Oauth

Contents

[Khái niệm 2](#_Toc72622942)

[Oauth và ApIs 2](#_Toc72622943)

[Scop and consent (phạm vi và sự đồng ý) 3](#_Toc72622944)

[Oauth Actor 4](#_Toc72622945)

[Oauth Tokens 6](#_Toc72622946)

[Front back Channel 7](#_Toc72622947)

[Giả Xác thực Với Oauth 2.0 Dùng OpenID 9](#_Toc72622948)

[Custom Claims in the Token 11](#_Toc72622949)

[Cấu hình trên app keyloak 11](#_Toc72622950)

[Cấu hình bằng file.json lúc start app authorization server 17](#_Toc72622951)

[Configuration to Add/Remove/Rename Claims Trên Resouce Server 19](#_Toc72622952)

[GetToken từ Controller 19](#_Toc72622953)

[Configuration to Add/Remove/Rename Claims 20](#_Toc72622954)

[Ví Dụ 1 Cơ bản 20](#_Toc72622955)

# Khái niệm

Oauth không phải là 1 Api hoặc 1 service . Nó là 1 chuẩn Open để xác thực và bất kì ai cũng có thể triển khai nó.

Cụ thể hơn, Oauth là một chuẩn cho các app có thể được sử dụng để cung cấp cho các client app với “secure delegate access”. Oauth làm việc trên Https và xác thực các thiết bị, Các Api, các server và các ứng dụng với access token hơn là sử dụng chứng chỉ (credential).

Có 2 phiên bản của Oauth 1.a và 2.0 . Những kĩ thuật của 2 version này khác nhau hoàn toàn và không được sử dụng với nhau, nó thì cũng ko tương thích ngược luôn.

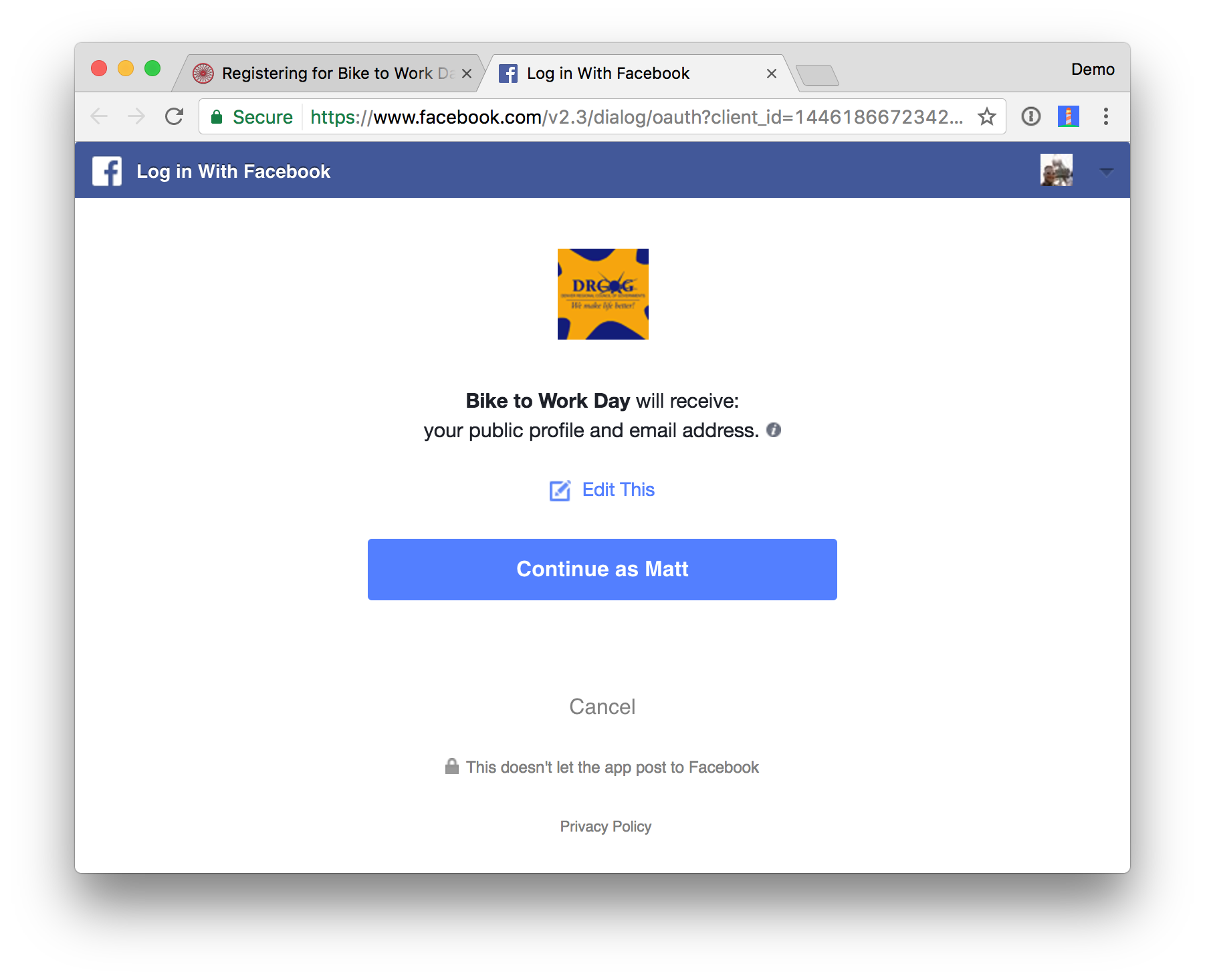
Vậy cái nào được sử dụng phổ biến? Ngày nay Oauth 2 được sử dụng rộng rãi . và ngay từ bây giờ bất kì nơi đâu tôi nói “Oauth” là đang nói về Oauth 2.0.

## Oauth và ApIs

Có Sự thây đổi rất nhiều về việc build các APIs. Bây giờ hầu hết các develop đã chuyển sang Rest và stateless Apis . Tóm lại Rest là sử dụng giao thức Http chuyển Json trên network.

Các develop build nhiều Apis. Các API Economy là thông dụng và bạn có thể nghe nó ở bất cứ nơi đâu . các Company cần phải bảo vệ các Rest Apis theo cách cho phép nhiều thiết bị truy cập vào.

Đây à Oauth



Oauth là một ủy quyền xác thực framwork cho Rest/apis. Nó cho phép các app đạt được các quyền (scope) truy cập data của bạn mà không cần phải có password. Nó tách việc xác thực và hỗ trợ nhiều use . Hỗ trợ server to server , brower-based apps, mobile/native apps và consoles/TVs.

