Universidad Nacional de La Matanza

Agenda

- Diferenciando los conceptos
  - Identificación
  - Autenticación
  - Autorización
- Autenticación e identificación por terceros openId/oauth2.
- Que resuelve firebase auth.
- Detalles de la herramienta.

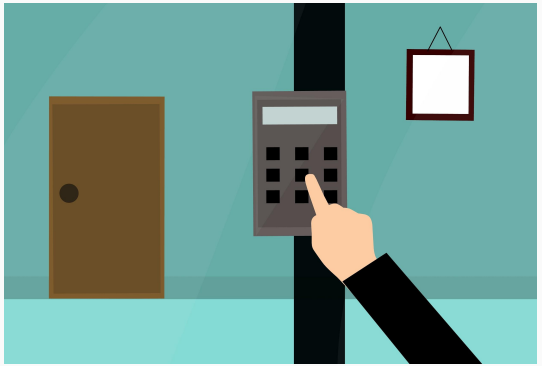
Que es la identificación y la autorización

Identificación

- Es la forma en que se identifica un usuario
- La capacidad de identificar a un usuario es algo que debe diferenciarlo del resto
  - email
  - nombre de usuario
  - Id
- No pueden existir dos usuarios con el mismo identificador, ya que perderíamos la capacidad de diferenciarlos
- El identificador representa la identidad de ese usuario

Autenticación

- La autenticación de un usuario es el proceso por el cual se valida la identidad del usuario
- Se puede resumir en tres factores
  - Algo que se sabe. Ej una contraseña
  - Algo que se tiene. Ej un celular
  - Algo que se es.Ej una huella digital
- Este proceso en conjunto con la identificación, son el proceso que nos dará acceso a un sistema
- Existe lo que se conoce como segundo factor de autenticación.
  - Para esto podemos juntar dos de los tres factores anteriormente mencionados



Autorización

- Si asumimos que un usuario fue identificado y autenticado, sería el tercer paso
  - Define si el usuario tiene acceso al recurso que intenta utilizar
  - Podemos tener acceso a un sistema por estar autenticados, pero no autorización para utilizarlo
- Son los derechos y permisos que se le otorgan a un usuario sobre un sistema
- En general podemos observar niveles o roles de autorización

