Learning OAuth2.0

Wei Yao

Authentication and Authorization

- Authentication is the process of confirming the identity of a user or a device (e.g. an entity)
  - *Login your amazon or google account with username and password*
  - *Check In hotel room with your driver license.*
  - *Face recognition unlock your iphone.*

- Authorization is the process of verifying what resources entities (users or devices) can access, or what actions they can perform.
  - *A hotel key card is a permit for entering your room after you checked in.*
  - *Software application use Token during authorization.*

Authentication leads to authorization, but authorization does not lead to authentication.

Authentication

Who you are

Authorization

What you can do

https://jads.blog/identity-management-saml-vs-oauth2-vs-openid-connect-c9a06548b4c5

What is OAuth?

- OAuth is *not* an API or a service, but an open *standard* for **authorization**.
- OAuth is a delegated authorization framework for REST/APIs.

Used by:

- server-to-server apps
- browser-based apps
- mobile/native apps
- IoT devices

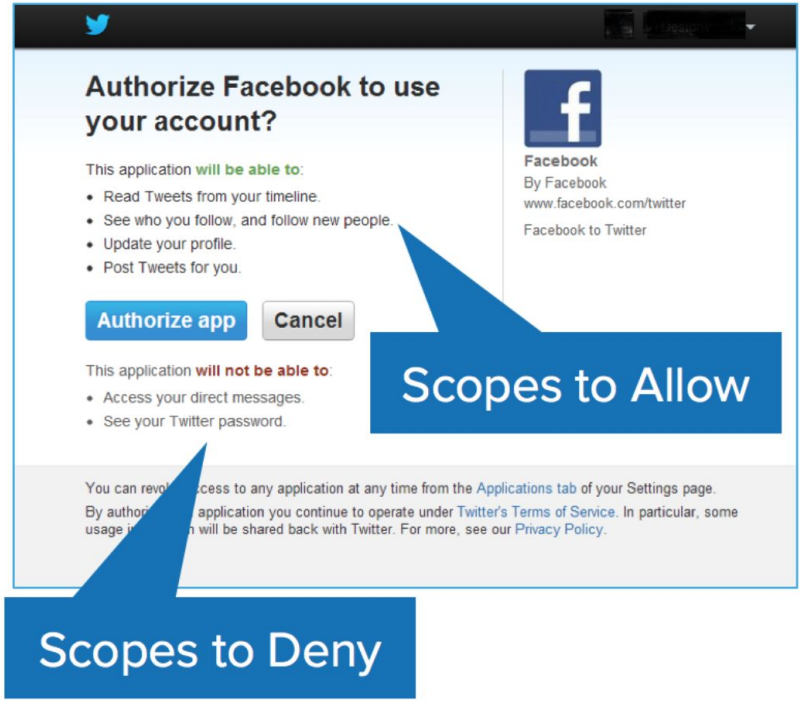
There two versions of OAuth: OAuth 1.0a and **OAuth 2.0**.
https://www.oauth.com/oauth2-servers/differences-between-oauth-1-2/

Often OAuth is solving this type of question:

"How can I allow an app to access my data without necessarily giving it my password?"

