



Fecomércio RS



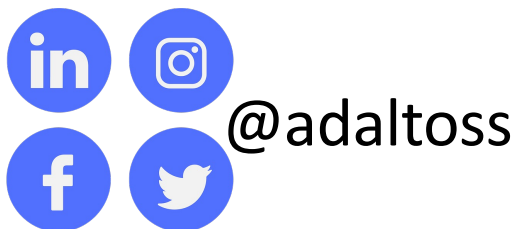
Senac

Desenvolvimento de Serviços e APIs - Aula14

Segurança e Autenticação nos Web Services RESTful (**oAuth**)

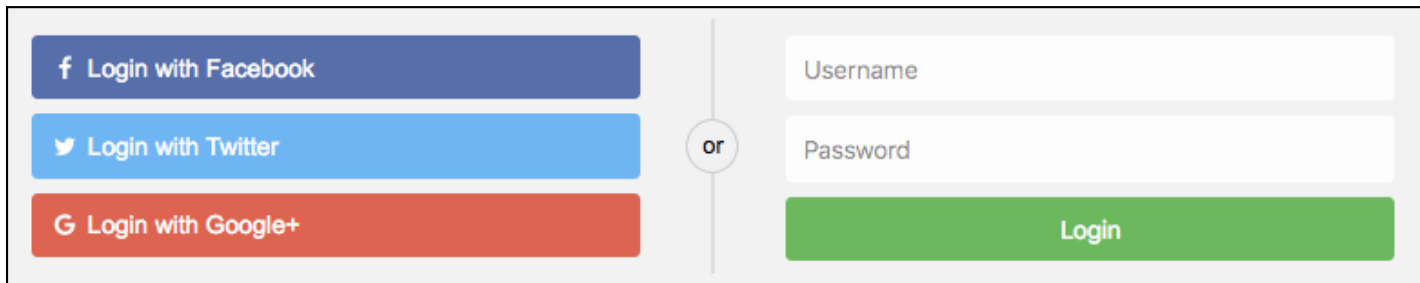
Prof. MSc. Adalto Selau Sparremerger




assparremerger@senacrs.com.br



OAuth

- Protocolo padrão para autenticação e autorização.
- O OAuth 2.0 fornece fluxos de autorização específicos para aplicativos da Web, aplicativos de desktop, telefones celulares e dispositivos de sala de estar.
- Esta especificação e suas extensões estão sendo desenvolvidas dentro do IETF OAuth Working Group.
- A especificação principal deixa muitas decisões para o desenvolvedor, geralmente com base nas compensações de segurança da implementação.



 Login with Facebook	or	<input type="text" value="Username"/>
 Login with Twitter		<input type="password" value="Password"/>
 Login with Google+		<input type="button" value="Login"/>

oAuth – Roles (“Papéis”)

- O aplicativo de terceiros: **"Client"**
 - O cliente é o aplicativo que está tentando obter acesso à conta do usuário. Ele precisa obter permissão do usuário antes de fazê-lo.
- A API: **"Resource Server"**
 - O servidor de recursos é o servidor da API usado para acessar as informações do usuário.
- O servidor de autorização: **"Authentication Server"**
 - Este é o servidor que apresenta a interface em que o usuário aprova ou nega a solicitação. Em implementações menores, esse pode ser o mesmo servidor que o servidor da API, mas implantações em maior escala geralmente o constroem como um componente separado.
- O Usuário: **"Resource Owner"**
 - O proprietário do recurso é a pessoa que está dando acesso a uma parte da conta.

oAuth - Criando um aplicativo

- Antes de iniciar o processo OAuth, você deve primeiro registrar um novo aplicativo no serviço. Ao registrar um novo aplicativo, você geralmente registra informações básicas como nome do aplicativo, site, logotipo etc. Além disso, é necessário registrar um URI de redirecionamento para ser usado para redirecionar usuários para aplicativos de servidor da Web, baseados no navegador ou móveis .

