Sphere

Annex 1

Key requirements for the central User Management System

Table of contents

1. Introduction

Sphere has transformed from a project into a globally acting organisation with a network of over 100,000 practitioners and focal points in 38 countries.

It is envisaged that users and followers who actively interact with Sphere should have one unique digital identity across all platforms provided by Sphere. For that reason, Sphere plans establishing a central identity management solution, the so-called User Management System (UMS).

This document aims at describing the main requirements for the new UMS.

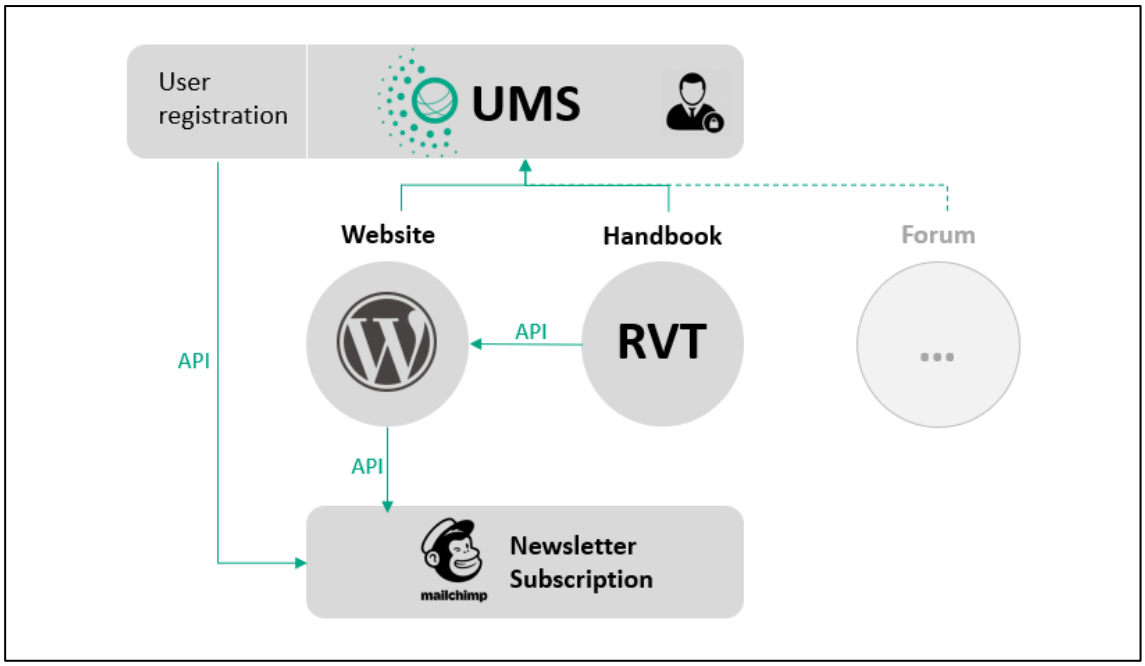
2. System context

Sphere is already operating digital platforms as the Interactive Handbook, the Sphere website and a cloud-based newsletter solution. More platforms / features are expected to be implemented as part of the digitalisation strategy of Sphere (e.g. an online forum or e-Learning solutions).

For the reason of flexibility and openness towards future integration scenarios, the new UMS will be implemented as a stand-alone solution (in contrast to be a part or module of another solution).

The integrations between the UMS and other digital solutions should be possible based on standardised application programming interfaces (API).

