Mecanismes de securització

Autenticació bàsica

És la forma més bàsica d'autenticació disponible per les aplicacions web, es va definir en la primera especificació del protocol HTTP. Sense ser un mecanisme elegant acompleix la seva funció. Aquest mecanisme no requereix la utilització de cookies, ni identificadors de sessió, ni pàgines de login.

Aquest procés fou dissenyat amb la finalitat que el navegador web pugui aportar les credencials basades en l'usuari i la contrasenya i que així li permetin autenticar-se davant d'un servei. Les dades s'envien codificades únicament en Base64. Aquest mecanisme és completament reversible i permet obtenir les dades que s'hi codifiquen sense cap dificultat.

> Cyberchef. Base64

Com funciona aquest protocol

Quan el servidor vol que el client s'autentiqui envia dins la capçalera de resposta a la petició el camp **WWW-Authenticate** per una autenticació bàsica.

```
WWW-Authenticate: Basic realm="nmrs_m7VKmomQ2YM3:"
```

El client en el moment de rebre-ho, demana a l'usuari les credencials sol·licitades, per a construir la capçalera d'autorització que és una cadena del tipus "usuari:contrasenya", la cadena de caràcters resultant es codifica en RFC2045-MIME de Base64 sense la limitació de 76 caràcters que imposa la RFC. D'aquesta forma quedaria una cadena d'autenticació com la següent:

```
Authorization: Basic YWRtaW5pc3RyYWRvcjoxMjM0
```

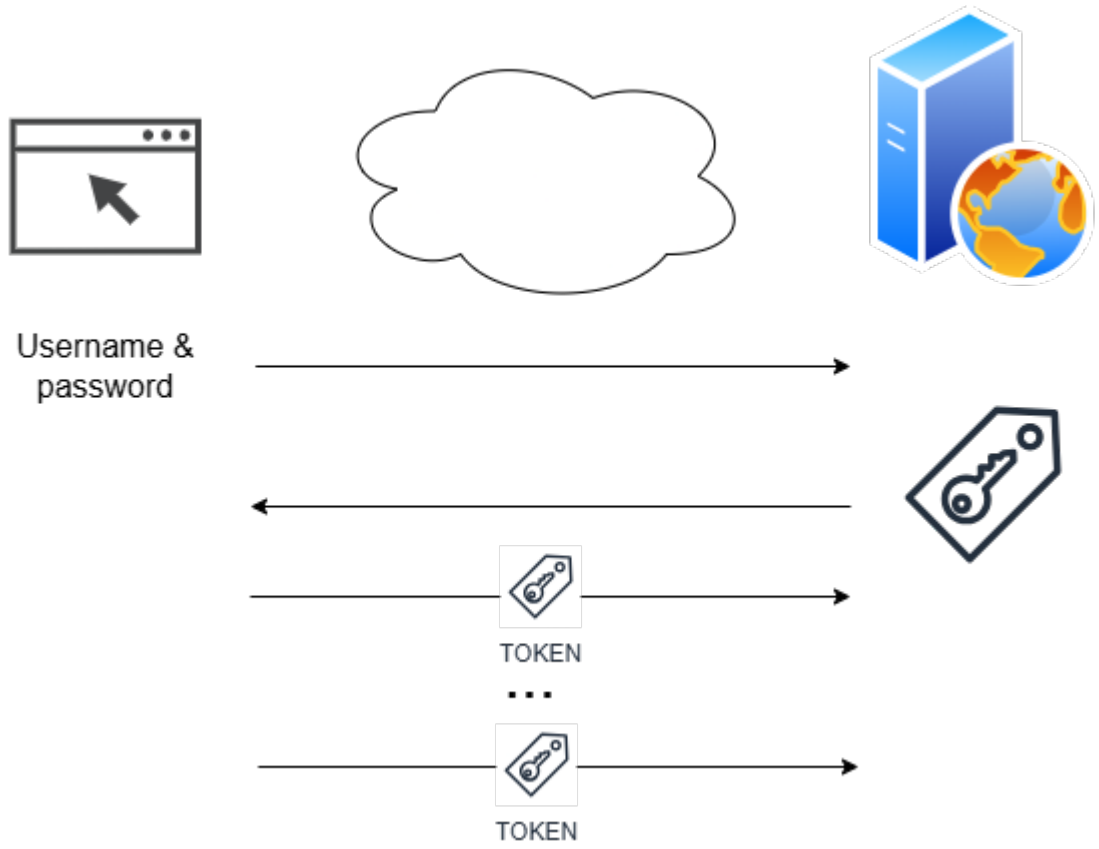
Si utilitzem Cyberchef podem obtenir usuari i password fàcilment

> https://es.wikipedia.org/wiki/Autenticación_de_acceso_bàsica

Autenticació del portador

L'autenticació del portador consisteix en la comunicació mitjançant un token que s'envia en cada crida. Aquest element permet verificar la identitat o el rol de l'usuari a la part client.

