



Protocolos de autenticación y autorización en aplicaciones y servicios web

Marc Cerrillo

Raúl Cutillas

Àlex Fernández

Marc Fonseca



Índice

- Definición
- Protocolos de autorización
 - OAuth 1.0 i 2.0
- Protocolos de autenticación
 - OpenID
 - Kerberos
- Protocolos híbridos
 - Hybrid protocol OpenID OAuth
 - Radius
- Conclusiones
- Bibliografía
- Reparto del trabajo



Autenticación vs Autorización

- **Autenticación** es el proceso responsable de verificar la identidad de un usuario o sistema

- **Autorización** es el proceso que permite identificar si un usuario o sistema tienen permisos para acceder a ciertos recursos o hacer ciertas tareas

Protocolos de autorización:

- OAuth



¿Qué es OAuth?

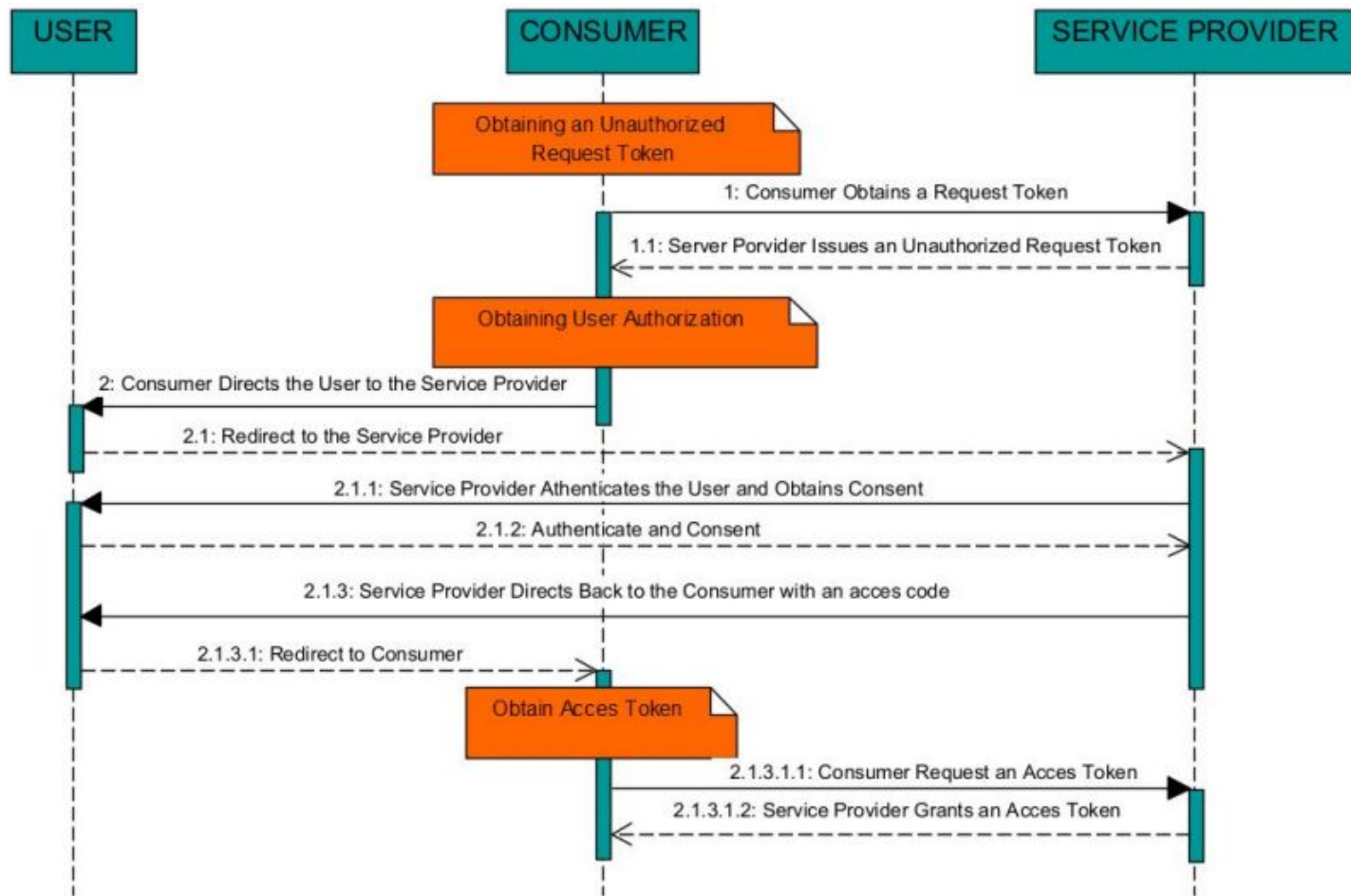
- Open standard para la delegación de acceso basado en tokens
- Diseñado para utilizar con HTTP
- Utilizado en grandes compañías como Amazon, Google o Microsoft