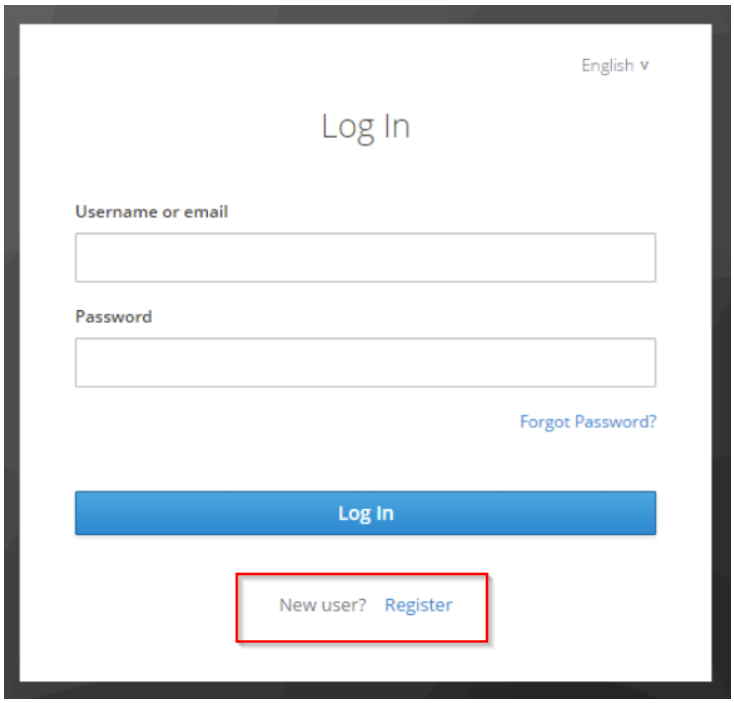
The following figure outlines the envisaged system integration at a glance.



3. Functional Requirements

3.1 Self-registration

The UMS should provide features to support the self-directed user registration process. The login screen will be the central landing page for all authentication requests coming from integrated digital solutions. The screen should therefore allow for easily accessing the registration service.



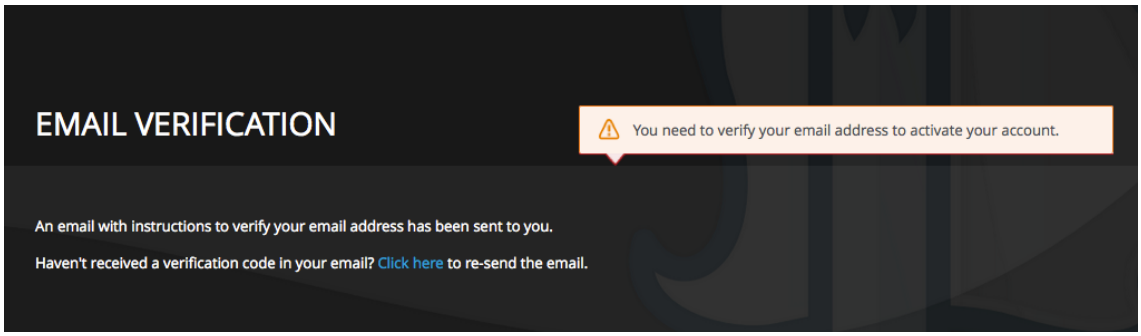
During the registration process a minimum set of data should be requested from the user in order to create a new user account.

Field	Option
First Name	
Surname	
Email	
Password	
Roles	Multiple Choice
Monthly Newsletter	Yes / No
Special campaigns	Yes / No
Language preferences	

When creating a user account, newsletter preferences can be set. An API connection to Mailchimp needs to be configured to forward newsletter preferences.

3.2 Email verification

The email address used by users to create a new account in the UMS should be verified before activating the account. This will be achieved by sending an email including a verification link or code to the given email address. As long as the verification link or code is not activated, any login attempt will prompt a warning message to the user.

