



Co-funded by the
European Union



Grant Agreement Number: 101202831

Project Title: European Vaccines Hub for Pandemic Readiness

Project Acronym: EVH

EU4Health Programme

Deliverable: D3.10 – SSO, Identity Provider, Group & Access-Management

“Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.”

Document overview

Deliverable number	D3.10
Deliverable name	SSO, Identity Provider, Group & Access-Management
Work package number / name	3
Task number / name	T3.2 / User Portal & Dashboard (M1-M48)
Due date	M12
Dissemination level	PU
Authors	Vasilii Tulsii, Elias Hamacher, Markus Brechtel
Lead Beneficiary	5 - DZIF
Project website	https://europeanvaccineshub.org/

Table of Contents

1. Introduction.....	4
2. Identity and Access Management Infrastructure Implementation.....	4
3. Achieved Two-Step Registration and Approval Process	5
4. Achieved Group Structure and Access Model	5
5. Outcome.....	5
Document approval / review (the coordinator).....	6

1. Introduction

Single Sign-On (SSO) is a central security concept that allows users to authenticate once and gain access to multiple applications within a system landscape without repeated logins. This approach follows the principle of "one account – one session – many applications" and improves both usability and security by centralizing authentication and session handling.

To implement this concept, a centralized Identity and Access Management (IAM) solution based on Keycloak was deployed. Keycloak is a free and open-source Identity Provider that supports industry-standard authentication and authorization protocols. It manages user identities, credentials, sessions, roles, and group memberships and acts as the authoritative source for authentication within the EVH Portal ecosystem.

In addition to the Identity Provider, the following applications were integrated:

1. The RPS Admin Interface, which enables portal managers to review user registrations and take administrative actions such as approval or rejection of access requests.
2. The RPS Groups Interface, which supports structured assignment of users to groups in order to enable fine-grained, group-based access to protected resources.

Together, these components form the foundation for centralized authentication, controlled user onboarding, and group-based authorization within the EVH Portal.

2. Identity and Access Management Infrastructure Implementation

A centralized IAM infrastructure was deployed, configured, and put into operation. The application stack was self-hosted on infrastructure operated within the European Union, ensuring data sovereignty and alignment with EU data protection requirements.

The system was configured to serve as the single point of truth for user identities and group memberships. A one-way synchronization mechanism was established to propagate users and groups from Keycloak to the applications used by EVH Portal users. These include the data cloud, the chat service, the groups management application, and the administrative interface.

Through this integration, all connected applications rely on a consistent and centrally managed identity and authorization model, while authentication and session management remain fully centralized.

3. Achieved Two-Step Registration and Approval Process

A two-step user registration and approval process was implemented to ensure controlled access to the EVH Portal and to protect sensitive resources.

The first layer of security consists of user self-registration combined with an automated email verification process. This ensures that only users with valid and reachable email addresses can proceed with registration.

The second layer consists of a manual review of registration requests by the portal managers team using the RPS Admin Interface. Portal managers are able to assess applications and explicitly approve or deny access based on defined criteria.

This combination of automated verification and manual oversight significantly reduces the risk of unauthorized access and ensures that only approved users become active EVH Portal users.

4. Achieved Group Structure and Access Model

A structured group hierarchy was designed and implemented to reflect the organizational structure of the EVH.

The primary grouping follows the division of EVH into major pillars, which are represented technically as top-level groups. Each pillar consists of several work packages, which are represented as subgroups. This hierarchical model enables clear assignment of users and fine-grained control of access rights at different organizational levels.

In addition to the pillar-based structure, further groups were created to support access to shared or cross-cutting resources. These groups allow users who are not directly assigned to a specific pillar or work package to access relevant services where required.

This group-based access model enables role- and group-based access control, supports multi-level protection of resources, and follows the principle of least privilege.

5. Outcome

The delivered solution provides EVH with a centralized, self-hosted, and EU-compliant foundation for Single Sign-On, identity management, group-based authorization, and controlled user onboarding. The implemented tooling supports secure access to multiple portal applications, improves usability for EVH Portal users, and establishes a strong basis for future extensions of the EVH Portal ecosystem.

Document review / approval (the coordinator)

Name	Role	Action (review / approval)	Date
Rino Rappuoli	Coordinator	Approval	27/02/26
Donata Medaglini	Scientific Coordinator	Approval	27/02/26