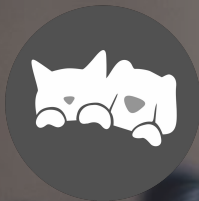


# Oauth2

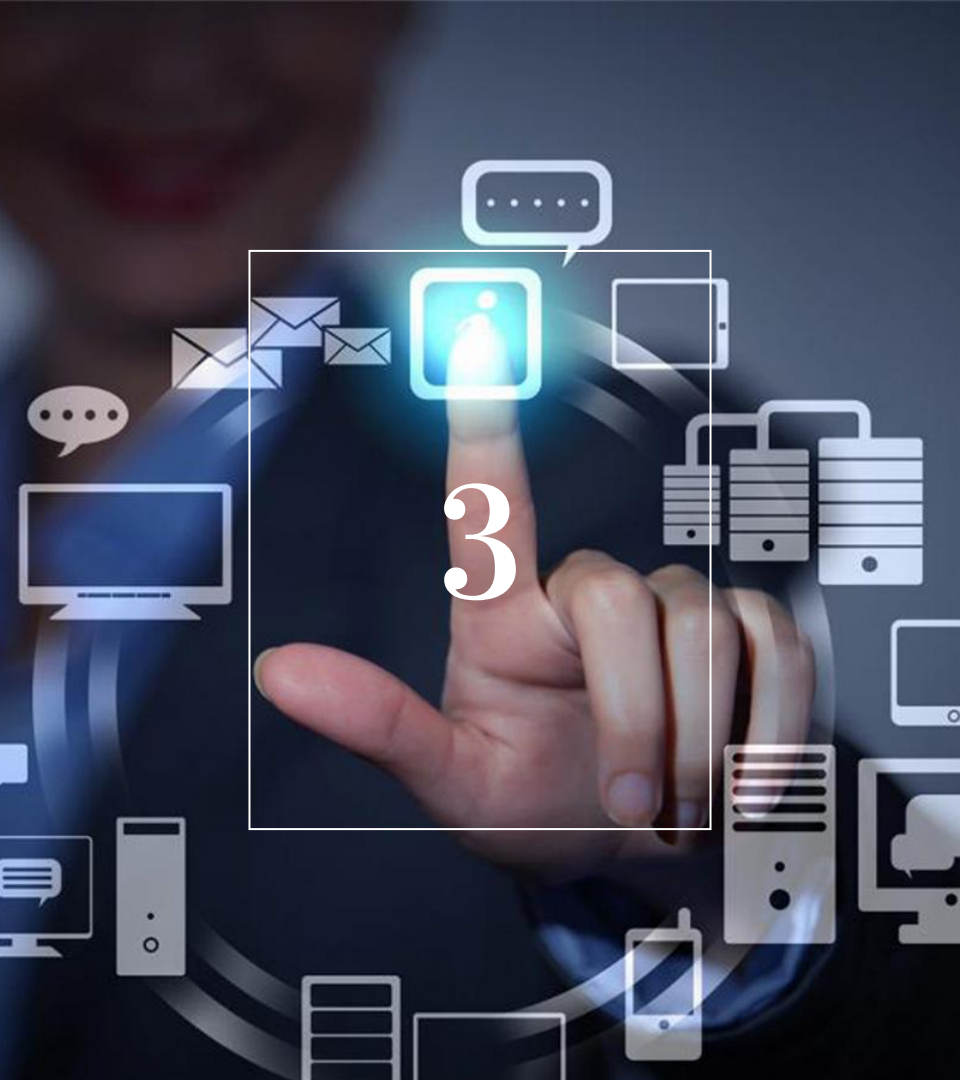




**Karl MARQUES BERNARDO**

karl@kmarques.dev  
[ESGI] [DEVSDK]

