

Un Servidor de Autorización OAuth 2.0

An OAuth 2.0 Authorization Server

OAuth es un estándar abierto para autorización. OAuth provee a aplicaciones cliente de un “acceso delegado seguro” a servidores de recursos en nombre del propietario del recurso. Especifica un proceso para que propietarios de recursos autoricen el acceso de terceras partes a sus servidores de recursos sin compartir sus credenciales. Diseñado específicamente para trabajar con HTTP, OAuth esencialmente permite que un servidor de autorización entregue tokens de acceso a aplicaciones cliente, con la aprobación del dueño de los recursos o usuario final (el token de acceso es una cadena indicando un ámbito específico, un tiempo de vida y otros atributos de acceso). La aplicación cliente hace uso del token de acceso para acceder a los recursos protegidos alojados en el servidor de recursos.

OAuth es comúnmente usado como una manera para que los usuarios accedan a sitios web de terceros usando sus cuentas de Microsoft, Google, Facebook, Twitter, etc. sin preocuparse por si sus credenciales de acceso están siendo comprometidas.

Los objetivos marcados para el desarrollo de este proyecto son los siguientes:

1. El principal objetivo es implementar un servidor de autorización utilizando el estándar OAuth 2.0 que permita a usuarios de aplicaciones de terceros conectarse a dichas aplicaciones sin que éstas tengan la necesidad de conocer ni validar las credenciales de los usuarios. Además de tokens de acceso, también emitirá tokens de refresco, que sirven para obtener nuevos tokens de acceso sin necesidad de que el usuario tenga que volver a introducir sus credenciales. El servidor se desarrollará en C# usando el Framework de .NET, siguiendo la arquitectura OWIN y con tecnologías como Web API 2, Entity Framework 6, ASP.NET Identity 2 y Autofac.
2. Dicho servidor hará también las funciones de servidor de recursos, para permitir la gestión de la configuración de todos los datos referidos a la autorización de usuarios.
3. También se ha pensado en la realización de una aplicación web de una sólo página (*SPA* por sus iniciales en inglés, *Single Page Application*) realizada principalmente con AngularJS, HTML5 y Bootstrap. Esta aplicación tendrá varias secciones entre las que se incluyen la gestión de los usuarios, la gestión de las aplicaciones cliente que vayan a hacer uso del servidor de autenticación y la gestión de los tokens de refresco que el servidor haya emitido, lo que permitirá invalidarlos por cualquier motivo, forzando al usuario a introducir nuevamente sus credenciales.

Estos objetivos han sido llevados a cabo, lo que queda patente en la memoria a la que acompaña el presente documento.