OAuth

OAuth adalah open standard [standar terbuka] untuk access delegation [delegasi akses], yang biasa digunakan sebagai cara bagi pengguna Internet untuk memberikan situs web atau aplikasi akses ke informasi mereka di situs web lain tetapi tanpa memberi mereka kata sandi. [1] Mekanisme ini digunakan oleh perusahaan seperti Amazon, [2] Google, Facebook, Microsoft dan Twitter untuk mengizinkan pengguna untuk berbagi informasi tentang akun mereka dengan aplikasi pihak ketiga atau situs web.

Secara umum, OAuth memberikan kepada klien "secure delegated access" [akses aman yang didelegasikan] ke server resources atas nama resource owner [pemilik data]. Ini menentukan proses bagi resource owner untuk mengotorisasi akses pihak ketiga ke server resource mereka tanpa berbagi kredensial mereka. Dirancang khusus untuk bekerja dengan Hypertext Transfer Protocol (HTTP), OAuth pada dasarnya memungkinkan token akses yang akan dikeluarkan untuk klien pihak ketiga oleh authorization server, dengan persetujuan dari resource owner. Pihak ketiga kemudian menggunakan token akses untuk mengakses sumber daya yang dilindungi yang diselenggarakan oleh resource server.

OAuth adalah layanan yang saling melengkapi dan berbeda dari OpenID. OAuth tidak terkait dengan OATH, yang merupakan arsitektur referensi untuk otentikasi, bukan standar untuk otorisasi. Namun, OAuth secara langsung terkait dengan OpenID Connect (OIDC), karena OIDC adalah lapisan otentikasi yang dibangun di atas OAuth 2.0. OAuth juga tidak terkait dengan XACML, yang merupakan standar kebijakan otorisasi. OAuth dapat digunakan bersama dengan XACML, di mana OAuth digunakan untuk persetujuan kepemilikan dan delegasi akses sedangkan XACML digunakan untuk menentukan kebijakan otorisasi (mis., Manajer dapat melihat dokumen di wilayah mereka).

* Resource Owner : pemilik sumber daya
* Server Resource : sumber daya server
* Authorization Server: server otorisas