Autenticación e identificación por terceros openId/oauth2

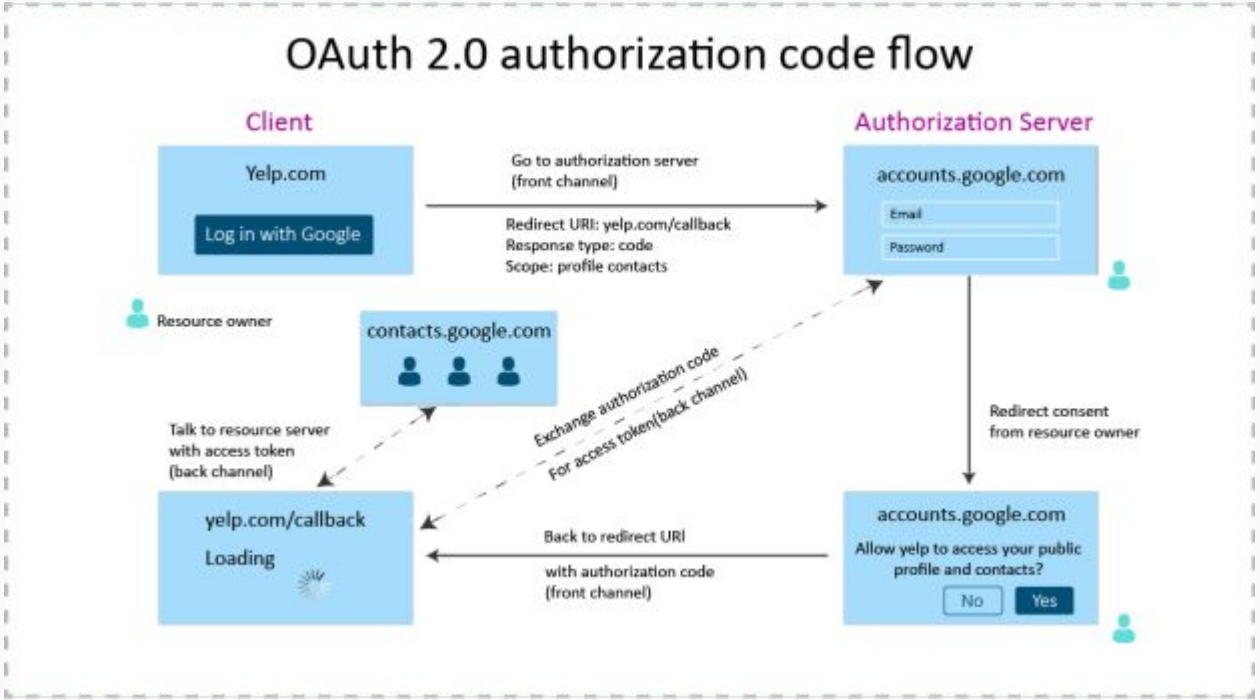
Servicios de autenticación de terceros

- OAuth2
  - Basado en autorización
  - Se suele confundir con acceso a identidad
- OpenID
  - Es la forma en que obtenemos la identidad digital de un usuario
  - Para ello se requiere que el usuario esté autenticado
  - NO tiene como finalidad la autorización
- OpenID Connect
  - Es lo mejor de ambos mundos
  - Más detalles adelante (NO SPOILER)

OAuth2

- Es un framework que busca obtener el permiso del usuario para acceder a un recurso en su nombre
  - Para ello el usuario debe estar identificado y autenticado
  - Quien tiene la responsabilidad de esto es el servidor donde se encuentra recurso
- Normalmente obtenemos un access token que representa el acceso otorgado por el usuario para actuar en su nombre
  - Existen distintos flujos para obtenerlo
  - Los access token tienen un tiempo finito de vida o TTL
  - El token debe ser reconocido y validado por el servidor que lo otorgó antes de permitir el acceso a un recurso
  - En caso de vencer puede ser renovado

Flujo OAuth2 de ejemplo



OpenID

- Se basa en obtener la identidad de un usuario de un tercero
- Para esto se requiere un proveedor de identidad (IdP)
- Tiene la capacidad de identificar y autenticar al usuario
- Es un estándar de la industria ampliamente conocido
- Es muy común que se utilice para obtener identidades federadas, y de esta forma hacer que el usuario no deba iniciar la sesión en múltiples sistemas
  - Esto es muy conocido como Single Sign On (Inicio único de sesión)
- Existe una fundación que se encarga de mantener este estándar
  - Deprecado en 2014 :(
  - Reemplazado por OpenID connect :D