<https://github.com/kmarques>

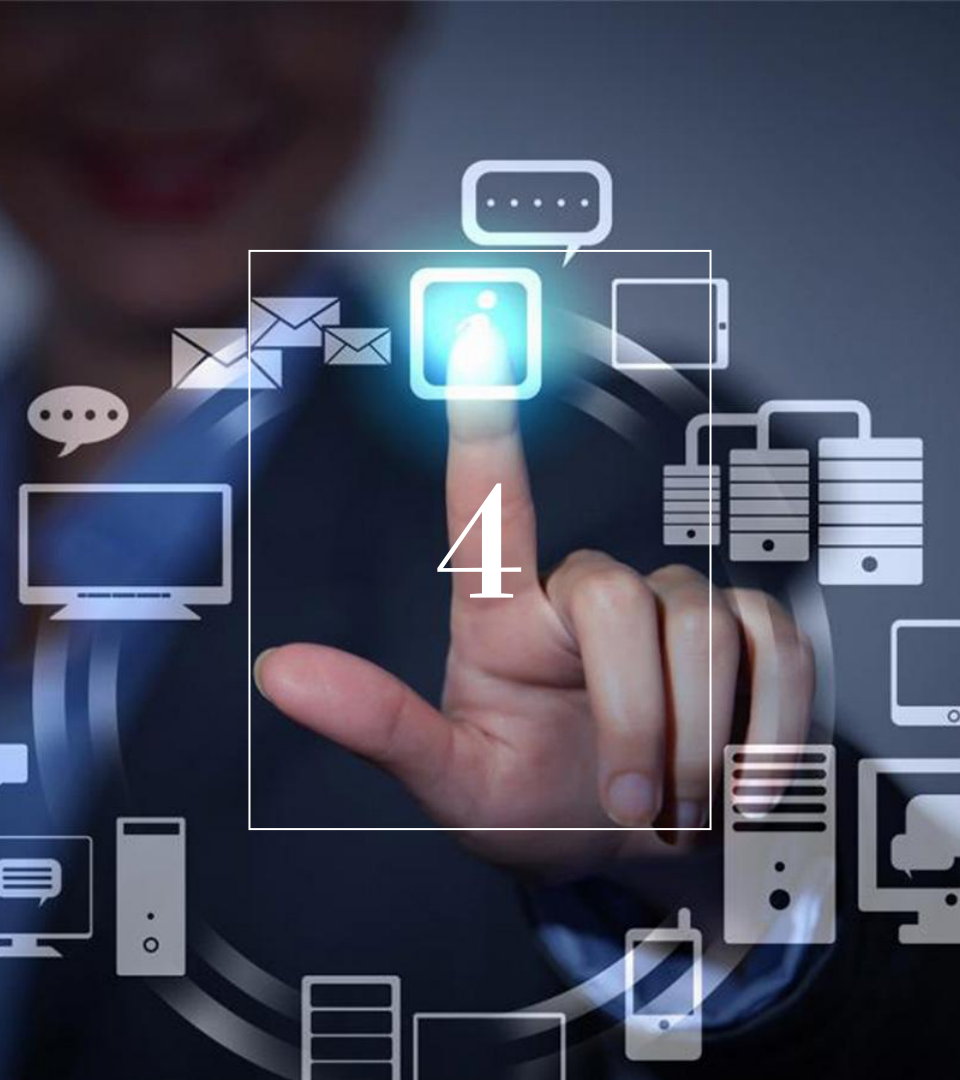


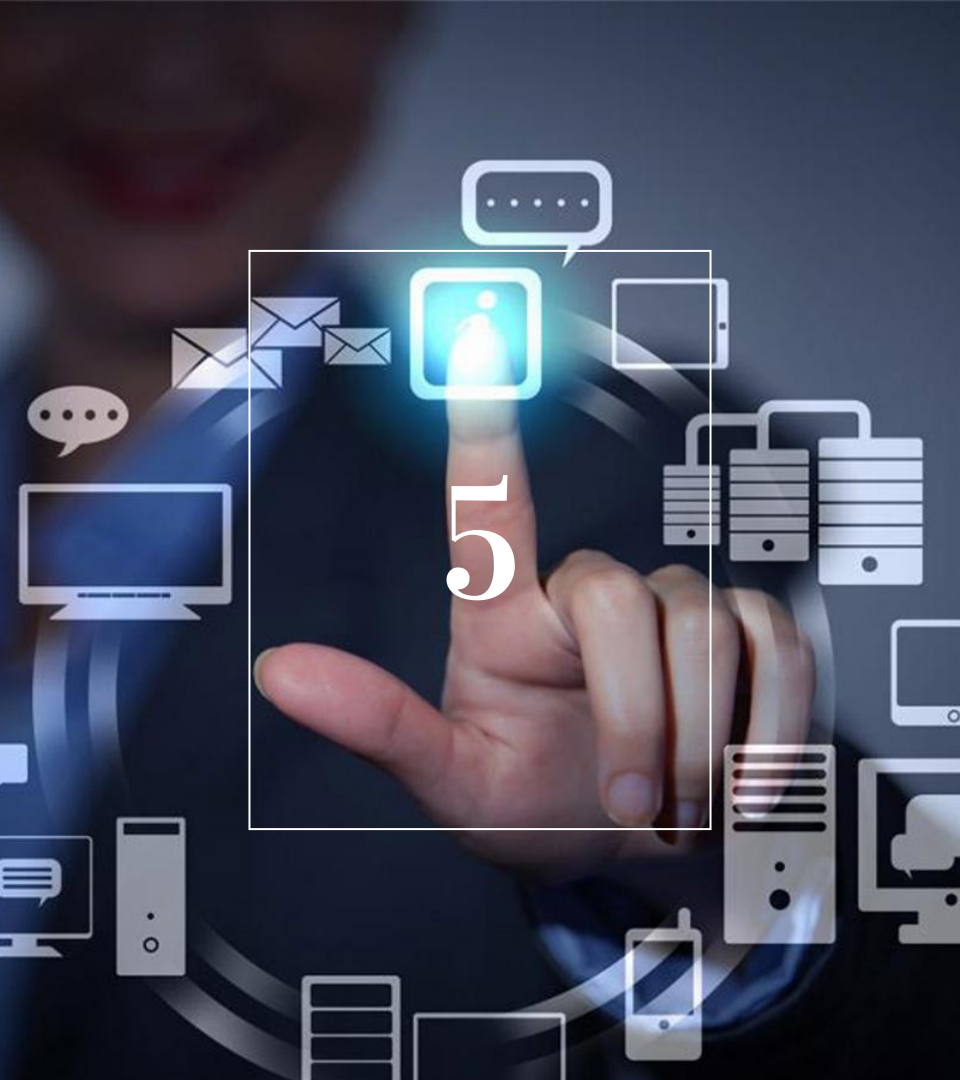
## Les différents acteurs

1. Application Client
2. Serveur API
3. Serveur d'autorisation
4. Utilisateur

## Première étape: L'enregistrement de l'application

1. Inscrire l'application client auprès du serveur d'autorisation
  - Nom de l'application
  - Url du site
  - Description
  - Logo
  - Urls de redirection
    - Succès
    - Echec
2. Le serveur d'autorisation produit des credentials
  - Client ID
  - Client Secret





## Deuxième étape: Demande d'autorisation

4 type d'autorisations:

