Sebastian HIRTIE
Anul IV, AC-IS

Tema1-DATC

S-a ajuns in situatia in care unei entitati i-ar fi util sa foloseasca detatliile unei persone gazduite intr-o alta entitate. Astfel a luat fiinta un protocol de autorizare securizat care confera unei aplicatii terte acces limitat pe o perioada de timp la datele utilizatorului fara ca aceste sa isi expuna credentialele. Standardul care realizeaza acest lucru poarta numele de OAuth, el ofera clientilor un delegat de acces la informatiile de pe server al unui proprietar de resurse. În acest scenariu, un utilizator final vorbește cu furnizorul de identitate, iar el generează un token semnat criptografic, pe care îl transferă în aplicație pentru a autentifica utilizatorul.

Pentru a intelege mai bine, se poate observa asemanarea dintre OAuth si cheia de valet a unui automobile, care ii permite,temporar, sa conduca si a parcheze masina, dar nu poate deschide portbagajul sau torpedoul, accesul nefiind complet sau nelimitat.

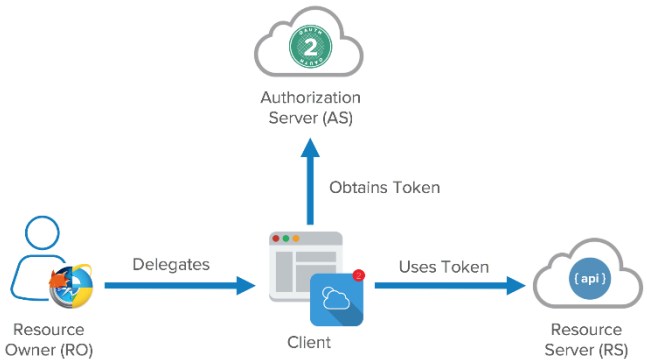
Principalele componente OAuth:

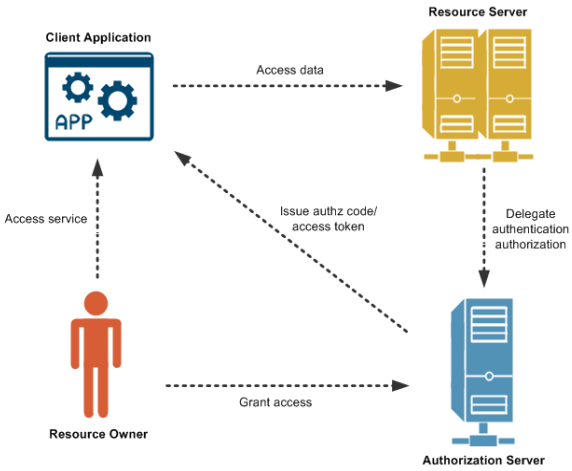
- Clienti — aplicatia care doreste acces la date
- Serverul de autorizare — cere aprobarea proprietarului si ofera jetoane
- Resource server — locul unde sunt stocate informatiile
- Resource owner — persoana careia ii apartin datele
- Token — folosite de client pentru a accesa api-ul

Sunt 4 moduri in care OAuth poate fi utilizat, folosit in functie de serviciul oferit:

1. **Codul de acordare a autorizatiei** : utilizatorul se conecteaza la client care il redirectioneaza catre serverul de autorizare impreuna cu id, tipul permisiunei si o adresa URL. Serverul de autorizare verifica numele si parola si redirectioneaza utilizatorul inapoi la client adaugand codul de accees la adresa URL Aceasta de obicei indica spre un script care solicita un token de acces, clientului ii se cere codul de acces primit anterior.
2. **Flux implicit** : folosit de aplicatiile cu o singura pagina care ruleaza pe browser si care nu au o componenta de server.
3. **Acordare prin parola** : destinat aplicatiilor web si mobile realizate de acelasi programator, prentru a verifica un singur nume si parola in loc de redirectionare spre site-ul initial. Utilizatorul doreste sa se conecteze in aplicatie folosind identitatea lor stocata in serviciul OAuth. Credentialele sunt verificate printr-un apel API si se returneaza un jeton de acces.
4. **Credentialele Clientului** : Aplicatia solicita serviciul API-ului utilizand datele de identificare a aplicatiei si primeste un acces token inapoi folosit pentru cereri API.

Sebastian HIRTIE
Anul IV, AC-IS





https://stormpath.com/blog/what-the-heck-is-oauth
https://developer.okta.com/blog/2017/06/21/what-the-heck-is-oauth
https://www.quora.com/How-does-OAuth-2-0-work