Activities tracking

3.4.5 Searching and Filtering

The search and filter functionality in DIVINE Library allows users to quickly find and manage their files and activities. The search feature allows users to perform keyword-based searches across files, folders and even content within documents. Filtering options allow users to refine search results by various parameters such as file type, modification date and tags. This feature increases productivity by allowing users to quickly navigate through large amounts of data, ensuring they can easily find the information they need and take the appropriate action.

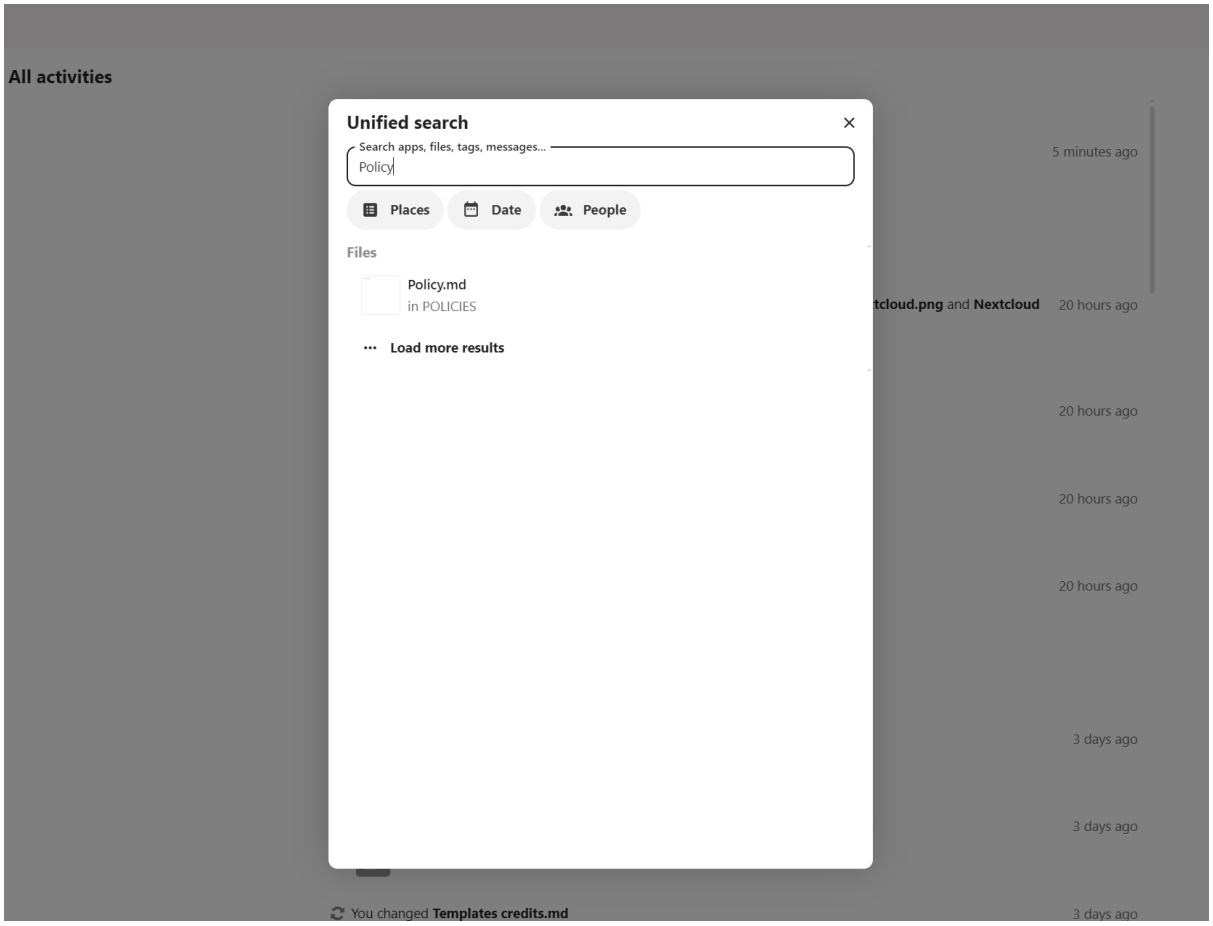


Figure 13. Searching and Filtering

4 Testing and Validation

4.1 Testing Strategy

The testing strategy for the AgriDataSharing platform will ensure the platform's functionality, performance, security, and compliance with relevant regulations. The purpose of strategy is to validate the platform's ability to handle, process, and share agricultural data policies securely and efficiently. This includes functional testing, performance testing, security testing, and compliance testing. Developers, pilot leaders, project managers, and stakeholders involved in the development and deployment of the data-sharing platform are most appropriate for conducting test of the platform.

4.1.1 Functional testing

Functional testing aims to verify that the platform functions according to the specified requirements. This includes:

- User authentication and authorization: Ensure that users can securely log in, register, and access data based on their roles and permissions.
- Agricultural data policies upload and retrieval: Validate the process of uploading, storing, and retrieving data, ensuring data integrity.
- Agricultural data policies sharing: Test the mechanisms for sharing data with other users or systems, including link generation and permission settings.
- User interface: Verify the usability and accessibility of the platform's interface, ensuring it meets user needs and expectations.