- Authorization code

Redirige vers une page d'approbation sur le serveur d'autorisation

**Agit en tant que l'utilisateur sur l'API**

- Password

Demande un token d'accès en utilisant directement les user/password du client

**Agit en tant que l'utilisateur sur l'API**

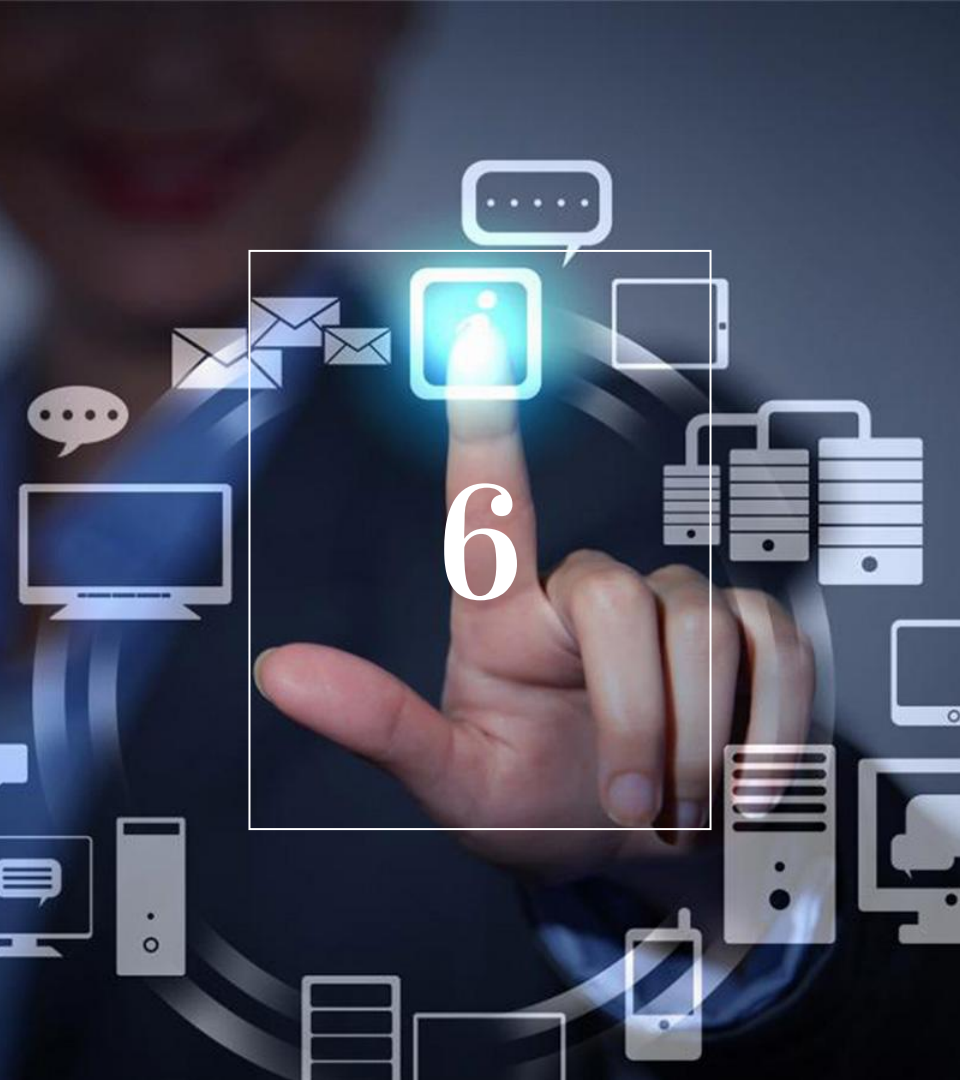
- Client Credentials

Demande un token d'accès en utilisant les credentials de l'application cliente

**Agit en tant que l'application sur l'API**

- Implicit: Abandonné





