The Goal - Replicating Doubtfire

OnTrack (Which is Deakin's interpretation of Doubtfire) allows for different authentication/authorisation methods based on four particular methods (protocols).

Key	Description	Default
`DF_AUTH_METHOD`	The authentication method you would like Doubtfire to use. Possible values are `database` for standard authentication with the database, `ldap` for LDAP, `aaf` for AAF Rapid Connect, or `SAML2` for SAML2.0 auth.	`database`

Figure 1.) Doubtfire API README.md

Although figure 1 highlights three protocols, a fourth is also used in a testing environment which is called `auth_db` signifying that the server will use a local database for authentication through basic authentication. The three other terms can be defined as:

LDAP - authentication against an Active Directory such as Azure AD
SAML - authentication based using a markup language to an online identity management system, mainly used for Single Sign On (SSO)
AAF - Australian Access Federation, used for securing Australian Universities authentication with different application's.

OnTrack uses the auth_aaf approach since it is a University. Thus, the goal with Dream Big is to add aaf authentication which is utilising the SAML protocol.

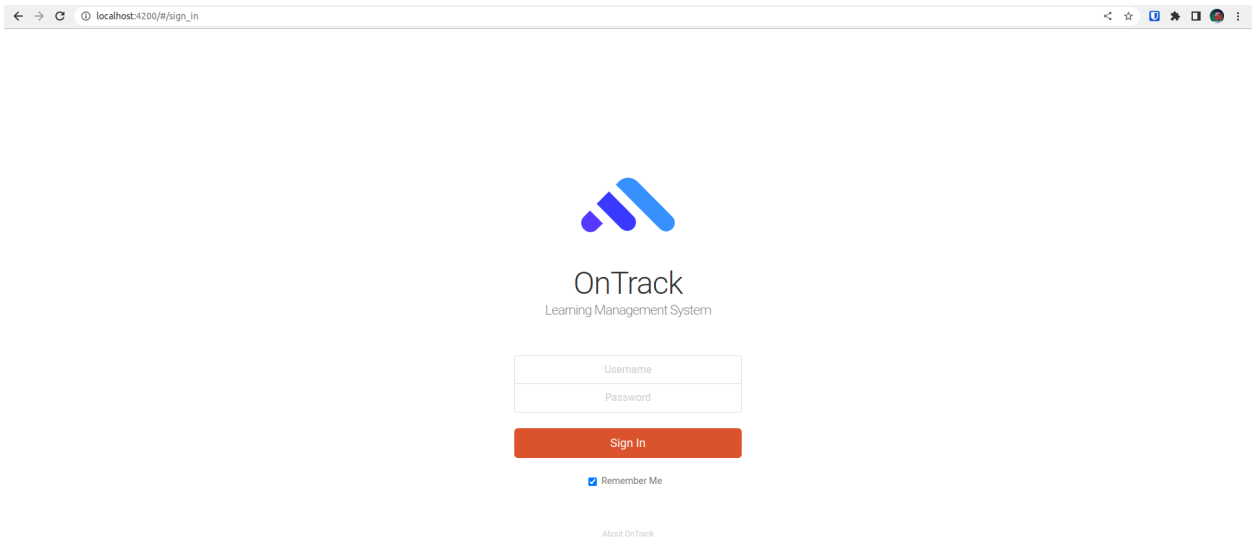

Figure 2.) OnTrack Login using auth_db

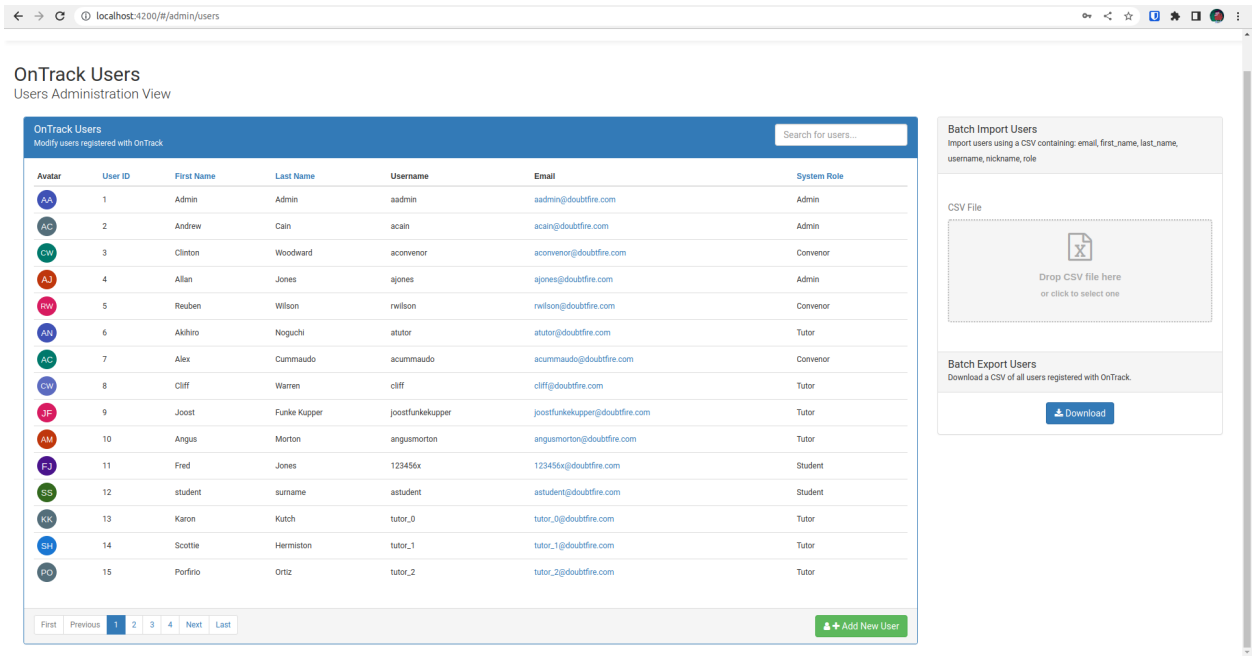

Figure 3.) OnTrack Creating a User as a Unit Convenor

The Design - Replicating Doubtfire

High Level Overview of Single Sign On with SAML and AAF:

- GET /auth/method type where `auth_aaf` is returned for Deakin SSO.
- Rapid Connect (AAF) deals with the log in and returning a secure JWT token.
- POST /auth to log in.

Below highlights the Deakin SSO process following Google Chrome's networking tab.

