

OpenID Connect

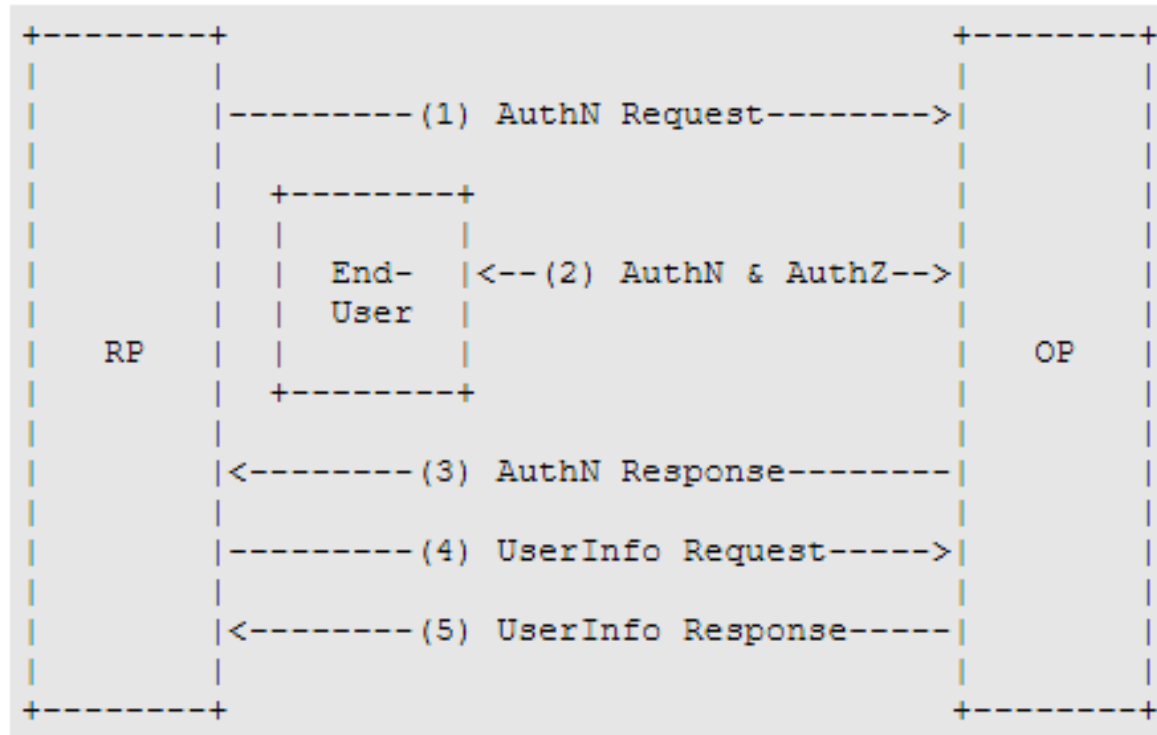
Introdução ao protocolo para delegação de autenticação em ambientes *web*

