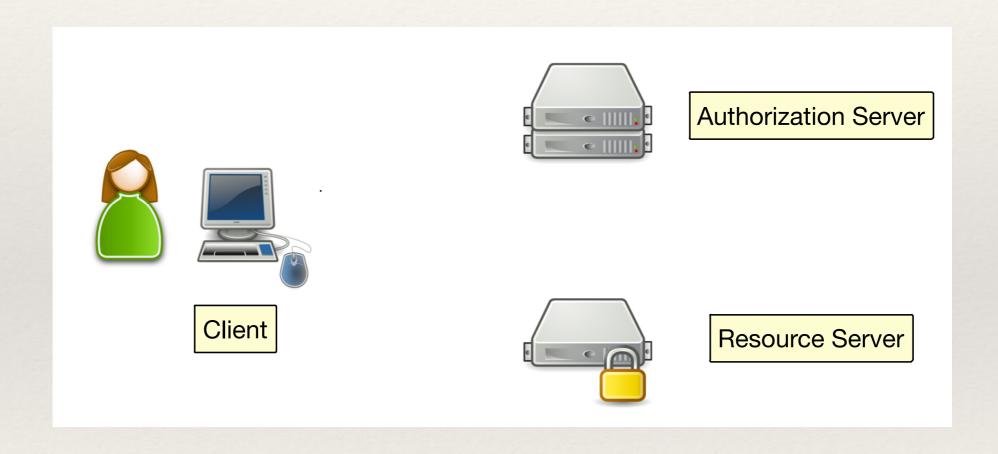
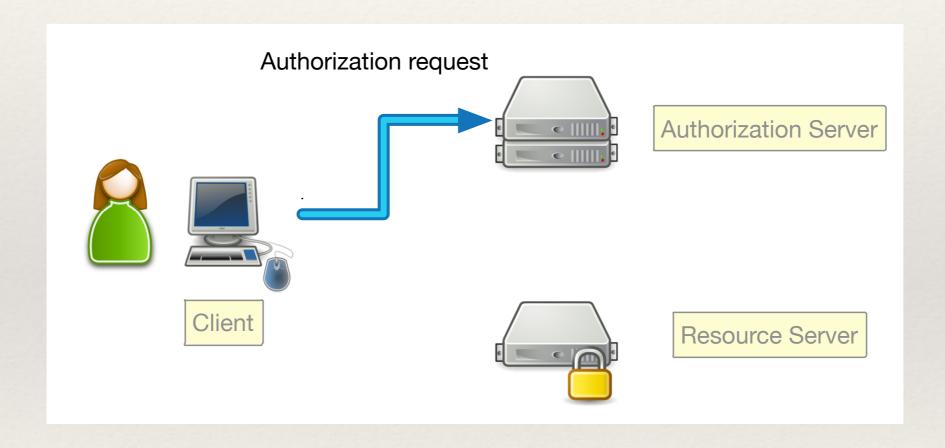
OAuth2

- * The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service,
 - * either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service,
 - * or by allowing the third-party application to obtain access on its own behalf.

