

Autenticação e Autorização em Sistemas Web

Capítulo 4. OAuth 2.0

Prof. Angelo Assis

Autenticação e Autorização em Sistemas Web

Aula 4.1. Introdução ao OAuth 2.0

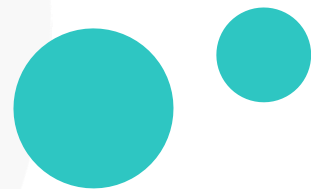
Prof. Angelo Assis

Nesta aula



- ❑ Introdução ao OAuth 2.0.

Por que OAuth 2.0?



IGTi

- Exemplo: Álbum de fotos personalizados com fotos do Facebook.
- Opções:
 - Criar uma conta no site do serviço;
 - Fazer download das imagens.
 - Fornecer usuário e senha;
 - Acesso irrestrito à conta.

OAuth 2.0



- Não é uma implementação;
- É um padrão aberto para delegação de acesso (identificação, autenticação e autorização) às APIs ;
- Garante acesso a uma aplicação cliente;
- Executa ações em nome do dono do recurso.

Vantagens OAuth 2.0



- Padrão de mercado;
- Favorece a proteção dos dados;
- Cliente limita acesso aos recursos;
- Cliente revoga o acesso quando quiser;
- Basta um usuário / senha.

OAuth 2.0 – Papéis

1. Resource Owner;
2. Client;
3. Authorization Server;
4. Resource Server.



OAuth 2.0 – Papéis



- Resource Owner:
 - Proprietário do recurso / usuário;
 - Fornece acesso aos seus recursos.
- Client:
 - Aplicação que quer acessar a conta do usuário;
 - Deve ser autorizado pelo usuário;
 - Deve ser validado pelo servidor de autorização.

OAuth 2.0 – Papéis



- Authorization Server:
 - Obtém o consentimento do proprietário do recurso;
 - Emite tokens de acesso para os clientes.
- Resource Server:
 - Servidor que hospeda os recursos;
 - Geralmente um provedor de API que armazena e protege os dados.

Próxima aula



- ❑ Autenticação e Autorização.

Autenticação e Autorização em Sistemas Web

Aula 4.2. Autenticação e Autorização

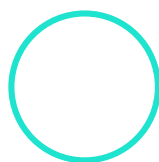
Prof. Angelo Assis

Nesta aula



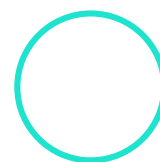
- ❑ Autenticação e Autorização.

Autenticação vs Autorização



Autenticação verifica a identidade digital do usuário.


- Mundo real: CPF, RG.
- Mundo digital: Login, senha.




Autorização verifica os privilégios e permissões do usuário.


- Mundo real: Carteira de motorista.
- Mundo digital: Perfil de usuário.

Autenticação vs Autorização



SIGN IN

 USERNAME

 PASSWORD


LOGIN

☒ Remember Me [Forgot Password?](#)



CONTROLE DE ACESSO

 123.456.789-10
 Maria Antônia Silva Santos
 Financeiro

Contas a Pagar	
Contas a Receber	
Controle de Estoque	
Cadastro de Usuários	
Cadastro de Clientes	
Vendas	
Pedidos	

Autenticação vs Autorização



- Autenticação:
 - Processo de verificação de identidade de usuário.
- Autenticação Federada:
 - Dependência entre serviços para verificação da identidade do usuário.
- Autorização:
 - Verificação dos direitos de um usuário.
- Autorização Delegada:
 - Conceder acesso para uma parte realizar ações em nome de outra.

Controle de Acesso



Suponha que a intenção é controlar a entrada em uma boate:

- ACL (Access-control list): seu nome está na lista.
- RBAC (Role-based access control): Você tem uma pulseira que permite o acesso.
- ABAC (Attribute-based access control): Você tem a idade certa.
- RAdAC (Risk-Adaptive Access Control): Você não esteve em um país com gripe espanhola.

Próxima aula



- ❑ Funcionamento do OAuth 2.0.

