OAuth Grant Flow

Well I don't know if you can cal this a "OAuth server" but whatever it's how I've done it so I don't care

This is the client or the user

This can be any one of your applications that require authentication

This is the authentication server that possesses a lot of information regarding the users

Client

Application

OAuth server

Here, if the client_id or the redirect_uri doesn't belong to an authorized application, the server will return a 403 error

This prevents unauthorized applications to access users data: This is the first level of protection

The user accesses a protected route on your application and is not yet logged in

Redirects to auth.whatever.xyz/auth/login? client_id=abc123&redirect_uri=xxx.xxx

GET /auth/login? client_id=abc123&redirect_uri=xxx.xxx

Returns login page

POST /auth/login

Grants authorization code

You'll need to exchange your authorization_code with an authorization_token which is the Bearer token to access every protected route of the api

Here it redirects to the redirect_uri? callback=authorization_code

Exchange the authorization_code for a authorization_token

If the authorization_code is ok, give the token

Either give the tokens directly to the user or store it in a session in the application storage and give a sessionID