The players



Authorization Request



Authorization Request - details

Parameters

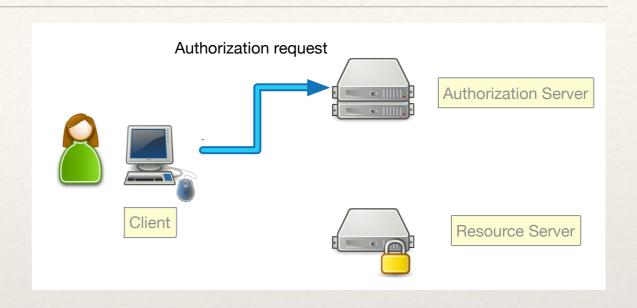
client_id

redirect_uri

response_type

scope

state

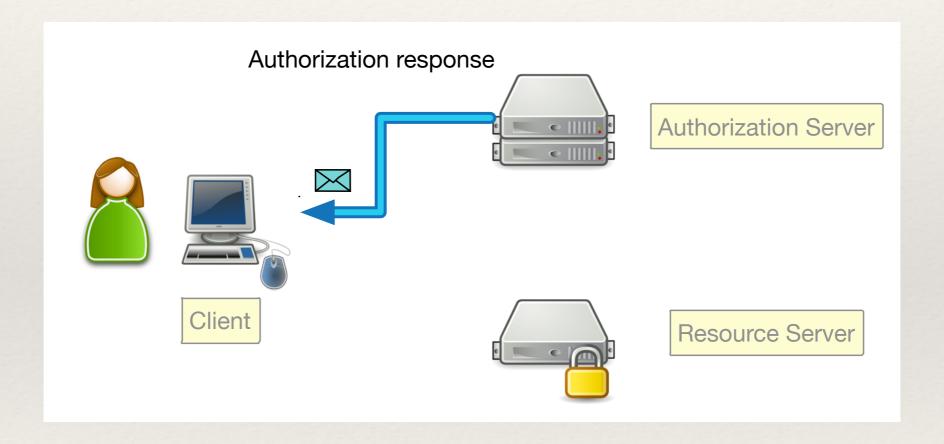


GET

```
http://example.com/authorization?state=1521671980316802035&redirect_uri=https://example.org/authz_cb&response_type=code&client_id=SFEBuhC7sp3a
```



Authorization Response

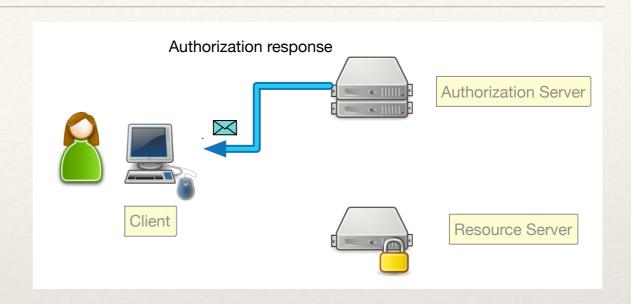


Authorization Response - details

Parameters

code access_token
state token_type
expires_in

scope



GET

https://example.org/authz_cb?state=1521671980316802035&code=s87BT60pp2UbNX2HnkWpZ9YhPVHRZaoTuU9XJul6JMuQaKUidUM6y1Boab6

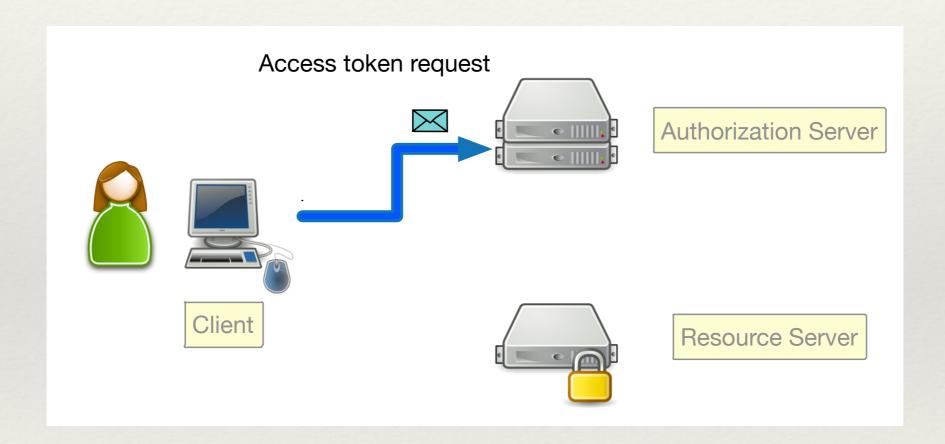
Access Token

A string representing an authorization issued to the client. The string is usually opaque to the client.

Bearer Token

'A security token with the property that any party in possession of the token (a "bearer") can use the token in any way that any other party in possession of it can.'

