Seguridad y uso de APIs

Seguridad y uso de APIs

- Muchas veces se necesita una clave (**API key**) para hacer uso de APIs comerciales
- Esto permite saber quién usa los servicios y cómo los usa
- Pueden existir distintos niveles de servicios (gratuitos y de pago), o políticas que limitan el número de peticiones que un usuario puede realizar durante un determinado periodo de tiempo

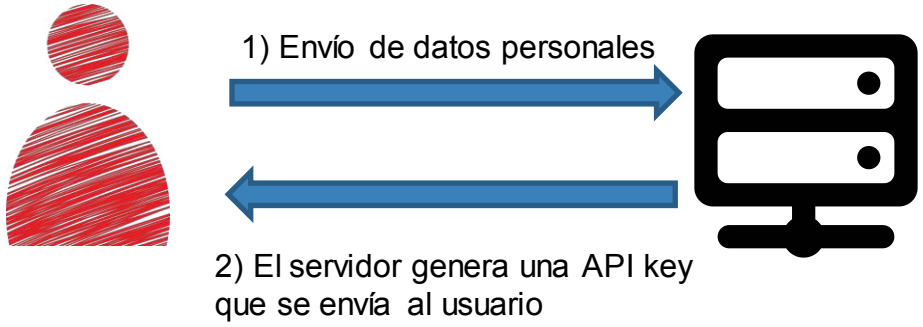
Autenticación en API REST

Existen dos métodos de autenticación:

- **API key**: cadena larga de caracteres, que se asigna a un consumidor de una API cuyo valor es único y es utilizada por parte de ese consumidor en cada una de las solicitudes a la API.

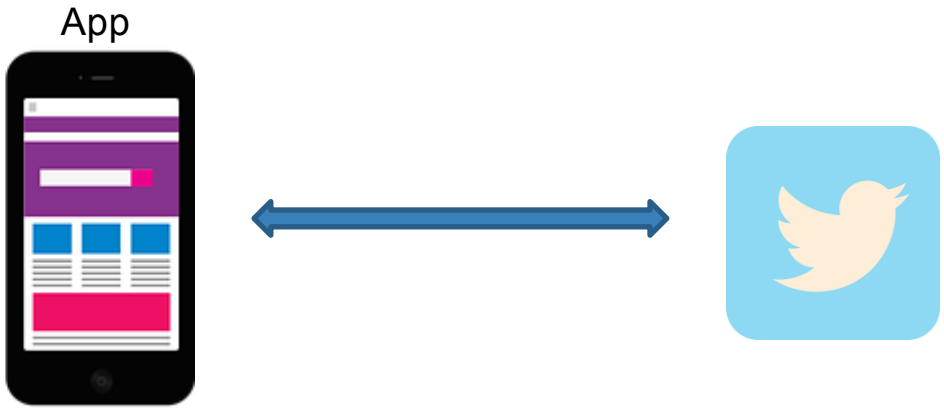
- **Open Authorization** (**OAuth**) es un protocolo que permite la autorización segura de una API de modo estándar y simple, basada en el uso de un token de acceso (o **access token**)

API key


1) Envío de datos personales
2) El servidor genera una API key que se envía al usuario
3) Para acceder al servicio web, el usuario envía la API key como parámetro

OAuth

- OAuth es un framework que permite delegar la autorización de acceso a las APIs
- Los tokens de acceso no contienen información sobre la identidad del usuario
- Empresas como Twitter o Facebook utilizan este framework



¡GRACIAS!

¿Preguntas?