MyAcademicID Service Registration for EuroTeq University Alliance

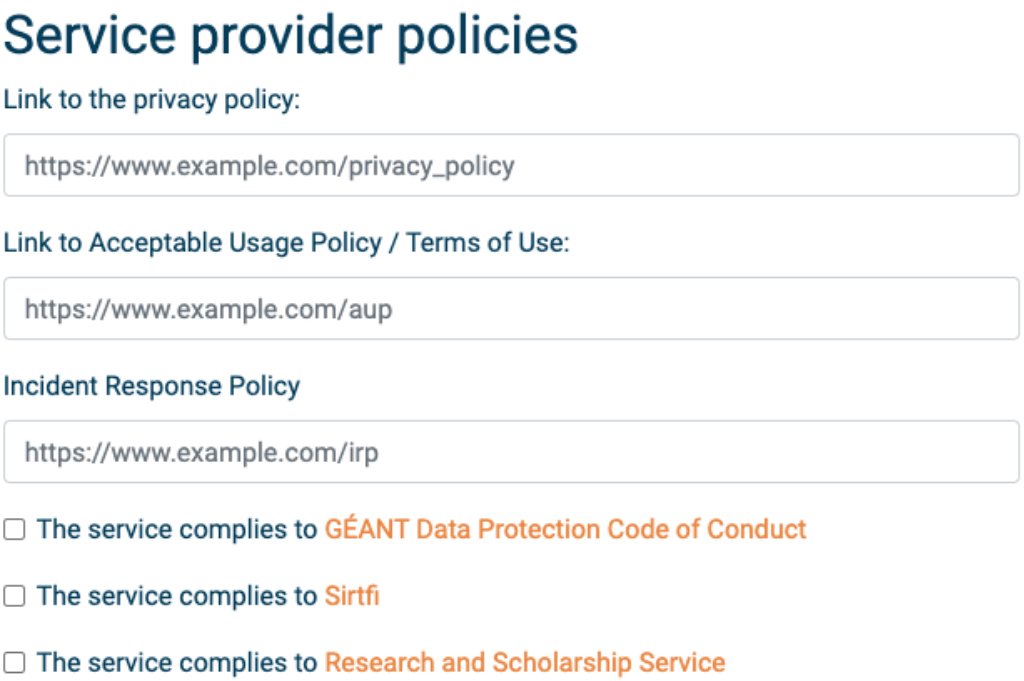
This document is to describe the process for Higher Educational Institutions (HEIs) that are part of the EuroTeQ University Alliance about how they can register on MyAcademicID.

- Each HEI needs to Submit **2** Service registration on: https://webapp.prod.erasmus.eduteams.org/sp_request?
  - **Relying Party** (RP)
  - **Resource Server** (RS)
- Both registration NEEDS:
  - Contact Information: The email has to be a team email NOT personal.

  - Service provider policies MUST:
    - **Link to the privacy policy:** Each organisation, which is an individual Data Controller must have its own policy. If the question is whether all HEIs that are part of EuroTeq can agree to use the same text for all

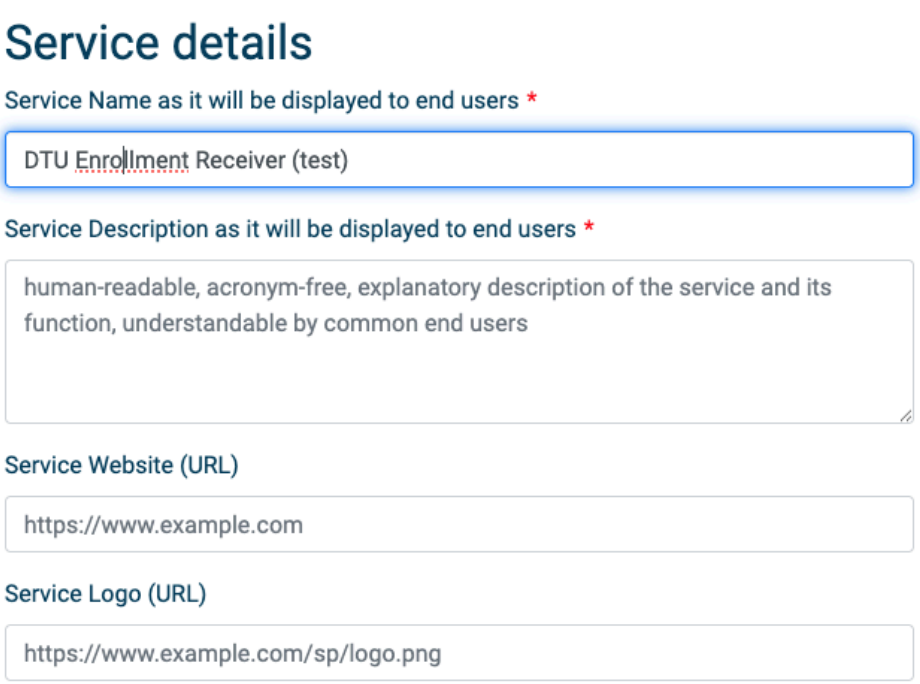
organisation, that is up to EuroTeq, as long as each Data Controller has its own version.