## Authorization Code: Process (1/2)

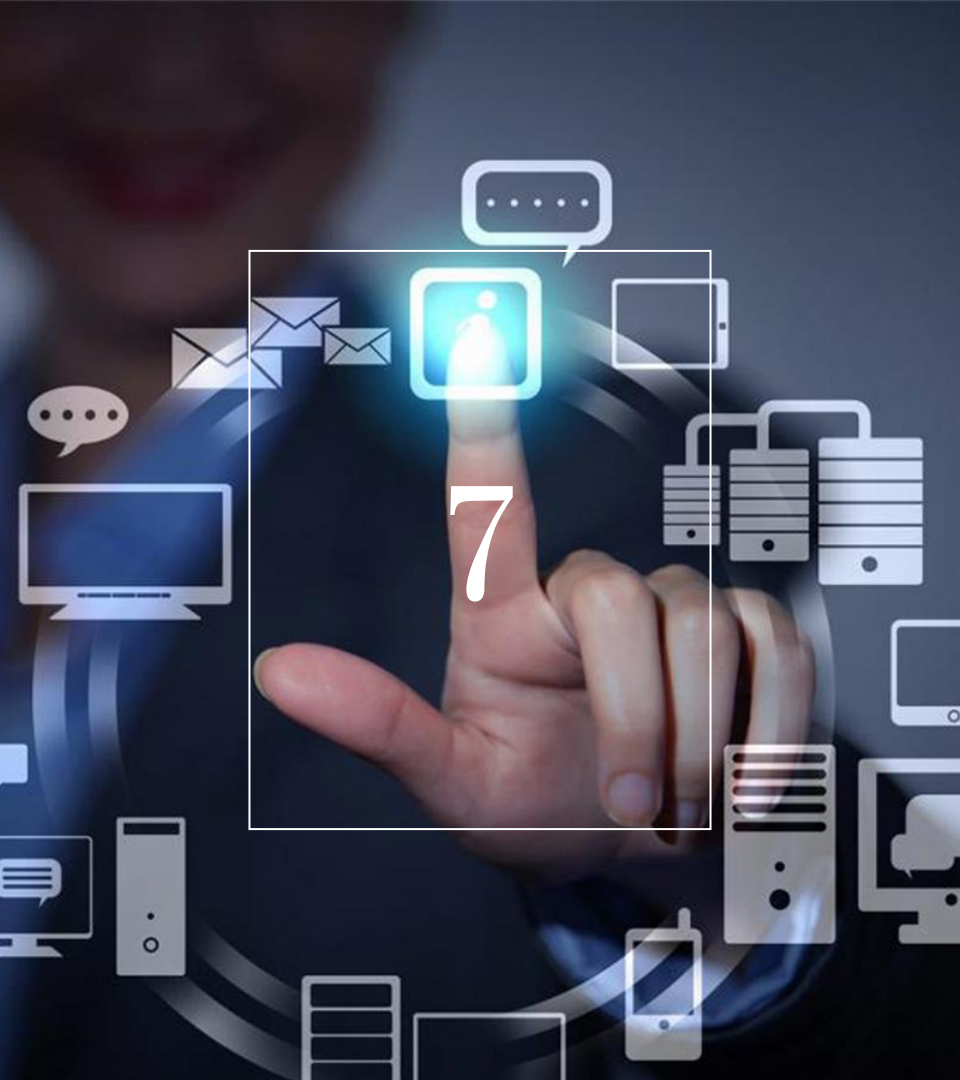
- Création d'un lien de connection vers le serveur d'autorisation

4 query params: **client\_id**, **scope**, **state**,  
**redirect\_uri**

[https://auth-server/auth?response\\_type=code&client\\_id=..&scope=...&state=...&redirect\\_uri=...](https://auth-server/auth?response_type=code&client_id=..&scope=...&state=...&redirect_uri=...)

- L'utilisateur autorise l'application à accéder à l'API
- Redirection vers l'application

