INTEGRATING INSPIRE WITH CITIZEN SCIENCE AND EO AUTHENTICATION SYSTEMS

Dubrovnik INSPIRE Hackathon 2020 – Challenge Final Report

March 30 – June 11

Mentors/Team leaders

Andreas Matheus, Secure Dimensions GmbH

Valantis Tsiakos, Institute of Communication and Computer Systems

Overview & process

The scope of the challenge is to enhance geospatial and/or INSPIRE enabled web-based or mobile application so as to connect to either Citizen Science and/or Earth Observation data. More specifically, the challenge focused on improving accessibility to protected citizen-science resources while also enabling their direct consumption and utilisation by third party applications.

In this context, infrastructure implemented by the H2020 Citizen Observatories (GROW, GroundTruth2.0, LandSense, SCENT) was utilised. In particular, the Identity Access Management system of H2020 SCENT Harmonisation platform (http://scent-harm.iccs.gr/) was utilised as a reference implementation in the context of this activity. The SCENT Identity Access Management has been implemented so as to secure the SCENT Harmonisation Platform resources from unauthorized access. Thereafter, the security mechanism has been implemented with a Keycloak[1] instance which holds the database of the Harmonisation Platform users and groups. It should be noted that the Identity Access Management system offers user interfaces for changing its configuration, for creating new users, for creating new roles and for login/logout purposes. Also, relevant interfaces exist for defining certain user management policies and role-mappings.

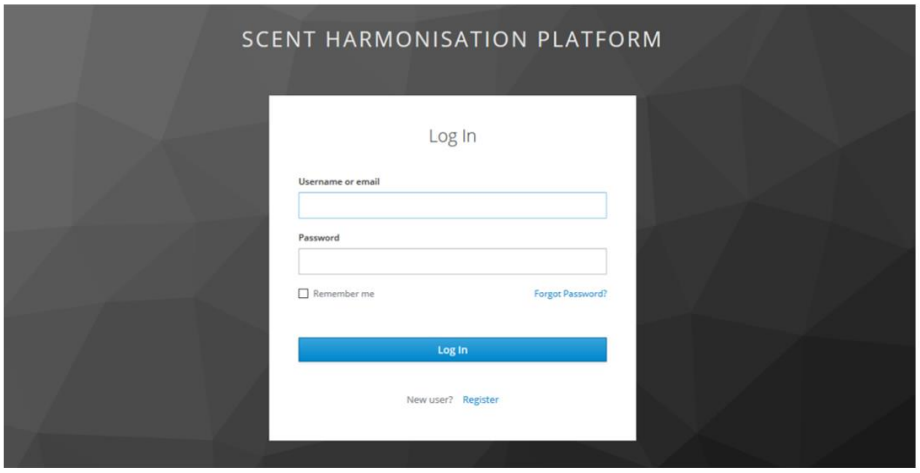

FIGURE 1: SCREENSHOT FOR AUTHENTICATING THE USER (LOGIN) TO THE SCENT HARMONISATION PLATFORM

In the context of this activity, front-end JavaScript applications were able to connect with the SCENT Harmonisation platform Identity Access Management system by applying Implicit Grant Type[2] of authorisation. This happens because client-side applications cannot guarantee the client secret confidentiality (which is essential for the other OAuth2 flows). Following the user log in, the access token is issued immediately allowing users to access and use protected resources and operations. In addition to the access token, an ID token is also issued from the Authorization Server. The ID token takes the form of a JSON Web Token (JWT) which is a JSON payload that is signed with the private key of the issuer (SCENT Identity Access Management) and can be parsed by the third-party application. Inside the JWT (ID token), there are a handful of defined property names that provide information to the third-party application. This information includes a unique identifier for the user, the identifier for the server that issued the token, the identifier for the client that requested the token, etc.

