1 LOPEZ ALMEIDA, ANDRES ISAIAS

What is OAuth?

OAuth is an open standard authorization protocol that provides applications with the ability to secure specific access. OAuth uses authorization tokens to prove identity between consumers and service providers, allowing you to authorize one application to interact with another application on your behalf without revealing your password.

For example, you can tell Facebook ESPN.com can access your profile or post updates to your timeline without telling ESPN your Facebook password. This greatly reduces risk: if ESPN is compromised, your Facebook password remains safe.

OAuth works in 6 steps:

Step 1 - User Display Intent
Step 2 - The consumer Gets Permission
Step 3 - The user will be redirected to the service provider
Step 4 - User Grants Permissions
Step 5 - Consumer receives an access token
Step 6 - Consumer Access to Protected Resources

Reference:
Sobers R. (April 5, 2012). *What is OAuth? Definition and How it Works.*
https://www.varonis.com/blog/what-is-oauth

2 MALTE VILLARREAL, DENNIS MARCELO

OAuth is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices.

It works by delegating user authentication to the service that hosts a user account and authorizing third-party applications to access that user account.

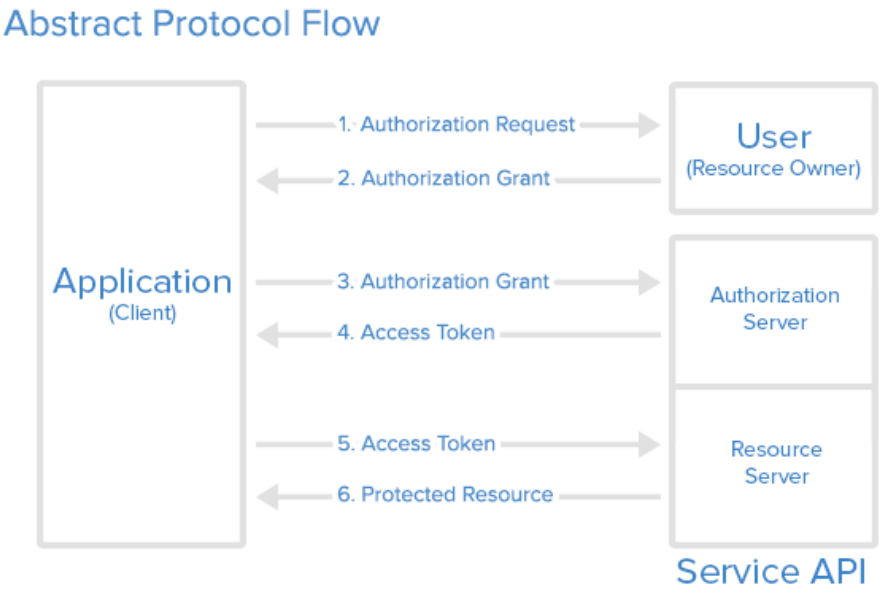
OAuth Roles

Resource Owner: The resource owner is the user who authorizes an application to access their account.

Client: The client is the application that wants to access the user ’s account.

Resource Server: The resource server hosts the protected user accounts.

Authorization Server: Verifies the identity of the user then issues access tokens to the application.



Reference:
https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

3 MEDINA ARMIJOS, MARTIN ANDRES

4 PAEZ ZAPATA, DIEGO ALEXANDER

5 PAREDES MEDRANO FERNANDO PATRICIO

6 POMA AGUILAR, DAYSE NICOLE

What is OAuth?

It is an authorization protocol that gives applications the ability to “secure designated access”, which allows you to approve an application that interacts with another on your behalf without revealing your password. Allowing to minimize the risk of data leakage.

The OAuth (Open Authorization) protocol was developed by the Internet Engineering Task Force and enables secure delegated access. Allows an application to access a resource controlled by another person (end user). This type of access requires Tokens, which represent the delegated right of access. This is why applications gain access without impersonating the user who controls the resource.

