oAuth2

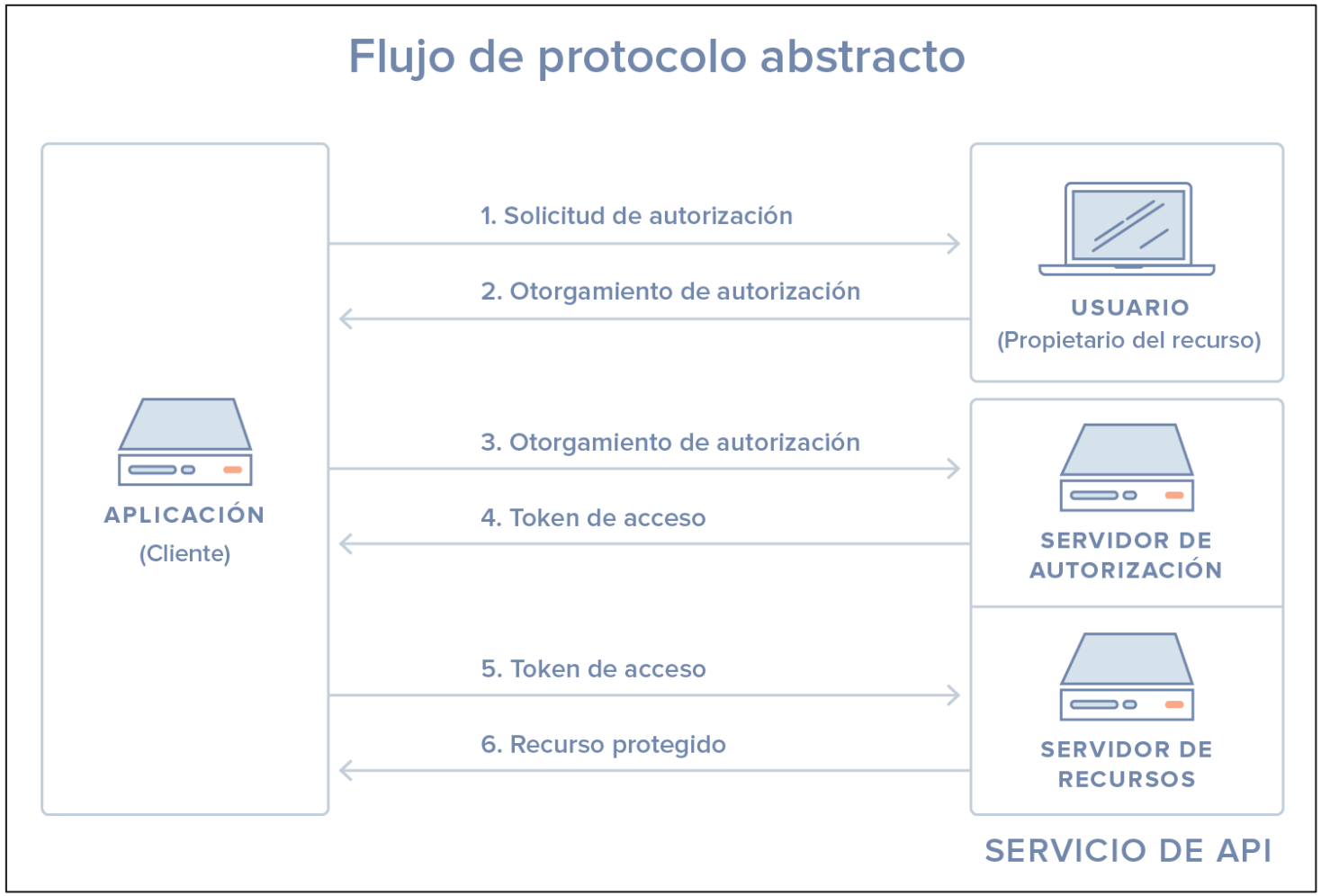
oAuth2

introducción

- oAuth2: Framework de autorización, que permite a las aplicaciones obtener acceso limitado a las cuentas de usuario de servicios como Facebook, Twitter, Google, LinkedIn, etc.
  - Delega la autenticación de usuario al servicio que gestiona las cuentas
  - Provee el flujo para la autorización de aplicaciones web, aplicaciones móviles, etc.
- *Entidades involucradas* en el flujo de oAuth2:
  - *Propietario de recursos:* Generalmente es una persona.
  - *Aplicación cliente:* Sitio web o aplicación que accederá a los recursos protegidos de un usuario con la autorización del mismo
  - *Servidor de autorización:* Valida usuario y credenciales y genera tokens de acceso.
  - *Servidor de recursos:* Recibe peticiones de acceso a los recursos protegidos autorizando acceso, si el token es válido.
- Casos de uso:
  - Una persona con cuenta en Facebook o Twitter quiere publicar contenido a través de otra aplicación
  - Una persona con cuenta en Facebook o Twitter quiere acceder a otra plataforma pero sin tener que registrarse

oAuth2

protocolo



oAuth2

ejemplo (parte 1)

Supongamos la página de DISNEY que permite acceder a través de Facebook (se debe haber registrado la web con el servicio y dar permisos para su uso):

- El usuario entra en la página de DISNEY y hace clic en "Ingresar usando Facebook".
- La aplicación lo va a redirigir a una URL como la siguiente: facebook.com/oauth2/auth?client_id=ABC&redirect_uri=disney.com/oauth_response
- Esta URL contiene los siguientes parámetros: un **client_id**, una **redirect_uri** y opcionalmente un parámetro *scopes* (para indicar a qué información de Facebook queremos acceder)
- Facebook primero va a ver si nuestro **client_id** es válido (comparándolo con la lista de **oauth_client** permitidos).
- Si todo está correcto, entonces define una variable de sesión que guarda nuestro **client_id** y **redirect_uri**. y entonces:
  - Redirige al usuario a facebook.com/login o avanza si ya hay una sesión activa en Facebook.
- Facebook muestra el logo de DISNEY y el nombre de la app (lo reconoce a partir del **client_id**), indicando al usuario: "Esta app quiere acceder a tus datos de Facebook, ¿le das permiso?" (según el scope indicado previamente).

oAuth2

ejemplo (parte 2)

Si se acepta lo anterior entonces ...

- Facebook genera un código **client_secret** (que tiene un sólo uso válido para DISNEY, el usuario y el *scope*). Facebook redirige al usuario según la redirect_uri indicada al inicio.
- Entonces Facebook enviará el código generado hacia la aplicación DISNEY: disney.com/oauth_response?code=aqui_un_codigo_extenso
- DISNEY toma el código que recibe de Facebook y vuelve a hacer una petición a Facebook, incluyendo ahora su **client_secret**

  Para probar su identidad, DISNEY hace una petición de la siguiente forma:
  facebook.com/oauth2/token?client_id=ABC&client_secret=XYZ&code=aqui_un_codigo_extenso
- Facebook verifica que el código sea válido, lo invalida en ese instante (ya que son de uso único).
- Por último, Facebook responde con un **AccessToken**, que DISNEY podrá usar (hasta que expire) para hacer peticiones a la API, en nombre del usuario que ha otorgado los permisos.

oAuth2

referencias

- https://oauth.net/2/
- https://openwebinars.net/blog/que-es-oauth2/
- https://developers.google.com/identity/protocols/oauth2