

OAuth and OpenID for mere mortals

And for developers

How I am?

- Leonardo Micheloni
- From Argentina
- Working for Tokiota Madrid
- Microsoft MVP
- Auth0 Ambassador
- CSM since 2012



[@leomicheloni](https://twitter.com/leomicheloni)

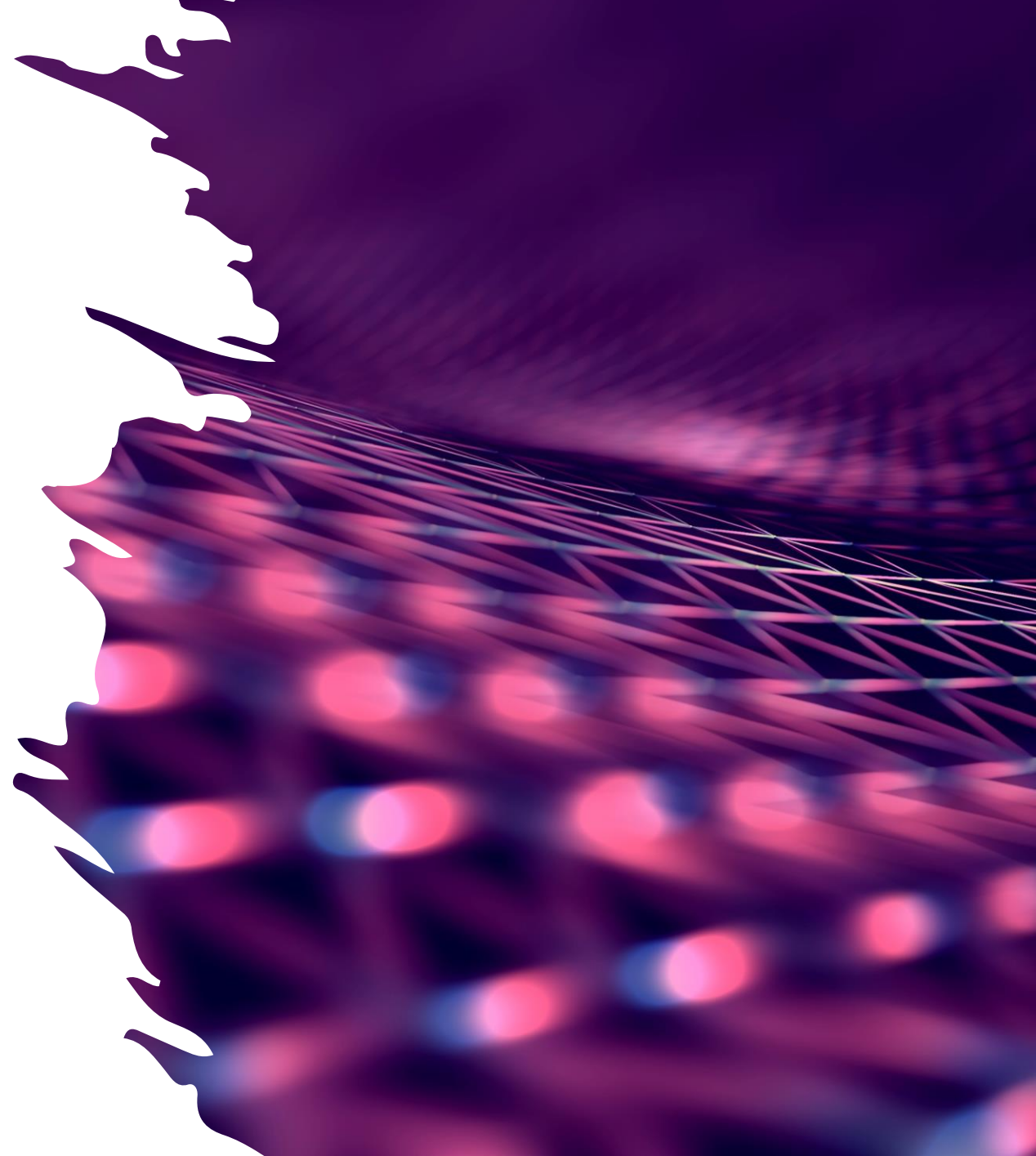


TOKIOTA



Agenda

- The problem
- OAuth
- Client Credentials flow
- Token
- Implicit Flow
- Code Flow
- Open ID Connect



Are your friends already on Yelp?

Many of your friends may already be here, now you can find out. Just log in and we'll display all your contacts, and you can select which ones to invite! And don't worry, we don't keep your email password or your friends' addresses. We loathe spam, too.

Your Email Service



Your Email Address

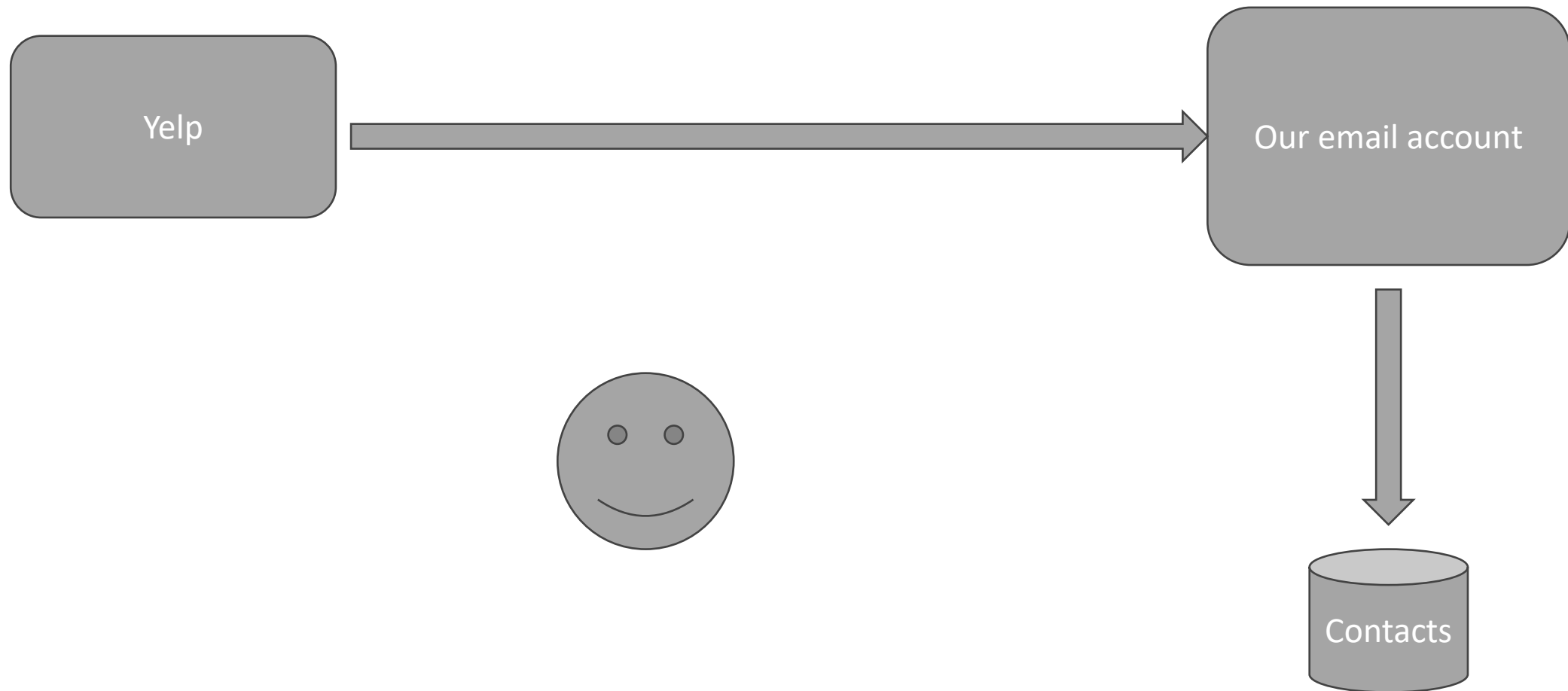
(e.g. bob@gmail.com)

Your Gmail Password

(The password you use to log into your Gmail email)

[Skip this step](#)

Check Contacts



Step 1
Find Friends

Step 2
Profile Information

Step 3
Profile Picture

Are your friends already on Facebook?

Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.



Gmail

Your Email:

Email Password:

Find Friends



Facebook will not store your password.



Yahoo!

[Find Friends](#)



Windows Live Hotmail

[Find Friends](#)



Other Email Service

[Find Friends](#)

103,00 € ▾

Particulares / Private

Empresas

Por favor, asegúrese de usar los mismos datos de acceso de su banca online

MODO DE IDENTIFICACIÓN:

Documento ▾

Tipo de documento:
NIF ▾

Número de documento
[REDACTED]

Clave de acceso:
●●●●●●●●

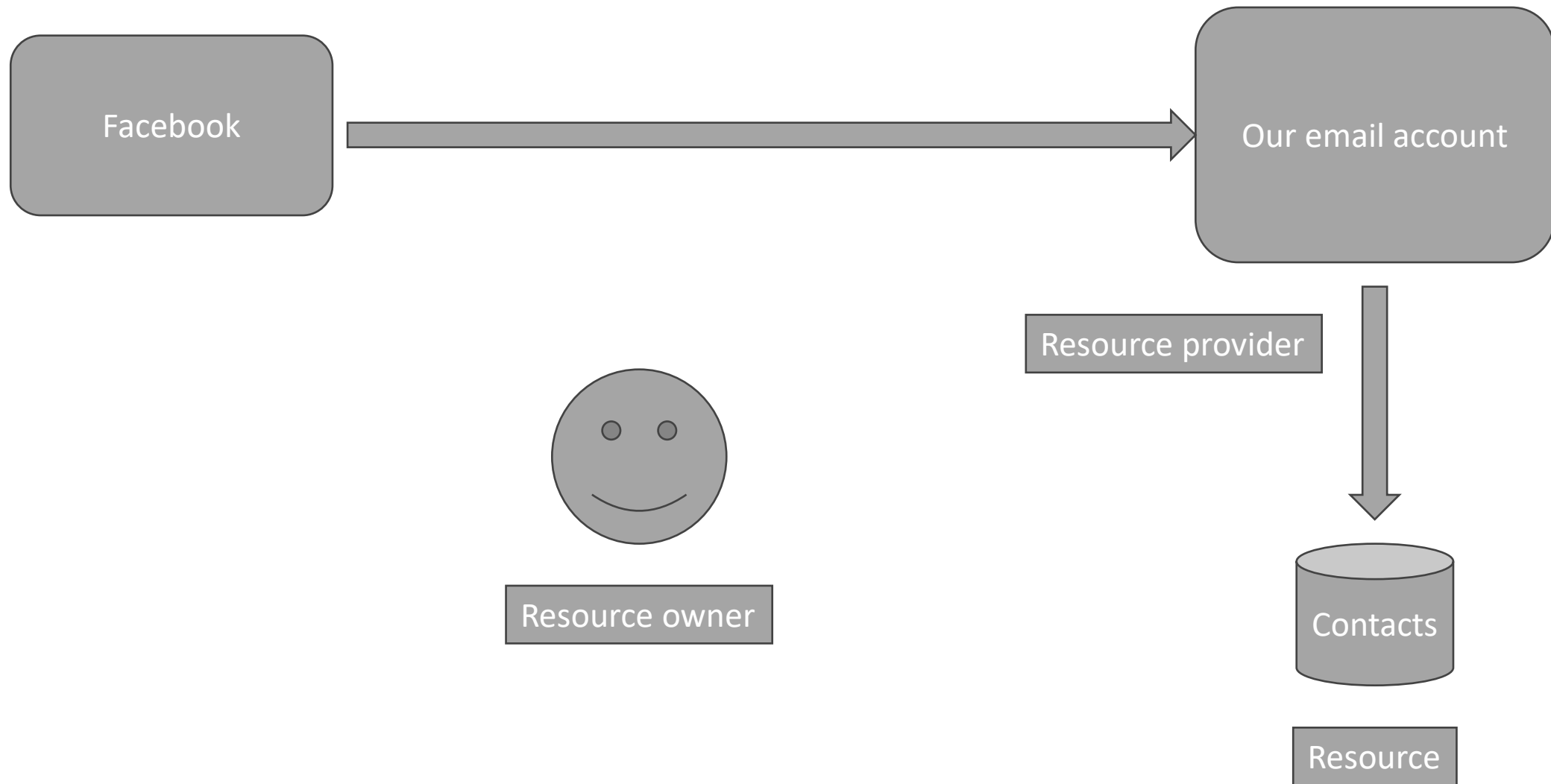
Ich akzeptiere die Verwendung des Zahlungsinisierungsdienstes oder des Kontoinformationsdienstes von Sofort, damit Sofort eine Zahlung initiieren oder auf mein Zahlungskonto zugreifen kann.

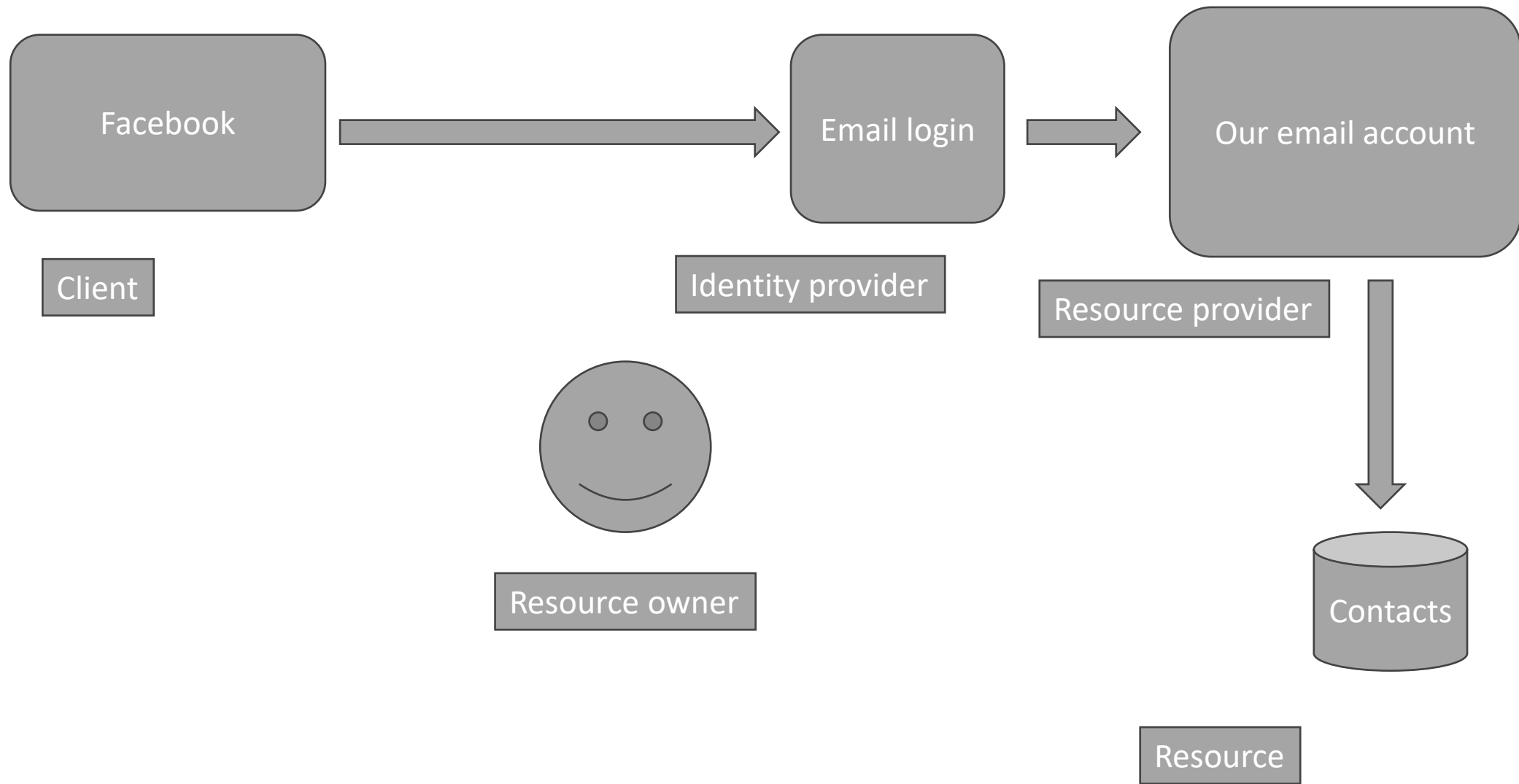
Se aplica nuestra [Política de protección de datos personales](#)

Continuar

Whats going on here?