Features
The idea of roles is central to the OAuth framework and defines the essential components of a system:

- Resource Owner: The user or system that owns the protected resources and can grant access to them.
- Client: The client is the system that requires access to the protected resources. To access the resources, the Client must have the appropriate access token.
- Authorization server: This server receives requests for access tokens from the client and issues them upon successful authentication and consent of the resource owner. The authorization server exposes two endpoints: the authorization endpoint, which handles interactive authentication and user consent, and the token endpoint, which is involved in machine-to-machine interaction.
- Resource Server: A server that protects user resources and receives access requests from the Client. Accepts and validates an access token from the client and returns the appropriate resources to it.

Bibliography

Google Developers OAuth 2.0 Playground. Retrieved June 10, 2022 from https://developers.google.com/oauthplayground/

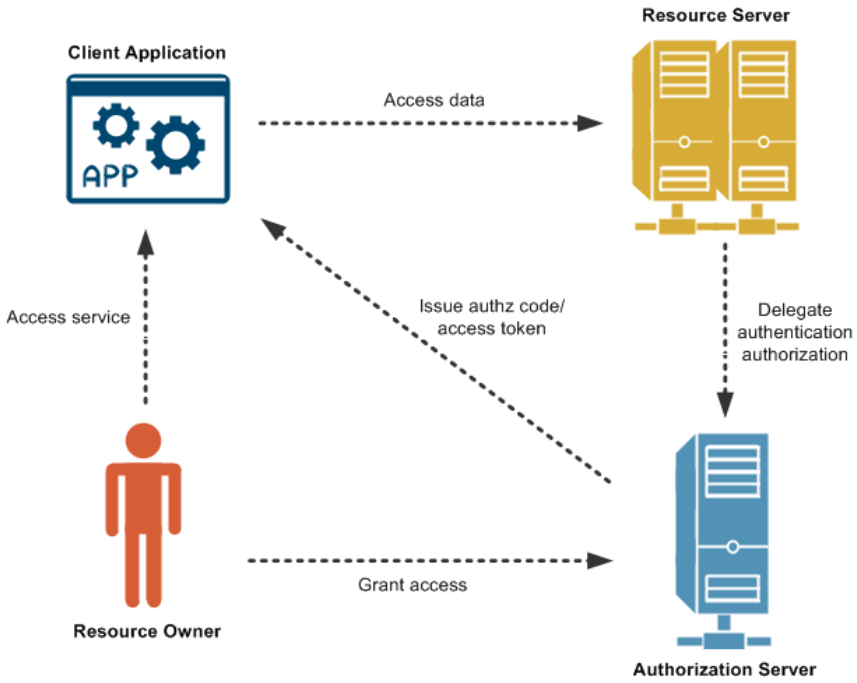
7 RIASCOS MORENO, ERICK GERMAN

OAuth 2.0 is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. This specification and its extensions are being developed within the IETF OAuth Working Group.

OAuth started in November 2006, when Blaine Cook was developing the OpenID implementation for Twitter. Meanwhile the company Ma.gnolia, with a social bookmarking service, needed a solution that would allow its members with OpenID to authorize dashboard widgets to access their service. That's when Blaine Cook, Chris Messina, and Larry Halff of Ma.gnolia (now Gnolia) met with David Recordon to discuss using OpenID with the Twitter and Ma.gnolia APIs to delegate authentication. They concluded that there was no open standard for delegating access to APIs.

In April 2007, the OAuth discussion group was created for a small group of developers to write a draft proposal for an open protocol. Google's DeWitt Clinton heard about the OAuth project and was interested in supporting the effort. The team finished the initial draft of the specification in July 2007. Eran Hammer-Lahav joined and coordinated the

various contributions to OAuth, creating a more formal specification. The final Oauth Core 1.0 draft was released on October 3, 2007.

