

OpenID Connect

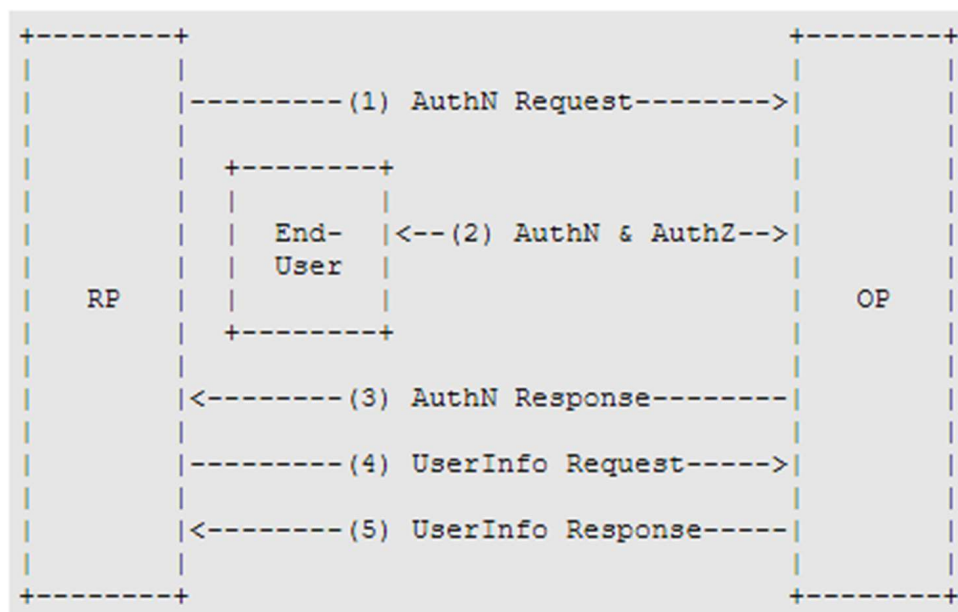
Introdução ao protocolo para delegação de autenticação em ambientes *web*

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

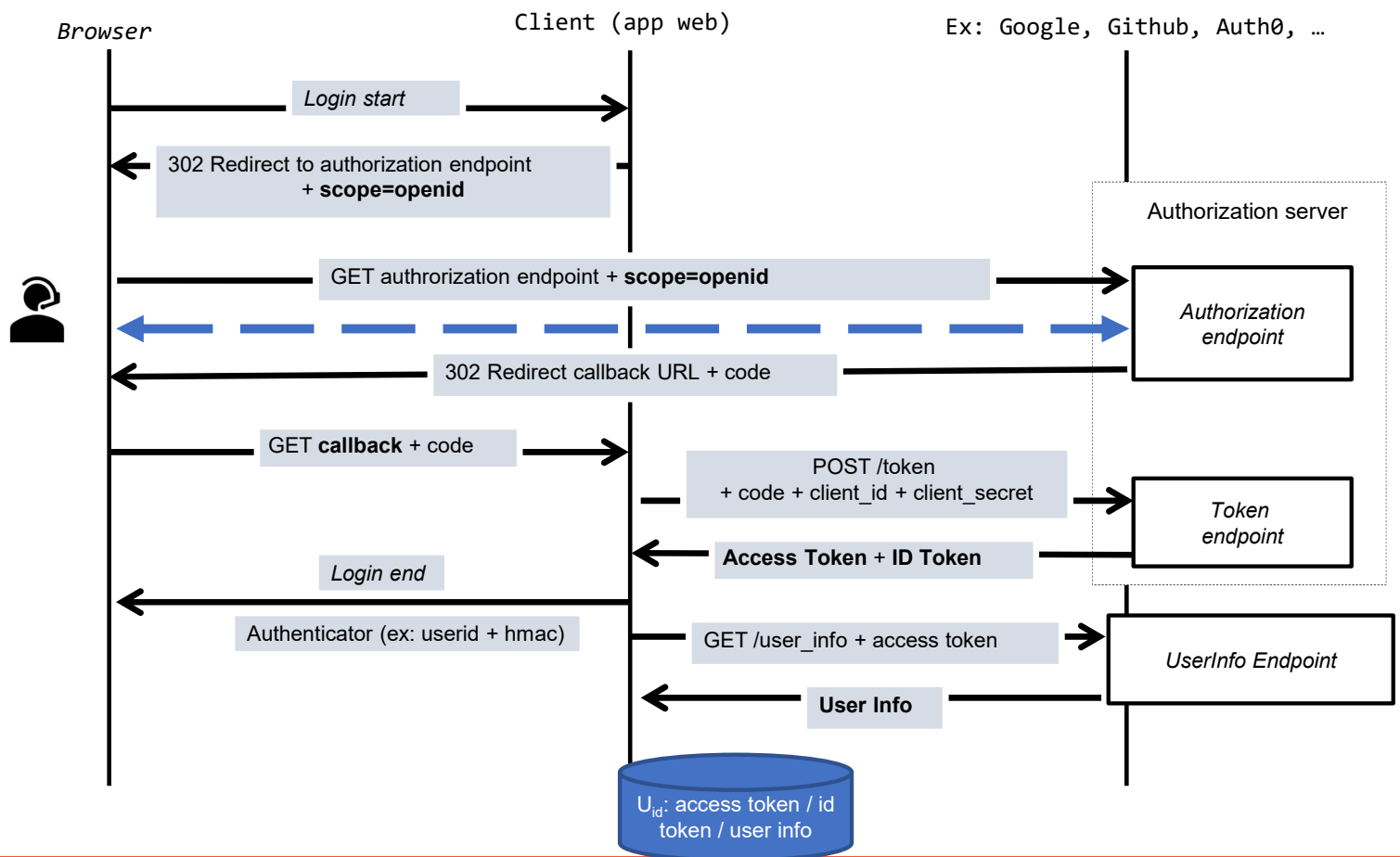
- https://openid.net/specs/openid-connect-core-1_0.html#Overview



