**Autenticación federada – Federated Authorization:**

En un entorno comporativo la autorización federada consisten en centralizar la autenticación en un sistema como LDAD server, Active Directory server o SAML.

En un entorno web el sistema de autenticación federada es OPENIID, proporcionado porGooble o Yahoo. El sucesor de OPENID e AOuth2.

**Autorización delegada – Delegated Authorization:**

Se trata de autorizar a otra persona o aplicación (cliente) para poder realizar acciones en nuestro nombre.

**OAuth2 frente OAuth1:**

OAuth WRAP, predecesor de OAuth2, eliminino los requerimientos de firma cifrada en los requerimientos y creo los tokens bearer.

La implementación de AOuth2 debe confirmar:

* Comprobar que el nombre del servidor devuelto por la cadena de certificación devuelta por el servidor, coincide con el nombre del host de la URL a la que se accede.
* Verificación de que cada certificado de la cadena tiene una Autoridad de certificación (CA).
* Asegurarse que el paquete de autoridad de certificación sea seguro y no pueda modificarse por atacantes.

**Roles en el protocolo OAuth2**:

Resource Server:

El servidor que aloja recursos propiedad del usuario que están protegidos por OAuth.

Resource Owner:

Típicamente el usuario de la aplicación. Es el propietario de los recursos protegidos por OAuth2.

Client:

Se trata de la aplicación que por medio del API solicita acceso a los recursos protegidos con la autorización del propietario (resource owner).

Authorization server:

Tiene el consentimiento del propietario del recurso, emite el token de acceso hacia el cliente para poder acceder a los recursos protegidos por el “resource server”.

Es posible el Authorization y el Resource server estén en la misma máquina.

**Firma de solicitudes OAuth2:**

El API OAuth2 proporcionada por la7 entidad puede soportar o requerir la firma de las solicitudes. Para su implementación hay un estándar llamado MAC Access Authentication.

Obtención de la clave MAC:

Para elaborar la solicitud utilizando MAC Authentication, necesitamos un clave que es proporcionada junto con el token de acceso por el server de autorización.

También la clave MAC puede emitirse por un proceso fuera de banda (out-of-band process) como cuando el desarrollador registra su aplicación con el proveedor del API.

**Registro de la aplicación (desarrollador):**

Las credenciales obtenidas en este registro con el servidor de autorización, son esenciales para proteger la autenticidad de las solicitudes a la hora de obtener los token de acceso y de actualización de token.

Google proporciona el registro de un cliente desde API´s CONSOLE <https://console.developers.google.com/apis/library>

Y para Facebook <https://developers.facebook.com/apps>

Una vez rellenado el formulario de registro, el desarrollador recibirá las credenciales : client-id y client-secre.