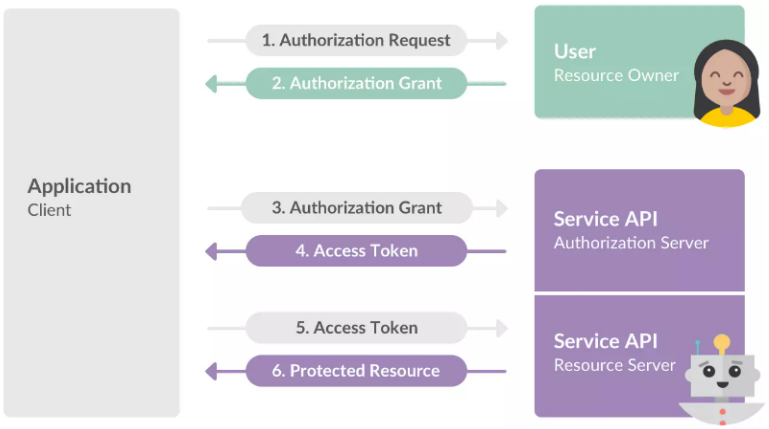


8 RISUEÑO ZAPATA, SANTIAGO FABIAN

OAuth stands for Open Authorization, it allows interaction between two applications, allowing them to use your name with the security of not revealing your password. It is possible because it provides access tokens to third-party services without exposing user credentials.

OAuth is about authorization and not about authentication. Request and receive permission to access specific data, features, or areas of an application or system. It only authorizes secure access in the form of temporary tokens.

- OAuth Flow
    1. The application requests authorization to access a protected service provider.
    2. The user authorizes the request.
    3. The application provides proof of user authorization to the service provider in exchange for an access token.
    4. The user is redirected to the service provider to provide permission.
    5. Once approved by the user, the application obtains the access token.
    6. The application requests access to the protected resources from the service provider.



Reference:

https://www.fortinet.com/
Fortinet | Enterprise Security Without Compromise

https://www.redeszone.net/tutoriales/seguridad/que-es-oauth/

9 RIVERA VEGA, STALIN BLADIMIR

OAuth

Open Authorization is an open standard that enables simple authorization flows for web sites or computer applications. It is a protocol proposed by Blaine Cook and Chris Messina, which allows secure authorization of an API in a simple and standard way for desktop, mobile and web applications.

OAuth: how this service works for web pages

OAuth was born as a result of the development of Open ID for Twitter, when its developer Blaine Cook received a special request to see if with Open ID he could authorize widgets in the dashboard to access his services.

In 2007, the discussion group was formed on how what we know today as OAuth should be. Its function at that time was none other than to write a preliminary project with all the ideas and proposals to create a free and open protocol, that is, free software so that any company and user could incorporate it into their websites or online services.

How OAuth 2.0 works

OAuth 2.0 is really an authorization framework, which allows applications to gain limited access to user accounts for some services like Facebook, Google, Twitter and GitHub. Its operation basically consists of delegating the user's authentication permission to the service that manages these accounts, so that it is the service itself that grants access to third-party applications.

Client

It would be the application that wants to access the user account of a certain service, such as Facebook, Twitter, Google, etc. It is a process that will serve to save time and also verify the authenticity of a user.

User

The user is the one who authorizes the application to access his account, through a pop-up window that asks for authorization, and information about the data that is going to be shared with the new service is usually included.

Server

The authorization server receives access requests from applications that want to use the login of some of the services such as Facebook, Twitter or Google.

10 ROMAN VERDEZOTO, IVETTE YULLIANA

11 ROSERO MOSQUERA, THEO MARTIN

Definition of Oauth OAuth is an open standard authorization framework or protocol that describes how servers and unrelated services can securely allow authenticated access to their assets without actually sharing the login credential. Created and strongly supported early on by Twitter, Google and other companies, OAuth was released (Oauth 1.0) as an open standard in 2010 as RFC 5849 Oauth and Authentication Systems, and quickly became widely adopted. Over the next two years, it underwent substantial revision, and version 2.0 of OAuth was released in 2012 as RFC 6749.