- An external application needs access to some resource
- This resources is in another external application





Whats going on here?

- An external application (a client) needs access to some resource
- This resources is in an external entity (a resource provider)
- The client needs credentials to get the resources

There are some little problems

- We are given our credentials to a “unknown” application.
 - The application will have access not only to the resource itself but to all the resources in the account (emails, etc.)
 - The application will act in our behalf
-
- This is similar to give the cinema hall keys to all the people that want to watch a particular movie

What if...

- The identity provider gives some type of ticket (token) to the client?
- This token has no relation with my credentials?
- This token only allows the client to access to specific resources?
- This token has a limited lifetime?

OAuth2

Authentication is the process of ascertaining that somebody really is who they claim to be.

Authorization refers to rules that determine who is allowed to do what. E.g. Adam may be authorized to create and delete databases, while Usama is only authorised to read.

OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.^[1] This mechanism is used by companies such as [Amazon](#),^[2] [Google](#), [Facebook](#), [Microsoft](#) and [Twitter](#) to permit the users to share information about their accounts with third party applications or websites.

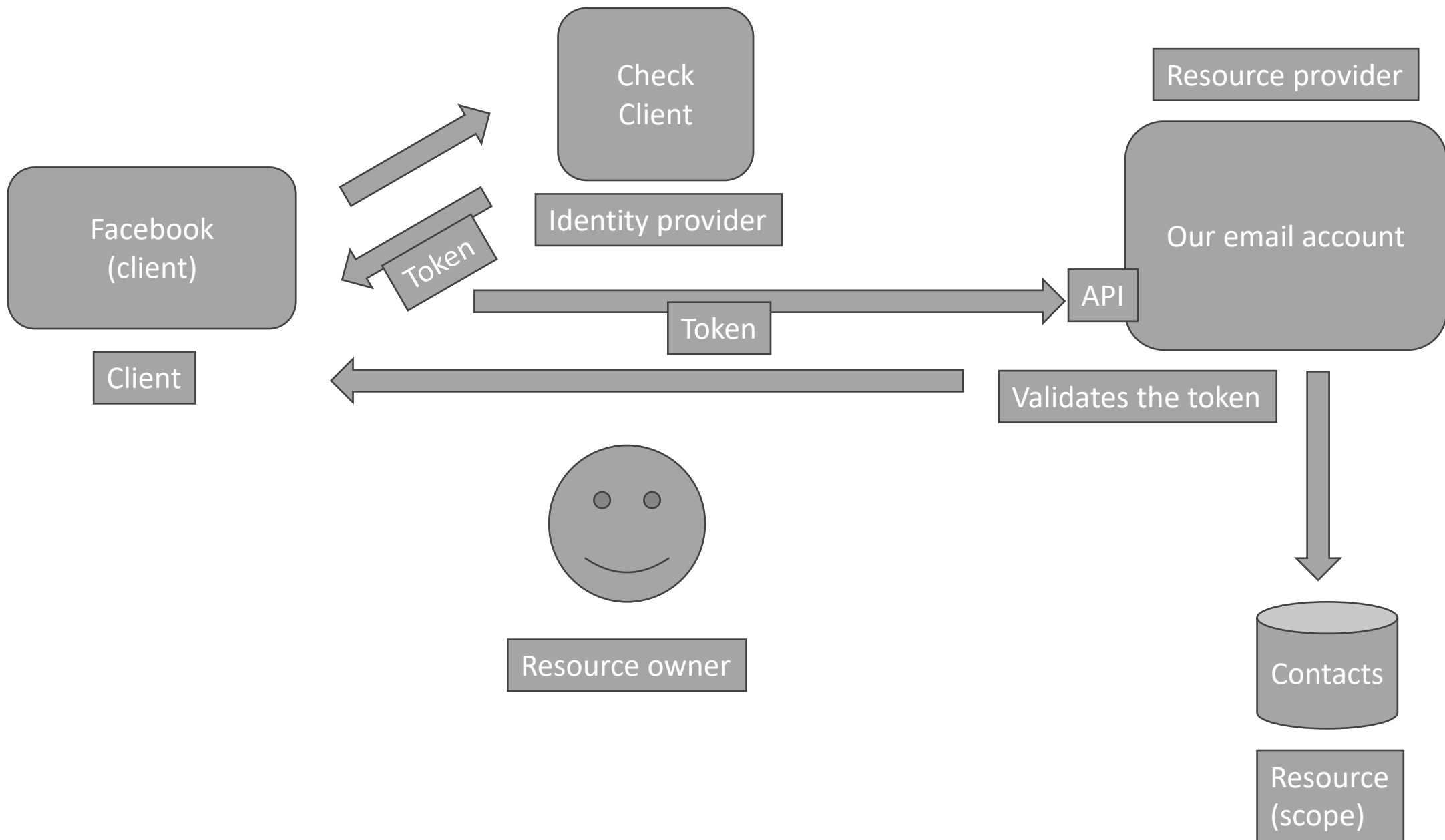
Generally, OAuth provides to clients a "secure delegated access" to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. Designed specifically to work with [Hypertext Transfer Protocol](#) (HTTP), OAuth essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the resource owner. The third party then uses the access token to access the protected resources hosted by the resource server.^[3]



<https://oauth.net/2/>

There are several benefits

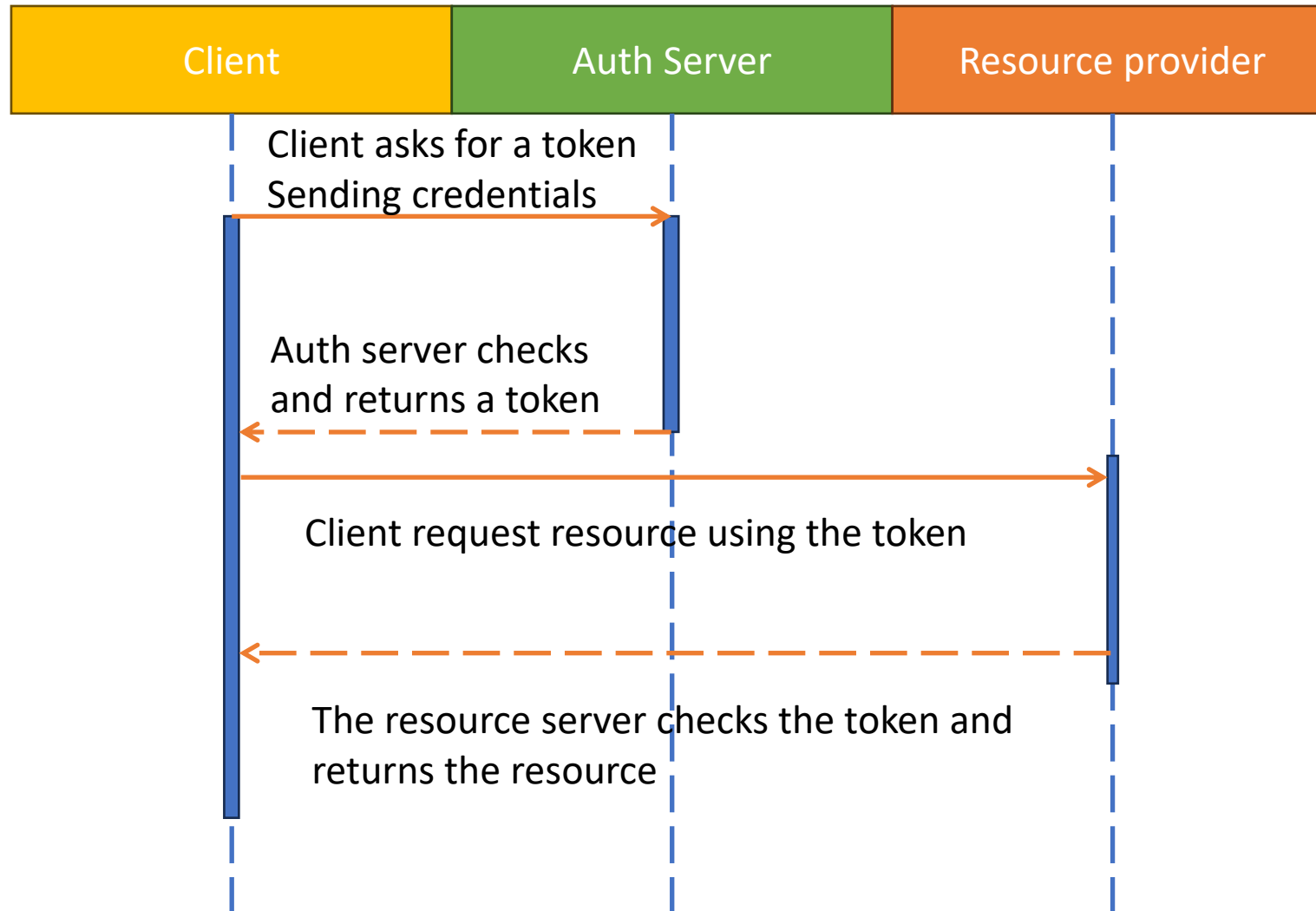
- No password compromised
 - Limited access in time and resources
 - Limited time
-
- This is similar to give tickets to a specific movie valid on a specific date