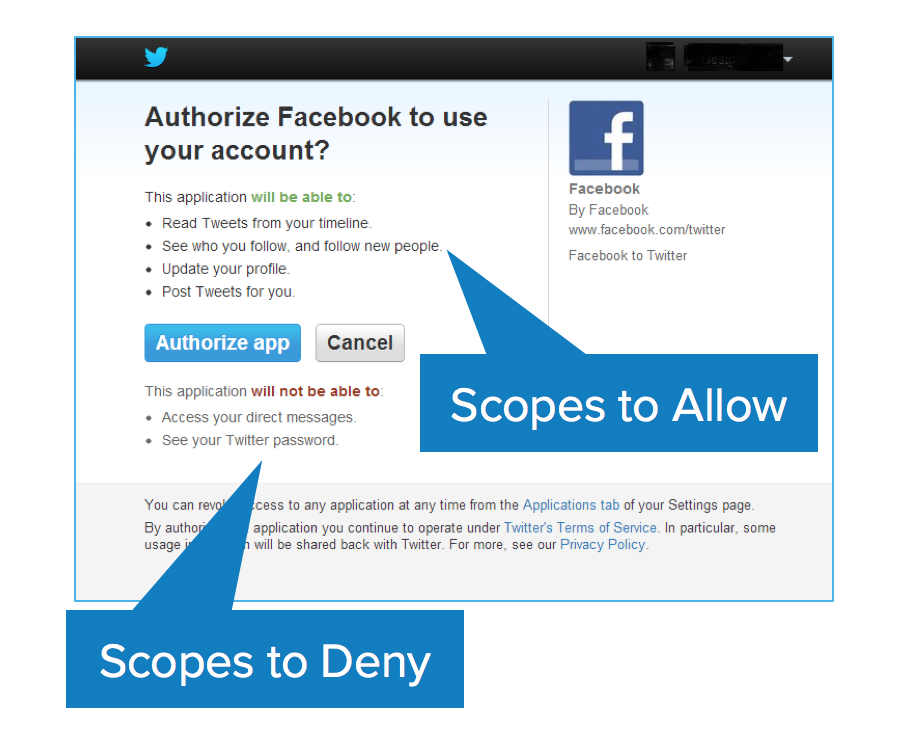
Các thành phần Chính

* Scop and consent (phạm vi và sự đồng ý)
* Actors (hành động)
* Client
* Token
* Authorization Server
* Flows

## Scop and consent (phạm vi và sự đồng ý)

Scope là những gì bạn thấy xác thực trên màn hình khi mà 1 app yêu cầu Quyền hạn. Chúng là các gói quyền được yêu cầu khi mà client request 1 token. Những quyền này được code bởi các nhà phát triển khi viết code.

Bạn cũng có thể vào trang dashboard để xem ứng dụng nào bạn đã cấp quyền truy cập vào và thu hồi sự đồng ý (revoke consent)



## Oauth Actor

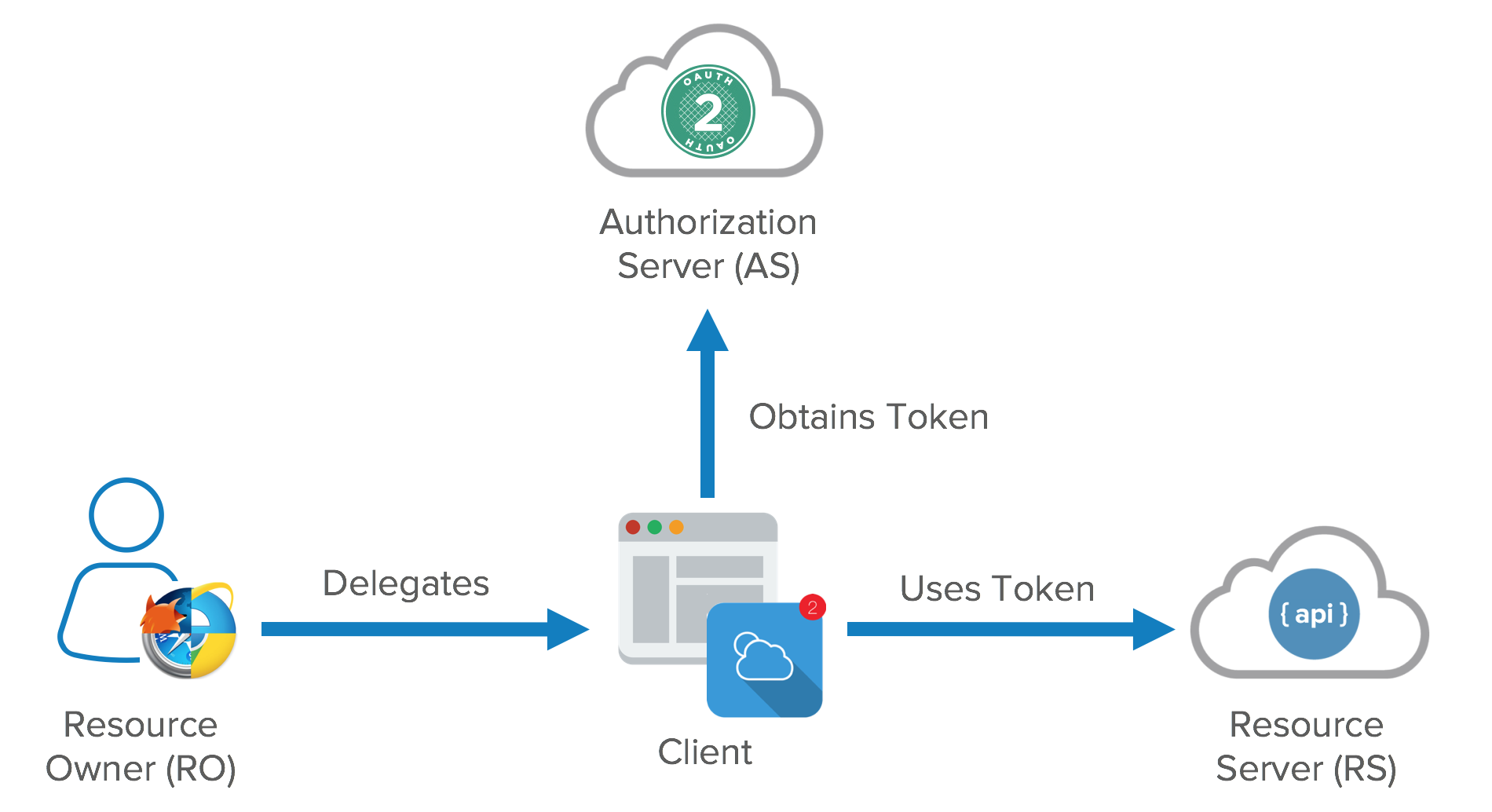
Các actors trong Oauth như sau

Resource Owner: Sở hưu data bên trong resource Owner. Vd: Tôi có resouce owner của tôi là Facebook profile.

Resource Server: Api nơi lưu trữ data application muôn truy cập

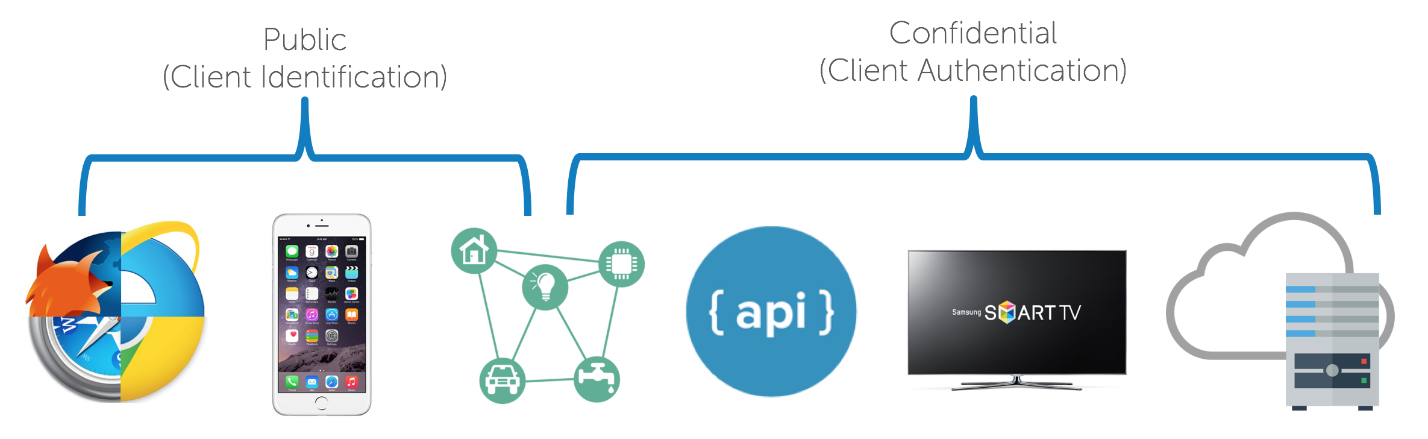
Client : Là ứng dụng bạn muốn truy cập vào