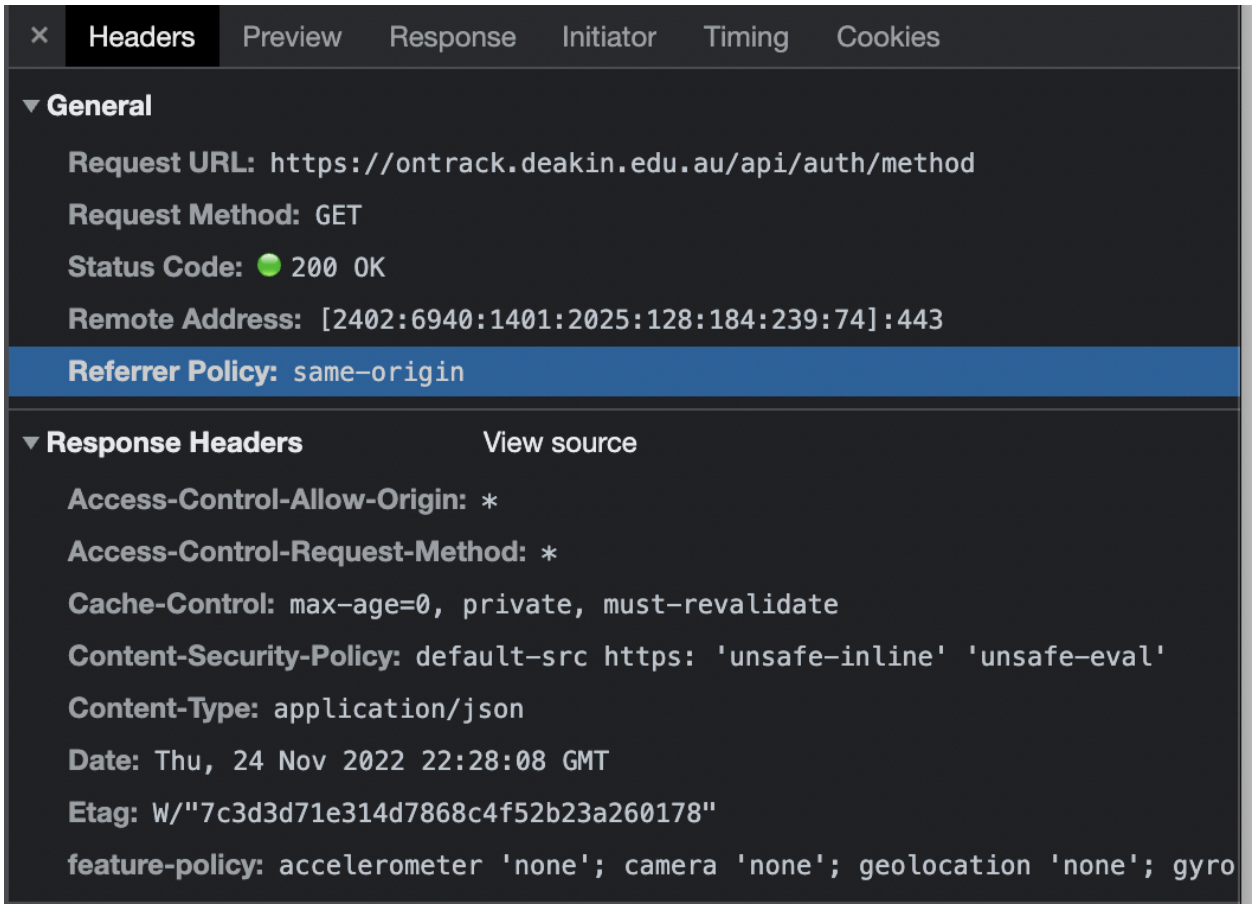

Figure 4.) GET /auth/method request

Figure 5.) GET /auth/method response

Note >> the response from figure 5, we want to replicate this endpoint in Dream Big while also accommodating for the existing implementation with the authentication automatically using auth_db. Otherwise, the existing implementation will break. This is a major concern given we cannot test SSO locally without hosting it on a web server. Thus, it is recommended we use Test Driven Development here.

The redirect_to property is used where *shibboleth* is associated with AAF rapid api. Thus, we are navigated to that redirect url.