<https://app/cb?code=..&state=...>



## Authorization Code: Process (2/2)

- Récupération d'un token d'identification directement serveur à serveur

5 query params: **client\_id**, **client\_secret**, **code**

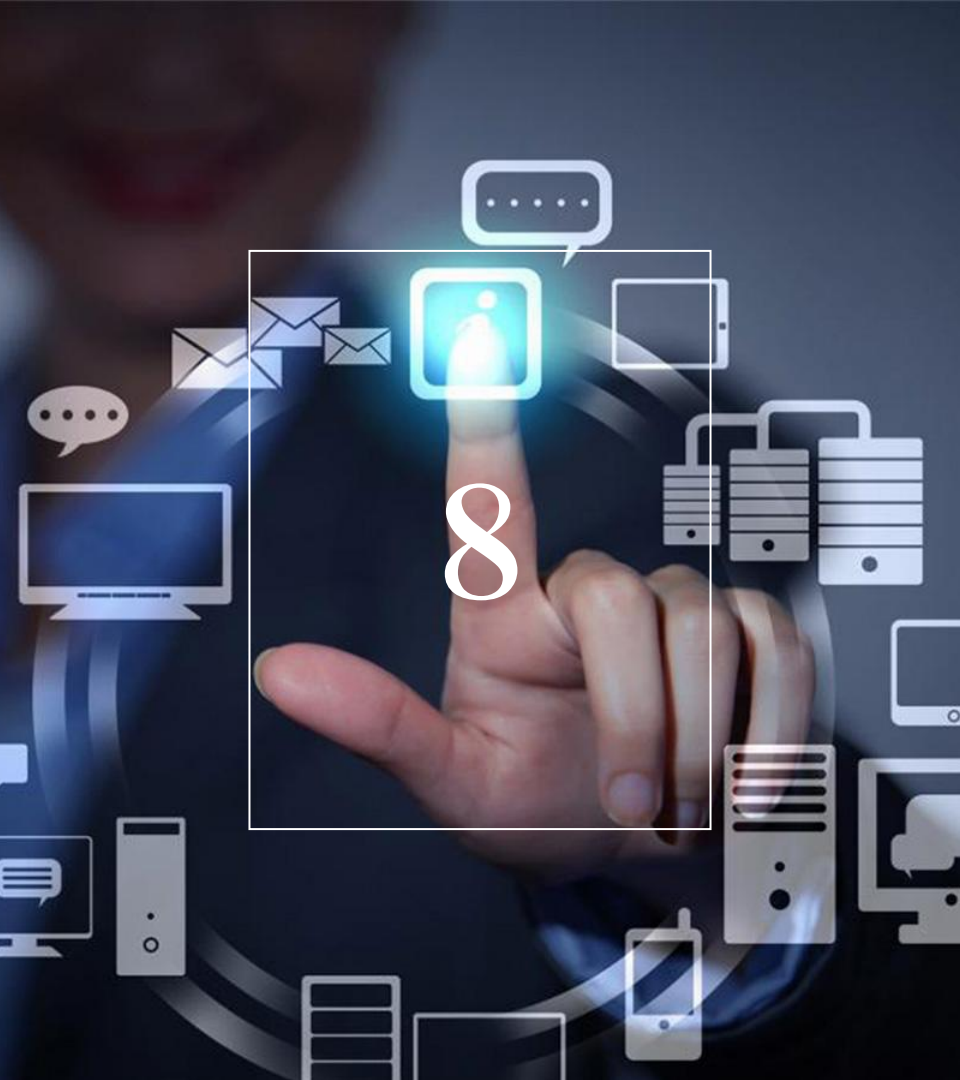
[https://auth-server/token?grant\\_type=authorization\\_code&client\\_id=..&client\\_secret=...&code=...&redirect\\_uri=...](https://auth-server/token?grant_type=authorization_code&client_id=..&client_secret=...&code=...&redirect_uri=...)

⇒ {"access\_token":"TOKEN", "expires\_in":3600}

- L'application peut utiliser l'API en tant que l'utilisateur grâce au token reçu

GET <https://api/my-movies>

Authorization: Bearer **TOKEN**



## Password: Process

- Récupération d'un token d'identification directement serveur à serveur

3 query params: **client\_id**, **client\_secret**,  
**username**, **password**

[https://auth-server/token?grant\\_type=password&client\\_id=..&client\\_secret=...&username=...&password=...](https://auth-server/token?grant_type=password&client_id=..&client_secret=...&username=...&password=...)