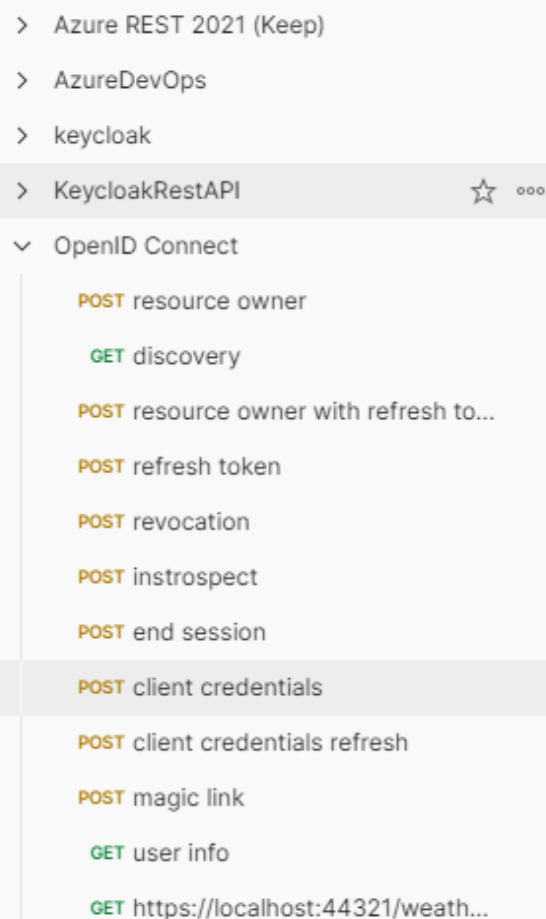
In OAuth world

- We need an identity server or authorization server
- We need a client (an application)
 - The client is always an application
 - The user has nothing to do with authorization
- We need a resource server
 - That trusts the IDP
 - Where the resources are located

Complete sequence



Demo



POST <http://localhost:8088/realms/master/protocol/openid-connect/token>

☐ none
 ☐ form-data
 ☒ x-www-form-urlencoded
 ☐ raw
 ☐ binary
 ☐ GraphQL

	Key	Value
<input checked="" type="checkbox"/>	grant_type	client_credentials
<input checked="" type="checkbox"/>	client_id	cc
<input checked="" type="checkbox"/>	client_secret	jk69FoPtQJd5y5d2wHtBnY40YUa99fj9
	Key	Value

Pretty Raw Preview Visualize JSON

```
1 {"access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJMOXNfd0xzWE5kV29SRDAzTGv3cDRHbmZDZm1iRElUMGpUbHkwS2RGNS+
```

▼

G

Authorization ●

Settings

▼

Token

Token

Token

Body

Test Results



Status: 200

Visualize

∇



```
1 [
2   {
3     "date": "2024-02-04T22:47:05.6873057+01:00",
4     "temperatureC": 31,
5     "temperatureF": 87,
6     "summary": "Scorching"
7   },
8   {
9     "date": "2024-02-05T22:47:05.6875778+01:00",
10    "temperatureC": 30,
11    "temperatureF": 85,
12    "summary": "Cool"
13  },
14  {
15    "date": "2024-02-06T22:47:05.6875863+01:00",
16    "temperatureC": 3,
17    "temperatureF": 37,
18    "summary": "Freezing"
19  },
20 ]
```

The interaction between the client and the IDP to get a token is called
“authorization flow or grant”

Tokens

Token

- In most of the cases we will use JWT token
- A token is only a piece of information
- In this case in JSON format
- Has 3 main part
 - Header
 - Payload
 - Signature

Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjVpc09lMkV4dU1iQmJLeHU2ejlIS0EiLCJ0eXAiOiJhdCtqd3Qi
fQ.eyJyYmYiOiJ0eXAiOiJhdCtqd3QiLCJ0eXAiOiJhdCtqd3Qi
DMxNjEyNSwiaXNzIjoiaHR0cDovL2xvY2FsaG9zd
Do1MDAwIiwiaXNzIjoiaHR0cDovL2xvY2FsaG9zd
CI6ImNjLmNsaWVudC5vYXV0aCIsInNjb3BlIjpbI
mFwaTEiXX0.JHjJozdDaIi5SixBK2sxLGM1bUvAc
wTxvqADzQpTd2obyMirocNeejfnBVRy1iFNKSK4o
7uoTn7kAf_BwI0E4SF9NpJ7LV3826InL1EexPw09
VwsCTN_Sq1u2fUzJDz9FcAPS5tbb4R5R6VJpzPo
BONxBk5qc-lJjiK-
uXT20g3huxScQxm1N_imQCTWP6m0-qRaNq-
1rhwcPM5WUBkKNcDXQqbVZWhaqy_Rs5lCm_PbE0h
ekM0VptaGq3JikziFvL6uaaRF1zAFsP5gh7jhyAj
rZH-
gXLQI1YohAqaR2c5t29etGW1G3eL5yjkWHipW5i
HXizw94yyh2uLyU48w
```

ALGORITHM

RS256

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "kid": "5is0e2ExuMbBbKxu6z9HKA",
  "typ": "at+jwt"
}
```

PAYLOAD: DATA

```
{
  "nbf": 1590312525,
  "exp": 1590316125,
  "iss": "http://localhost:5000",
  "aud": "api1",
  "client_id": "cc.client.oauth",
  "scope": [
    "api1"
  ]
}
```

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key or Certificate. Enter
  it in plain text only if you
  want to verify a token