Authorization Server: Công cụ chính của Oauth (vd keyloak)



**Resource Owner** là vai trò nó có thể thay đổi với các chứng chỉ khác nhau có thể là enduser, hoặc là company.

**Clients (Fontend)**: có thể là public hoặc bí mât (sử dụng secret key) . Nó có sự khác biệt khá lớn. Bí mật (confidential) clients có thể được tin tưởng để lưu secret key. Họ không chạy trên desktop hoặc thông qua app store. Chúng ta không thể đảo ngược chúng để get secret key. Họ cho chúng run tại nơi được bảo về enduser không thể truy cập được chúng.



## Oauth Tokens

Access token là token mà client dùng để sử dụng để truy cập Resouce Server (API) . Token có thời gian sống theo phút giờ hoặc ngày. Chúng ta có thể get token bằng 2 cách dùng public hoặc confidential như đã nêu trên .

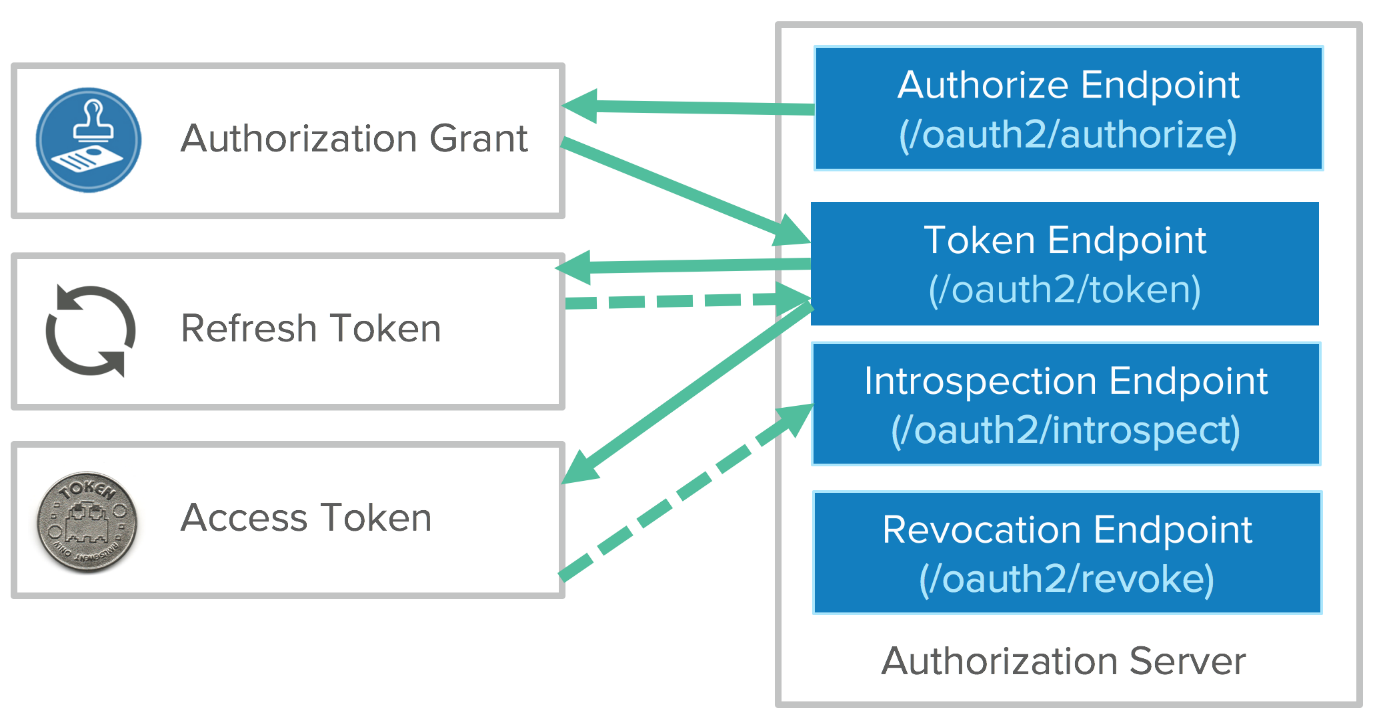
Còn 1 token khác đó là Refresh token. Cũng có thời gian tồn tại tương ứng với access-token tùy từng ứng dụng Oauth quy định. Như keyloak là chúng có thời gian sống giống nhau.



Ví dụ trên là 5 tiếng là 1800 giây. Dùng refresh token để get lại 1 access token mới khi nó đã expried hêt hạn .

Có thể lưu mọi thứ trên payload của token bằng các claim của chúng

Tokens được lấy từ endpoint trên Authorization Server. Hai main endpoint chính là authorize endpoint và token endpoint. Chúng được tách biệt cho các trường hợp sử dụng khác nhau.



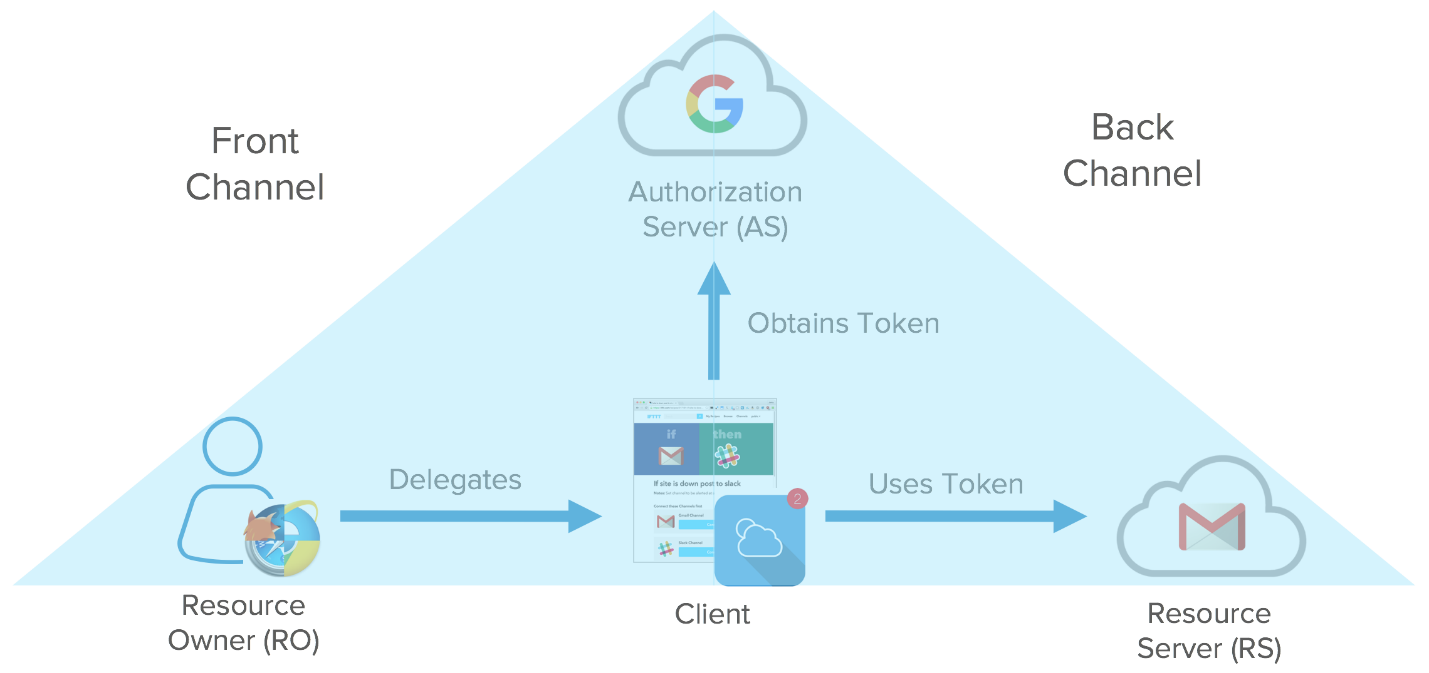
Bạn có thể sử dụng access token để truy cập vào Apis. Khi nó hết hạn, bạn sẽ quay lại token endpoint với refresh token để get mới 1 token access.