oAuth - Criando um aplicativo

- **Redirecionar URIs**

- O serviço redirecionará apenas os usuários para um URI registrada, o que ajuda a evitar alguns ataques. Quaisquer URIs de redirecionamento HTTP devem ser veiculados via HTTPS. Isso ajuda a impedir que os tokens sejam interceptados durante o processo de autorização.
- Aplicativos nativos podem registrar um URI de redirecionamento com um esquema de URL personalizado para o aplicativo, que pode parecer com **demoapp://redirect**.

oAuth - Criando um aplicativo

- **ID do cliente e senha**

- Depois de registrar seu aplicativo, você receberá um ID do cliente e, opcionalmente, um segredo do cliente.
- O ID do cliente é considerado informação pública e é usado para criar URLs de login ou incluído no código-fonte Javascript em uma página.
- A senha do cliente deve ser mantida em sigilo. Se um aplicativo implantado não puder manter a senha em sigilo, como aplicativos Javascript de página única ou aplicativos nativos, a senha não será usada e, idealmente, o serviço não deve emitir uma senha para esses tipos de aplicativos.

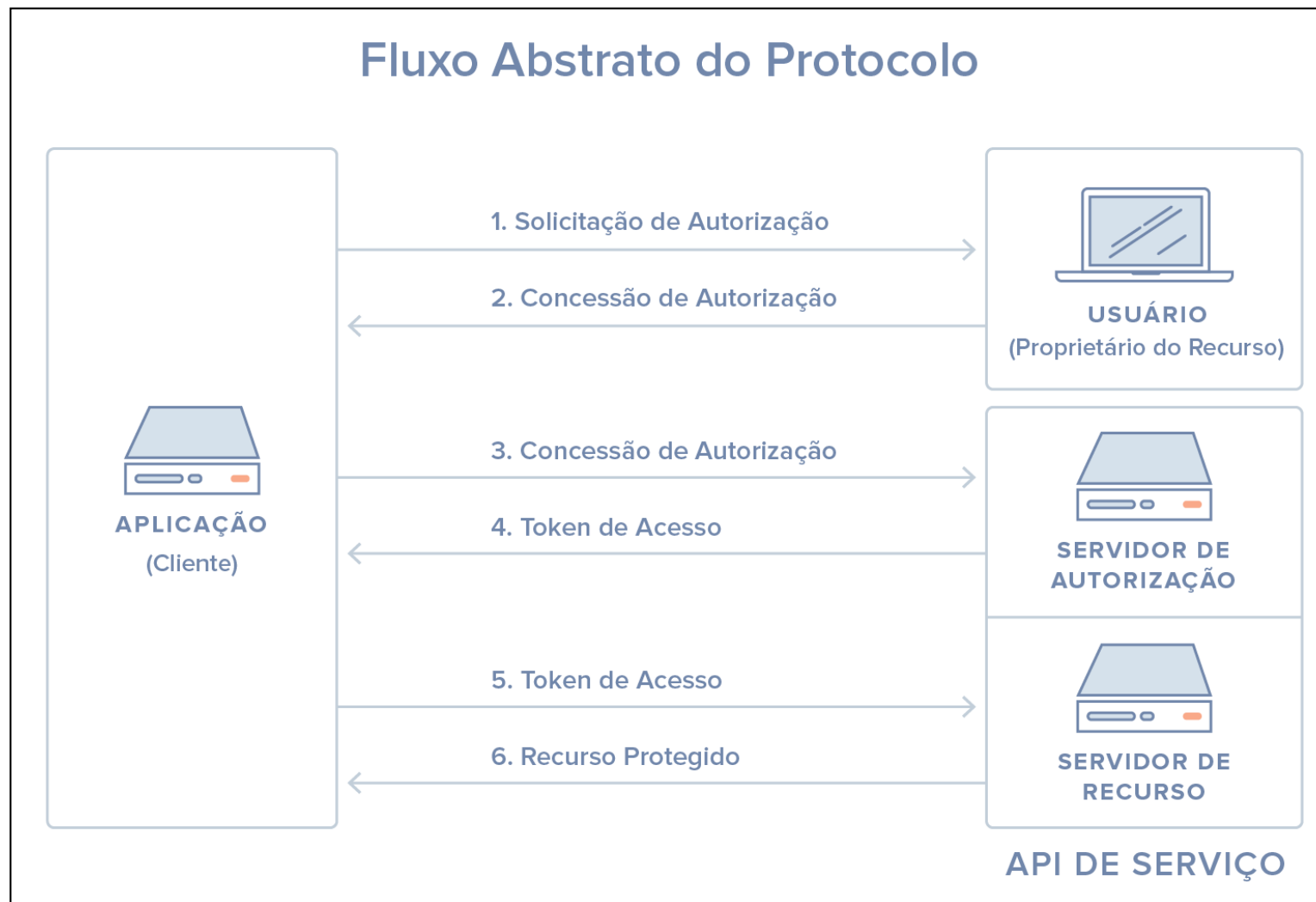
oAuth - Autorização

- A primeira etapa do OAuth 2 é obter autorização do usuário. Para aplicativos móveis ou baseados em navegador, isso geralmente é realizado exibindo uma interface fornecida pelo serviço ao usuário.

OAuth - Autorização

- O OAuth 2 fornece vários "tipos de concessão" para diferentes casos de uso. Os tipos de concessão definidos são:
 - **Código de autorização** para aplicativos em execução em um servidor Web, aplicativos móveis e baseados em navegador
 - **Senha** para fazer login com um nome de usuário e senha (apenas para aplicativos primários)
 - **Credenciais** do cliente para acesso ao aplicativo sem a presença de um usuário