[1] https://www.keycloak.org/

[2] https://oauth.net/2/grant-types/implicit/

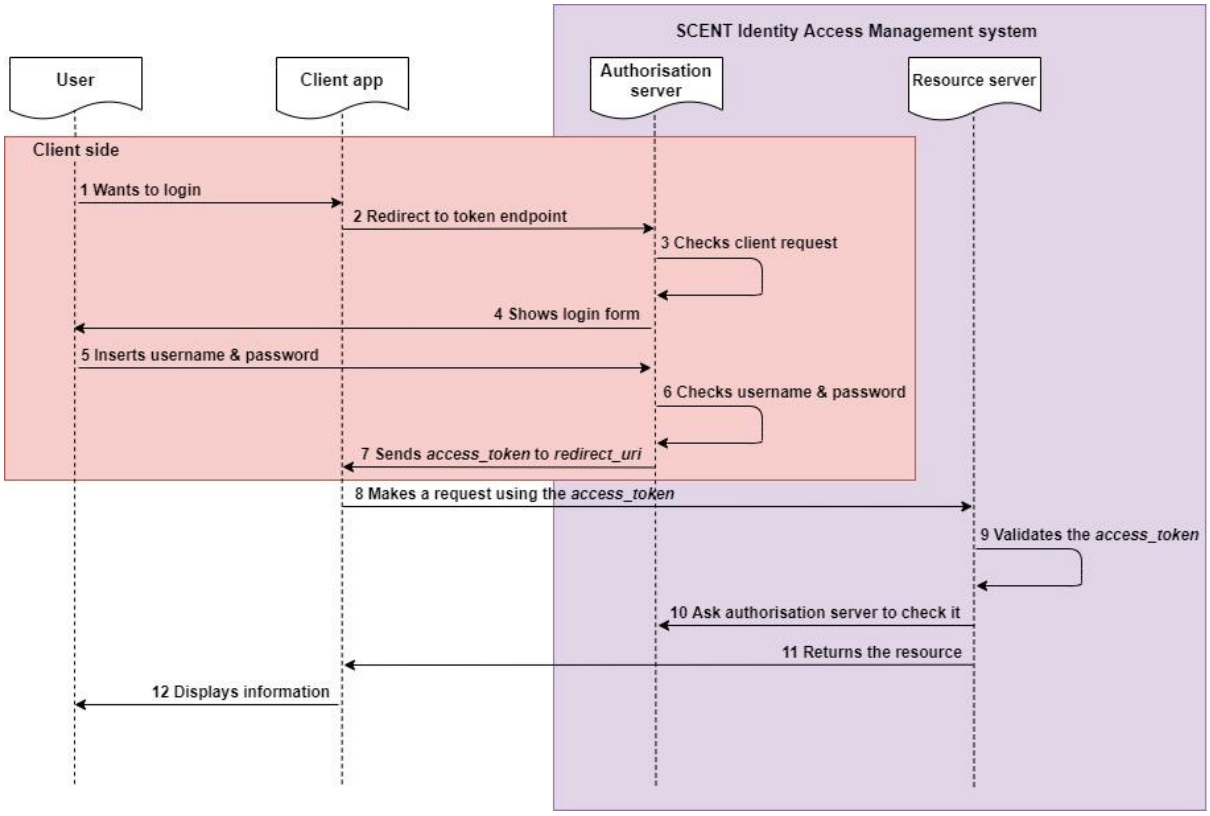

FIGURE 2: WORKFLOW THAT HAS TO BE FOLLOWED IN ORDER FOR A USER TO AUTHENTICATE AND ACCESS A PROTECTED SCENT RESOURCE

Results

The implemented scenario involves the following steps:

- Registration of the app to the SCENT Identity Access Management system. During this process, the following parameters are defined:
  - client_id: A publicly exposed string that is used by the service API to identify the application;
  - redirect_uri: The location where the service will redirect the user after they authorise (or deny) the application and therefore the part of the application that will handle access and ID tokens;
  - scope: It specifies the level of access that the application is requesting;
  - response_type: In this flow, the value is "id_token," which means that a successful response must include both an access token and an ID token.
- Then there is an interaction of the user with the web-browser (i.e., choosing to log in) upon which the client generates and sends a login request to the authorization server (i.e., SCENT authorization server, in our case). The request is sent in the form of a HTTP request and the information is sent as URL query parameters. The following parameters are specified during the request: client_id, redirect_uri, scope, and response_type
- In what follows, the authorisation server checks the request, and if it is valid, it presents to the user the login form.
- The user inserts his/her credential and following the conclusion of this process, the access and ID tokens are verified. In particular the SCENT Identity Access Management system i) checks that JWT is well formed, ii) checks the signature, iii) validates the standard claims, iv) checks the application permissions (scopes)

- In case of successful verification, the protected resource is offered to the third-party client application.