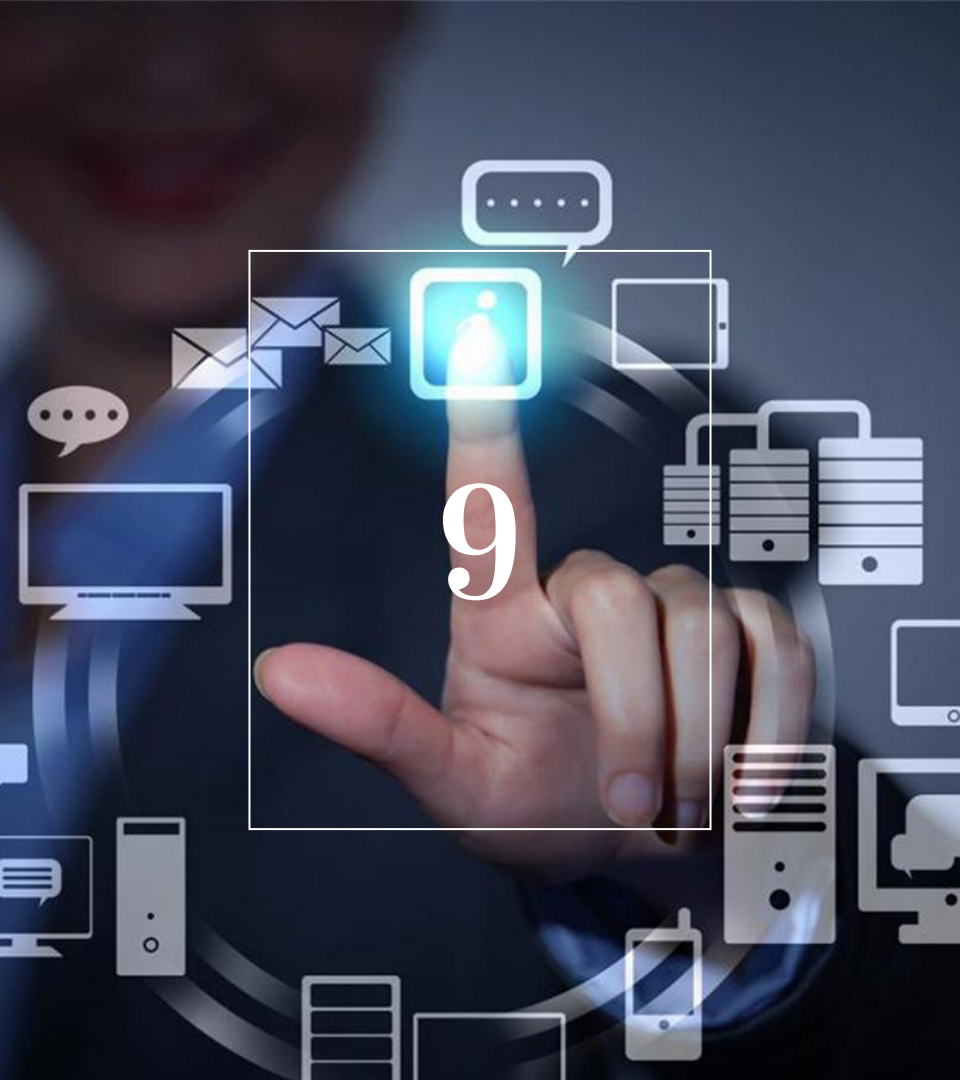
⇒ {"access\_token":"TOKEN", "expires\_in":3600}

- L'application peut utiliser l'API en tant que l'utilisateur grâce au token reçu

GET <https://api/my-movies>

Authorization: Bearer **TOKEN**





## Client credentials: Process

- Récupération d'un token d'identification directement application à serveur

2 query params: **client\_id**, **client\_secret**

[https://auth-server/token?grant\\_type=client\\_credentials&client\\_id=..&client\\_secret=...](https://auth-server/token?grant_type=client_credentials&client_id=..&client_secret=...)

⇒ {"access\_token":"TOKEN", "expires\_in":3600}

- L'application peut utiliser l'API en tant qu'elle-même grâce au token reçu

GET [https://api/stats\\_movies](https://api/stats_movies)

Authorization: Bearer **TOKEN**