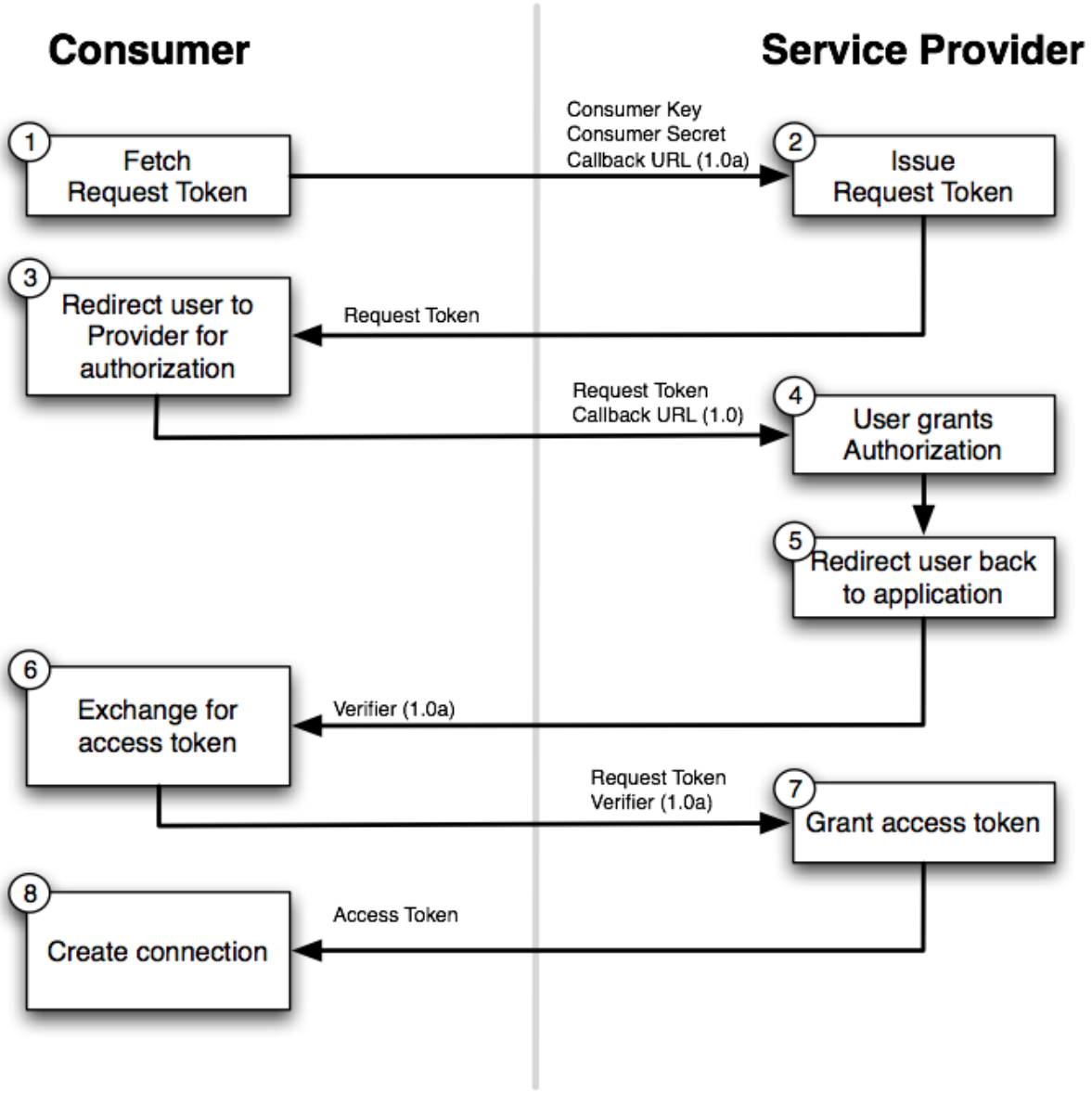
Criado como uma *API* de verificação, o *OAuth*, tem a função de ser uma simplificador e gerenciador de acesso a outros aplicativos, e funciona provendo uma aplicação com acesso através de um token, que representa a permissão do usuário para o *client* acessar seus dados, melhor representado na imagem a seguir.



Utilizando o protocolo *OAuth 2.0a* tem-se o seguinte fluxo: inicia-se aplicação e é solicitada a autorização do usuário para poder ter acesso a seus serviço, e, após a confirmação, é enviada uma concessão para ao servidor de autorização, que através de sua identificação, permite o acesso solicitado pela *API*. Se tudo estiver autenticado, e esta autorização for válida, o servidor retorna um token ao programa que repassa a confirmação feita pelo usuário ao servidor, para assim, no servidor de recursos, os dados serem protegidos.

O maior problema de utilizar essa ferramenta tão poderosa, pode-se dar pela falha de segurança de dados, apesar de ser muito utilizada já houveram casos, como o de 2014 (*link* da matéria), em que vários dados, através de links maliciosos, foram expostos através do *Oauth*. Essa vulnerabilidade pode ser utilizada por *hackers*, na criação de códigos mal intencionados, em sites genuínos, fazendo consumidores acreditarem estar na página desejada mas na

verdade estarem enviando informações pessoais, sendo sempre bom reforçar a importância de não acessar *links* desconhecidos.

Grande parte das empresas, dos mais variados segmentos, que necessitam de alguma confirmação de conta, utilizam essa *API*, para agilizar o acesso e facilitar cadastros com informações pessoais já disponíveis em outros sites (como redes sociais) , e alguns dos nomes mais conhecidos são: *Amazon*, *Battle.net*, *Discord*, *GitHub* e o *GitHub*, *Instagram*, *Spotify*, *Trello*, *Twitter*, *Steam*, *Netflix*. A lista continua por várias outras, indo desde *fintechs* a redes sociais, passando por sites de notícias e serviços de jogos.