 - O **implícito** foi anteriormente recomendado para clientes sem segredo, mas foi substituído pelo uso da concessão do Código de Autorização com o PKCE.

oAuth - Fluxo



Fonte: <https://www.digitalocean.com/community/tutorials/uma-introducao-ao-oauth-2-pt>



Fecomércio RS



oAuth - Autorização

1. A *aplicação* solicita autorização para acessar recursos do serviço do *usuário*
2. Se o *usuário* autorizar a solicitação, a *aplicação* recebe uma concessão de autorização
3. A *aplicação* solicita um token de acesso ao *servidor de autorização* (API) através da autenticação de sua própria identidade, e da concessão de autorização
4. Se a identidade da aplicação está autenticada e a concessão de autorização for válida, o *servidor de autorização* (API) emite um token de acesso para a aplicação. A autorização está completa.
5. A *aplicação* solicita o recurso ao servidor de recursos (API) e apresenta o token de acesso para autenticação.
6. Se o token de acesso é válido, o *servidor de recurso* (API) fornece o recurso para a *aplicação*

O fluxo real desse processo será diferente dependendo do tipo de concessão de autorização em uso, mas essa é a ideia geral.

Vídeos resumindo oAuth

- <https://www.youtube.com/watch?v=z-RuvnMlw34>
- <https://www.youtube.com/watch?v=zCcetcy8RuM>

Obs: copie o link e cole no navegador

Desafio

- Construir uma aplicação utilizando OAuth2 que permita realizar login em um serviço de sua escolha: Facebook, Twitter, Github...
- Esta aplicação deve retornar alguma informação como por exemplo o Nome do usuário que fizer login.

Referências

- <https://oauth.net/2/>
- <https://www.brunobrito.net.br/oauth2/>
- <https://aaronparecki.com/oauth-2-simplified/>
- <https://www.digitalocean.com/community/tutorials/uma-introducao-ao-oauth-2-pt>
- <https://imasters.com.br/desenvolvimento/como-funciona-o-protocolo-oauth-2-0>



Fecomércio RS



Senac



Fecomércio RS



Senac