  Private Key. Enter it in plain
  text only if you want to genera
  te a new token. The key never l
  eaves your browser.
```

@leomicheloni

oAuth has different flows (grants)

- Client credentials
- Implicit
- Code
- Code + PKCE
- Resource owner
- Device
- Hybrid

<https://oauth.net/2/grant-types/>



Nice to see you again

You know the drill - just click on a network you've registered with, and we'll let you in.

See you inside.

Login with your preferred account

 Facebook


 Google


 Microsoft

 Office 365

 X / Twitter

 Classic Login

 If you haven't logged in before, you'll be able to register.

 Using social networks to login is faster and simpler, but if you prefer username/password account - use Classic Login.

Cancel



Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Back

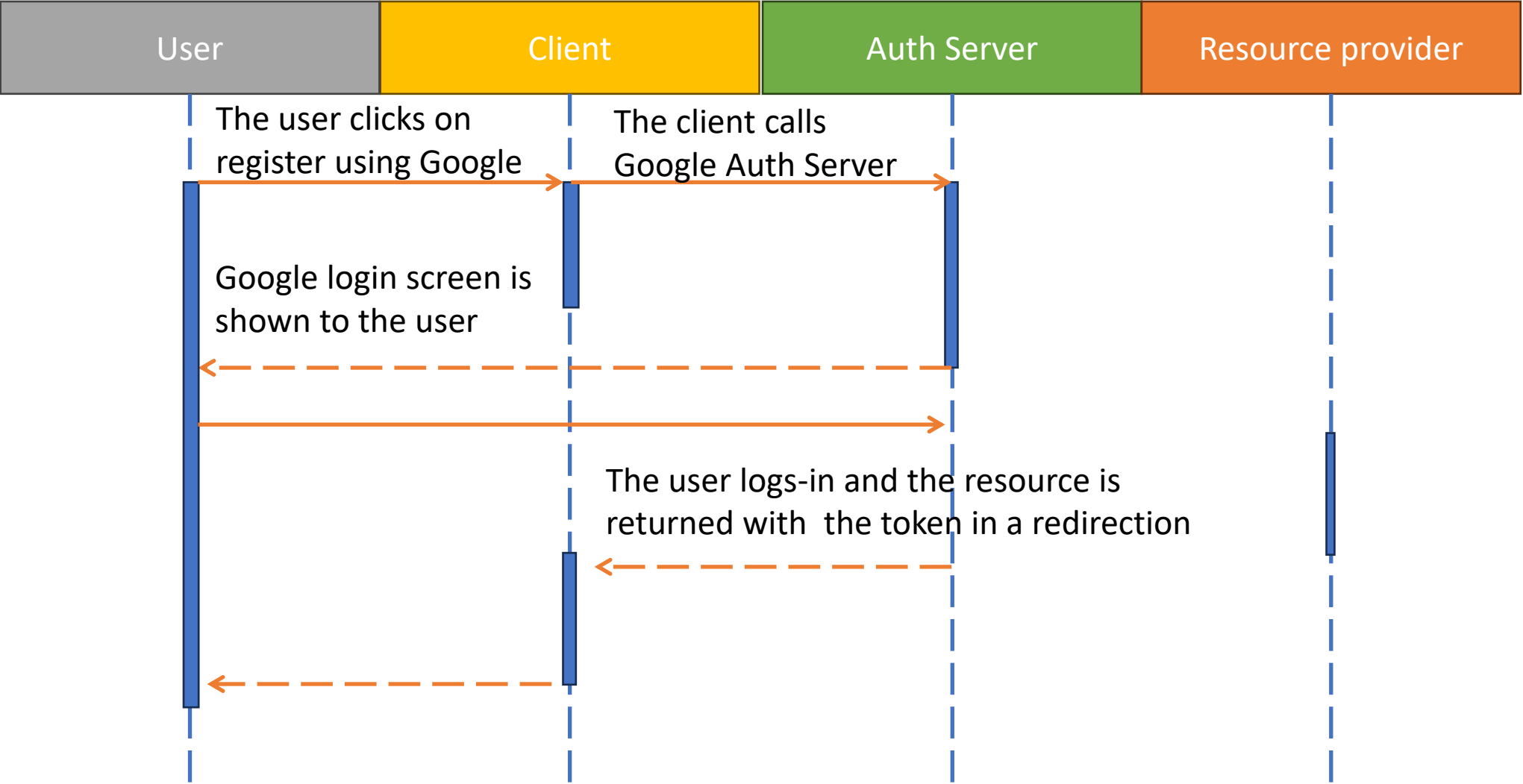
Next



Sign-in options

Thinking about it

- The application wants to register us
- To avoid the process of entering our email, name, etc. it will ask someone else that already knows this information
- The application is registered as a client in all these external login providers
- Since the information is retrieved using a browser (and user credentials are required) it needs us to login in the external IDP



In detail

- We need the participation of a user
- We need a web browser
- We need to redirect the client so the person enters credentials and authorize the client
- Then the token is returned with additional information
- This flow is called Implicit flow

Demo

master

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

Access settings

Root URL ?

Home URL ?

Valid redirect URIs ?

/*

http://localhost:44386

+ Add valid redirect URIs



Valid post logout
redirect URIs ?

http://localhost:44386/unauthorized

+ Add valid post logout redirect URIs



Web origins ?

/*

+ Add web origins



Admin URL ?

Path

/main.js

/styles.js

/ng-cli-ws

/realms/master/protocol/o...

/resources/yczrw/common/ke...

/resources/yczrw/common/ke...

/resources/yczrw/common/ke...

/resources/yczrw/common/ke...

/resources/yczrw/login/keyclo...

/resources/yczrw/login/keyclo...

Headers

Payload

Preview

Response

Initiator

Timing

Cookies

General

Request URL: http://localhost:8088/realms/master/protocol/openid-connect/auth?client_id=implicit&redirect_uri=http%3A%2F%2Flocalhost%3A44386&response_type=id_token%20token&scope=openid%20email%20profile&nonce=7c03b6f22755e1c7526b23e20277961facf08pGJr&state=8e9a5da8c696c8508f6f7163acbd60763c1ET8YR1

Request Method: GET

Status Code: 200 OK

Remote Address: [::1]:8088

Referrer Policy: strict-origin-when-cross-origin

Response Headers

Raw

Path

/main.js

/styles.js

/ng-cli-ws

/realms/master/protocol/ope...

/resources/yczrw/common/ke...

/resources/yczrw/common/ke...

/resources/yczrw/common/ke...

/resources/yczrw/common/ke...

/resources/yczrw/login/keyclo...

/resources/yczrw/login/keyclo...

/resources/yczrw/login/keyclo...

/resources/yczrw/login/keyclo...

/resources/yczrw/common/ke...

/realms/master/login-actions/...

/

/bootstrap/4.4.1/css/bootstra...

/jquery-3.4.1.slim.min.js

/npm/popper.js@1.16.0/dist/u...

/bootstrap/4.4.1/js/bootstrap....

/styles.css

/runtime.js

/polyfills.js

/vendor.js

/main.js

/styles.js

/realms/master/protocol/ope...

Headers

Payload

Preview

Response

Initiator

Timing

Cookies

Request Method:

POST

Status Code:

302 Found

Remote Address:

[::1]:8088

Referrer Policy:

no-referrer

Response Headers

Raw

Cache-Control:

no-store, must-revalidate, max-age=0

Content-Length:

0

Content-Security-Policy:

frame-src 'self'; frame-ancestors 'self'; object-src 'none';

Location:

http://localhost:44386#state=8e9a5da8c696c8508f6f7163acbd60763cIET8YR1&sessio