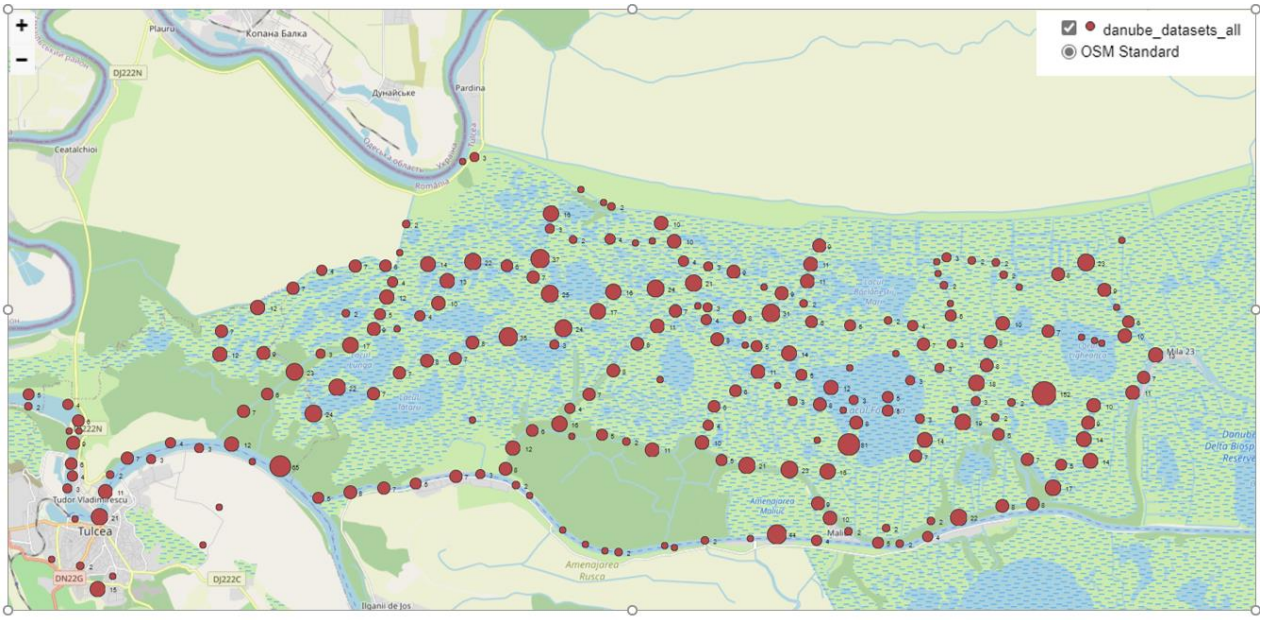

FIGURE 3: EXAMPLE OF A WEB MAPPING APPLICATION ACCESSING PROTECTED RESOURCES (LAND COVER / LAND USE DATA) FROM SCENT CITIZEN OBSERVATORY IN THE AREA OF DANUBE DELTA, ROMANIA

Impact

Cross sectoral and boundary interoperability

The number of citizen-science project, activities and initiatives that take place in European and global scale are constantly increasing, leading to the implementation of various systems and architectures that facilitate the whole data management cycle of the produced resources. This landscape often leads to the creation of various isolated repositories that host the produced citizen-science resources and may also consist restrictions in data access. The latter can be a limiting factor to the re-use of such protected resources in a n efficient and automated way by other projects and third-party applications. Thus, this challenge aims to address this barrier by demonstrating a methodology that allows a single authentication process (managed by a single Identity Provider, or other authentication mechanism) to be used across multiple systems within a single organization or across multiple organizations (i.e., common login credentials across systems). Infrastructure that has been developed in the context of H2020 Citizen Observatories such as LandSense and SCENT as well as other external web applications are utilised in order to showcase how protected resources can be exploited when having different systems across multiple organizations (projects) trusting/connecting to a single third-party Identity Provider.

It should be noted that the approach is based on OAuth 2.0, an open industry-standard protocol for authorization, that can ensure interoperability and scalability between various related applications and scenarios.

Contacts

In case you want to integrate your application and to access resources and services being offered by the H2020 Citizen Observatories (GROW, GroundTruth2.0, LandSense, SCENT) following the principles employed in this challenge, feel free to contact: info@weobserve.eu

- END OF DOCUMENT -

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 776740.