Autenticação e Autorização em Sistemas Web

Aula 4.3. Funcionamento do OAuth 2.0

Prof. Angelo Assis

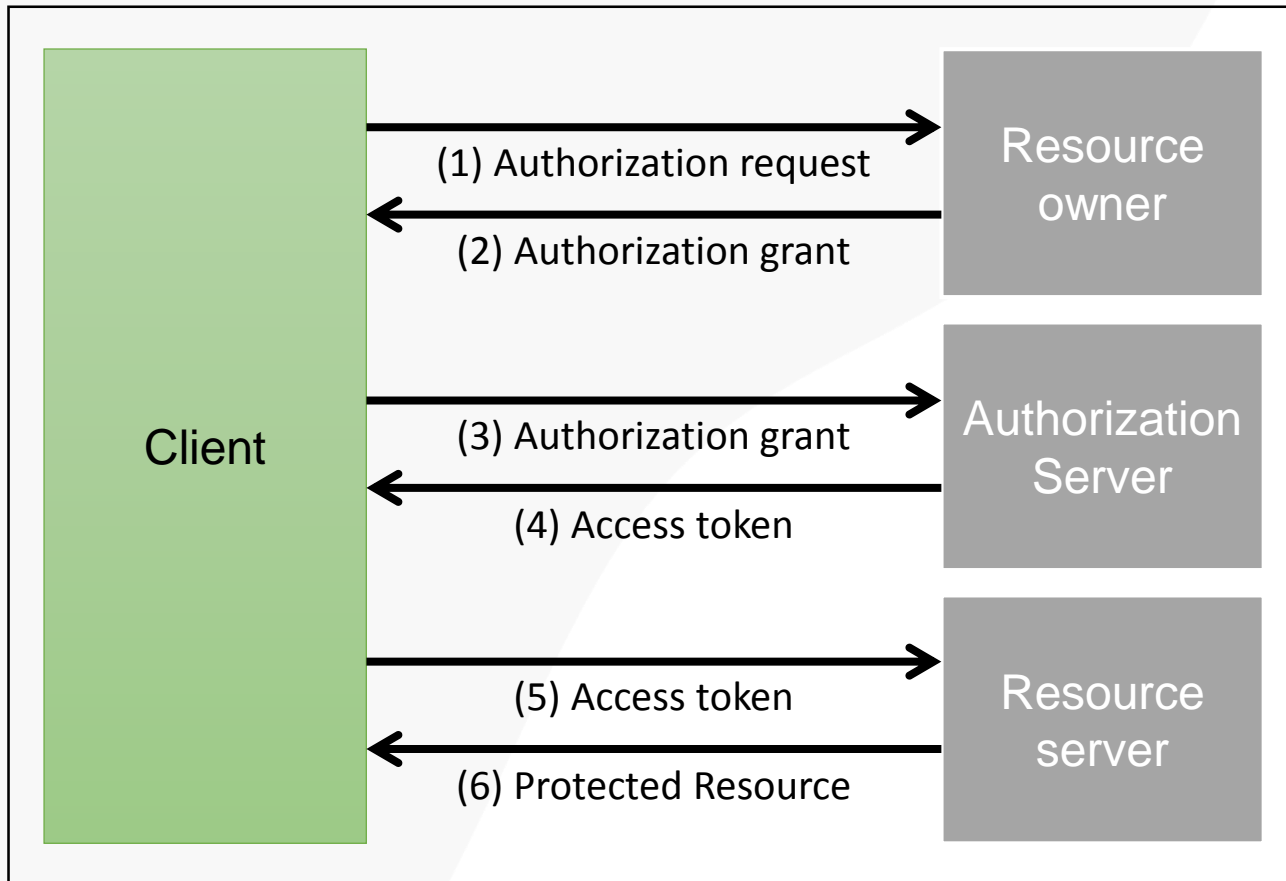
Nesta aula



- ❑ Funcionamento do OAuth 2.0.

Fluxo Abstrato

IGTi



Tokens



- Tipos de token:
- Token de acesso:
 - Chave para obter os recursos.
- Token de atualização:
 - Chave utilizada para obter um novo token de acesso.

Clientes OAuth 2.0



- Cliente confidencial:
 - Aplicação servidora;
 - Ambiente seguro;
 - Habilidade de manter a confidencialidade das credenciais.
- Cliente público:
 - Aplicações clientes (web, mobile);
 - Não é capaz de manter a confidencialidade das credenciais.