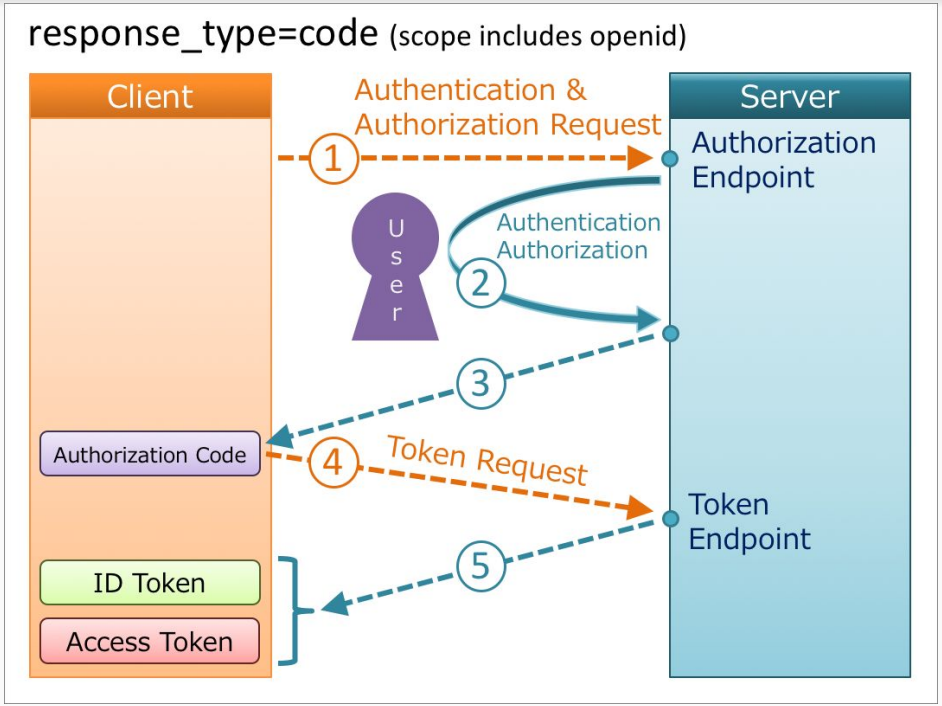
OpenID Connect

- Está escrito sobre OAuth2
- Unifica de alguna forma los dos mundos
  - Podemos conocer la identidad del usuario y tomarla como propia
  - Podemos actuar sobre recursos autorizados por el usuario en su nombre
  - Podemos delegar entonces todo un un IdP que se encargue de devolvernos un ID token y un access token (igual al de OAuth2)
- ID token
  - Representa la identidad del usuario y lo que él reclama ser (Claims)
  - Al igual que el access token tiene un TTL y debe ser validado por el IdP

OpenID Connect

- El IdP debe saber cómo alcanzar y autenticar a quien lo llama
  - Callback URL
- Está preparado para identificar y autorizar
  - Clientes (otras apps)
  - Usuarios
- NO deberíamos, aunque podríamos, basar nuestra autorización en roles externos del IdP
  - Excepto que… seamos los dueños del IdP

OpenID connect flujo de ejemplo



Que resuelve firebase auth

Firebase auth

- Firebase posee un SDK de autenticación de usuarios completo
  - Resuelve todo el proceso de identificación y autenticación de un usuario
  - Se integra con reglas de autorización de acceso a servicios de firebase
  - Se encarga de recordar y mantener logueado al usuario
  - Permite incluir la identificación y autenticación con servicios de terceros
    - OpenID
    - OAuth2
- Permite desde la consola de firebase administrar los usuarios
- Existe tanto para
  - Web
  - iOS
  - Android

Escenarios de autenticación

- Autenticación directa
  - Es la solución recomendad por firebase auth
  - Nos provee una UI y un flujo controlado y customizable con toda la experiencia de Google aplicada
  - Es la más simple de implementar
- Autenticación con email/password
  - Debemos implementar nuestro propio flujo de autenticación al igual que nuestra UI
  - La experiencia es la más customizable de todas
  - Requiere de mayor tiempo de implementación y conocimiento
  - Debemos administrar los callbacks según ciertas reglas

Escenarios de autenticación

- Integración con identidades federadas
  - Trae resuelta la integración con los servicios más populares
    - Facebook
    - Google
    - Github
    - Twitter
    - Apple
    - Otros
- Autenticación utilizando el número de teléfono
  - Para identificar al usuario se utiliza su número telefónico
  - El usuario accede al sistema ingresando un código provisto por un SMS
  - Este flujo está resuelto en firebase UI
  - Puede ser implementado de forma manual

Escenarios de autenticación

- Integración con sistemas propios de autenticación e identificación
  - Si contamos con un sistema propio puede manejar la autorización de nuestros usuarios con los servicios de firebase. Ej realtime database
  - Nuestro servicio debe implementar access tokens y id tokens los cuales firebase va a almacenar
- Usuarios anónimos
  - Son cuentas temporales
  - El objetivo primario es que el usuario pueda probar nuestra app y decida registrarse posteriormente
  - Firebase tiene un flujo para convertir una cuenta anónima en una identificada

¿Preguntas?

Donde aprendo más?

Más...

- Firebase auth
- Android OAuth2
- OpenID foundation
- Auth0 blog