Although version 2.0 was widely criticized for multiple reasons, it gained much popularity in authentication systems. Today, it is adopted by many services such as Amazon, Facebook, Instagram, LinkedIn, Microsoft, Netflix, Paypal, among others. The simplest example of OAuth is when you go to log in to a website (let's call it A) and you are offered one or more options to log in with the login of another website/service (let's call it B). You then click on the button linked to the other website (B), and this other website authenticates you, and finally, you can connect to the

original website (A) after using the permission obtained on the second website (B).

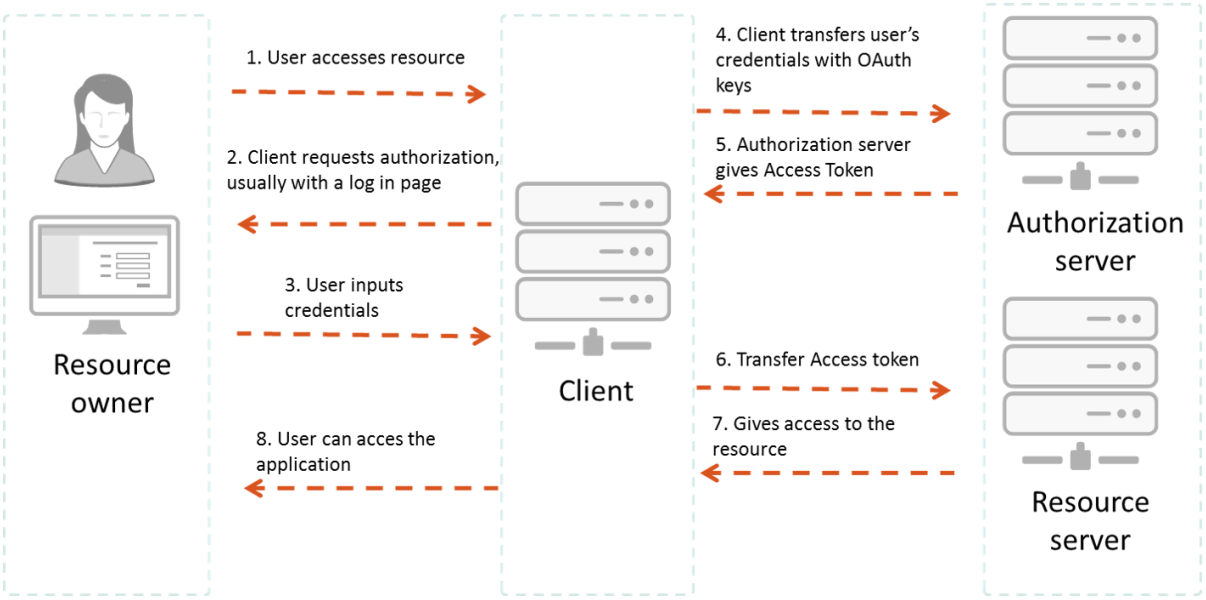
12 RUIZ MAFLA, JERICÓ BENJAMIN

13 SUNTAXI LEMA, STALYN FRANCISCO

OAuth

OAuth (Open Authorization), It is an identity and access management solution, Its main purpose is to grant authorizations to users. This is a protocol for passing authorization from one service to another without sharing actual user credentials, such as a username and password. In this way a user can log in to one platform and then be authorized to perform actions and view data on another platform.

How it works?



In 2012 OAuth 2.0 replaced OAuth 1.0 and is now the standard providing consented access and restricting what actions the client application can perform on resources on behalf of the user, never sharing the user's credentials.

These are the essential components of an OAuth 2.0 system.

Resource Owner: Is the user or system that owns the protected resources.
Client : The client is the system that requires access to the protected resources.
Authorization server: The server receives requests for access tokens from the client and issues them upon successful authentication and consent of the resource owner.
Resource Server: A server that protects the user's resources and receives access requests from the Client, in addition to returning the appropriate resources.