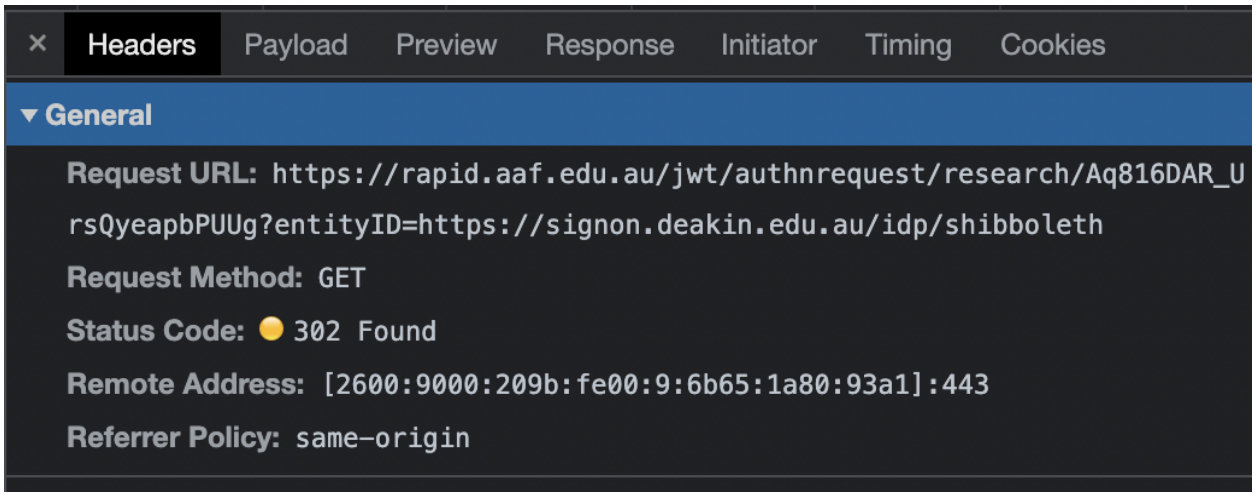

Figure 6.) Redirect to url based in auth/method response

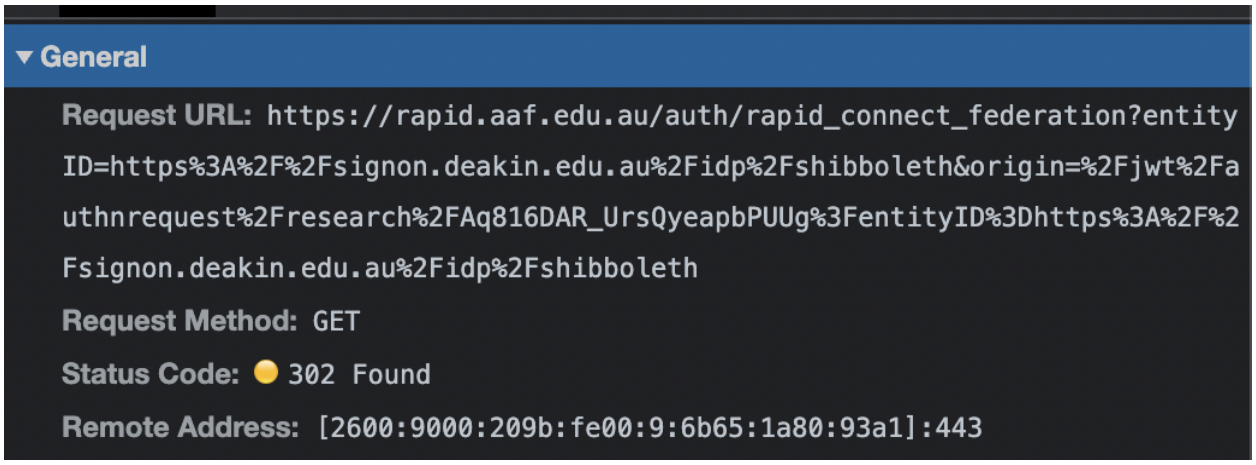

Figure 7.) Retry GET request with URL encoding

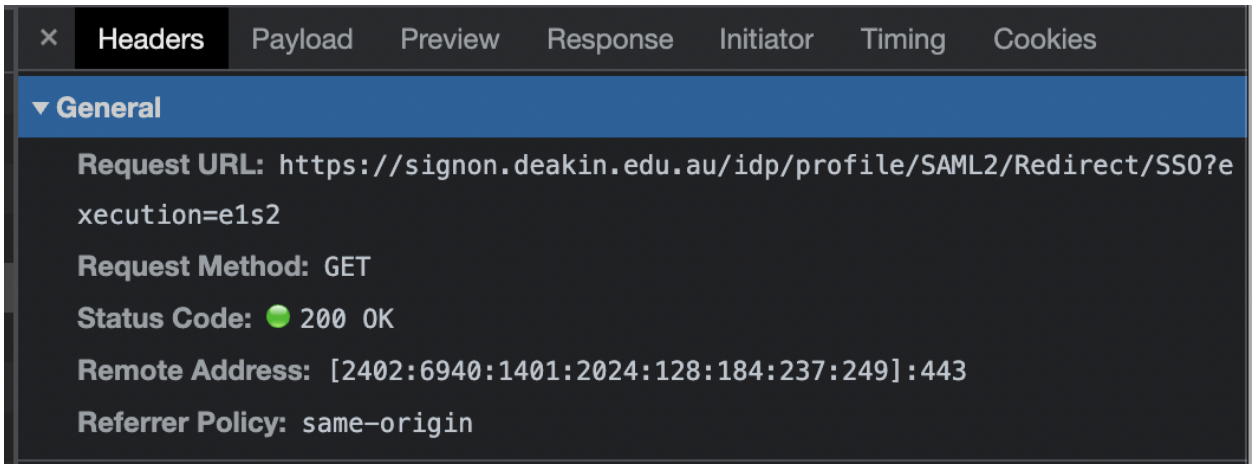

Figure 8.) Redirected to Sign On Deakin

After the login to Deakin's SSO succeeds, we are given an auth_token from AAF.