RP - *Relying Party*

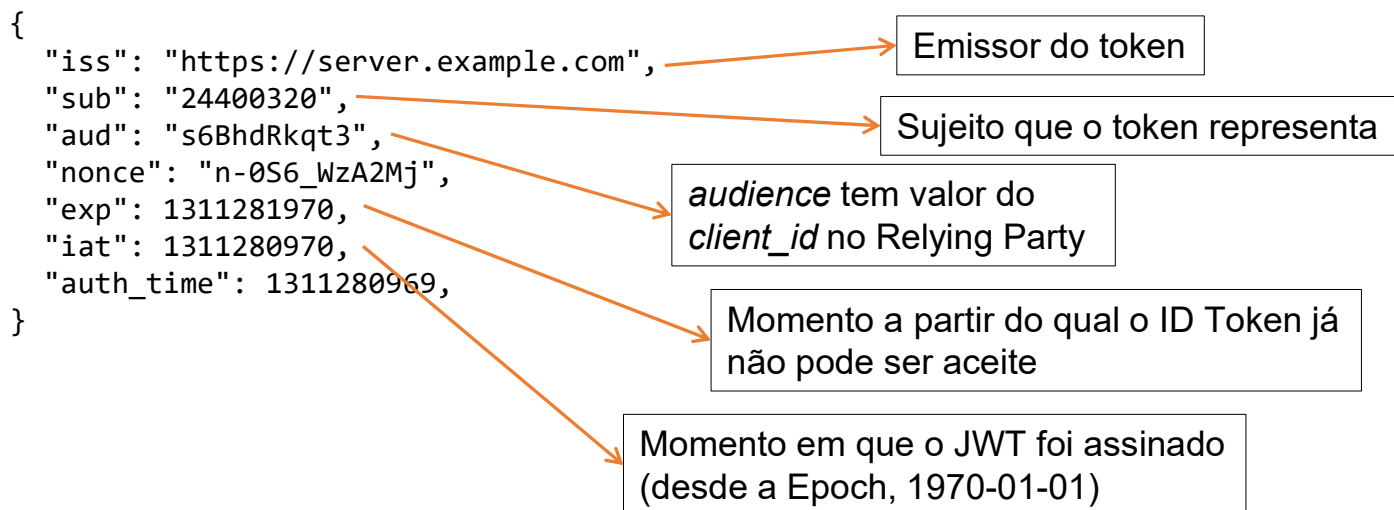
OP - *OpenID Provider / Identity Provider*