L'usuari envia el nom d'usuari i la seva contrasenya i el servidor després de verificar-ho li retorna un token. A partir d'aquell moment aquest token és l'element que envia a cada petició que fa el client.



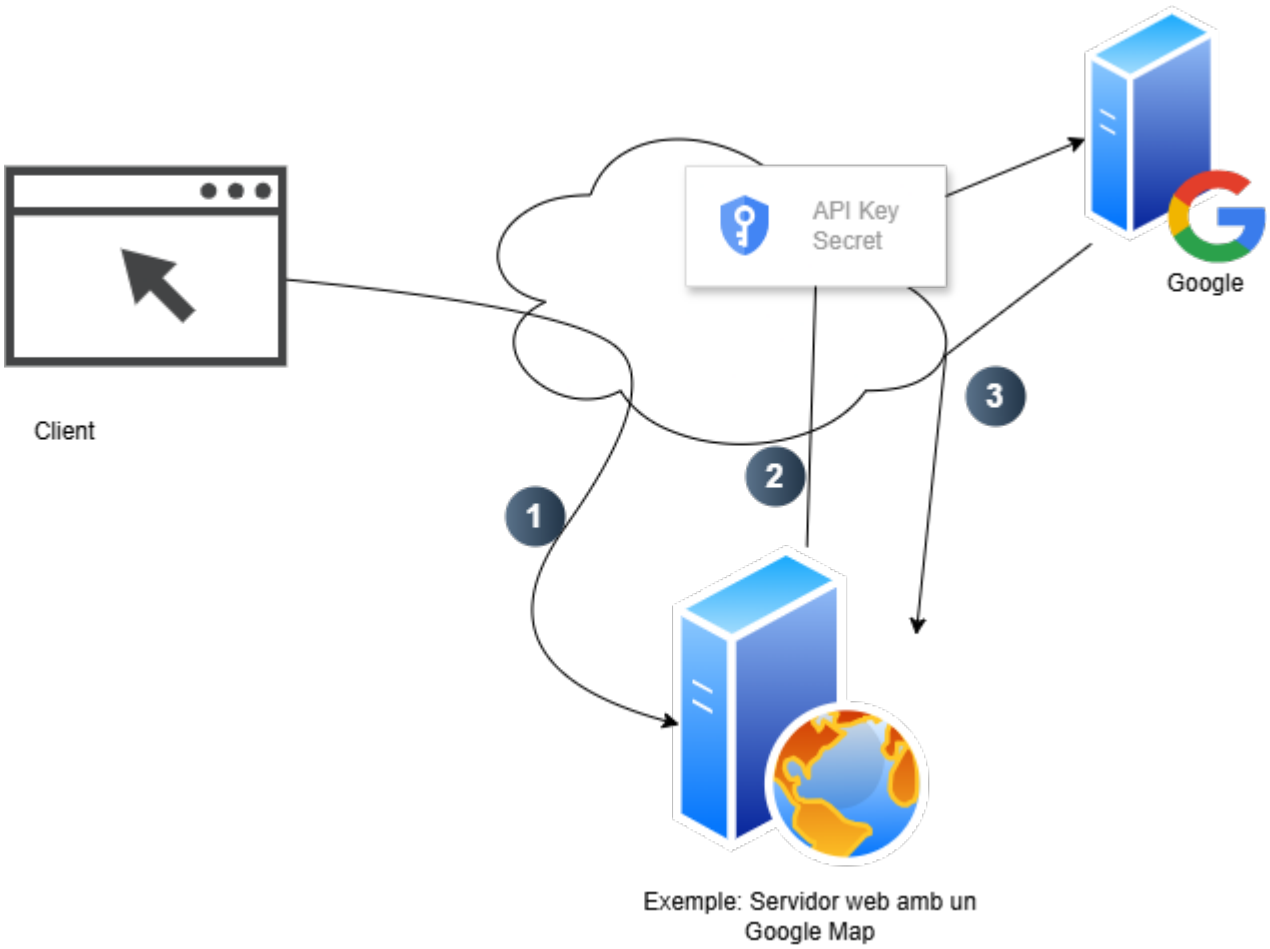
Els tokens generats poden ser de diferents tipus:

- Codi basat tipus UUID que s'emmagatzema en el servidor per saber qui l'ha generat i els privilegis que té aquest usuari.
- Token en format Tokens JWT

Claus API

En alguns casos l'usuari final o client no serà l'encarregat d'utilitzar l'API sinó que són serveis externs que faran la funció de client i, per tant, seran l'origen de la crida a l'API. En aquestes ocasions a cada origen se li assigna una clau API per així fer el seguiment de com està essent usada l'API, i així evitar utilitzacions malicioses o abús de l'API.