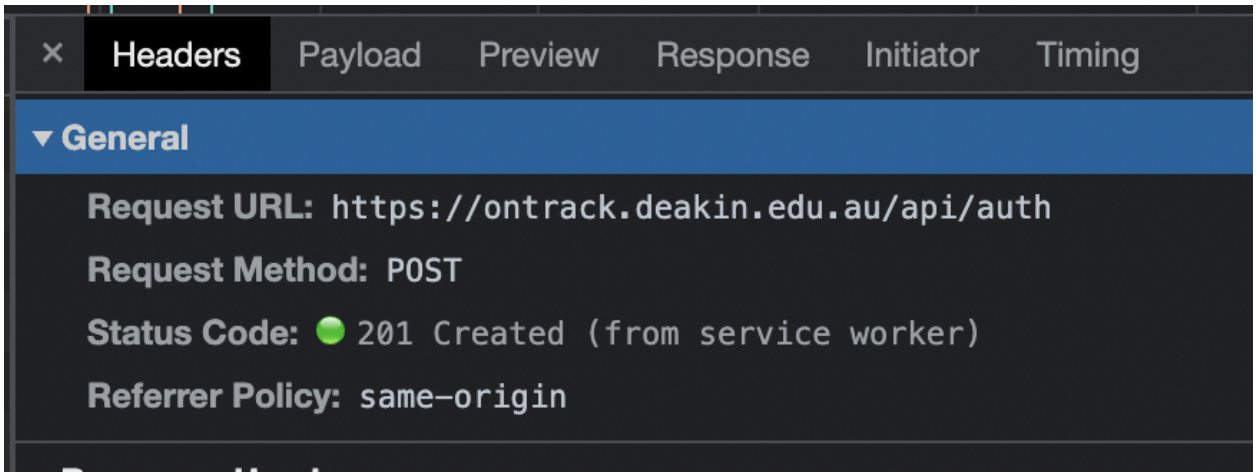

Figure 9.) POST /auth request

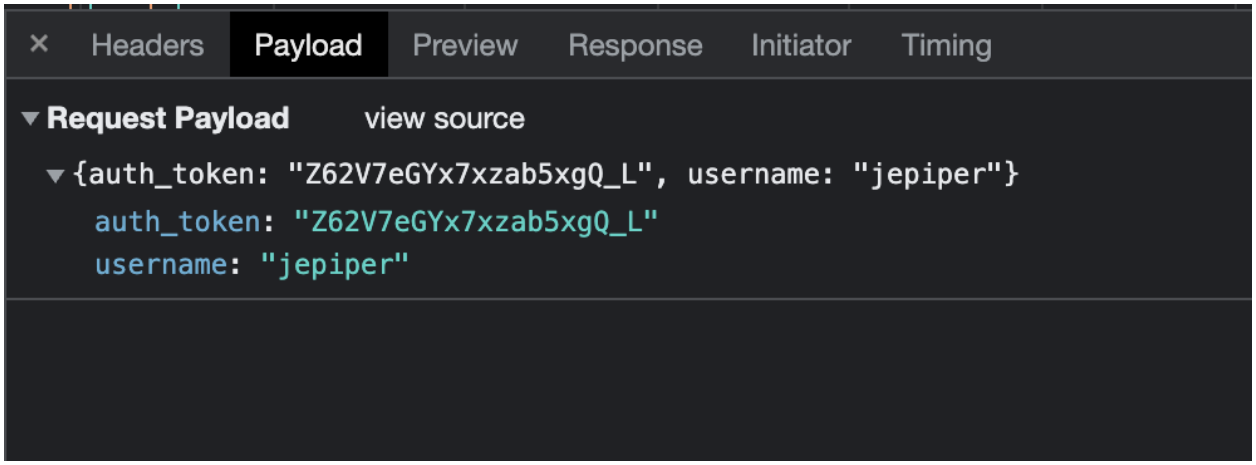

Figure 9.) POST /auth request payload

After completing figure 9 we are logged into OnTrack using Deakin's SSO.

Dream Big's Approach

We want to support SAML, AAF and database connections. Do NOT consider using LDAP or other protocols for this scope.

Using Rapid Authentication via AAF we will utilise a test environment where the AAF test environment uses localhost as our (AAF) callback and test registry. The private key value we put in the test environment is a generated encryption value that we will use for secure connections.

See the authentication helpers from Doubtfire to see how to deal with the auth tokens, and retrieving user information before reaching the authentication/login APIs. The User model is also relevant for how Doubtfire deals with the JWS token from Rapid Connect.