4.1.2 Performance testing

Performance testing assesses how well the platform performs under various conditions:

- Load testing: Simulate multiple users accessing the platform simultaneously to evaluate its ability to handle concurrent usage.
- Stress testing: Determine the platform's breaking point by pushing it beyond normal operational capacity.
- Scalability Testing: Test the platform's ability to scale up and down in response to changes in user load.

4.1.3 Security testing

Security testing ensures that the platform is protected against potential threats and vulnerabilities:

- Vulnerability scanning: Use automated tools to scan for known vulnerabilities in the platform's software and infrastructure.
- Penetration testing: Conduct simulated attacks to identify and address security weaknesses.
- Data encryption: Verify that data is encrypted both in transit and at rest, ensuring confidentiality and integrity.
- Compliance testing: Ensure the platform adheres to relevant regulations such as GDPR, ensuring lawful and transparent data processing.

4.1.4 Compliance Testing

Compliance testing involves verifying that the platform meets all regulatory requirements:

- GDPR Compliance: Ensure that data subjects' rights are protected, and data processing activities comply with GDPR requirements, including obtaining explicit consent and ensuring data portability.
- Audit trails: Verify that all data processing activities are logged, providing a clear audit trail for accountability and transparency.

4.2 Test Cases and Results

Test cases can be reasonable defined for the above testing areas. These tests can include:

1. Test case ID: A unique identifier for each test case.
2. Description: A brief description of the test case.
3. Preconditions: Any prerequisites that must be met before executing the test case.
4. Test steps: A list of steps to execute the test case.
5. Expected results: The expected outcome of the test case.
6. Actual results: The actual outcome observed during testing.
7. Status: Pass or fail status based on whether the actual results match the expected results.

4.3 Validation

Validation is important process in the development and deployment of the AgriDataSharing platform, ensuring that the system meets the requirements and expectations of its users and stakeholders. This process includes various stages to verify that the platform functions correctly, securely, and efficiently in real-world scenarios.

4.3.1 User Acceptance Testing (UAT)

User Acceptance Testing (UAT) is an essential step in the validation process. This involves engaging a group of end-users to test the platform under realistic conditions. The goal of UAT is to ensure that the platform meets the functional requirements and user expectations. During UAT, users interact with the platform as they would in their daily operations, providing feedback on usability, performance, and any encountered issues. This feedback is crucial for identifying areas of improvement and ensuring the platform's readiness for broader deployment.

4.3.2 Feedback Mechanism

Implementing an effective feedback mechanism is vital for the continuous improvement of the platform. This mechanism allows users to easily report issues and suggestions during and after the UAT phase. Regularly reviewing and acting on this feedback ensures that the platform evolves to better meet user needs.

4.3.3 Continuous Improvement

Continuous improvement is a proactive approach to maintaining and enhancing the platform over time. Insights gained from UAT and ongoing user feedback drive this process. Regular updates, feature enhancements, and bug fixes ensure that the platform remains effective, secure, and aligned with evolving user needs.

Testing strategy is important for ensuring the success of a AgriDataSharing platform. By systematically testing functionality, performance, security, and compliance, stakeholders can be confident that the platform will perform reliably and securely in real-world conditions. Regular updates and continuous improvement based on testing outcomes will help maintain the platform's integrity and user trust.

5 Conclusion

In conclusion, Deliverable D6.4 represents a significant milestone in the advancement of agricultural data governance through the development and integration of sophisticated data-sharing governance models, policies, and regulations. The document provides a comprehensive overview of the software tool designed to facilitate the seamless addition and management of policies within the agricultural data-sharing ecosystem. By leveraging NextCloud, a robust and secure open-source platform, stakeholders can ensure efficient and secure storage, sharing, and management of data policies.

The detailed description of key functionalities, system architecture, and user guidelines underscores the platform's commitment to providing a user-friendly and scalable solution. The integration of advanced security measures, such as self-sovereign identities and end-to-end encryption, further enhances the platform's ability to protect sensitive agricultural data.

Moreover, the rigorous testing and validation strategy outlined in this document ensures that the platform meets the necessary functional, performance, security, and compliance requirements. The emphasis on continuous improvement and user feedback mechanisms highlights the platform's dedication to evolving with the needs of its users.

Ultimately, the development and deployment of this agile, secure, and transparent agricultural data governance framework are poised to drive innovation, enhance efficiency, and foster trust among stakeholders. By ensuring that data governance practices align with the latest regulatory requirements and technological advancements, this initiative supports the broader goals of sustainability, data sovereignty, and technological advancement within the agricultural sector. This deliverable lays the groundwork for a resilient and future-ready agricultural data-sharing infrastructure, capable of adapting to the dynamic needs of the industry.

6 Figures