Participantes

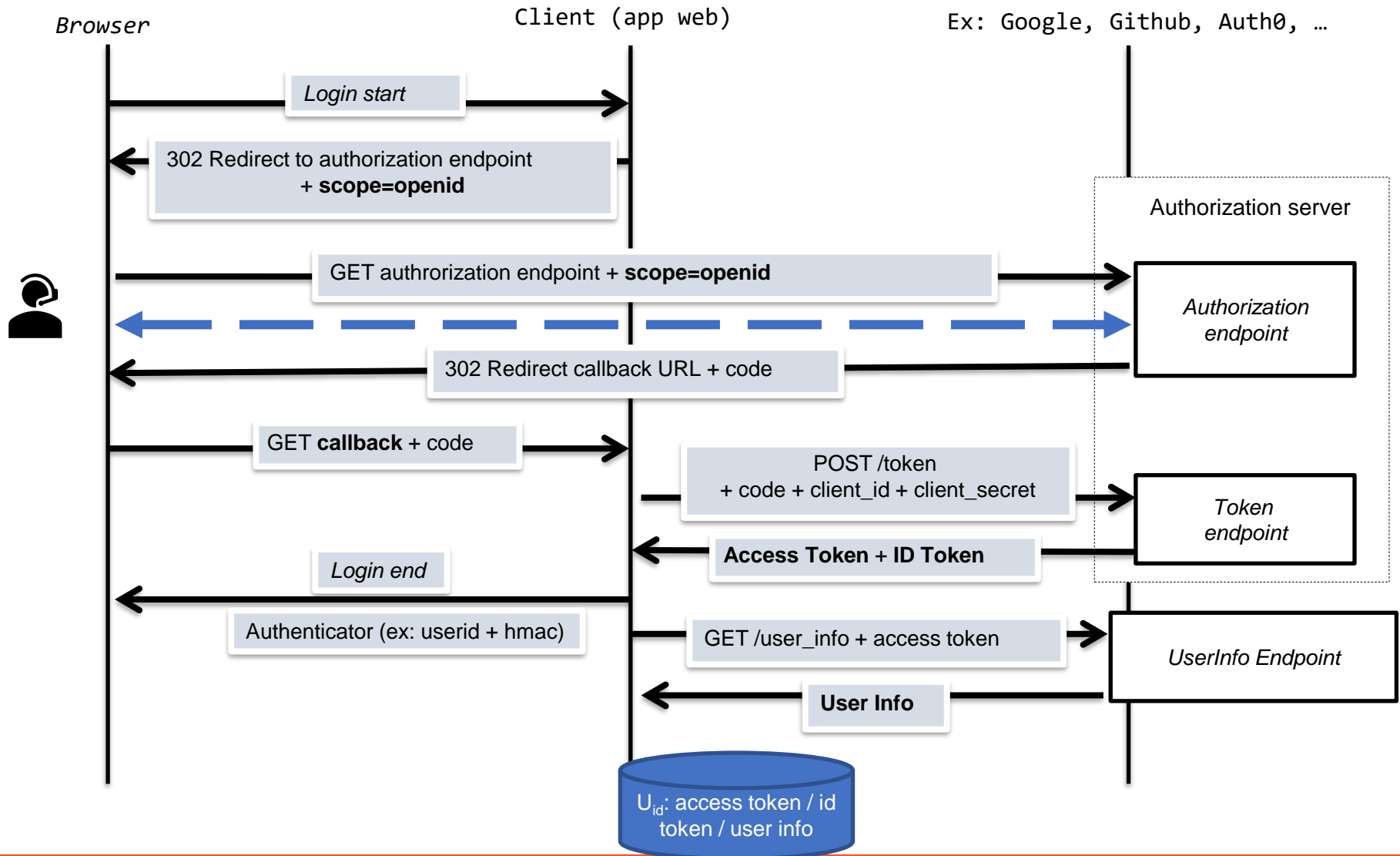
- Utilizador (*End-User*)
 - Utilizador humano que pretende aceder a um serviço na aplicação cliente
 - A aplicação cliente apenas fornece o serviço a utilizadores autenticados
 - Caso prático com utilizador a aceder via browser
- Aplicação cliente (*Relying Party*)
 - Aplicação cliente que fornece o serviço
 - Delega no fornecedor de identidade a autenticação do utilizador
- Fornecedor de identidade (*Identity Provider*)
 - Guarda registo do utilizador e da sua informação de autenticação (password, certificado, ...)
 - Guarda registo de aplicações cliente que pretendam autenticar utilizadores