Endpoints



- Servidor de autorização:
 - Autorização: Utilizado pelo cliente para realizar a autorização;
 - Token: Utilizado para obter acesso ao token.
- Cliente:
 - Callback: Servidor de autorização envia o token para o cliente.

Escopo de acesso

- Cliente tem controle sobre os recursos;
- Facilita a autorização de acesso a recursos;
- É uma grande vantagem do OAuth 2.0.



igti

Próxima aula



- ❑ Fluxos do OAuth 2.0.

Autenticação e Autorização em Sistemas Web

Aula 4.4. Fluxos do OAuth 2.0

Prof. Angelo Assis

Nesta aula



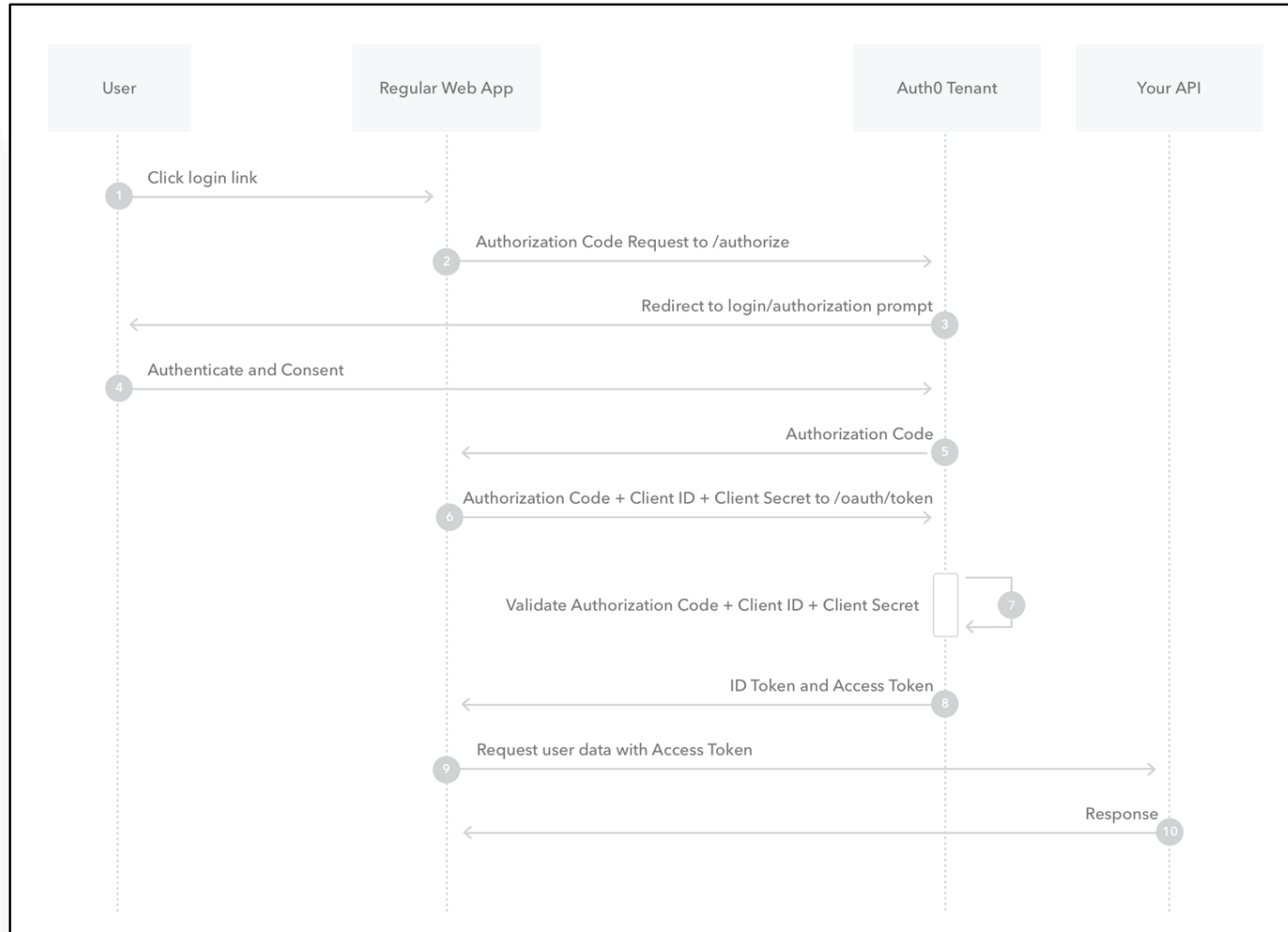
- ❑ Fluxos do OAuth 2.0.