```
...ZCI6ImFjY291bnQiLCJzdWIiOiIiYzk2Mjg5MC1
kMWI3LTQ3ZWYtYjAxZC0xYzBjODFhNWU1ZDQiLC
J0eXAiOiJCZWYyZXIiLCJhenAiOiJpbXBsaWNpd
CIsIm5vbmNlIjoiMzRmODhhNGY3NDg1ZjVmNjk5
NjUyMzg0WF1NDVhNTI4NmZVNDJ1NlgiLCJzZXN
zaW9uX3N0YXRlIjoiYzA5ZGZjYjAtOGE4ZC00Y2
JlLWEzNWMtZDZmZmUxYTI5NDUwIiwiaWYWNyIjoiM
SIsImFsbG93ZWQtb3JpZ2lucyI6WyIvKiJdLCJy
ZWFSbV9hY2Nlc3MiOmsicm9sZXMiOlsiZGVmYXV
sdC1yb2xlc1tYXN0ZXIiLCJvZmZsaW5lX2FjY2
VzcyIsInVtYV9hdXRob3JpemF0aW9uI119LCJyZ
XNvdXJjZV9hY2Nlc3MiOmsiYWNjb3VudCI6eyJy
b2xlc1tYWNjb3VudCI6eyJybnZS1hY2NvdW50LWxp
bmtzIiwidmldy1wcm9maWx1I119fSwic2NvcGUiOiJvcGVuaWQgcHJvZmlsZ
SB1bWFpbCI6InNpZCI6ImMwOWRmY2IwLTlhOGQ0t
NGNiZS1hMzVjLWQ2ZmZlMWEyOTQ1MCI6ImVtYW1
sX3Zlcm1maWVkaWVjYWNyZWxzZSwibmFtZSI6Ikxlb2
5hcmRvIE1pY2h1bG9uaSI6InByZWZlcnJlZF91c
2VybmFtZSI6Imxlb25hcmRvIiwiaWZlZlZlZW5fbmFt
ZSI6Ikxlb25hcmRvIiwiaWZmFtaWx5X25hbWUiOiJ
NaWNoZWxvbmkiLCJlbWFpbCI6Imxlb21pY2h1bG
9uaUBob3RtYWlsLmNvbSJ9.14WHEQtIc5nAwaAf
CYccW2TjSucb99Av2fN-V0ds3-
WFW0fF4IVCMoi_w1TGeP9x2GQR0hTGKKbhJk5u_
7rgH_f0sA-
_79SnFUIPrama1AbdXixUUAUcE5zkS_7EzRAZKC
LqmQIIN5ZyRzVIYnuTDYa_yNR1wVfIC-
```

```
{
  "exp": 1707068604,
  "iat": 1707067704,
  "auth_time": 1707067704,
  "jti": "5851881b-09d8-4a97-84dc-2efb384a657a",
  "iss": "http://localhost:8088/realms/master",
  "aud": "account",
  "sub": "5c962890-d1b7-47ef-b01d-1c0c81a5e5d4",
  "typ": "Bearer",
  "azp": "implicit",
  "nonce": "34f88a4f7485f5f6996523889ae45a5286fU42u6X",
  "session_state": "c09dfcb0-8a8d-4cbe-a35c-
d6ffe1a29450",
  "acr": "1",
  "allowed-origins": [
    "*"
  ],
  "realm_access": {
    "roles": [
      "default-roles-master",
      "offline_access",
      "uma_authorization"
    ]
  },
  "resource_access": {
    "account": {
      "roles": [
        "manage-account",
        "manage-account-links",
        "view-profile"
      ]
    }
  },
  "scope": "openid profile email",
  "sid": "c09dfcb0-8a8d-4cbe-a35c-d6ffe1a29450",
  "email_verified": false,
  "name": "Leonardo Micheloni",
  "preferred_username": "leonardo",
  "given_name": "Leonardo",
  "family_name": "Micheloni",
  "email": "leomicheloni@hotmail.com"
}
```

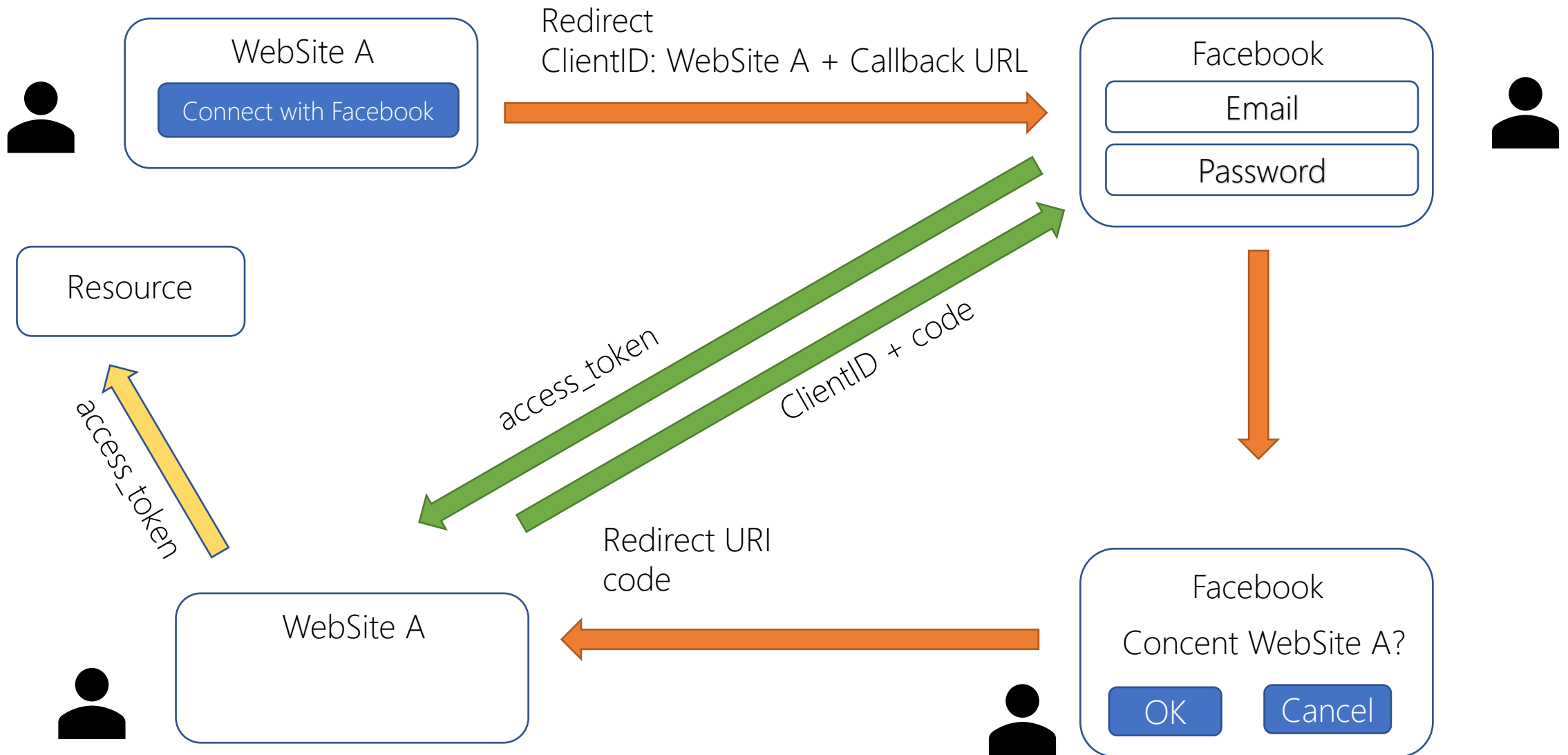
To have in mind

