Temă DATC

OAuth este un protocol de autorizare, care permite unei aplicații să folosească date despre un utilizator al altei aplicații.Acesta nu partajează datele de autentificare ale utilizatorului, ci se folosește de o entitate numită **Authorization Token**, despre care voi aminti mai târziu.Spre exemplu, utilizatorul poate să anunțe aplicația Facebook că este de acord ca ESPN.com să se folosească de datele acestuia, dar fără ca ESPN să știe parola contului de Facebook.

Este des folosit de granzii internetului: Google, Facebook, Yahoo, Amazon, etc .În momentul de față se folosește versiunea OAuth 2.0, fiind o variantă mai optimă decât 1.0. Alte alternative pentru această situație de autorizare este protocolul SAML, dar OAuth este mai versatil și ușor de folosit.

După cum am vorbit mai sus, autentificarea se face prin Authorization Token, un obiect în format **JSON** ce poate avea 2 forme: serializat (folosită în cazurile în care jetonul este transferat) și deserializat (folosită pentru citirea și scrierea jetonului).

Forma deserializată este constituită din 2 părți: antetul (folosit pentru a specifica funcțiile criptografice aplicate jetonului) și conținutul (folosit pentru a stoca informațiile despre autentificare).Exemple de înregistrări din conținut sunt: numele celui ce a generat jetonul, sau celui căruia îi este destinat, data expirării , data generării jetonului, etc.

Forma serializată este un string generat de către codificarea base64URL a antetului, conținutului și a semnăturii (opțional).

Acestui jeton i se pot aplica funcțiile de semnare și criptare.Prima funcție se folosește pentru a demonstra autenticitatea jetonului, iar cea de a doua se asigură că informația nu poate fi citită de către un terț.Aceasta poate fi realizată prin criptare cu cheie privată sau criptare cu cheie publică.

Un alt fel de jeton, utilizat pentru a genera un Authorization Token, este **Refresh Token**.În majoritatea cazurilor este folosit când se dorește accesul la o nouă resursă pentru prima oară sau când timpul jetonului de autorizare a expirat și este necesar unul nou, Refresh Token având o durată de viață mai îndelungată.Din cauza acestui aspect, este nevoie de o mai bună securitate față de jetoanele precedente.

Un exemplu a celor două interacționând este **Sliding-sessions**.După o perioadă de inactivitate, utilizatorul nu mai va putea accesa resurse deoarece sesiunea este expirată.În momentul în care utilizatorul acționează el va primi un jeton de autentificare, după perioada de inactivitate timpul jetonului expiră așa că va fi nevoit să recurgă la un jeton de refresh.