Provides an introduction to Rapid Connect

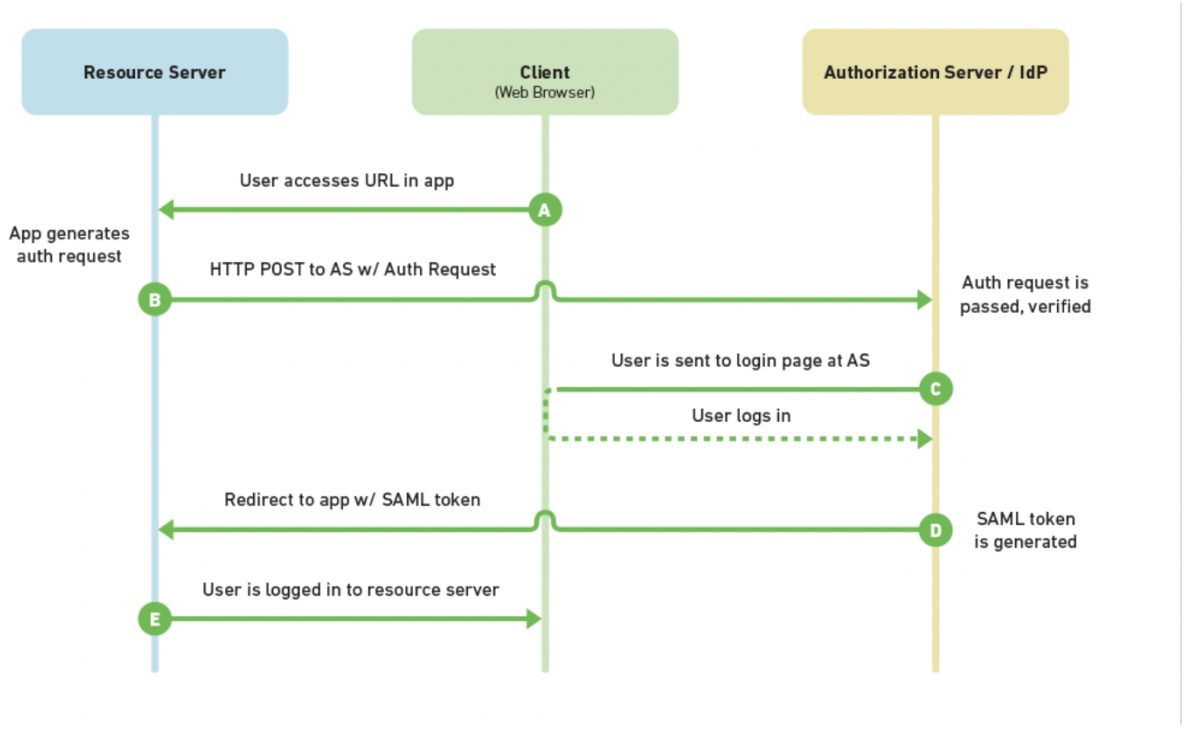

Figure 10. Introduction to Rapid Connect (AAF)

Provided claims

The following claims are provided by AAF Rapid Connect:

- **iss**: Identifies the principal that issued the JWT. For AAF Rapid Connect this is always https://rapid.aaf.edu.au in the production environment, and https://rapid.test.aaf.edu.au in the test environment.
- **iat**: Identifies the time at which the JWT was issued.
- **jti**: Provides a unique identifier for the JWT that can be used to prevent the JWT from being replayed.
- **nbf**: Identifies the time before which the JWT MUST NOT be accepted for processing
- **exp**: Identifies the expiration time on or after which the JWT MUST NOT be accepted for processing
- **typ**: Declare a type for the contents of this JWT Claims Set in an application-specific manner in contexts where this is useful to the application
- **aud**: Identifies the audiences that the JWT is intended for. Each principal intended to process the JWT MUST identify itself with a value in audience claim. For Rapid Connect this is the value of your application's primary URL (provided as part of service registration)

Figure 11. JWS token values we can use

Trello Board

https://trello.com/b/8wHFSQO7/dream-big-deakin-sso

Handover

Talk to Andrew Cain about gaining testing access for AAF Rapid Connect. The current integration of POST /auth/jwt is incomplete since it needs the frontend and quality assurance teams synchronised. Therefore, inform the relevant teams of the tasks they need to complete such as accommodating the newly created GET /auth/method endpoint which will dictate whether the frontend will redirect a user to SSO or let them login via username and password.

The POST /auth/jwt API highlights the next stages by the `TODO` prefix within the code. This includes providing a more verbose token service.

Please view the `ToDo - High Priority` list within the T3-2022 backend Trello board to see the next tasks to complete. For example: