Article
Alberto Fuentes · Apr 5, 2022 2m read

Open Exchange

Learn how to use OAuth2 / OpenID Connect in InterSystems IRIS in a simple way

You have read about **OAuth2** / **OpenID Connect** but you don't know how to use it? Have you ever needed to implement Single Sign-On (SSO) or secure web services based on tokens? Did you have to add authentication / authorization to your web applications or services and you didn't know how to start?

What about a step by step example where you can set up an authorization server, a client and a resource server? Here you can find an example where you will configure InterSystems IRIS instances to act as each one of these OAuth2 roles.

A brief introduction

Authentication is the process of verifying that users are who they say they are.
Authorization is the process of giving those users permission to access resources.

OAuth is an authorization framework. OpenID Connect (OIDC) is extension to OAuth 2.0 to handle authentication.

In OAuth2 there are different roles:

- Resource owner — Usually a user.
- Resource server — A server that hosts protected data and/or services.
- Client — An application that requests limited access to a resource server (e.g. a web application).
- Authorization server — A server that is responsible for issuing access tokens, with which the client can access the resource server.

OAuth2 uses scopes as a mechanism to limit access. A client can request one or more scopes.

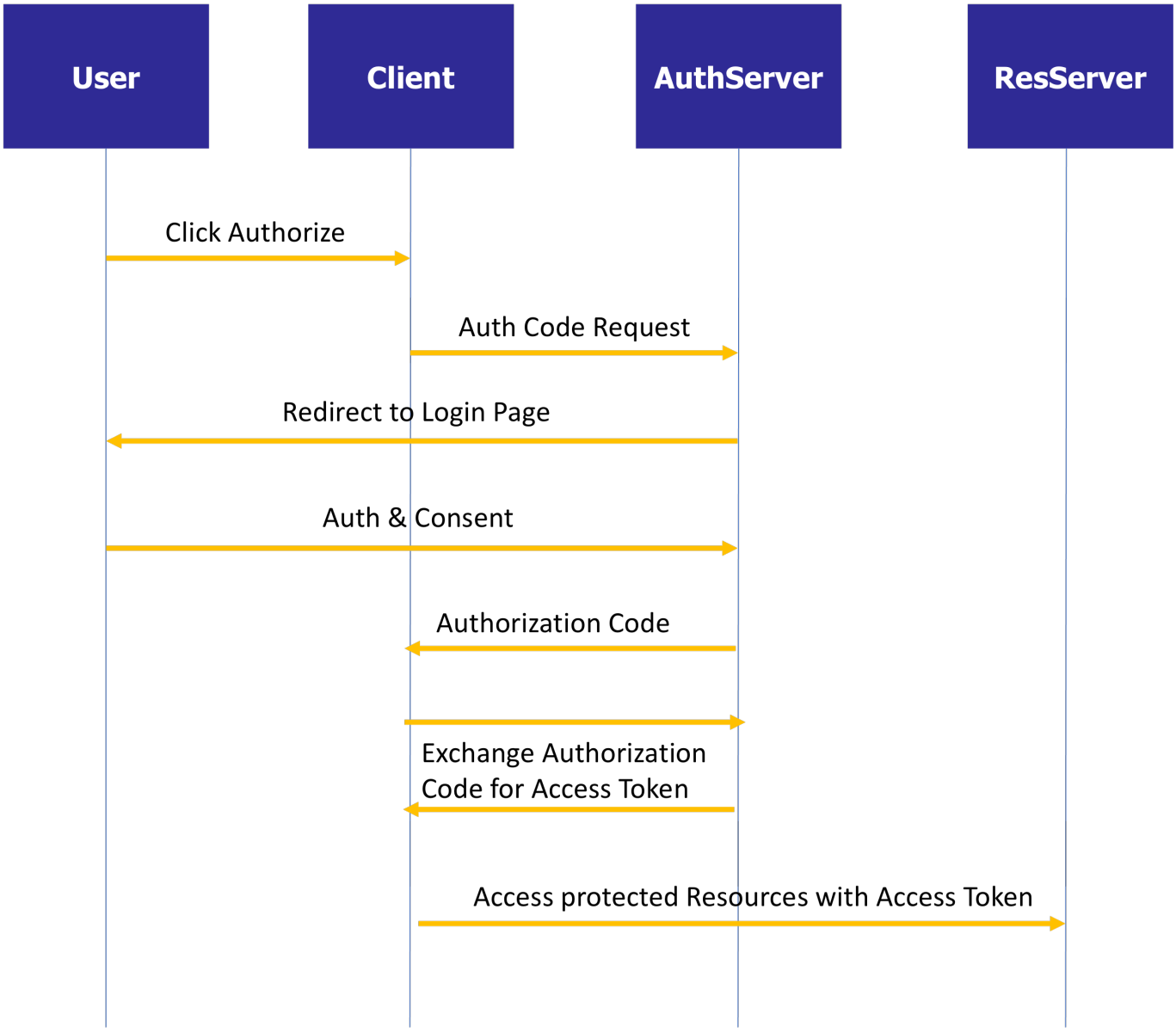
Finally, OAuth2 supports different grant types. Each grant type can have a different behaviour which can be better suited for some scenarios.

What can you test in the example?

You can test two different scenarios. One using Authorization Code grant type and the other using Client Credentials.
You will have 3 InterSystems IRIS instances that you will configure to act as each different need OAuth2 role.

Authorization Code

Authorization Code is a grant type suited for web / mobile application scenario.



In the example, you will set up a web application as the client who accesses the protected resources using an access token.

Client Credentials

Client Credentials is a different grant type, which typically is used when a client access the resources directly in its own name (and not on behalf of a user).

In the example, you will access the protected resources using Postman as the client.

#OAuth2 #Security #InterSystems IRIS
Check the related application on InterSystems Open Exchange

Source URL:https://community.intersystems.com/post/learn-how-use-oauth2-openid-connect-intersystems-iris-simple-way