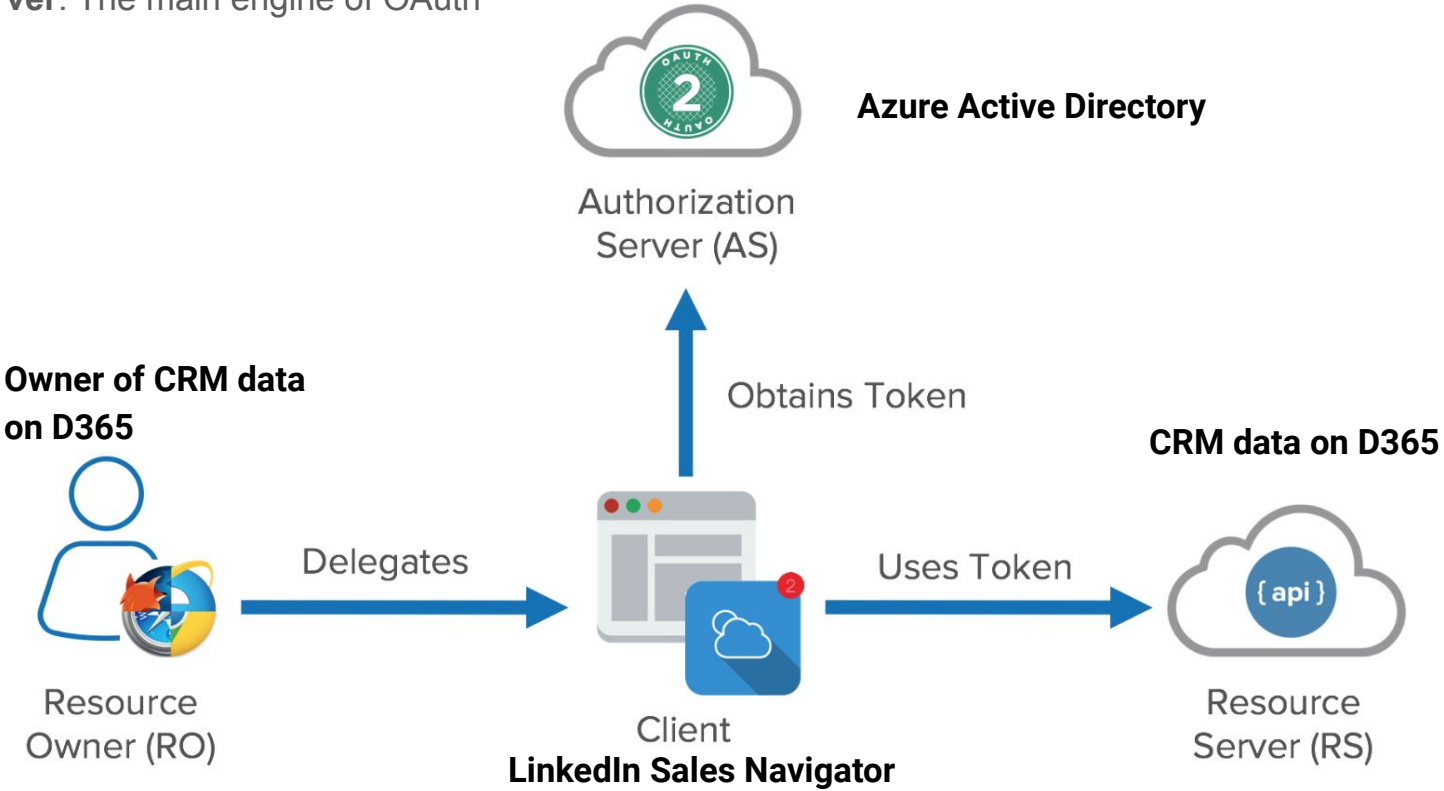
OAuth is built on the following central components:

- Scopes and Consent
- Actors
- Clients
- Tokens
- Authorization Server
- Flows



The **actors** in OAuth flows are as follows:

- **Resource Owner**: owns the data in the resource server.
- **Resource Server**: The API which stores data the application wants to access
- **Client**: the application that wants to access your data
- **Authorization Server**: The main engine of OAuth



SALES NAVIGATOR | ADMIN

Admin Home | Usage Reporting | Admin Settings | Account Center | Go to Sales Nav

Admin Settings

CRM

- Production
- Sandbox

FEATURES

- Inmail and Messaging
- TeamLink™
- Smart Links

ADVANCED

- Seat Transfer

Step 1

Log into your CRM

1 — 2 — 3 — 4

Login | Salesforce

login.salesforce.com/?startURL=%2Fsetup%2Fsecur%2FRemoteAccessAuthorizationPage.apexp%3Fsource%3...

salesforce

Username

Password

Log In

Remember me

Forgot Your Password?

Use Custom Domain

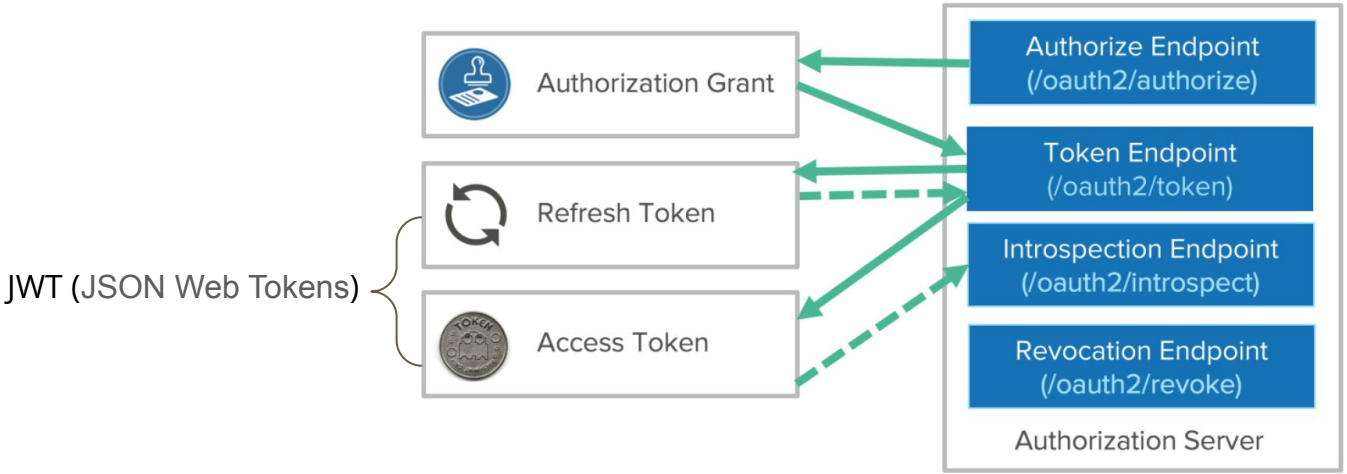
nfigure Settings

OAuth Tokens

Access tokens are the token the client uses to access the Resource Server (API). Short-lived, hours or minutes. It can't be revoked, but waiting it to expire.

