

OAuth 2 et OpenID

AREA Bootstrap

Sommaire

- **Explication d'OAuth et OpenID**
- **Démonstration**

La naissance de OAuth

Creation en octobre 2012

Il a été créé pour résoudre le problème des utilisateurs qui devaient partager leurs informations d'identification avec des applications tierces pour accéder à leur compte sur un site Web ou une application.

OAuth c'est quoi ?



OAuth est un framework qui permet d'autoriser un site web, un logiciel ou une application à utiliser l'API sécurisée d'un autre site web pour le compte d'un utilisateur.

**OAuth n'est pas un protocole
d'authentification, mais de «
délégation d'autorisation ».**



Et OpenID ?

OpenID est un standard qui étend les capacités d'OAuth 2.0 en ajoutant l'identité pour créer un cadre unique permettant de sécuriser les API, les applications natives mobiles et les applications web au sein d'une architecture.



OpenID est comme une
extension de OAuth



Utilisation

Cependant, pour éviter de redemander les identifiants à l'utilisateur, les applications tierces avaient tendance à conserver le mot de passe de celui-ci en clair.

En plus des limites de sécurité liées à cette conservation du mot de passe en clair, l'application tierce était en mesure d'accéder à toutes les informations protégées sans distinction.

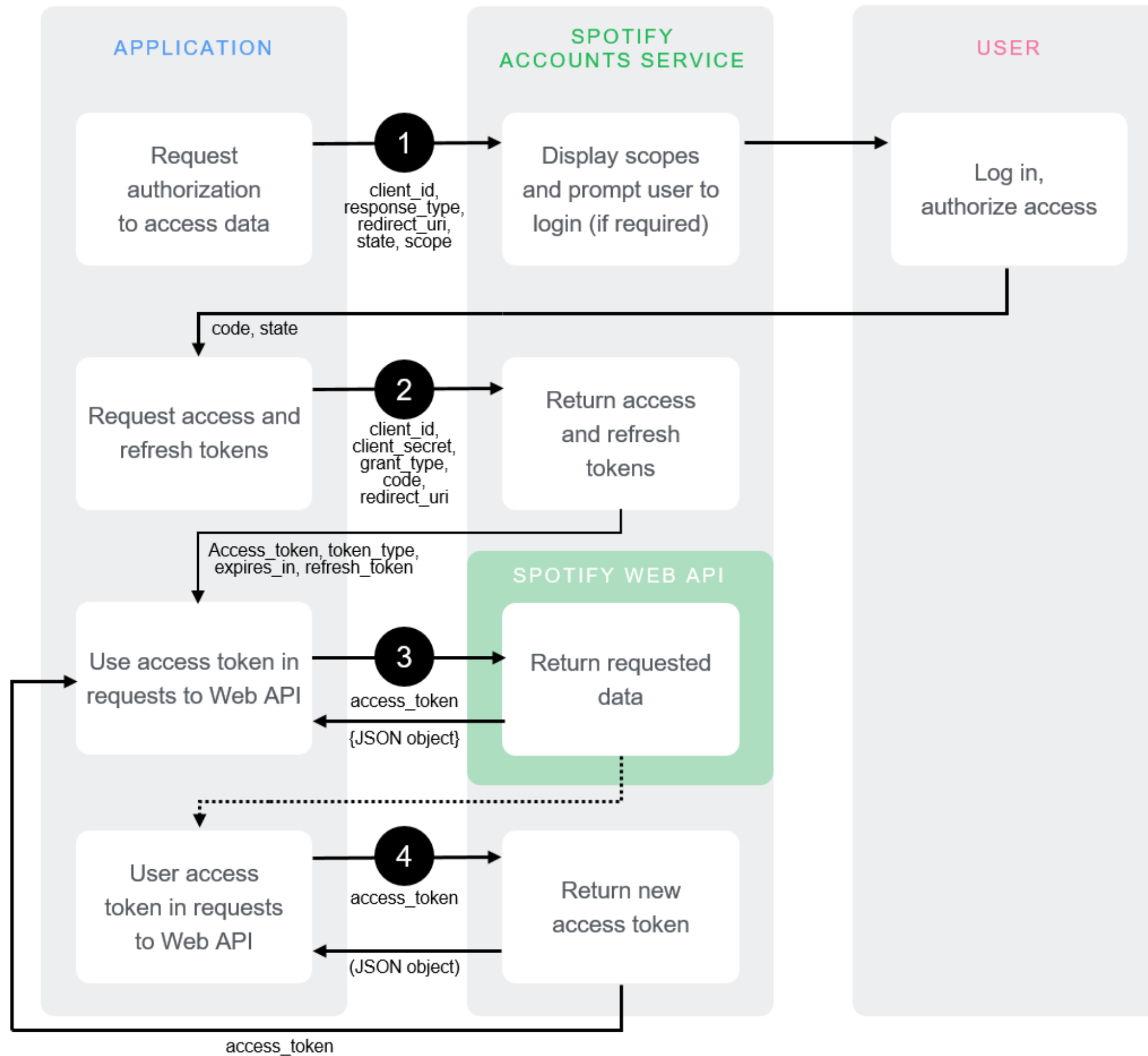
Et hormis ces problèmes de sécurité, une question d'ordre pratique se pose.

En effet, si l'utilisateur a fourni ses identifiants à plusieurs applications tierces et décide de les changer, il doit le modifier aussi pour toutes ces applications.

Pour répondre à ces problématiques, OAuth 2.0 a été créé afin de permettre des interactions entre applications dans un contexte sécuritaire optimal. OAuth 2.0 a été conçu pour être utilisé avec le protocole HTTPS.



Schéma du workflow



En Résumé

OpenID est principalement utilisé pour l'authentification.

Tandis que OAuth2 est principalement utilisé pour l'autorisation.



Merci pour votre attention