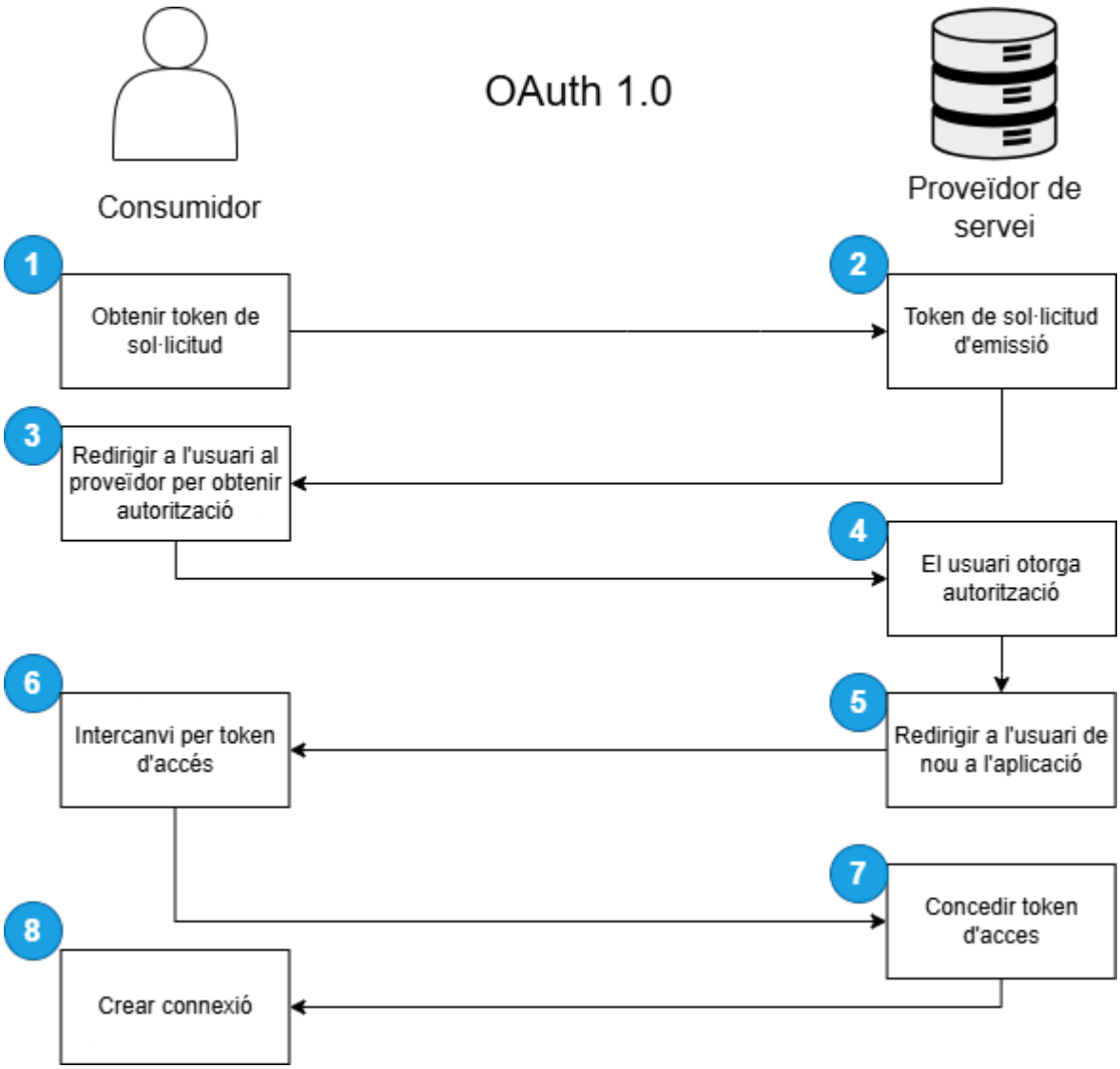
En moltes ocasions aquesta clau API actua com identificador únic i utilitza també un testimoni o token secret per la seva validació. Igual que en els casos anteriors aquesta clau tindrà associats uns drets d'accés. Aquestes claus API poden estar basades en el sistema d'identificació universal unívoca o UUID per assegurar que cada usuari té una clau única.

