Refresh token

Inainte ca o aplicatie sa poata accesa date private, ea trebuie sa obtina un acces token ce ii permite accesul la API. La un moment dat, aplicatia va cere un acces token pe care il va folosi in toate operatiile ulterioare.

Exista 3 moduri diferite de a garanta accesul :

- ➔ password grant – se foloseste cand se cunoaste contul, clientul si ID-ul
- ➔ authorization code – folosit cand aplicatia permite functionarea mai multor conturi intr-o sesiune de browsing
- ➔ refresh token – folosit pentru a obtine un nou acces token cand cel vechi expira

Un refresh token este un token special care poate fi folosit pentru a obtine un nou acces token, care permite accesul la resurse protejate, oricand. Refresh token-ul trebuie stocat protejat, pentru ca nu expira niciodata si permite userului sa ramane autentificat, pana cand userul ii revoca permisiunea.

Pentru a primi un nou acces token, trebuie facut un request care sa contina urmatorii parametrii :

- ➔ grant_type – ce trebuie setat pe “refresh_token”
- ➔ refresh_token – refresh token-ul primit de la ultimul request la endpoint

De asemenea trebuie sa incluzi un header de autentificare(autentificare de baza cu id client folosit ca user si cheie secreta folosit ca parola) care a fost folosit in requestul anterior catre endpoint.

Refresh tokenurile au o durata lunga de viata. Asta inseamna ca atunci cand un client primeste un token de la server, acesta trebuie securizat pentru a nu fi folosit de potentiali atacatori. De aceea nu e sigura pastrarea lui in browser. Daca un refresh token este aflat, poate fi folosit pentru a obtine noi acces tokenuri pana este blacklisted. Refresh token-urile trebuie trimise catre un singur client autentificat pentru a preveni folosirea de tokenuri aflate de alte parti. Acces token-ul trebuie si el tinut secret, dar datorita duratei lui scurte de viata, pastrarea lui secreta e mai putin inportanta.