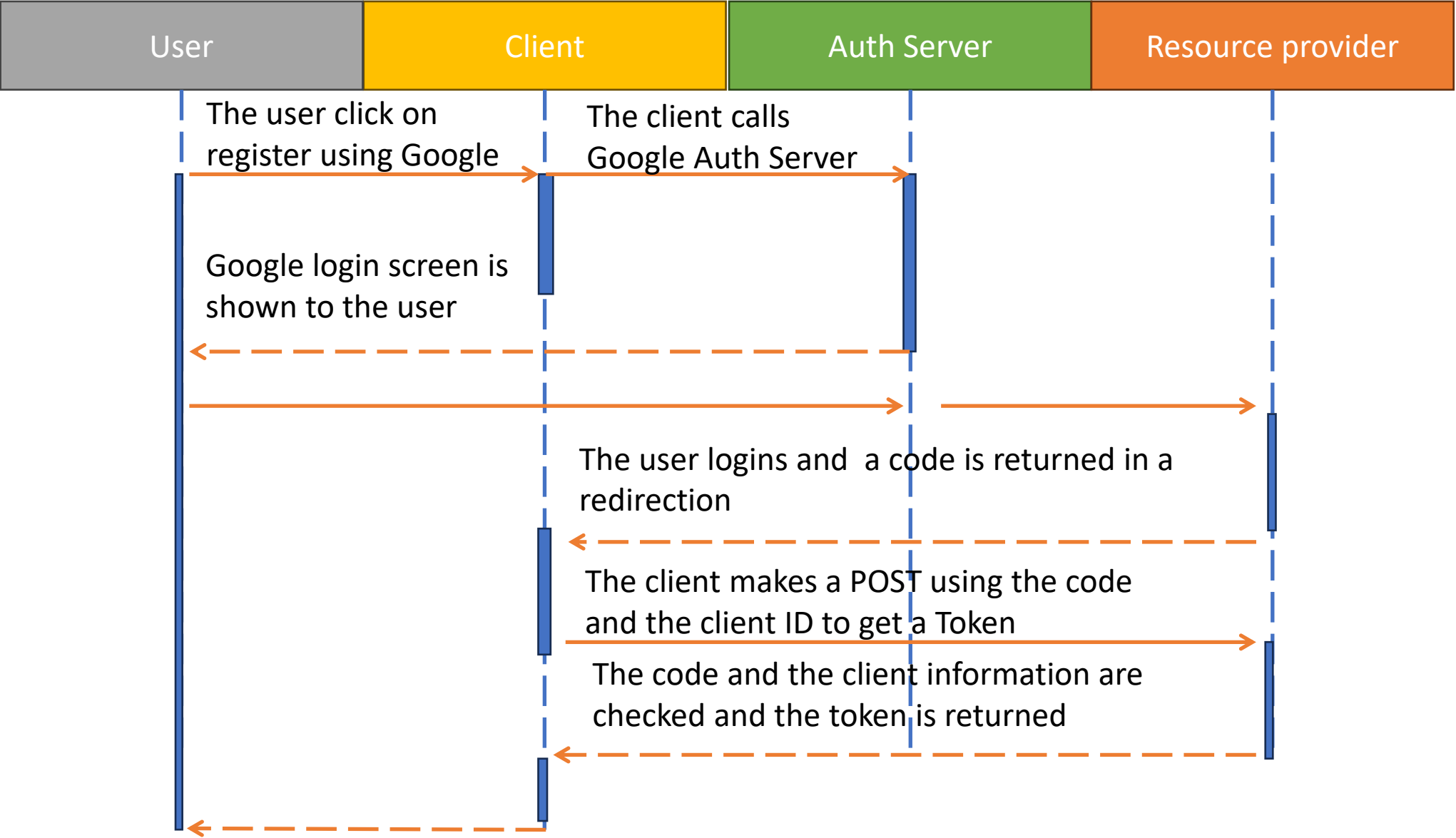
- The redirect URL es very important
- The redirect URL has the token
- We cannot refresh the token, so the lifetime must be sufficient

Implicit flow drawbacks

- We cannot use a secret in the client since we use a web browser
- The Token is returned in the redirection, so an interception is possible
- The URL can remain in the history of the browser or our session
- This flow is not more recommended

code flow





(i) When prefers-reduced-motion is enabled, a simpler highlighter can be enabled in the settings panel, to avoid flashing colors.

Inspector

Console

Debugger

↕ Network

{ Style Editor

🔊 Performance

💾 Memory

📁 Storage

♿ Accessibility

⚙️ Application

🗑 Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	localhost:4204	/?state=9a05dd39e18c75b618dec8823e4d4e4a4bYQsz	document	html	1.71 kB	1.42 kB
200	GET	localhost:4204	styles.css	stylesheet	css	1.17 kB (raced)	889 B
304	GET	localhost:4204	runtime.js	script	js	cached	12.99 kB
304	GET	localhost:4204	polyfills.js	script	js	cached	344.03 ...
200	GET	stackpath.bo...	bootstrap.min.css	stylesheet	css	cached	159.52 ...
304	GET	localhost:4204	styles.js	script	js	cached	235.35 ...
304	GET	localhost:4204	vendor.js	script	js	cached	2.67 MB
304	GET	localhost:4204	main.js	script	js	cached	335.80 ...
200	GET	code.jquery.com	jquery-3.4.1.slim.min.js	script	js	cached	71.04 kB
200	GET	cdn.jsdelivrn...	popper.min.js	script	js	cached	21.26 kB
200	GET	stackpath.bo...	bootstrap.min.js	script	js	cached	60.01 kB
101	GET	localhost:4204	ng-cli-ws	polyfills.js:5381 (...)	plain	129 B	0 B
200	POST	localhost:8088	token	polyfills.js:10485 (...)	json	4.29 kB	3.83 kB
	GET	localhost:4204	favicon.ico	FaviconLoader.sys...	vnd.mi...	948 B (raced)	948 B
200	GET	localhost:8088	certs	polyfills.js:10485 (...)	json	3.31 kB	2.92 kB
200	OPTIO...	localhost:8088	userinfo	xhr	plain	532 B	0 B
200	GET	localhost:8088	userinfo	polyfills.js:10485 (...)	json	653 B	214 B
200	POST	localhost:8088	token	polyfills.js:10485 (...)	json	4.29 kB	3.83 kB

|| + 🔍 🔄

AllHTMLCSSJSXHRFontsImages

HeadersCookiesRequestResponseTimingsStack Trace

Filter properties

JSON