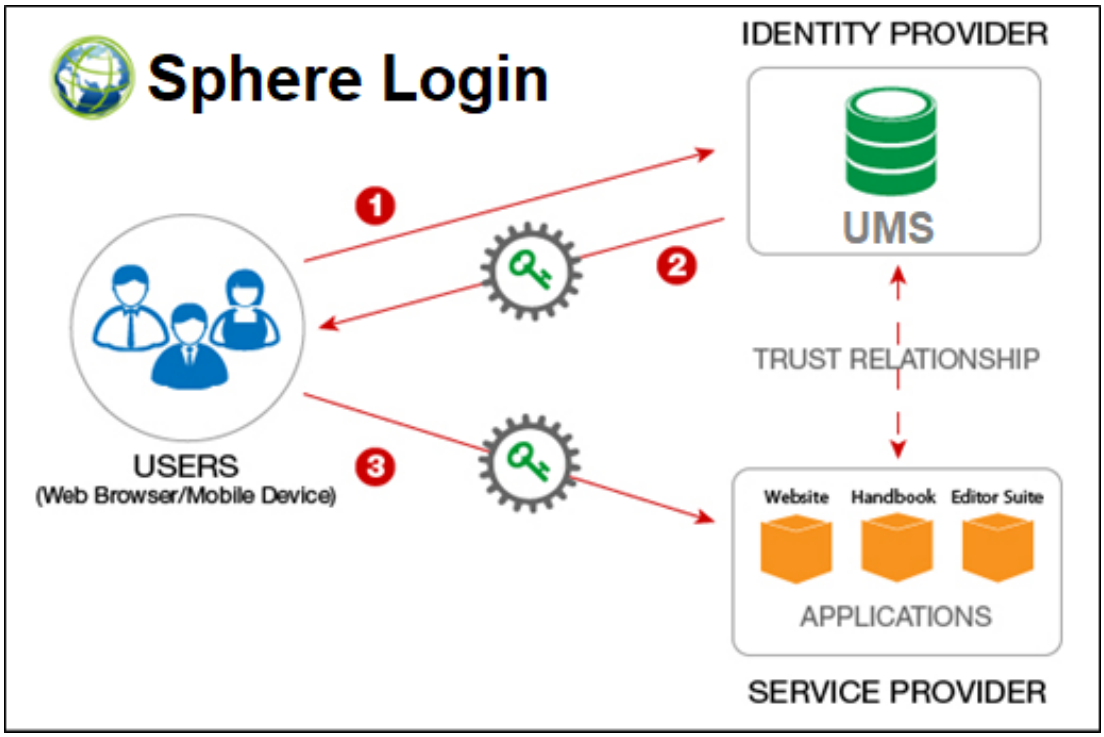


3.3 Central login

All integrated digital solutions will allow for accessing the centralised login screen of the UMS for authenticating and authorising the users. Logged in users will get access to more features and information based on their roles.

The new UMS should be capable of redirecting the users to the requesting platform after a successful login. The redirect will provide additional information to the requesting platform for authorisation purposes.

The following figure outlines the login processes at a glance.



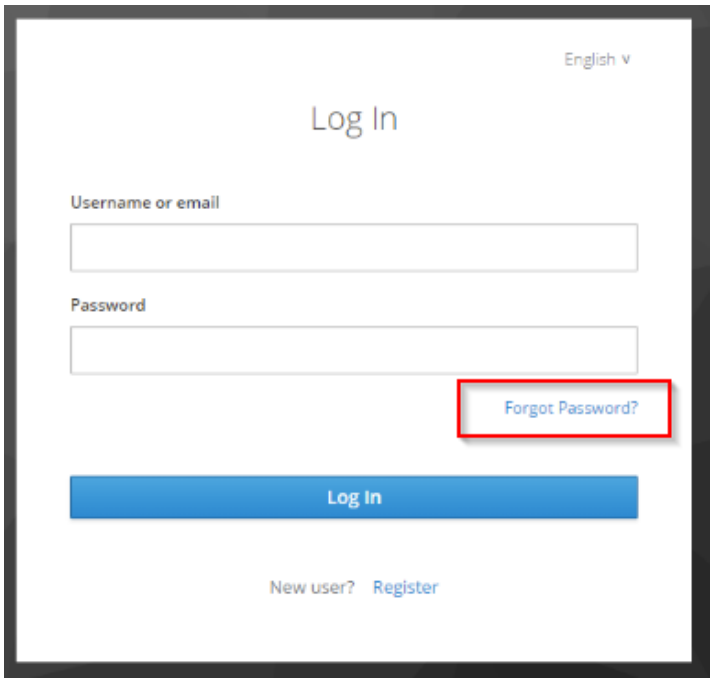
When logging in to the Sphere website, Interactive Handbook or other integrated digital solutions, the user will be forwarded to the UMS acting as the identity provider (1). The UMS checks the user credentials and provides a security token to be used with each authentication

request (2). The user will be redirected to the target platform (Sphere Website, Interactive Handbook or other) providing the security token through the HTTP-request (3).

This concept allows for a centralised user **authentication** (user is known) within the UMS. **Authorisation** (user permissions are applied) will be handled in the target platforms. User permissions will be passed to the platforms within the security token (3).

3.4 Password reset

Users who forget their password or want to react to a potential security breaches by changing their password should have the option to reset the password from the login screen. By activating this function, an email will be sent to the stored email-address with further instructions.



3.5 User profile

The new UMS should provide access to user account details for authenticated users. This user profile should be available through a link from the integrated digital solution. The user profile screen should enable authenticated users to edit their personal details but also to reset the password.