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

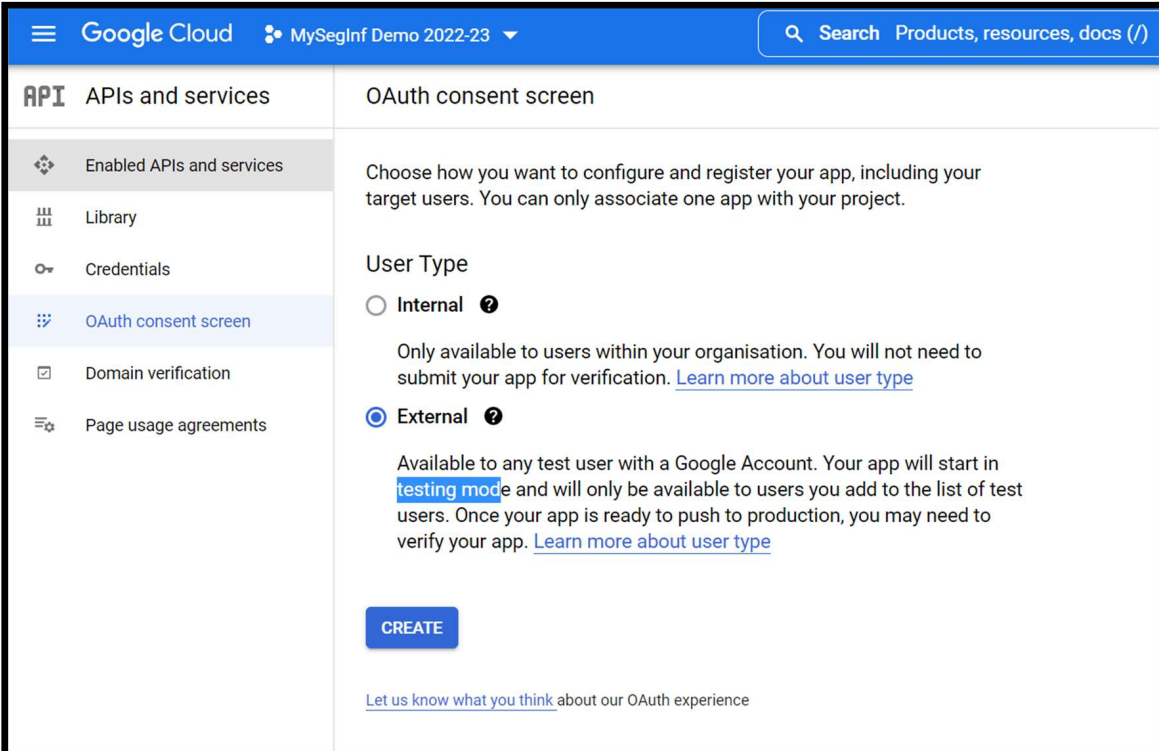


Recurso UserInfo

- 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. At the top, there's a blue header with 'Google Cloud' and 'MySegInf Demo 2022-23'. A search bar is on the right. On the left, a sidebar lists 'APIs and services' with sub-items: 'Enabled APIs and services', 'Library', 'Credentials', 'OAuth consent screen' (highlighted), 'Domain verification', and 'Page usage agreements'. The main content area is titled 'OAuth consent screen'. It contains a paragraph: 'Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.' Below this is the 'User Type' section with two radio buttons: 'Internal' (unselected) and 'External' (selected). The 'Internal' option has a help icon and text: 'Only available to users within your organisation. You will not need to submit your app for verification. [Learn more about user type](#)'. The 'External' option also has a help icon and text: '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](#)'. At the bottom of the main area is a blue 'CREATE' button and a link: '[Let us know what you think](#) about our OAuth experience'.

Obter client-id e client-secret (2)

Preencher
campos
obrigatórios

Não preencher

Email Google
do próprio e
dos colegas

Edit app registration

✓ OAuth consent screen — ✓ Scopes — 3 Test users — 4 Summary

Test users

While publishing status is set to 'Testing,' only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over the entire lifetime of the app. [Learn more](#)

+ ADD USERS

Filter Enter property name or value ?

User information

SAVE AND CONTINUE CANCEL

Obter client-id e client-secret (3)

The screenshot shows the Google Cloud Platform interface for creating an OAuth client ID. The 'APIs and services' sidebar is on the left. The 'Credentials' section is active, showing a dropdown menu with options: 'API key', 'OAuth client ID', 'Service account', and 'Help me choose'. The 'OAuth client ID' option is selected, and an arrow points to the 'Create OAuth client ID' wizard. The wizard has fields for 'Application type' (set to 'Web application'), 'Name' (set to 'My Demo 22/23'), 'Authorised JavaScript origins' (with an '+ ADD URI' button), and 'Authorised redirect URIs' (with a text input containing 'http://localhost:3001/callback-demo2223' and an '+ ADD URI' button). At the bottom are 'CREATE' and 'CANCEL' buttons.