Access Token Request



Access Token Request - details

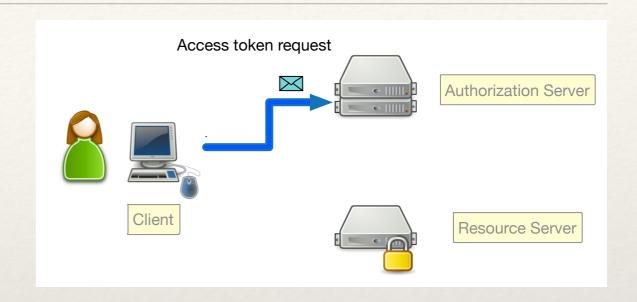
Parameters

client_id

code

grant_type

redirect_uri

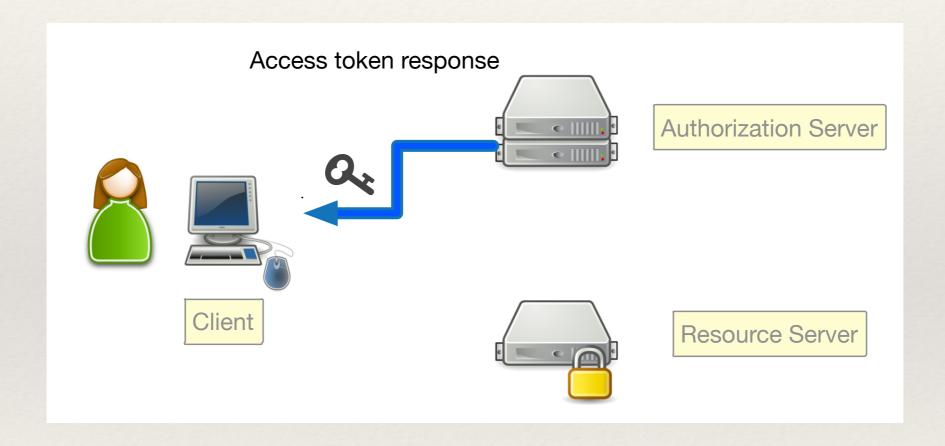


POST

http://example.com/token

code=s87BT60pp2UbNX2HnkWpZ9YhPVHRZaoTuU9XJul6JMuQaKUidUM6y1Boab6&
 grant_type=authorization_code&
 redirect_uri=https://example.org/authz_cb

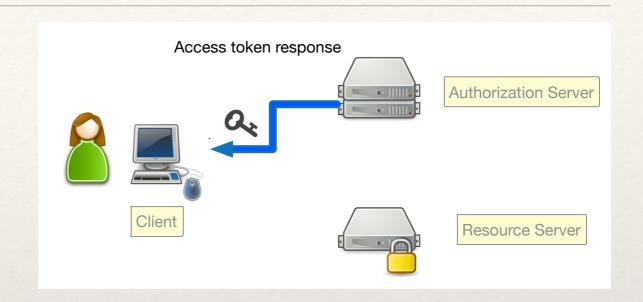
Access Token Response



Access Token Response - details

Parameters

access_token
expires_in
refresh_token
scope
token_type



```
'access_token': 's87BT60pp2UbNX2HnkWpfPfWNo9Gi7chACuWoa2IDND', 'expires_in': 3600, 
'refresh_token': 's87BT60pp2U+bNX2HnkWpVCnDYPsy8EOpI' 
'state': 'STATE0', 
'token_type': 'Bearer',
```

Refresh Token

Refresh tokens are issued to the client by the authorization server and are used to obtain a new access token when the current access token becomes invalid or expires, or to obtain additional access tokens with identical or narrower scope.