OAuth 1.0. ¿Cómo funciona?

Roles:

- Final User
- Consumer
- Service provider





OAuth 2.0. ¿Qué mejora?

Firmas simplificadas:

```
curl --get 'https://api.twitter.com/1.1/statuses/show.json' \
--header 'i'Authorization: OAuth \
  oauth_consumer_key="xRhHSCcKLl9VF7fbyP2eEw",
  oauth_nonce="33ec5af28add281c63db55d1839d90f1",
  oauth_signature="oBO19fJO8imCAMvRxmQJsA6idXk%3D",
  oauth_signature_method="HMAC-SHA1", oauth_timestamp="1471026075",
  oauth_token="12341234-ZgJYZOh5Z3ldYXH2sm5voEs0pPXOPv8vC0mFjMFtG",
  oauth_version="1.0"'
```

(Llamada get a api de twitter que necesita la autorización hecha con OAuth 1.0)



OAuth 2.0. ¿Qué mejora?

- Firmas simplificadas, Bearer Tokens

Un Bearer Token es un solo string que actúa como autorización de una solicitud.

```
"Authorization: Bearer XXXXXXXXXXXX"e -H
```

(Formato general de llamada que necesita autorización hecha con OAuth 2.0 usando Bearer Tokens)



OAuth 2.0. ¿Qué mejora?

- Renombramiento de roles
- Deja de estar orientado para navegadores
- Simplicidad



Puntos débiles de OAuth 1.0 y 2.0

OAuth 1.0

- Alta complejidad
- Muchas implementaciones
- Robusto y poco documentado
- Orientado a navegadores
- Problemas de seguridad

OAuth 2.0

- No hay formato común, cada servidor tiene su propia implementación
- A veces se tienen que hacer solicitudes adicionales en el proceso de verificación del usuario



Puntos fuertes de OAuth 1.0 y 2.0

- Acceso a los recursos mediante HTTP/HTTPS = OAuth en prácticamente todas las soluciones
- Muy popular y utilizado
- Simplicidad de implementación
- Gran cantidad de documentación



Protocolos de autenticación:

- OpenID

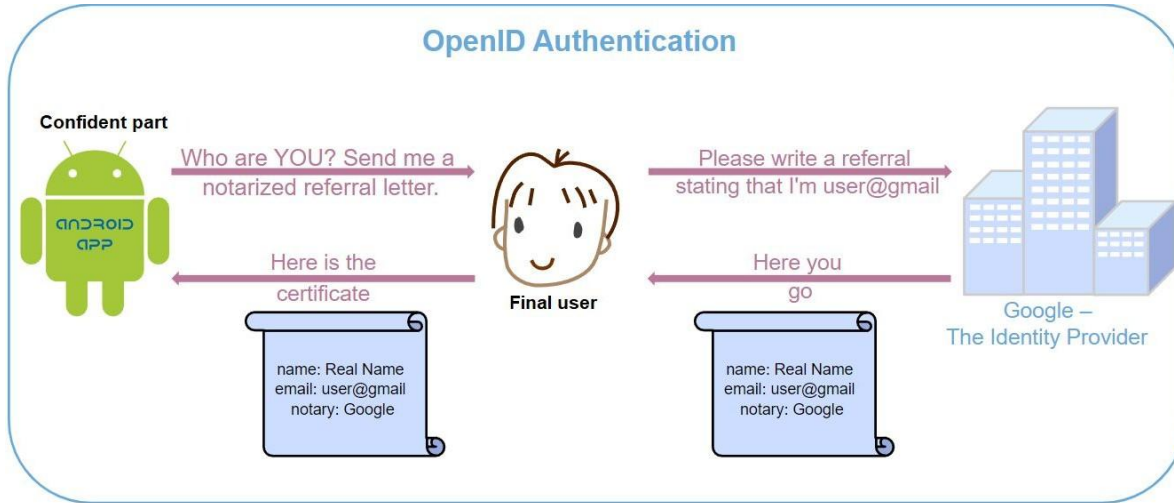


¿Qué es OpenID?

- Protocolo de autenticación que usa un servidor de autorización
- Capa de identidad encima del protocolo OAuth 2.0
- Single-sign-on



¿Cómo funciona OpenID?



- ROLES:
 - Parte confidente
 - Usuario final
 - Proveedor de identidad



Versiones y mejoras (OpenID Connect vs OpenID 2.0)

OpenID Connect:

- Mejora la estructura de los parámetros
- Facilita la usabilidad
- Añade funciones opcionales: cifrado de identidad, gestión de sesiones...
- Integra las capacidades de OAuth 2.0 en el propio protocolo

Puntos fuertes y débiles de OpenID

Puntos fuertes

- Single-sign-on
- El usuario puede escoger qué datos quiere compartir
- Estándar libre
- Ampliamente utilizado:



Puntos débiles

- Si no se crea un servidor de autenticación propio, la seguridad se basa en un servidor externo

Protocolos de autenticación:

- Kerberos

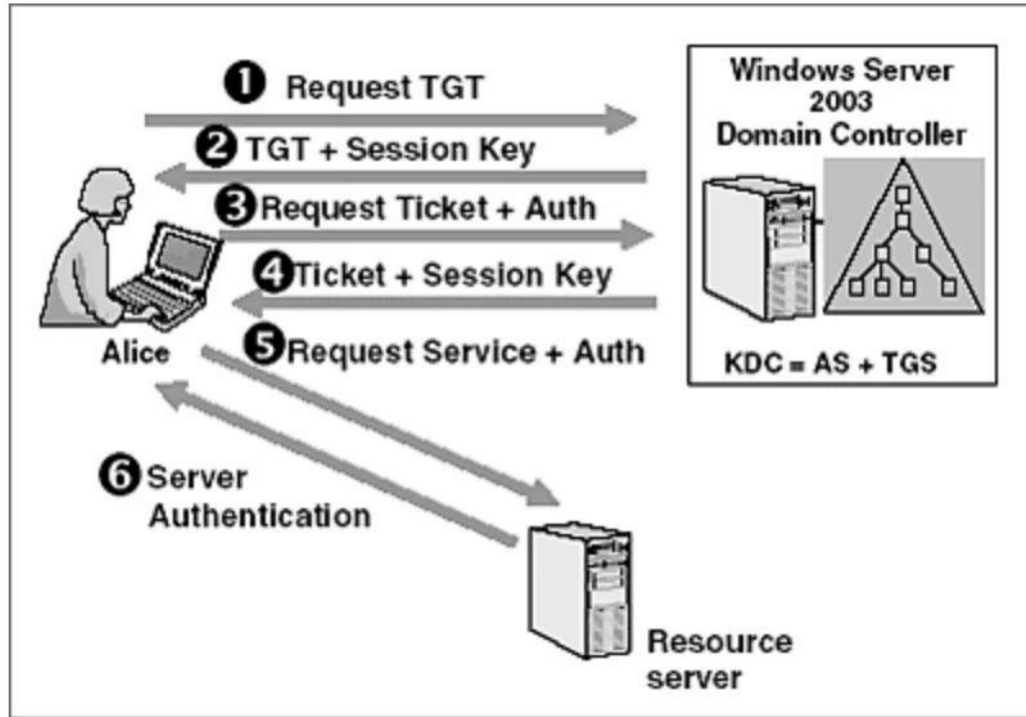


¿Qué es Kerberos?