```
access_token: "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXZWZlbnQiLCJpdjkiOiJkOGMyMmBmNy02MzZlRTIOWUtYmQxOXBwODgvcVhkbGlzL2ltH3RCicilsmF1ZC16ImFjy291bnQILCJzdWllOil1Yzk2Mjg5MC1kWmWi3LTQ3ZWYtYjAxZC0xYyY2xpZW50Liibm9uY2UiOiIiwTYT1NjE2NTNjNDAA4ZWUwN2lyZmYjaA0OBinWM5MJIT0hwduILNyl...
2hlbg9uaSlSnByZWZlcmlJZF91c2VybmFTZSI6Imxlbi25hcmlvliwiZ2l2ZW5fbmFTZSI6Imxlbi25hcmlvliwiZmFtaWwUBob3RtYWVsLnNbSj9.khdOdq-h1aoQEpoj58BJCU41D5T_QGXmHeqySiEfErObtfGxAphKj4qe0FuaruOgWwIPbIA1yg_DP5g4vqz2sxZZu1250-7Rgo0zMk7riLD_midIdNgkf6K3CrYMwk_p-q6r7OJLY7FNbpwkuYkrU4ivIXoslqksSMRS4KwHwCvl3PIPOASIJNPm4Pkvf2IOjrTVfo-VrcPeoy07drPH1QA8d-7xrCCYPk8f94IXbUVGtykt4p81dmm8JB3IAQHjoipaAhPZ7FJJ8CXzhVRUr7rPCDIgQHH8S1n41twGjpbge9GMQ"
```

expires_in: 60
refresh_expires_in: 0
refresh_token: "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXZWZlbnQiLCJpdjkiOiJkOGMyMmBmNy02MzZlRTIOWUtYmQxOXBwODgvcVhkbGlzL2ltH3RCicilsmF1ZC16ImFjy291bnQILCJzdWllOil1Yzk2Mjg5MC1kWmWi3LTQ3ZWYtYjAxZC0xYyY2xpZW50Liibm9uY2UiOiIiwTYT1NjE2NTNjNDAA4ZWUwN2lyZmYjaA0OBinWM5MJIT0hwduILNyl...
GluZV9hy2Nlc3MgcHJvZmlsZSBibWFpbiClSnNpZC16IjdINTMwMzdmLTlYTOWUtNGl5ZC1hNGlzLWZmNWWE3ODdG6M1gtUmkmIU9uGeY"

token_type: "Bearer"
id_token: "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXZWZlbnQiLCJpdjkiOiJkOGMyMmBmNy02MzZlRTIOWUtYmQxOXBwODgvcVhkbGlzL2ltH3RCicilsmF1ZC16ImFjy291bnQILCJzdWllOil1Yzk2Mjg5MC1kWmWi3LTQ3ZWYtYjAxZC0xYyY2xpZW50Liibm9uY2UiOiIiwTYT1NjE2NTNjNDAA4ZWUwN2lyZmYjaA0OBinWM5MJIT0hwduILNyl...
2hlbg9uaSlSnByZWZlcmlJZF91c2VybmFTZSI6Imxlbi25hcmlvliwiZ2l2ZW5fbmFTZSI6Imxlbi25hcmlvliwiZmFtaWw5X2p..."

Name ?

code-flow-client

Description ?

Always display in UI ?



On

Access settings

Root URL ?

Home URL ?

Valid redirect URIs ?



http://localhost:4204



+ Add valid redirect URIs

Valid post logout
redirect URIs ?

http://localhost:4204/unauthorized



http://localhost:4204



+ Add valid post logout redirect URIs

Web origins ?

http://localhost:4204



+ Add web origins

Consideration on code flow

- The redirection after the login contains a unique / one-use code
- This code is used to request the token via a POST request using and Ajax call
- CORS must be supported and correctly configured
- Token is not compromised
- It is the preferred option today against implicit flow

There's something more

- Code flow is the preferred option over implicit flow
- There's an extension called PKCE that is recommended
- User Authorization code flow with PKCE always you can

Open ID Connect



OpenID Connect (OIDC) is an [authentication](#) layer on top of [OAuth 2.0](#), an [authorization](#) framework.^[1] The standard is controlled by the [OpenID Foundation](#).

OpenID Connect is a simple identity layer on top of the [OAuth 2.0](#) protocol, which allows [computing clients](#) to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and [REST-like](#) manner. In technical terms, OpenID Connect specifies a [RESTful HTTP API](#), using [JSON](#) as a data format.

Open ID Connect

- Is an extension of OAuth2
- Adds some pre-defined scopes to ask for data
 - open_id
 - user_profile
 - email
- Adds an additional token with authentication information (id_token)
- All the additional information is received in the form of claims
- Discovery (metadata) endpoint
- The consent screen
- User profile endpoint

localhost:8088/realms/master/.well-known/openid-configuration

Name	X	Headers	Preview	Response	Initiator	Timing	Cookies
openid-configuration				<pre>1 { - "issuer": "http://localhost:8088/realms/master", - "authorization_endpoint": "http://localhost:8088/realms/master/protocol/openid-connect/auth", - "token_endpoint": "http://localhost:8088/realms/master/protocol/openid-connect/token", - "introspection_endpoint": "http://localhost:8088/realms/master/protocol/openid-connect/token/introspect", - "userinfo_endpoint": "http://localhost:8088/realms/master/protocol/openid-connect/userinfo", - "end_session_endpoint": "http://localhost:8088/realms/master/protocol/openid-connect/logout", - "frontchannel_logout_session_supported": true, - "frontchannel_logout_supported": true, - "jwks_uri": "http://localhost:8088/realms/master/protocol/openid-connect/certs", - "check_session_iframe": "http://localhost:8088/realms/master/protocol/openid-connect/login-status-iframe.html", - "grant_types_supported": [- "authorization_code", - "implicit", - "refresh_token", - "password", - "client_credentials", - "urn:openid:params:grant-type:ciba", - "urn:ietf:params:oauth:grant-type:device_code" -], - "acr_values_supported": [- "0", - "1" -], - "response_types_supported": [- "code", - "none", - "id_token", - "token", - "id_token token", - "code id_token", - "code token", - "code id_token token" -], - "subject_types_supported": [- "public", - "pairwise" -], - "id_token_signed_response_types_supported": [</pre>			

Path	X	Headers	Payload	Preview	Response	Initiator	Timing
/realms/master/.well-known/openid-configuration	1	-	-	-	{ "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2N... "expires_in": 60, "refresh_expires_in": 0, "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2N... "token_type": "Bearer", "id_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIA...", "not-before-policy": 0, "session_state": "e71a39f9-3dc0-441b-9e88-7ad940f8cc1b", "scope": "openid offline_access profile email" }	-	-
/realms/master/protocol/openid-connect/auth	-	-	-	-	-	-	-
/resources/yczrw/common/keycloak/node_modules...	-	-	-	-	-	-	-
/resources/yczrw/common/keycloak/node_modules...	-	-	-	-	-	-	-
/resources/yczrw/common/keycloak/node_modules...	-	-	-	-	-	-	-
/resources/yczrw/common/keycloak/lib/pficon/pfic...	-	-	-	-	-	-	-
/resources/yczrw/login/keycloak/css/login.css	-	-	-	-	-	-	-
/resources/yczrw/login/keycloak/js/passwordVisibili...	-	-	-	-	-	-	-
/resources/yczrw/login/keycloak/js/authChecker.js	-	-	-	-	-	-	-
/resources/yczrw/login/keycloak/img/keycloak-log...	-	-	-	-	-	-	-
/resources/yczrw/common/keycloak/node_modules...	-	-	-	-	-	-	-
/realms/master/login-actions/authenticate	-	-	-	-	-	-	-
/	-	-	-	-	-	-	-
/bootstrap/4.4.1/css/bootstrap.min.css	-	-	-	-	-	-	-
/jquery-3.4.1.slim.min.js	-	-	-	-	-	-	-
/npm/popper.js@1.16.0/dist/umd/popper.min.js	-	-	-	-	-	-	-
/bootstrap/4.4.1/js/bootstrap.min.js	-	-	-	-	-	-	-
/styles.css	-	-	-	-	-	-	-
/runtime.js	-	-	-	-	-	-	-
/polyfills.js	-	-	-	-	-	-	-
/vendor.js	-	-	-	-	-	-	-
/main.js	-	-	-	-	-	-	-
/styles.js	-	-	-	-	-	-	-
/realms/master/protocol/openid-connect/token	-	-	-	-	-	-	-

Authorize Sessionize.com to use your account?

Authorize app

Cancel

This application will be able to:

- Read Tweets from your timeline.
- See who you follow.
- See your email address.

Will not be able to:

- Follow new people.
- Update your profile.
- Post Tweets for you.
- Access your direct messages.
- See your Twitter password.



Sessionize.com

sessionize.com

Manage your schedule and sessions with ease

[Privacy Policy](#)

[Terms and Conditions](#)

Path

- /realms/master/protocol/openid-connect/auth
- /resources/yczrw/common/keycloak/node_modu...
- /resources/yczrw/common/keycloak/node_modu...
- /resources/yczrw/common/keycloak/node_modu...
- /resources/yczrw/common/keycloak/lib/pficon/p...
- /resources/yczrw/login/keycloak/css/login.css
- /resources/yczrw/login/keycloak/js/passwordVisi...
- /resources/yczrw/login/keycloak/js/authChecker.js
- /resources/yczrw/login/keycloak/img/keycloak-l...
- /resources/yczrw/common/keycloak/node_modu...
- /realms/master/login-actions/authenticate
- /
- /bootstrap/4.4.1/css/bootstrap.min.css
- /jquery-3.4.1.slim.min.js
- /npm/popper.js@1.16.0/dist/umd/popper.min.js
- /bootstrap/4.4.1/js/bootstrap.min.js
- /styles.css
- /runtime.js
- /polyfills.js
- /vendor.js
- /main.js
- /styles.js
- /realms/master/protocol/openid-connect/token
- /ng-cli-ws
- /realms/master/protocol/openid-connect/certs
- /realms/master/protocol/openid-connect/userinfo
- /realms/master/protocol/openid-connect/token

X Headers Preview Response Initiator Timing

```
1 {  
  "sub": "5c962890-d1b7-47ef-b01d-1c0c81a5e5d4",  
  "email_verified": false,  
  "name": "Leonardo Micheloni",  
  "preferred_username": "leonardo",  
  "given_name": "Leonardo",  
  "family_name": "Micheloni",  
  "email": "leomicheloni@hotmail.com"  
}
```

What we haven't seen today

- PKCE
- Device code flow
- Refresh tokens
- A looot of details

The background features a complex, abstract design. On the left, a solid purple rectangle is partially visible. The central area is white, containing the text 'Thank you!'. To the right, a large, irregular white silhouette of a person's head and shoulders is positioned against a vibrant, abstract background of purple and pink geometric patterns, including lines and circles, creating a sense of depth and movement.

Thank you!

- <https://github.com/leomicheloni/dotnet-oauth-for-mere-mortals>
- <https://www.oauth.com/playground>
- <https://www.youtube.com/watch?v=CHzERullHe8>