Advantages:

- OAuth 2.0 is a very flexible protocol that is based on SSL (Secure Sockets Layer), which ensures that data between the web server and browser remains private.
- OAuth 2.0 Secure cryptographic industry protocols and is used to maintain data security.
- It has the ability to share data for users without having to disclose personal information.
- It is easier to implement and provides stronger authentication.

References:

- outh0. (s.f.). What is OAuth 2.0? Retrieved on June 9, 2022, from https://auth0.com/intro-to-iam/what-is-oauth-2/
- Dharshika Singarathnam. (September 23, 2019). Introduction to OAuth 2.0 Protocol. Retrieved from https://medium.com/@dharshikasingarathnam/introduction-to-oauth-2-0-protocol-90b1ffc93f60

advanced web programming

OAUTH

Why OAuth arises

It arises to alleviate the need that is established for the continuous sending of credentials between client and server.

roles

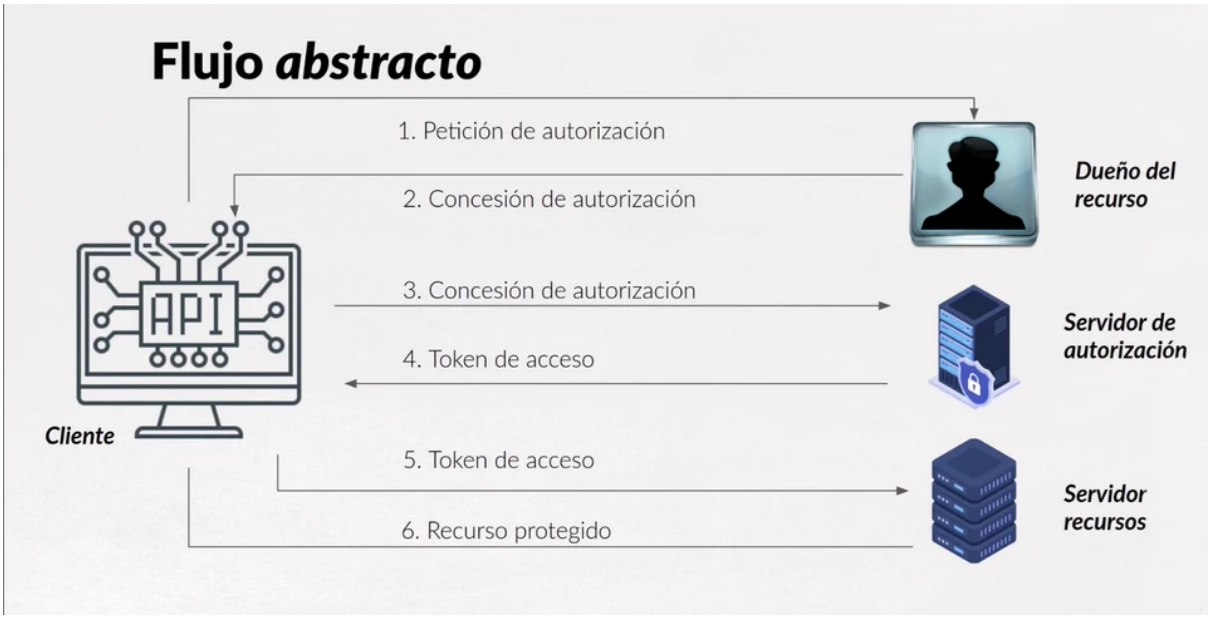
Within OAuth 2.0 we find different roles that will participate in the process:

- Owner of the resource (Owner).

- Client (Client).
- Protected resource server (Resource Server).
- Authorization Server.

If we plan to develop a REST API and a client application that can consume our services, if we want to have a minimum of security mechanisms, before OAuth2 we needed the user to send us the credentials.