## Front back Channel

Để thực hiện được các hành động xác thực và cung cấp token thì xảy ra trên 2 chanel . font channel và back channel.

The font channel là những gì xảy ra trên browser. The brower chuyển hướng để user đi đến authorization server, the user nhận được sự chấp thuận. Sau khi user mang authorization grant về client thì client không cần dùng đến browser nữa trong qua trình yêu cầu cấp token.

Có nghĩa là token được tiêu thụ bởi client application nên nó có thể truy cập resources trên chính bản thân nó (kiểu thư gọi ajax vậy) . Chúng ta gọi back channel . the backchannel được gọi trực tiếp từ 1 http từ client đến resource server để trao đổi authorization grant cho token. Những channel được sử dụng vào các flow khác nhau dựa vào thiết bị mà bạn đang sử dụng



Cho ví dụ : Front channel flow nơi bạn xác thực thông qua user agent :

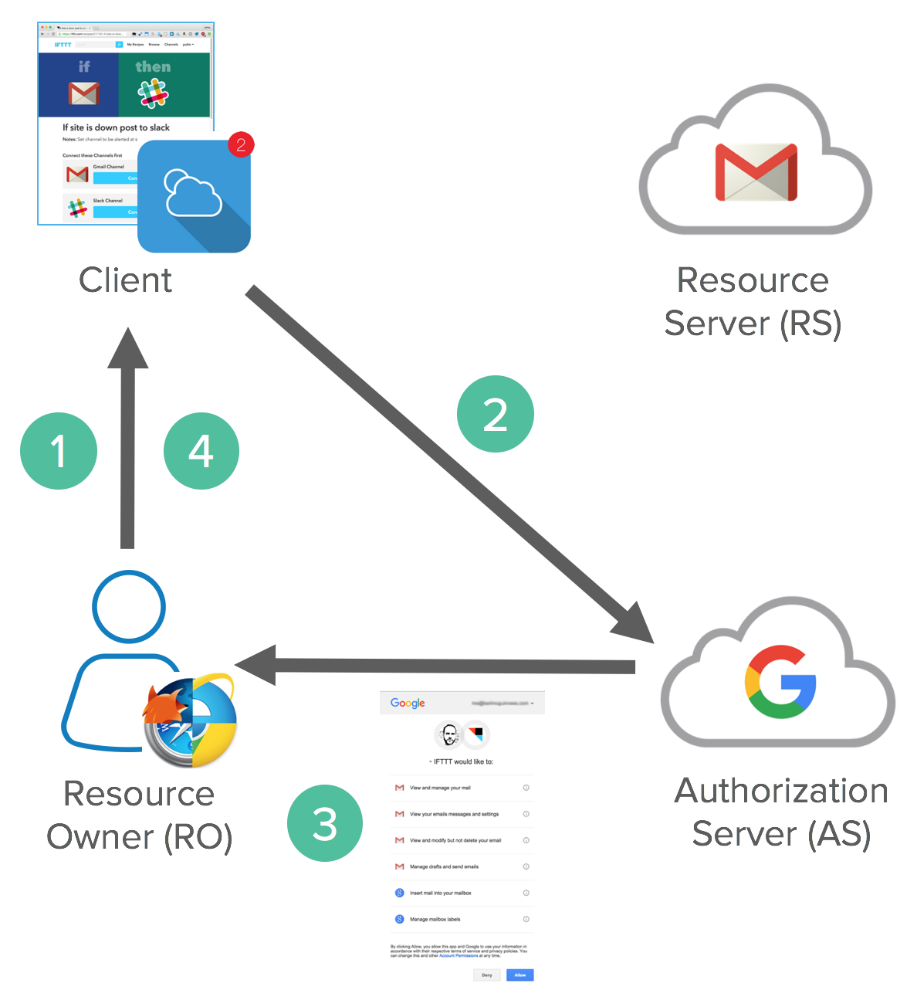
1 Resource Owner bắt đầu flow access đến resouce đang được bảo vệ

2 Client sends authorization request với các quyền scope mong muốn thông qua browser chuyển hướng đến Authorization Endpoint trên Authorization Server.

3 Authorization Server trả về 1 họp thoại chấp thuận “Do you allow this application to have access to these scopes ?” “Bạn có cho phép ứng dụng này có quyền truy cập vào những phạm vi này không? ”

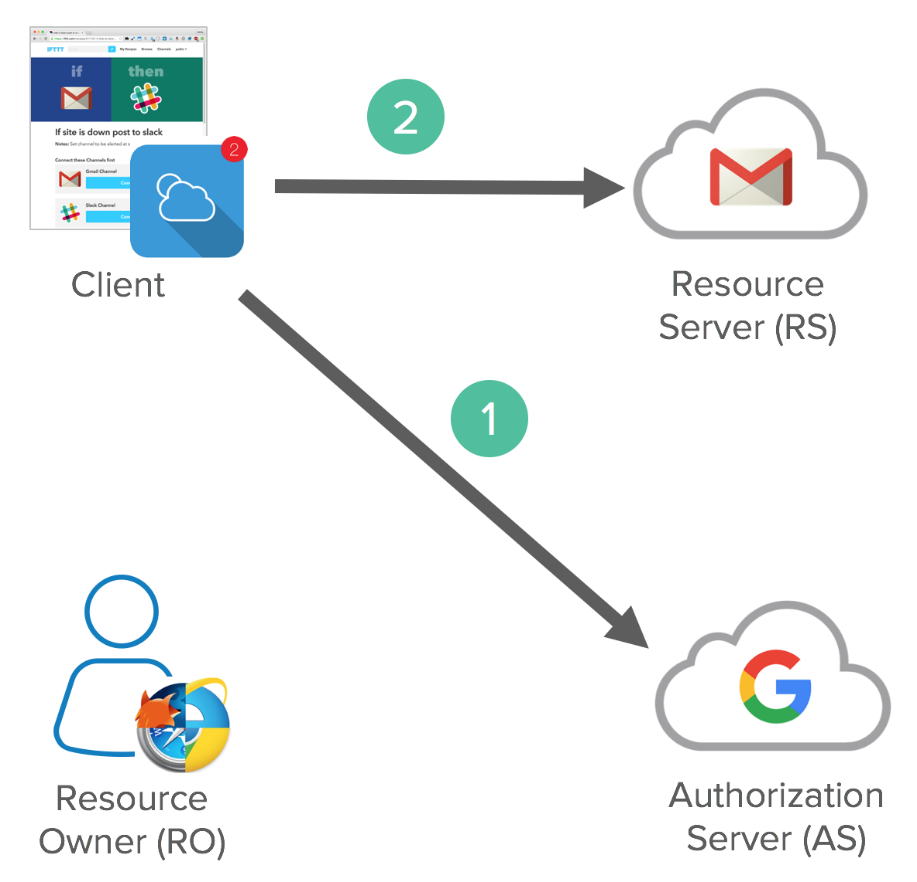
Dĩ nhiên bạn phải xác thực với application (client) này, nếu mà bạn chưa xác thực với Resouce server của bạn , nó sẽ bảo bạn login. Nếu bạn đã xác thực có trong cached session cookie, bản chỉ nhìn vào họp thoại yêu cầu chấp thuận các scope quyền sẽ view lên và chấp thuận nó. Có nghĩa là chưa login sẽ login, nếu login từ trước rồi sẽ hiển thị hộp thoại view các quyền scope để bạn nhấn agree chấp nhận applicaton này sử dụng các quyền này lên Resouce server của bạn.