Visão geral dos passos do protocolo

- https://openid.net/specs/openid-connect-core-1_0.html#Overview

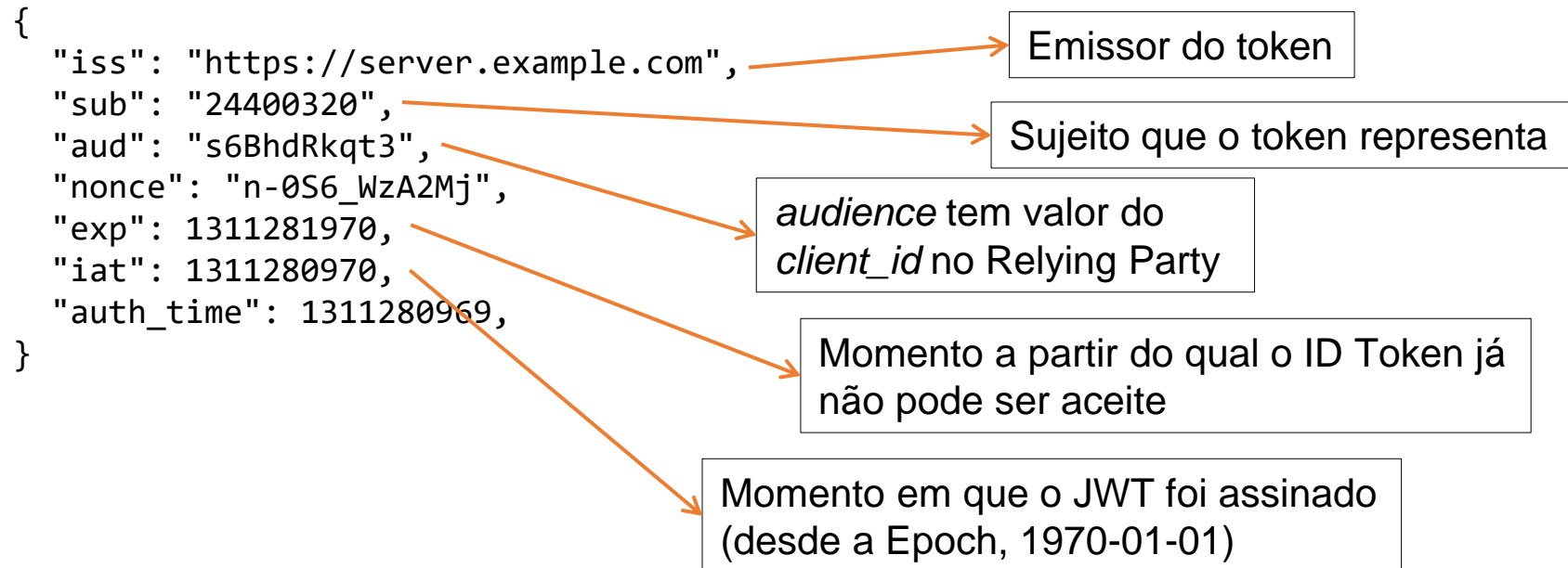


Fluxo do tipo *authorization code*



ID Token

- Um ID token é um conjunto de asserções sobre um utilizador autenticado
- JSON Web Token (JWT) assinado pelo fornecedor de identidade