Refresh Access Token Request - details

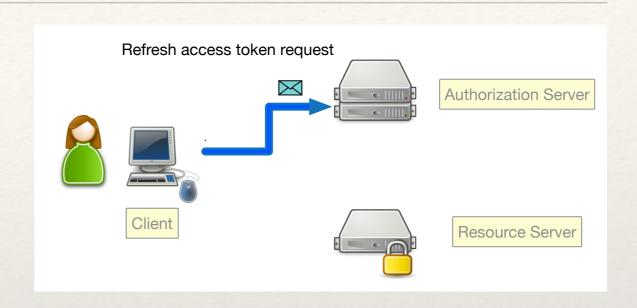
Parameters

client_id

grant_type

scope

refresh_token

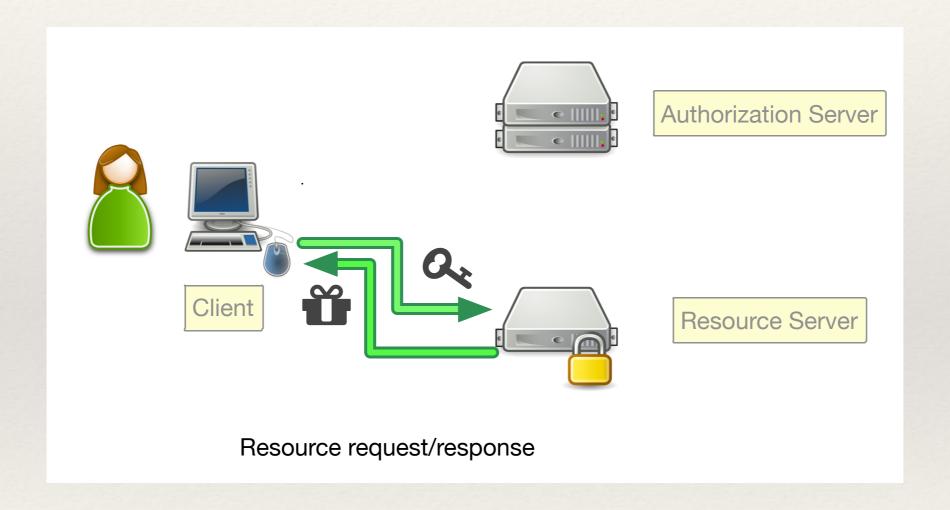


POST

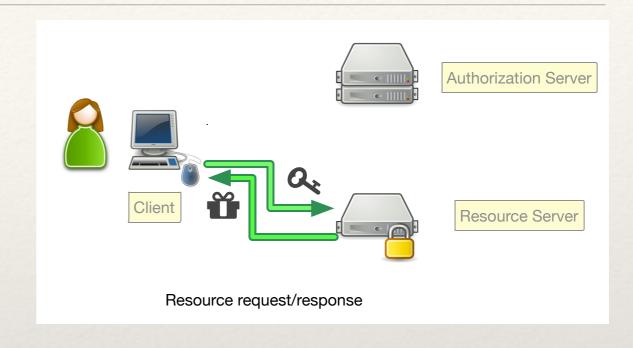
http://example.com/token

refresh_token=s87BT60pp2U+bNX2HnkWpVCnDYPsy8EOpI&grant_type=authorization_code

Resource Access



Resource Access - details



GET

https://example.com/resource

Header:

Authorization: 'Bearer s87BT60pp2UbNX2HnkWpfPfWNo9Gi7chACuWoa2IDND'

Authenticated Requests

* Authorization Request Header Field

```
POST /resource HTTP/1.1
Host: server.example.com
Authorization: Bearer mF_9.B5f-4.1JqM
```

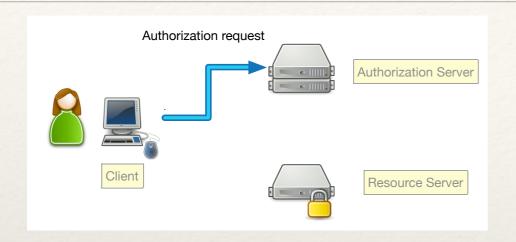
Form-encoded body part

```
POST /resource HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
access_token=mF_9.B5f-4.1JqM
```

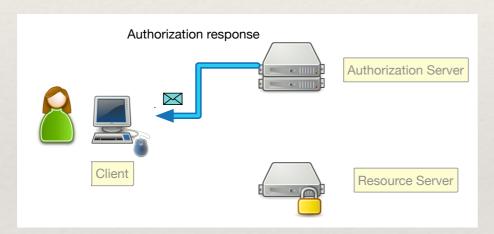
Uri query parameter

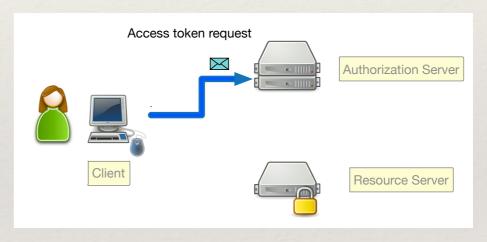
```
GET /resource?access_token=mF_9.B5f-4.1JqM HTTP/1.1
Host: server.example.com
```