4 The authorization grant được truyền về application thông qua điều hướng trên brower. Đó là tất cả những gì trên Front channel.



Sau khi Front channel hoàn thành, Back channel xảy ra , trao đổi the authorization code cho 1 access token.

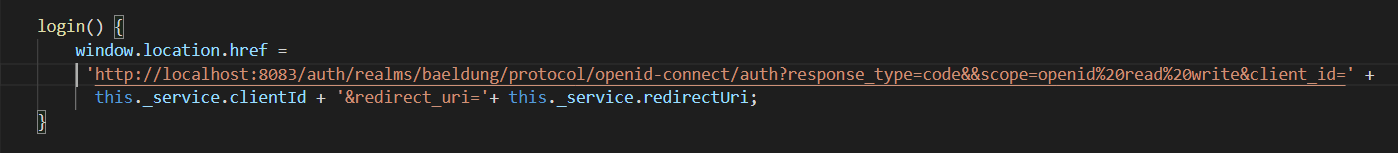
The Client application sends an access token request to the token endpoint on the Authorization Server with confidential client credentials and client id. This process exchanges an Authorization Code Grant for an Access Token and (optionally) a Refresh Token. Client accesses a protected resource with Access Token.



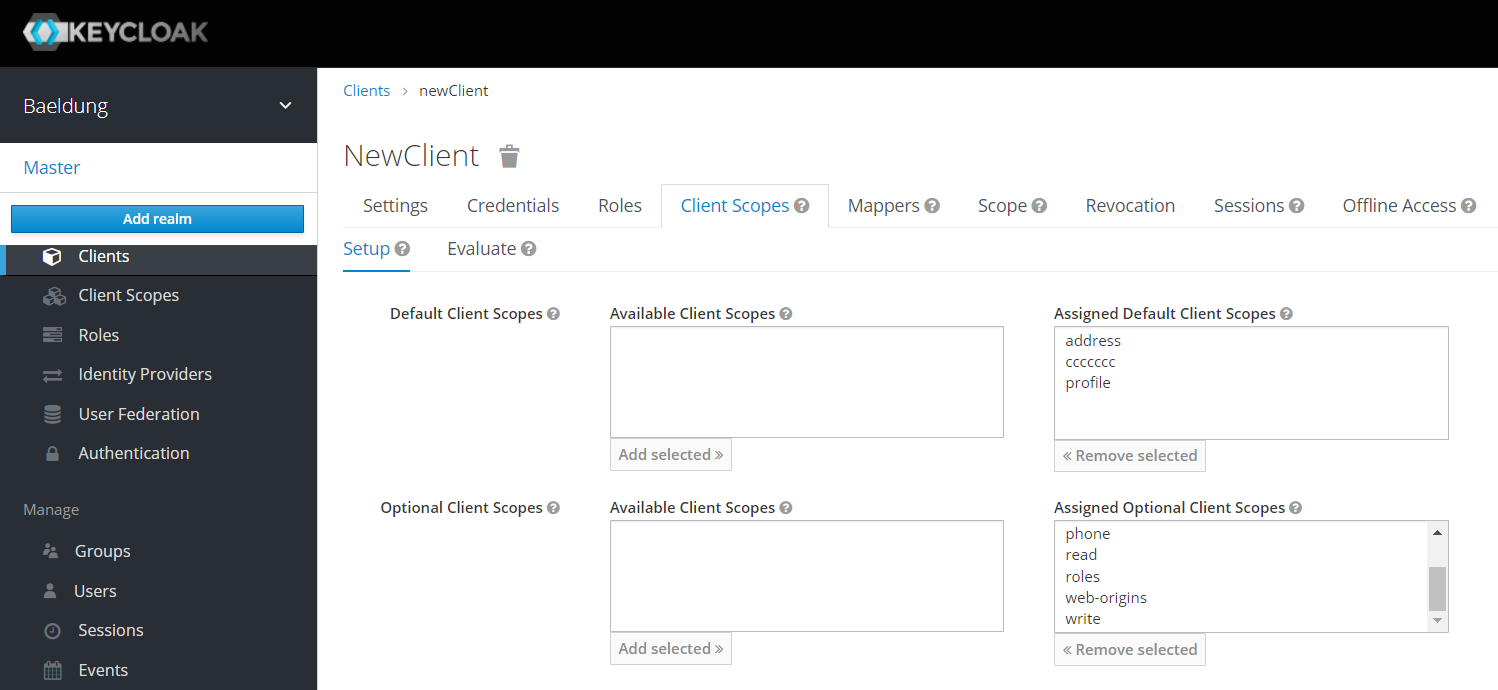
## Giả Xác thực Với Oauth 2.0 Dùng OpenID

Login với Oauth đã trở nên phổ biến bới Facebook và Twitter. Trong cái flow này, một client truy cập /me endpoint cùng với 1 access token. Tất cả chỉ là the client có truy cập resouce với 1 token. Nhiều người đã chế tạo ra endpoint fake lấy thông tin người khác với một access token . Không có chuẩn nào để get thông tin của user. Để giải quyết đều đó là dùng OpenID Connect. Nó sẽ tạo ra 1 id\_Token cho client và một UserInfo endpoint để lấy user attribute. Khác với Saml , OIDC cung cấp 1 chuẩn set scope và claims cho việc định danh ví dụ: profile, email, address, and phone.