- **Link to Acceptable Usage Policy / Terms of Use**
- **Comply** GEANT Data Protection Code of Conduct
- **Comply** Sirtfi
- **Comply** Research and Scholarship Service



- Relying Party
  - Service details:
    - **Service Name** as it will be displayed to end users: [HEI name] Enrollment Receiver (TEST/PRODUCTION) (e.g. DTU Enrollment

Receiver (TEST))



- Technical Information:
  - **SAML2 or OIDC:**
    - OIDC
  - **Supported grants:**
    - Authorization Code Flow
    - Refresh Token

Technical information

SAML2 or OIDC: *

OIDC

Supported grants: *

Authorization Code Flow
Refresh Token
Token Exchange
Device Code Flow
Client Credentials

You can select multiple grants by holding the Ctrl (or Cmd) key and clicking on the needed grants.

For more information on "Authorization Code Flow" and "Refresh Token" read the OpenID Connect Core 1.0 document.

For more information on "Token Exchange" read the RFC8693 — OAuth 2.0 Token Exchange document.

☐ Client is public

A "public" client is usually a Web/Javascript-based application. Because the code of public clients is exposed, they are incapable of maintaining the confidentiality of their credentials. For more information read the RFC6749 — The OAuth 2.0 Authorization Framework document, especially section 2.1. Client Types on the differences between "confidential" and "public" clients.

It is strongly recommended to require PKCE when the client is public.

☐ Require PKCE (Proof Key for Code Exchange)

PKCE stands for "Proof Key for Code Exchange". For more information read the RFC7636 — Proof Key for Code Exchange by OAuth Public Clients document.

Using PKCE is recommended for all grants based on the Authorization Code Flow. For more information read the OAuth 2.0 Security Best Current Practice document, especially section "2.1.1. Authorization Code Grant".

- **Redirect URL:**

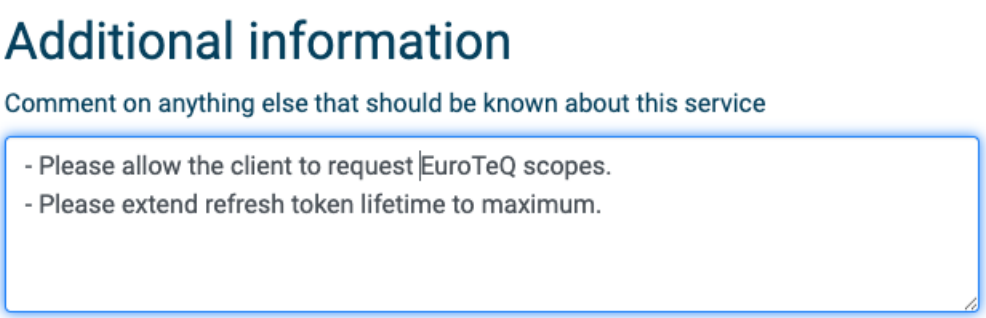
Redirect URLs: *

Note, wildcards and URL fragments are not supported. Links like `https://www.example.com/*` or `https://www.example.com#fragment` are considered invalid.

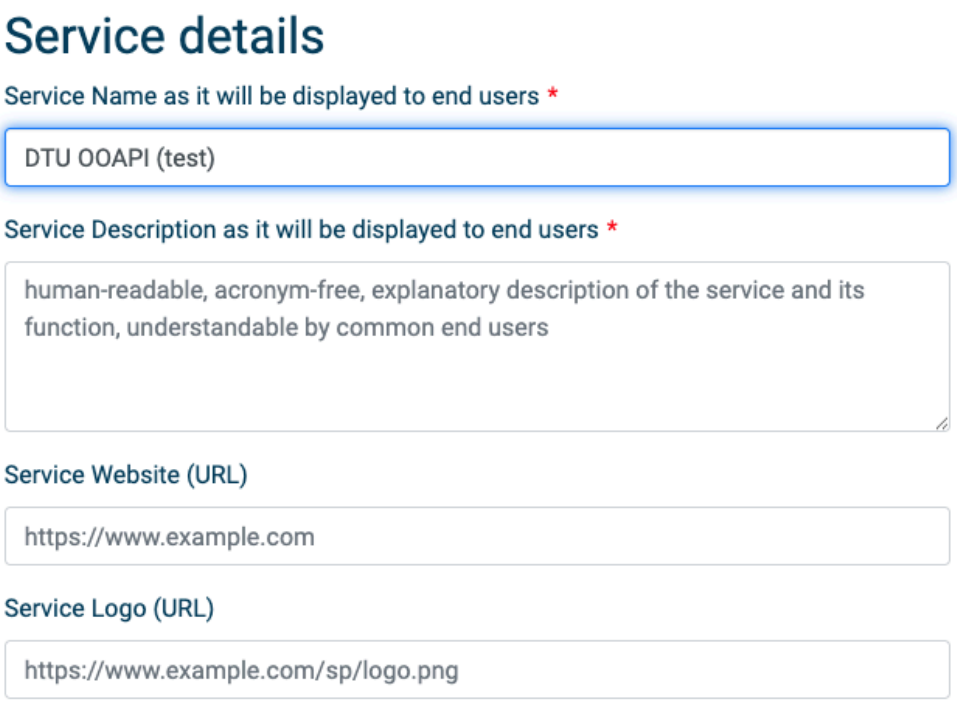
https://www.example.com/redirect

- Additional information:
  - Please allow the client to request [EuroTeQ University Alliance] scopes

- Please extend the refresh token lifetime to maximum.