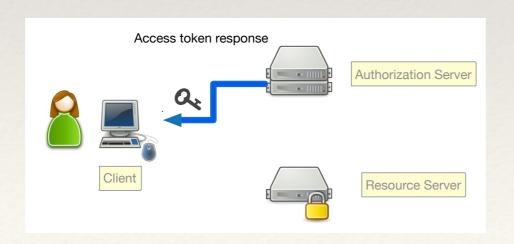
The whole

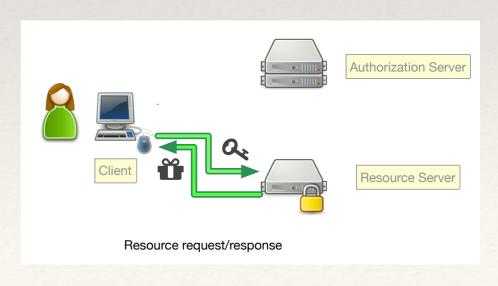








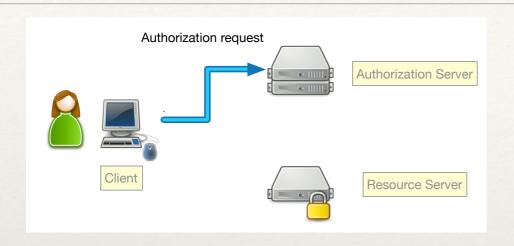




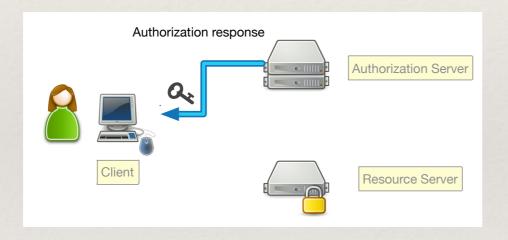
Flows

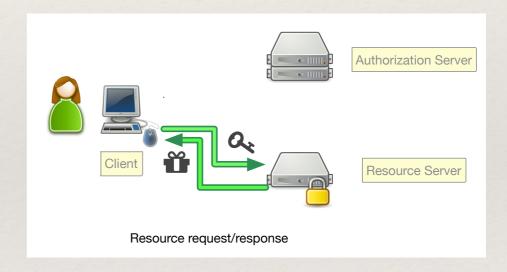
- * Authorization Code Grant
- Implicit Grant
- * Resource Owner Password Credentials Grant
- * Client Credentials Grant

Implicit grant





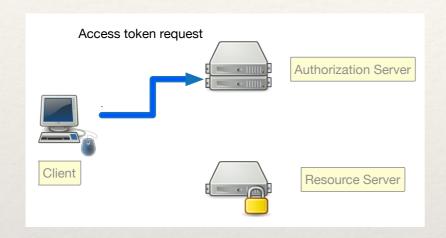


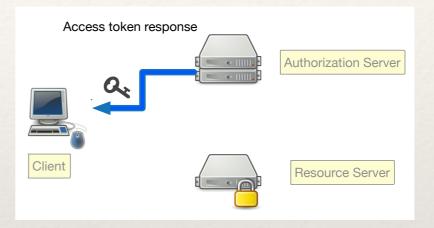


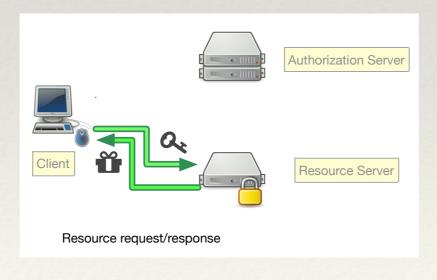
Resource Owner Password Credentials Grant



Client Credentials Grant







Links to documents

- * The OAuth 2.0 Authorization Framework
- * The OAuth 2.0 Authorization Framework: Bearer Token Usage