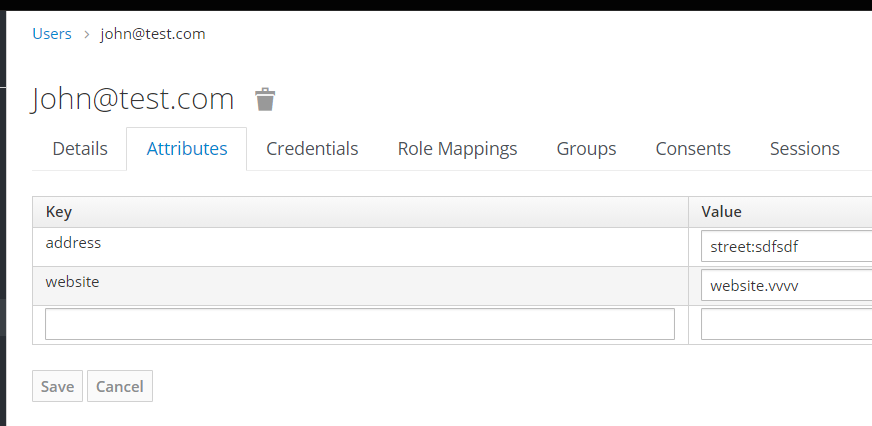
Set scope lúc yêu cầu page login:



Yêu cầu scope option có trong cài đặt tự chọn của clients: openid read write

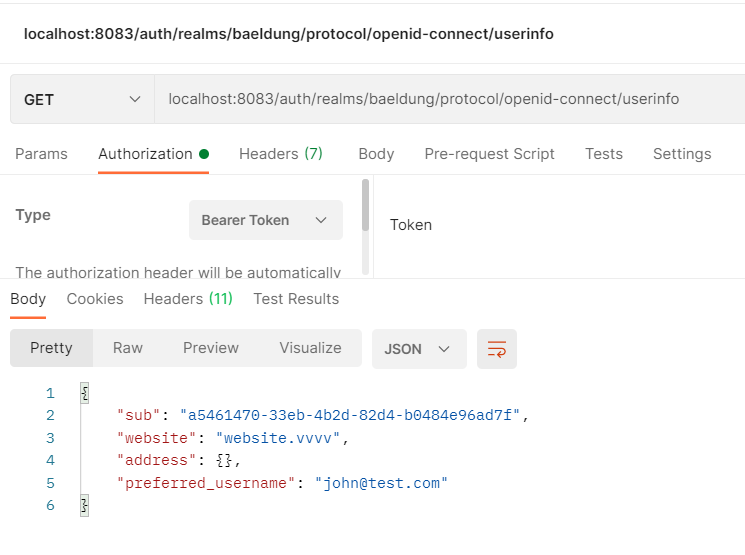


Set attribute cho user



Get thông tin user

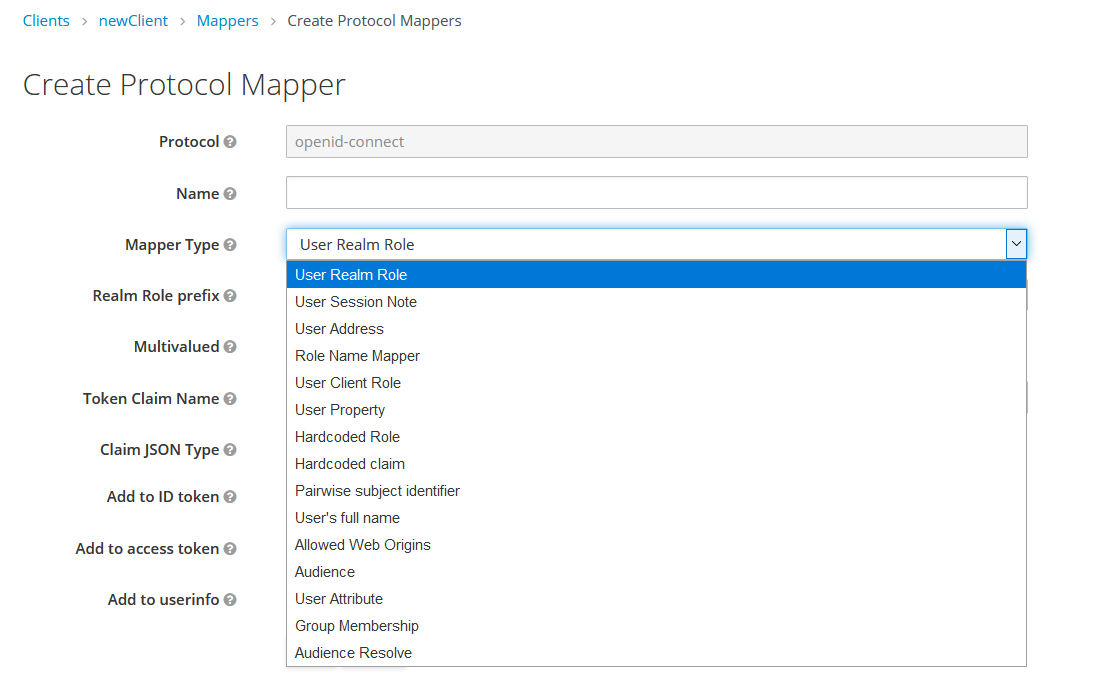
**Get:** localhost:8083/auth/realms/baeldung/protocol/openid-connect/userinfo