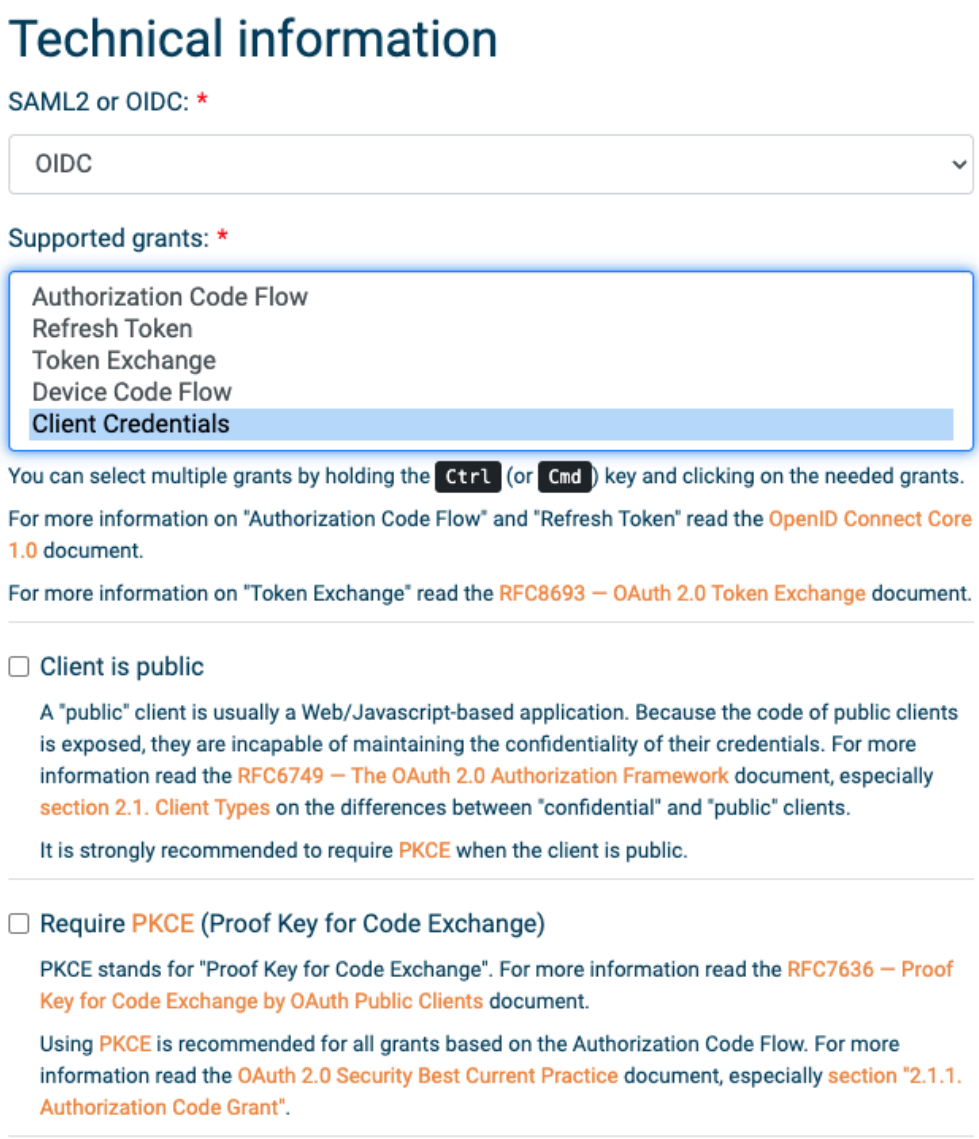
- Resource Server
  - Service details:
    - Service Name as it will be displayed to end users: [HEI name] OOAPI (TEST/PRODUCTION) (e.g. DTU OOAPI (TEST))



  - Technical Information:
    - **SAML2 or OIDC:**

- OIDC

- **Supported grants:**
  - Client Credentials



- Additional information:
  - This is a Resource Server, no need for any grant types supported.
  - Please register additional scopes for [EuroTeQ University Alliance] :
    - institution_primary_domain/persons (e.g. dtu.dk/persons)
    - institution_primary_domain/results (e.g. dtu.dk/results)

Additional information

Comment on anything else that should be known about this service

- This is a Resource Server, no need for any grant types supported.
- Please register additional scopes for EuroTeq:
- dtu.dk/persons
- dtu.dk/results