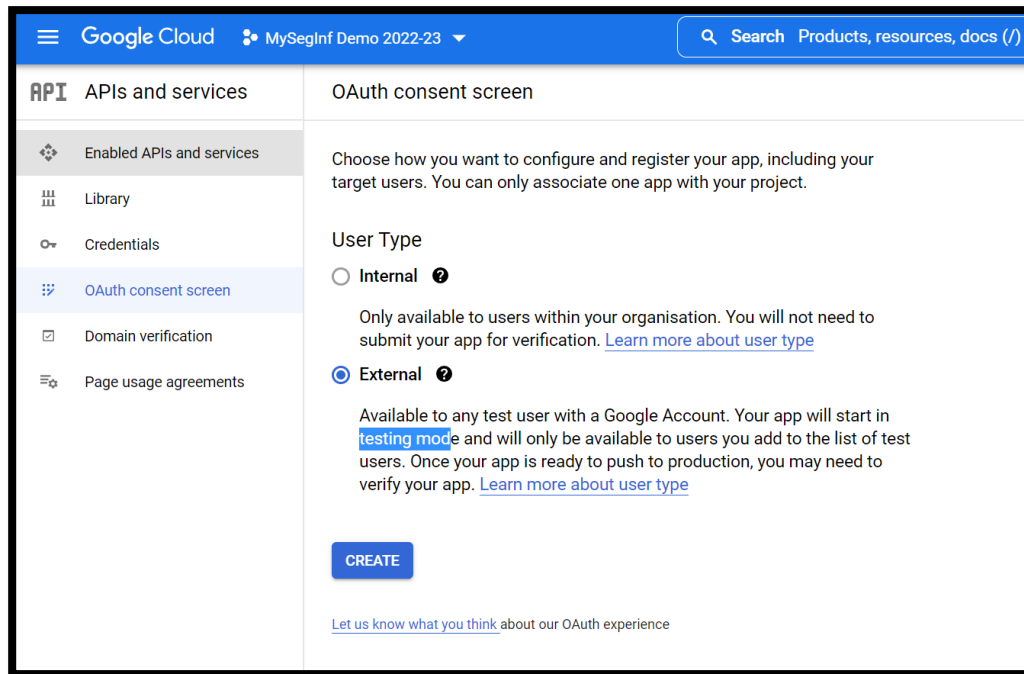


Recurso UserInfo

- A informação sobre um utilizador autenticado pode ser obtida através do UserInfo Endpoint
- Representada através de um objecto JSON
 - se assinada/cifrada será um JWT [5]
- Exemplo com *UserInfo endpoint*
<https://www.googleapis.com/oauth2/v3/userinfo>

```
{
  "family_name": "Surname",
  "name": "Alice",
  "picture": "...",
  "email": "alice@gmail.com",
  "gender": "female",
  "link": "https://plus.google.com/...",
  "given_name": "Alice",
  "id": "100...2243139"
}
```

Obter client-id e client-secret (1)



The screenshot shows the Google Cloud console interface for configuring an OAuth consent screen. The top navigation bar includes the Google Cloud logo, the project name "MySegInf Demo 2022-23", and a search bar. The left sidebar lists various API and service options, with "OAuth consent screen" selected and highlighted in blue. The main content area is titled "OAuth consent screen" and contains instructions on how to configure and register an app. It includes a "User Type" section with two radio button options: "Internal" and "External". The "External" option is selected. Below the radio buttons, there is a "CREATE" button and a link to "Let us know what you think about our OAuth experience".

Google Cloud MySegInf Demo 2022-23 Search Products, resources, docs (/)

API APIs and services

Enabled APIs and services

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

☐ Internal ⓘ

Only available to users within your organisation. You will not need to submit your app for verification. [Learn more about user type](#)

☒ External ⓘ

Available to any test user with a Google Account. Your app will start in **testing mode** and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

CREATE

[Let us know what you think](#) about our OAuth experience

Obter client-id e client-secret (3)

The screenshot displays the Google Cloud Platform interface for managing APIs and services. On the left, the 'APIs and services' sidebar is visible, with 'Credentials' selected. A dropdown menu is open over the 'Credentials' section, showing options: 'API key', 'OAuth client ID', 'Service account', and 'Help me choose'. The main content area shows the 'Create OAuth client ID' dialog. The dialog is for a 'Web application' named 'My Demo 22/23'. It shows the 'Authorised JavaScript origins' section with a URI 'http://localhost:3001/callback-demo2223' entered. The 'APIs and services' sidebar is visible on the left, and a dropdown menu is open over the 'Credentials' section.

APIs and services

- Enabled APIs and services
- Library
- Credentials**
- OAuth consent screen
- Domain verification
- Page usage agreements

OAuth client ID

Create credentials to access Google APIs

API keys

No API keys to display

OAuth 2.0 Client ID

No OAuth 2.0 client IDs to display

Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *

Web application

Name *

My Demo 22/23

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

Authorised JavaScript origins

For use with requests from a browser

[+ ADD URI](#)

Authorised redirect URIs

For use with requests from a web server

URIs 1 *

[http://localhost:3001/callback-demo2223](#)

[+ ADD URI](#)

Note: It may take five minutes to a few hours for settings to take effect

[CREATE](#) [CANCEL](#)