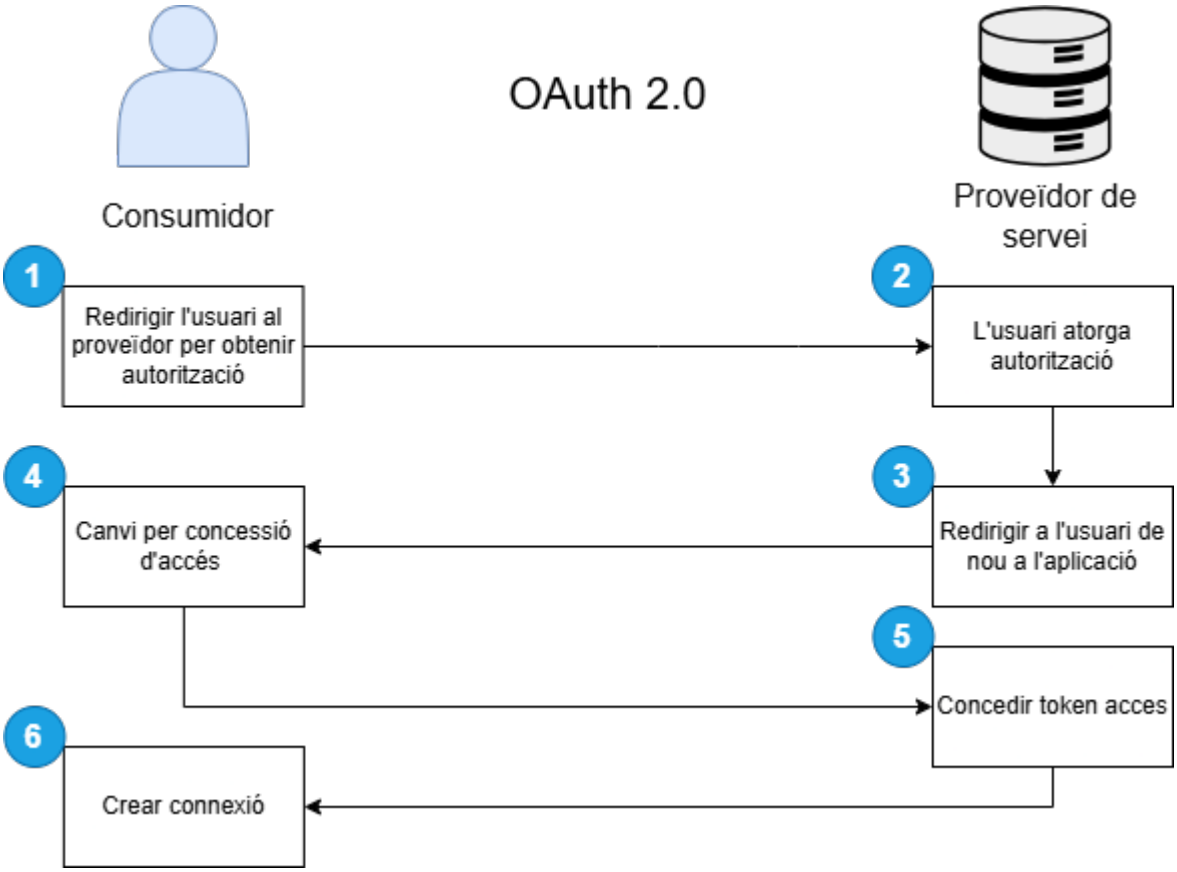


Exemple: Accedim un web que ens mostra per pantalla un mapa de google Maps

OAuth

Open Authorization és un estandard obert que permet fluxes d'autorització per a llocs web o aplicacions informàtiques. Aquest mecanisme permet a un usuari del lloc A (**proveïdor** de servei) comparteix amb el lloc B (**consumidor**) sense compartir tota la seva identitat. Per als desenvolupadors de consumidors OAuth els permet interactuar amb dades protegides i publicar-les, per als proveïdors aquest mecanisme proporciona als usuaris un acces a les seves dades al mateix temps que protegeix les credencials del seu usuari. Aquest mecanisme està molt utilitzat per Google, Facebook, Microsoft, Twitter, entre altres, per permetre als usuari compartir informació sobre els comptes amb aplicacions de tercers o llocs web.


OAuth 1.0
Consumidor
Proveïdor de servei
1
Obtenir token de sol·licitud
2
Token de sol·licitud d'emissió
3
Redirigir a l'usuari al proveïdor per obtenir autorització
4
El usuari otorga autorització
5
Redirigir a l'usuari de nou a l'aplicació
6
Intercanvi per token d'accés
7
Concedir token d'acces
8
Crear connexió



Revisió núm. 10
★Admin l’ha creat 2025-06-04 17:02:08 UTC
Admin l’ha actualitzat 2025-06-05 16:41:08 UTC