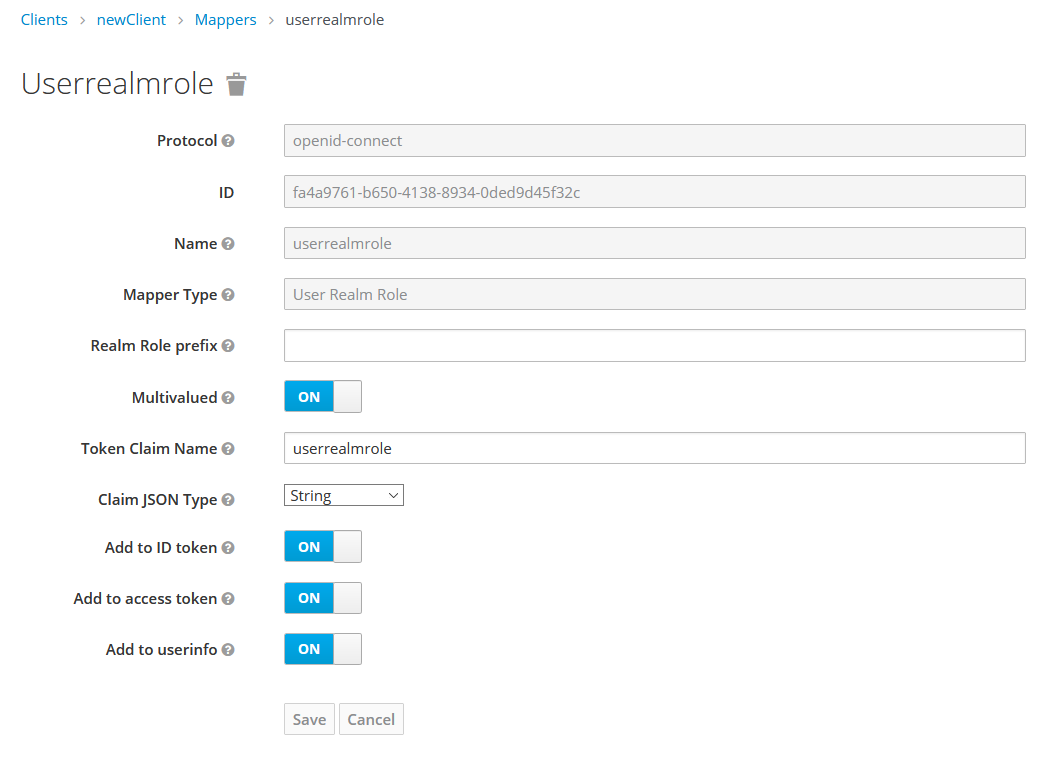
# Custom Claims in the Token

## Cấu hình trên app keyloak

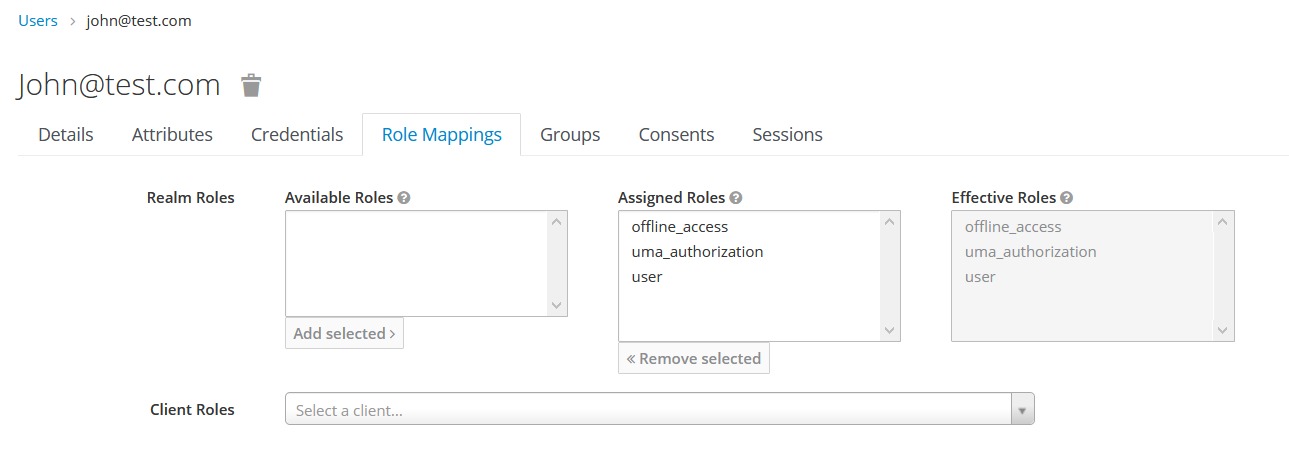
Nếu muốn thêm 1 claim và access token ta tạo ra 1 mapper ở menu Clients để đưa vào access token



Ví dụ thêm User Realm Role là get các role được chỉ định của user mà application đang sử dụng “john@test.com”



Nó sẽ đưa role của ở user vào access token



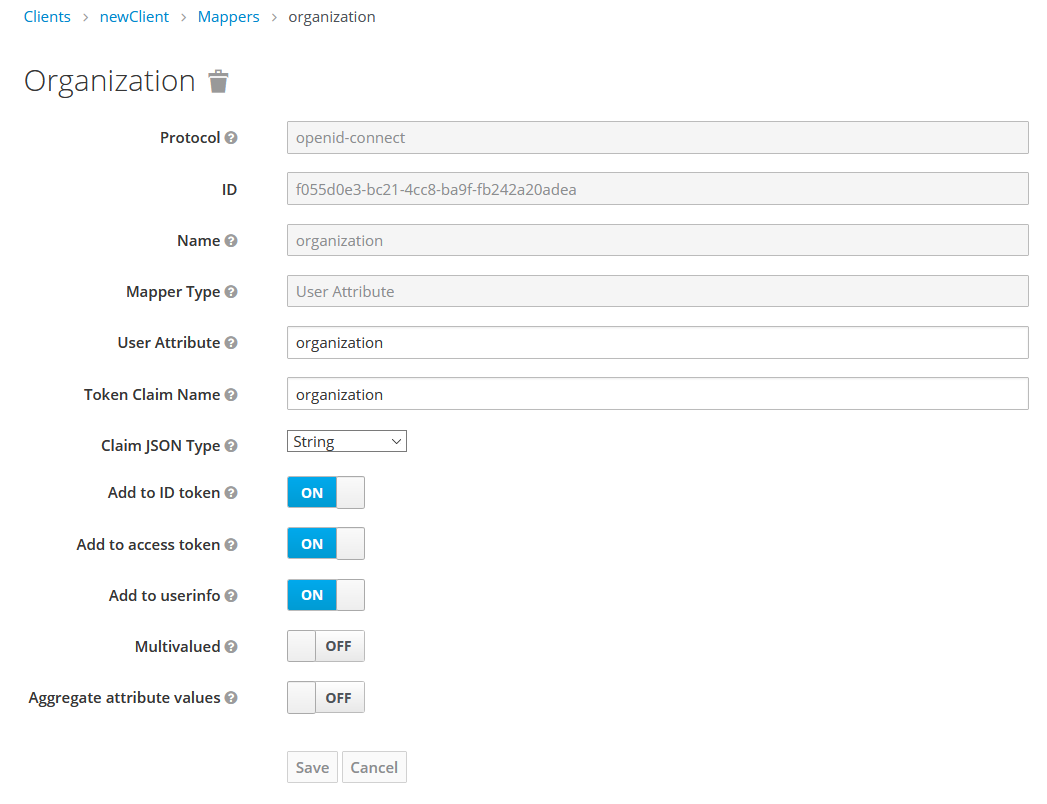
Graphical user interface, text, application

Description automatically generated

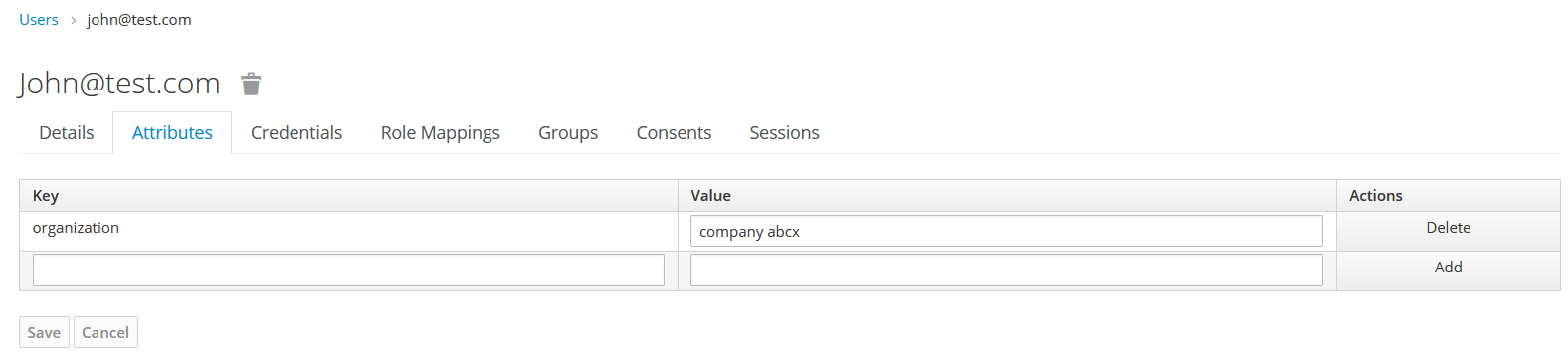
Còn nếu muốn đưa vào User attribute thì tạo ra Mappers Attribute mới trong Menu Clients hoặc là sử dụng các Mapper có sẵn trong keyloak Vd: mail, address, nicknam,...