- Protocolo para autenticar dos dispositivos que se conectan entre ellos
- Solución para los problemas de seguridad de la red
- Diseñado por el MIT.

¿Cómo funciona Kerberos?



TGT (Ticket de autorización)
KDC (Centro de distribución
de claves)



Puntos fuertes de Kerberos

- Los clientes y servidores se autentican mutuamente
- Compatible con diversos sistemas operativos
- Los tickets duran un periodo limitado. Si se roba el ticket, es difícil reutilizarlo debido a las fuertes necesidades de autenticación.
- Las contraseñas no se envían nunca a través de la red sin cifrar
- Se comparten claves secretas, son más eficientes que compartir claves públicas



Puntos débiles de Kerberos

- Vulnerable a contraseñas débiles o repetidas
- Solo proporciona autenticación para clientes y servidores.

Protocolos híbridos:

- OpenID Connect + OAuth 2.0
- Protocols AAA. Radius



Hybrid protocol OpenID + OAuth i Protocols AAA.

- Unificar en una única interfaz OpenID y OAuth
- AAA = Authentication, authorization y accounting
- RADIUS

CONCLUSIONES

- Protocolos ampliamente utilizados por todos
- Seguros y de confianza

Referencias

Andrukhanenko, O. (s/f). OAuth 2.0 explained in simple words, basic understanding. Stfalcon.com. Recuperado el 15 de mayo de 2022, de <https://stfalcon.com/en/blog/post/oauth-2.0>


Authentication protocol overview: OAuth2, SAML, LDAP, RADIUS, kerberos. (s/f). Getkisi.Com. Recuperado el 15 de mayo de 2022, de <https://www.getkisi.com/blog/authentication-protocols-overview>

Code, J. (2020, abril 2). Authentication & authorization in Web Apps. Jscrambler. <https://blog.jscrambler.com/authentication-authorization-in-web-apps>

Differences between OAuth 1 and 2. (2016, agosto 17). OAuth 2.0 Simplified. <https://www.oauth.com/oauth2-servers/differences-between-oauth-1-2/>

Kerberos. (s/f). Education-wiki.com. Recuperado el 15 de mayo de 2022, de <https://es.education-wiki.com/4067093-kerberos>

Kerberos: The Network Authentication Protocol. (s/f). Mit.edu. Recuperado el 15 de mayo de 2022, de https://web.mit.edu/kerberos/#what_is



Mizrachi, A. (2022, febrero 24). Authentication: Methods, protocols, and strategies. Frontegg.
<https://frontegg.com/blog/authentication>

OpenID connect. (2011, agosto 1). OpenID - The Internet Identity Layer. <https://openid.net/connect/>

¿Qué es OAuth? ¿Qué proporciona su protocolo? (2020, junio 19). NTS SEIDOR.
<https://www.nts-solutions.com/blog/oauth-que-es.html>

Recordon, D., Rae, L., & Messina, C. (2010). OpenID: The Definitive Guide. O'Reilly Media.
[https://www.ecured.cu/OpenID#Ventajas de utilizar OpenID](https://www.ecured.cu/OpenID#Ventajas_de_utilizar_OpenID)

Sánchez, J. (2011, junio). COMPUTACIÓN DISTRIBUIDA. SISTEMAS DE AUTENTICACIÓN Y AUTORIZACIÓN EN INTERNET. [https://jordisan.net/proyectos/Autent y auth-J Sanchez.pdf](https://jordisan.net/proyectos/Autent_y_auth-J_Sanchez.pdf)

Wikipedia contributors. (2022a, mayo 9). RADIUS. Wikipedia, The Free Encyclopedia.
<https://en.wikipedia.org/w/index.php?title=RADIUS&oldid=1086913506>

Wikipedia contributors. (2022b, mayo 14). OAuth. Wikipedia, The Free Encyclopedia.
<https://en.wikipedia.org/w/index.php?title=OAuth&oldid=1087749385>



Reparto del trabajo

Marc Cerrillo Molinero: transparencias

Raúl Cutillas Benítez: presentación

Àlex Fernández López: presentación

Marc Fonseca Pagès: transparencias