Flow



An example would be the following:

https://authorization.server.com//authorize?response_type=code&client_id=the-client-id&state=xyz&redirect_uri=https://client.example.com/cb&scope=api_read

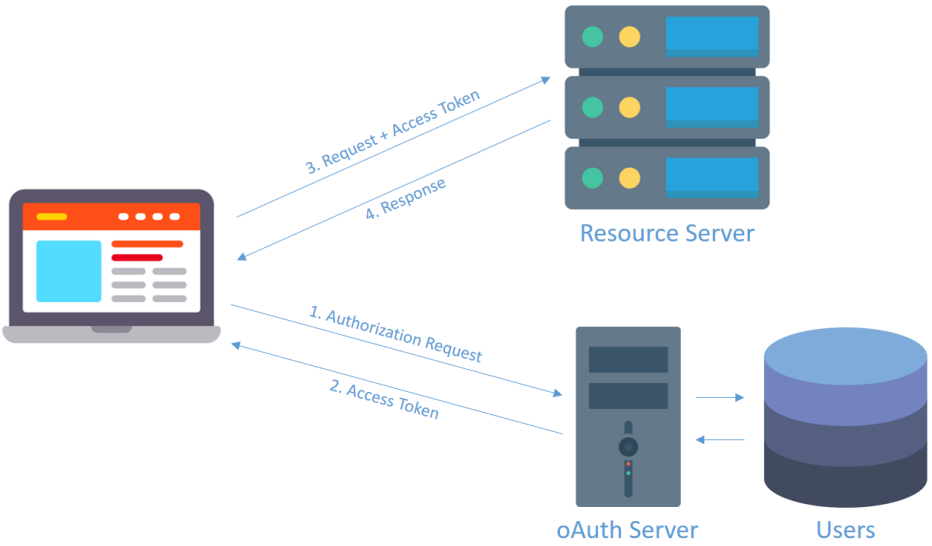
15 VACA CHUNGANA, EDISON MAURICIO

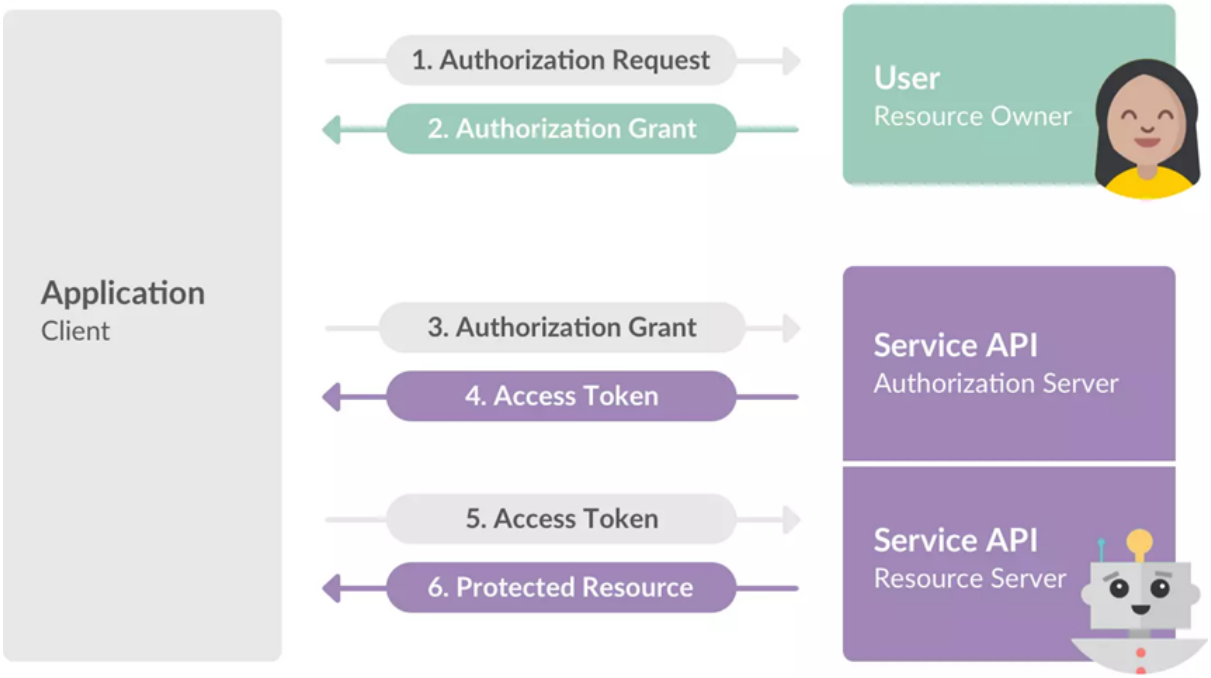
OAUTH

OAuth was born out of the development of Open ID for Twitter, when its developer, Blaine Cook, received a special request to see if Open ID could authorize dashboard widgets to access its services. In 2007, a focus group was formed to discuss what we know today as OAuth should look like. The test version was finally completed in July 2007, after only four months, and in October 2007 the Oauth Core 1.0 draft was finally released, which was a big change in access to services.

OAUTH 2.0

Recall that OAuth 2.0 is actually an authorization framework, which allows applications to gain limited access to the user accounts of some services such as Facebook, Google, Twitter and GitHub. It basically works by delegating the user's authentication permission to the service that manages those accounts, so that it is the service itself that grants access to third-party applications. Let's say we download a program or open a page that requires us to have a user. The latter will save us time, as we simply sign up through a third-party service, such as one of the most popular social networks or Google





OAuth comes from the root of the development of Open ID for Twitter, when its developer, Blaine Cook, received a special request to see if Open ID could authorize dashboard widgets to access their services. After Blaine Cook, Chris Messina and Larry Halff met, they realized that there was no free software standard to be able to delegate access to the different APIs.

OAuth 2.0 is really an authorization framework, which allows applications to gain limited access to user accounts for some services like Facebook, Google, Twitter and GitHub. Its operation basically consists of delegating the user's authentication permission to the service that manages these accounts, so that it is the service itself that grants access to third-party applications.