3.6 Single Sign On

The proposed UMS should allow for enabling Single Sign On (SSO) as comfort feature. This feature will omit prompting a login screen to the user when switching between integrated digital solutions. The user needs to provide the security credentials only once and the UMS will handle authentication requests from all integrated digital solutions automatically.

The proposed SSO solution should work for active browser sessions but may also be extended to use other browser features (e.g. cookies).

3.7 User administration

The new UMS should provide possibilities to add, manage and delete users when using an administrative account.

Even if an administrator adds a new user account, this account still needs to be verified by a link or code sent through email to the given email address. Additionally, users created by administrators should be forced to set a new password or change the initial password during the verification process.

3.8 Managing permissions

The proposed UMS solution should provide an interface to create and manage permissions which will be used by the integrated digital solutions for authorisation purposes. The granularity of permissions will highly depend on the integrated digital solution using them for granting access to functions and features.

To keep the implementation and configuration of the permission scheme flexible, a lightweight taxonomy or naming conventions should be possible, e.g.:

- Website
    - Calendar
        - View (website_calendar_view)
        - Add event (website_calendar_add)
        - Delete event (website_calendar_delete)
    - Restricted Area
        - View (website_restricted_view)
- Interactive Handbook
    - Comments
        - View (handbook.comment_view)
        - Add comment (handbook_comment_add)

The permissions to be used will be agreed between Sphere and the service providers of the integrated digital solutions.

3.9 Managing roles

Expecting a growing number of permissions, the new UMS should allow for grouping them into defined user roles in the system. User roles should be assigned to users in the UMS. The defined roles are basically a list or set of permissions. This concept simplifies the management of users and the respective permissions in the UMS.

The initial set of roles with respective permissions for the current platforms is outlined in the following figure (but will be refined during the implementation process of the UMS).

	Website					Interactive Handbook
	Access to restricted areas	Download Resources	Upload Resources	Calendar - view	Calendar - add event	Comments - add
Admin	✅	✅	✅	✅	✅	✅
Guest	❌	✅ (PopUp to sign-up for NL)	❌	✅	❌	❌
User	Page "Apply to be Trainer"	✅	✅	✅	✅ (Approval needed by Editor/Admin)	✅
Editor	Page "Apply to be Trainer" Edit post / articles	✅	✅	✅	✅ Approve other events	✅
Trainer	Edit own profile	✅	✅	✅	✅ (Approval needed by Editor/Admin)	✅
Member	Page "Member area"	✅	✅	✅	✅ (Approval needed by Editor/Admin)	✅
Board Member	Page "Board Member area"	✅	✅	✅	✅ (Approval needed by Editor/Admin)	✅

4. Non-functional requirements

4.1 System infrastructure

Sphere does not own a data centre or comparable system infrastructures. Therefore, bidders should outline the minimum requirements for operating the proposed UMS on servers. Low total costs of ownership should be considered in that regard.

4.2 Open standards, open source

Following the Principles for Digital Development (https://digitalprinciples.org/) endorsed by a growing community of organisations, the usage of open source solutions and open standards is highly desirable.

Main open standards to be considered for UMS are:

- OAuth2.0 (https://oauth.net/2/)
- OpenID Connect (https://openid.net/connect/)
- JSON Web Token (https://jwt.io/introduction/)

4.3 Maintainability, Operability and Configurability

The internal resources of Sphere to maintain and troubleshoot the new UMS in the future are limited. Therefore, maintenance procedures, system configurations, and system monitoring should be outlined in the proposal with an indication on capacity requirements.

4.4 Scalability and Performance

The bidder must propose architectural and technical solutions for scalability in order to ensure that the system remains performant and is not affected by the increased number of users and/or implementation of additional features.

4.5 Security

The bidder must elaborate their security model regarding security threats and mechanisms of user authentication to prevent unauthorised access to the UMS and associated components.

4.6 Localisation

User interfaces of the UMS have to be able to support/implement multiple language – including RTL.

4.7 Data Backup and Disaster Recovery

The bidder must describe data backup and disaster recovery procedures for the UMS.

4.8 Browser compatibility

The web-based user interfaces of the UMS shall be at minimum compatible with the following

web browsers: IE 11+, Edge 15+, Google Chrome 60+, Firefox Mozilla 56+, Safari 11+.