Refresh tokens are used to get new access tokens after authentication of confidential clients. Long-lived, days, months, years. It can be revoked.

The Authorization Server generated a **Client ID** and **Client Secret**, sometimes called the App ID and App Secret, and gave them to the Client to use for all future OAuth exchanges.



OAuth2.0 Http Request Details

Authorization Grant:

Request:

```
GET https://accounts.google.com/o/oauth2/auth?scope=gmail.insert gmail.send
&redirect uri=https://app.example.com/oauth2/callback
&response_type=code&client_id=812741506391&state=af0ifjsldkj
```

Response:

```
HTTP/1.1 302 Found
Location:https://app.example.com/oauth2/callback?code=MsCeLvIaQm6bTrgtp7&state=af0
ifjsldkj
```

Request Token:

Request:

```
POST /oauth2/v3/token HTTP/1.1
Host: www.googleapis.com
Content-Type: application/x-www-form-urlencoded
code=MsCeLvIaQm6bTrgtp7&client id=812741506391&client secret={client
 secret}&redirect uri=https://app.example.com/oauth2/callback&grant_
type=authorization_code
```

Response:

```
{"access token": "2YotnFZFEjr1zCsicMWpAA",
  "token type": "Bearer",
  "expires_in": 3600,
  "refresh_token": "tGzv3JOkF0XG5Qx2TlKWIA"}
```

Use Token:

```
curl -H "Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA" \
https://www.googleapis.com/gmail/v1/users/1444587525/messages
```

What is SSO? Use case: LinkedIn Sales Navigator

Single Sign-on: one login can be used across multiple applications

Sales Navigator SSO allows your company's employees to authenticate with SSO sign in using their corporate credentials before being prompted to verify their LinkedIn credentials. After this initial authentication, a cached sign in is stored, for both the SSO and LinkedIn sign in (depending on browser and SSO settings), for up to 12 hours before requiring re-authentication.

Using SSO allows you to:

- Leverage your existing company's authentication.
- Increase security when employees use your company's established password protocols rather than their individual accounts.
- Manage users more easily when employees leave your company.

LinkedIn is SAML 2.0 certified, however, we don't support OAuth2.0 or OpenID at this time.

SAML and OpenID Connect

Security Assertion Markup Language (**SAML**) is an XML-based open standard used for SSO implementations.

OpenID Connect is simple identity layer on top of the OAuth 2.0 protocol that allows for ‘Federated Authentication’. It is similar to the OAuth2 authorization flow with the major difference being a ‘id-token’ that allows the user authentication.

	SAML 2.0	**OAuth2**	**OpenID Connect**
What is it?	Open standard for authorization and authentication	Open standard for authorization	Open standard for authentication
History	Developed by OASIS in 2001	Developed by Twitter and Google in 2006	Developed by the OpenID Foundation in 2014
Primary use case	SSO for enterprise apps	API authorization	SSO for consumer apps
Format	XML	JSON	JSON

ACCOUNT CENTER People Settings Admin Home Reports

Sales Navigator (Gobbl
Linkedin Corporation

Admin Settings

Application Settings

Single Sign-On (SSO) Not connected

Set up Single Sign-On with a third-party identity provider.

Learn More about setting up SSO

Configure your Identity provider SSO settings.
Download the metadata file and import it into your Identity Provider
or click here to load and copy individual fields from the form.

Download

Go to your Identity Provider (e.g. Azure Active Directory) to get the information you need.

Upload XML file

Want to input the information manually? Click here

Go to SAML validator

Change to Google OAuth

Learning Resources:

- General knowledge on OAuth 2.0:

  www.oauth.com

  https://developer.okta.com/blog/2017/06/21/what-the-heck-is-oauth

- Authentication vs Authorization:

  https://auth0.com/intro-to-iam/authentication-vs-authorization/

- An Illustrated Guide to OAuth and OpenID Connect:

  https://developer.okta.com/blog/2019/10/21/illustrated-guide-to-oauth-and-oidc

- Identity Management: SAML vs. OAuth2 vs. OpenID Connect

  https://jads.blog/identity-management-saml-vs-oauth2-vs-openid-connect-c9a06548b4c5