Client

It would be the application that wants to access the user account of a certain service, such as Facebook, Twitter, Google, etc. For example, if we install an application on the mobile and it asks us for permission to see our data on any of these social networks or platforms. In this way we will avoid having to fill in all the content again and it will take it automatically.

User

The user is the one who authorizes the application to access his account, through a pop-up window that asks for authorization, and information about the data that is going to be shared with the new service is usually included. When we try to link any program with Facebook or Twitter, for example, we will have to authorize the application that can transfer that information.

Server

The authorization server receives access requests from applications that want to use the login of some of the services such as Facebook, Twitter or Google, for example, to log in to a web page, game, etc. This server is responsible for verifying the identity of the user and the service requesting access, allowing or denying access.

Bibliography

Espinosa, O. (23 of July 2021). *Redes Zone*. Obtained from https://www.redeszone.net/tutoriales/seguridad/que-es-oauth/

17 YANZAPANTA ONTANEDA, BRYAN SEBASTIAN

OAuth is the standardization and combined wisdom of many well-established industry protocols. It is similar to other protocols currently in use (Google AuthSub, AOL OpenAuth, Yahoo BBAuth, Upcoming API, Flickr API, Amazon Web Services API, etc). Each protocol provides a proprietary method of exchanging user credentials for an access token or ticker. OAuth was created by carefully studying each of these protocols and extracting best practices and commonalities that will enable new implementations as well as a smooth transition to existing services supporting OAuth.

OAuth 2.0 is an open standard for API authorization, which allows us to share information between sites without having to share identity.
It is a mechanism used today by large companies such as Google, Facebook, Microsoft, Twitter, GitHub or LinkedIn, among many others.

