
Artículo

[Alberto Fuentes](#) · 5 abr, 2022 · Lectura de 2 min

[Open Exchange](#)

Aprende a utilizar OAuth2 / OpenID Connect en Intersystems IRIS de forma sencilla

¿Te suenan OAuth2 / OpenID Connect pero no estás seguro de cómo se utilizan? ¿Has necesitado implementar alguna vez Single Sign On, servicios web seguros basados en tokens? ¿Has necesitado incorporar autenticación / autorización a tus aplicaciones web o servicios y no sabías por dónde empezar?

¿Que te parecería poder configurar paso a paso un servidor de autorización, un cliente y un servidor de recursos? [Aquí](#) tenéis un ejemplo donde se configuran instancias Intersystems IRIS para actuar como cada uno de esos roles de OAuth2.

Una breve introducción

Autenticación es el proceso de verificar que los usuarios son quienes dicen ser.

Autorización es el proceso de otorgar a esos usuarios permisos para acceder a recursos.

OAuth2 es un framework de autorización. OpenID Connect es una extensión de OAuth2 para gestionar autenticación.

En OAuth2, existen diferentes roles:

- Propietario de los recursos (resource owner) - normalmente un usuario.
- Servidor de recursos (resource server) - un servidor que alberga los datos o servicios protegidos.
- Cliente (client) - aplicación que solicita acceso limitado al servidor de recursos (e.g. una aplicación web).
- Servidor de autorización (authorization server) - servidor responsable de generar tokens de acceso con los que el cliente puede acceder al servidor de recursos.

Además, OAuth2 utiliza scopes o ámbitos como mecanismo para limitar acceso. Un cliente puede solicitar acceso a uno o varios scopes.

Y por último, OAuth2 soporta diferentes tipos de autorizaciones (grant types). Cada tipo de autorización puede tener un flujo diferente y ser más o menos indicada para un determinado tipo de escenario que nos interese montar.

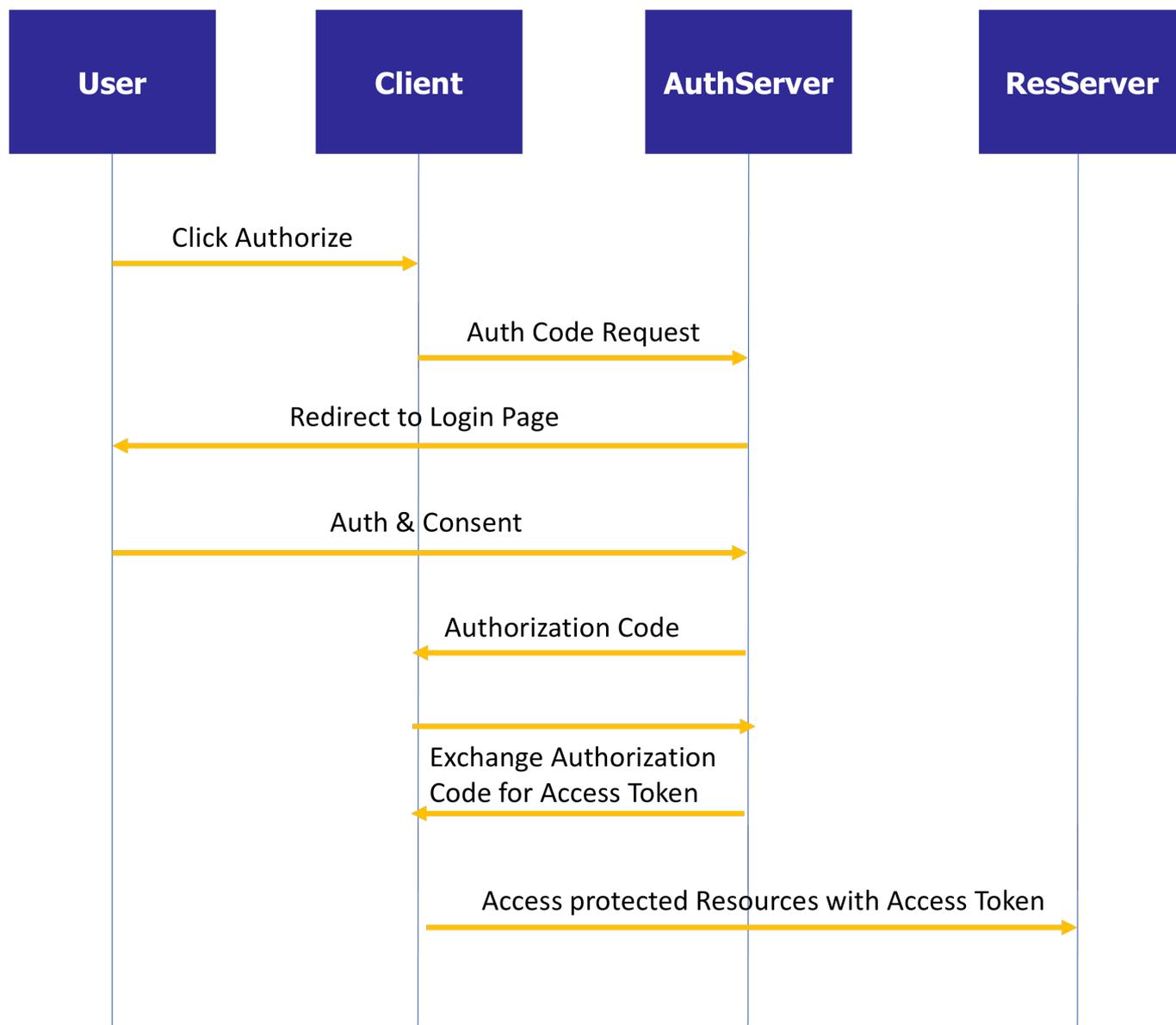
¿Qué podrás probar en en el ejemplo?

Probarás dos escenarios. Uno con el tipo de autorización Authorization Code y otro con Client Credentials.

Tendrás 3 instancias de InterSystems IRIS que configurarás para actuar como cada de uno de los diferentes roles.

Authorization code

Authorization code es un tipo de autorización indicada para escenarios de aplicaciones web / móviles.



En el ejemplo, configurarás lo necesario para tener un cliente web que accede a recursos protegidos utilizando un token de acceso.

Client Credentials

Client credentials es otro tipo de autorización, se utiliza típicamente cuando un cliente quiere acceder a recursos directamente en su nombre (y no en el de un usuario).

En el ejemplo, lo utilizarás directamente desde Postman.

[#OAuth2 #Seguridad #InterSystems IRIS](#)
[Ir a la aplicación en InterSystems Open Exchange](#)

URL de
fuente: <https://es.community.intersystems.com/post/aprende-utilizar-oauth2-openid-connect-en-intersystems-iris-de-forma-sencilla>