Vd ta tạo mới 1 mapper type user attribute và sử dụng 1 cái Mapper có sẵn để đưa vào access token

Tạo mapper mới



Thêm Attribute mới thêm vào Attribute của user đang login trên Application client (không phải user admin logint trên keyloak nhé)



Sử dụng Mapper User Property có sẵn là full name để get first name và last name user đang login

Graphical user interface, text, application, email

Description automatically generated

Xong setting trên Clients để đưa vào trong các mapper vào trong newClient để trả về cho app client access token chứa các mapper này

Chọn 1 để ta add User mapper có sẵn là full name.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

## Cấu hình bằng file.json lúc start app authorization server

Ta có thể cấu hình sẵn trong App keyloak rồi export ra file.json đưa vào Spring boot.

Lưu ý là keyloak không export được users nên nếu có thể add user từ Code của server Authorization luôn nhưng nhớ add user sau khi đã cài đặt Realm nếu không nó sẽ tạo user trong realm admin

Ta cũng có thể thêm 2 mapper này vào mapper của newClient trong Clients:

Text

Description automatically generated

"protocolMappers": [

{

"id": "6c10b4d2-4f69-4229-b62f-380919b38d7a",

"name": "full name",

"protocol": "openid-connect",

"protocolMapper": "oidc-full-name-mapper",

"consentRequired": false,

"config": {

"id.token.claim": "true",

"access.token.claim": "true",

"userinfo.token.claim": "true"

}

},

{

"id": "f055d0e3-bc21-4cc8-ba9f-fb242a20adea",

"name": "organization",

"protocol": "openid-connect",

"protocolMapper": "oidc-usermodel-attribute-mapper",

"consentRequired": false,

"config": {

"userinfo.token.claim": "true",

"user.attribute": "organization",

"id.token.claim": "true",

"access.token.claim": "true",

"claim.name": "organization",

"jsonType.label": "String"

}

}

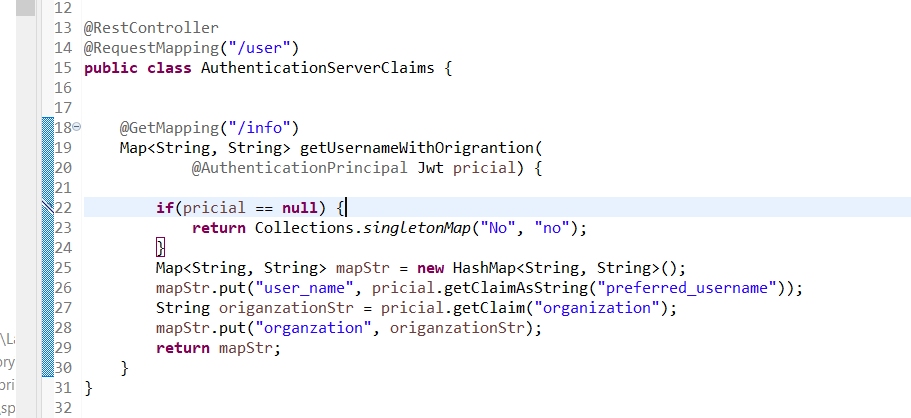
],

# Configuration to Add/Remove/Rename Claims Trên Resouce Server

## GetToken từ Controller

Có 2 đều lưu ý là mới chỉnh lại antMatcher("/\*\*") như thế này nó mới bao gồm hết tất cả các request nếu không thì security sẽ từ chối request cứ báo là Cors sai (lỗi thật sự là không có filter security nào)

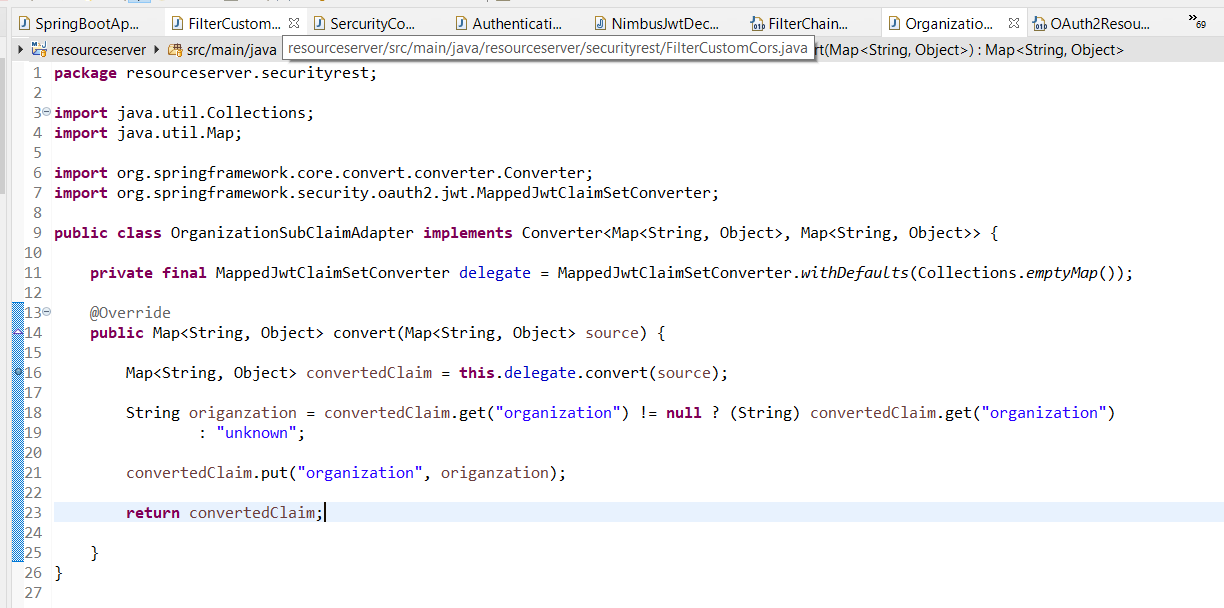
Thứ 2 là có thể xảy ra exception expried token .



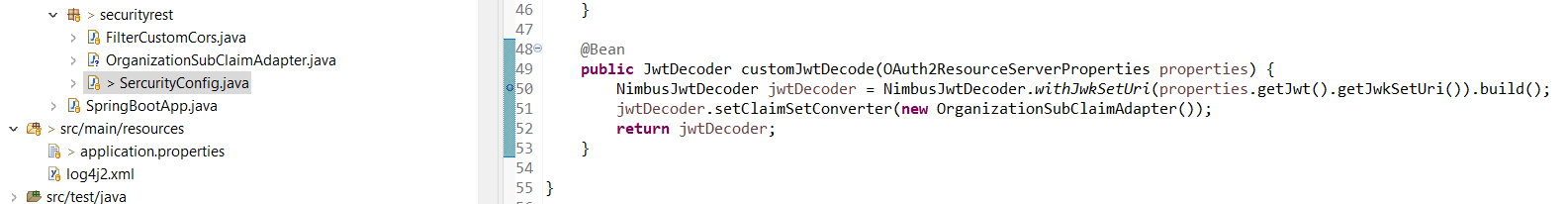
## Configuration to Add/Remove/Rename Claims

Ta chỉ cần custom lại hàm covert của JwtDecoder là ta có thể chỉnh sửa thêm xóa vv

Implements interface Convert của spring framwork



Tạo ra Bean trong config sercutiry để nhúng convert vào JwtDecoder.



# Ví Dụ 1 Cơ bản

Tổng quan:

Client: Dùng angular 12 làm FrontEnd để gọi CRUD

Resource Server : Dùng spring boot + RestContoller + Customize Cors.

Authorization Server: Dùng spring boot + Keyloak + cấu hình file .json