It uses different authentication flows, such as the authorization code flow, the password owner flow, the implicit flow, among others, as well as the extension of flows, which also allow us to define new flows.
It arises to alleviate the need that is established for the continuous sending of credentials between client and server.

Bibliography

Introduction — OAuth. (2007, 7 septiembre). OAuth.https://oauth.net/about/introduction/

18 YEPEZ CHANDI, CHRISTOPHER DANIEL

OAUTH

Open Authorization is an open standard that enables simple authorization flows for web sites or computer applications. It is a protocol proposed by Blaine Cook and Chris Messina, which allows secure authorization of an API in a simple and standard way for desktop, mobile and web applications.

OAuth allows a user from site A to share their information on site A (service provider) with site B (called consumer) without sharing their full identity. For consumer developers, OAuth

is a method of interacting with and publishing protected data. For service provider developers, OAuth gives users access to their data while protecting their account credentials. This mechanism is used by companies such as Google, Facebook, Microsoft, Twitter, and Github to allow users to share information about their accounts with third-party applications or websites.

19 ZAPATA SANDOVAL, JONATHAN ISMAEL

OAUTH

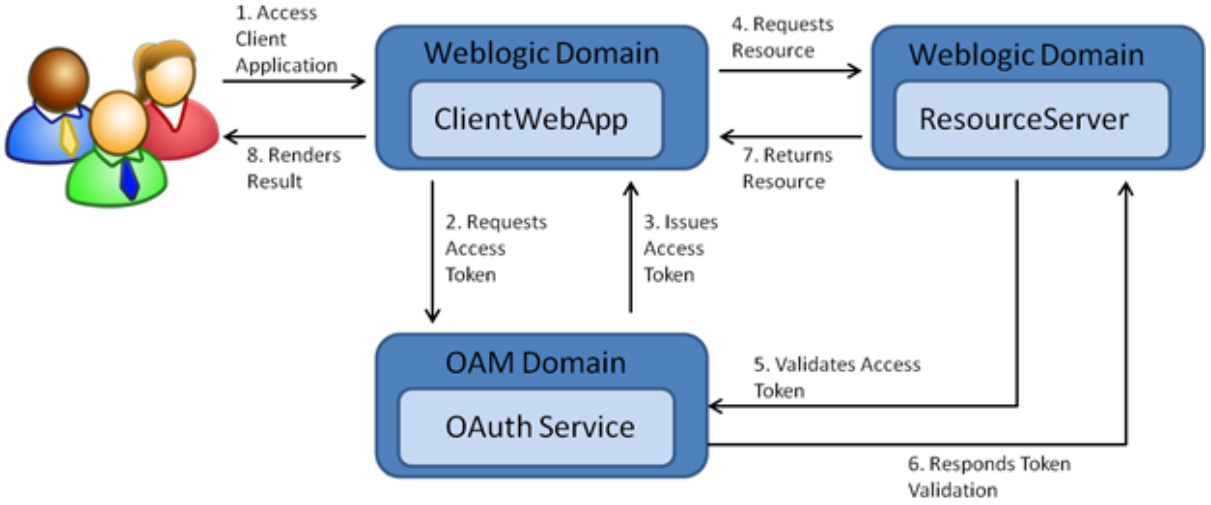
Open Authorization Performs Authorizations Or Accesses To Conte Users Also Hides The Credentials Of OTHER Users, Send Authorization Information Between Different Applications, Without Exposing The Data Of Any User, Also

It prevents us from being able to log in very easily on different websites, the condition for this to execute is within the https protocol, and

Redirects the User to the Client Application with an Access Code.

Oauth Allows Partial Access from one application to another, which is responsible for transforming it into an access token, finally

It is a great advantage in terms of access to services for the user (web pages and videogames).



Reference:

OAuth 2.0 (oracle.com)

20 ZAPATA ZAPATA, SEBASTIAN ALEXANDER