Tipos de Fluxos

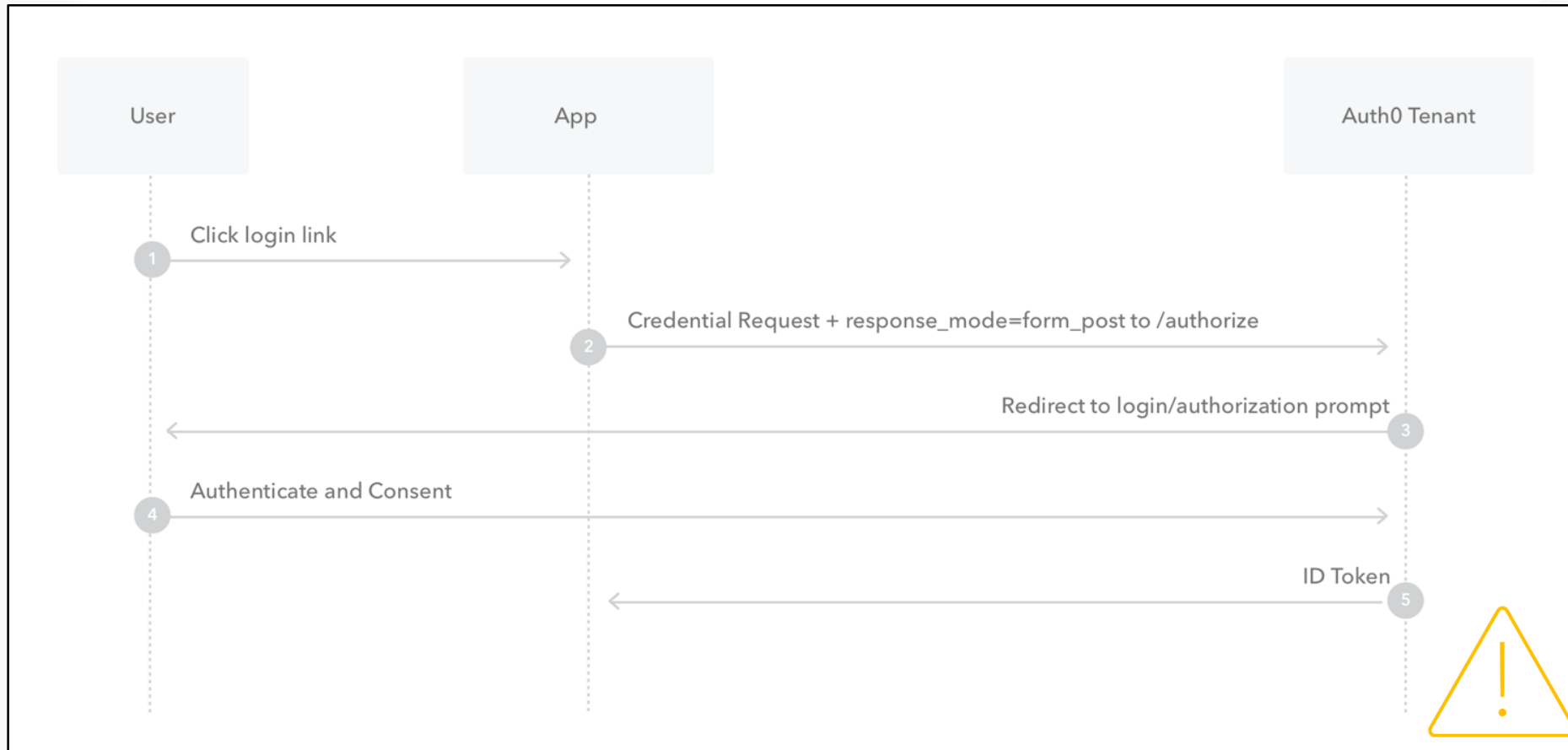
1. Authorization Code Flow;
2. Implicit Flow;
3. Resource Owner Password Flow;
4. Client Credentials Flow.



Authorization Code Flow



Implicit Flow

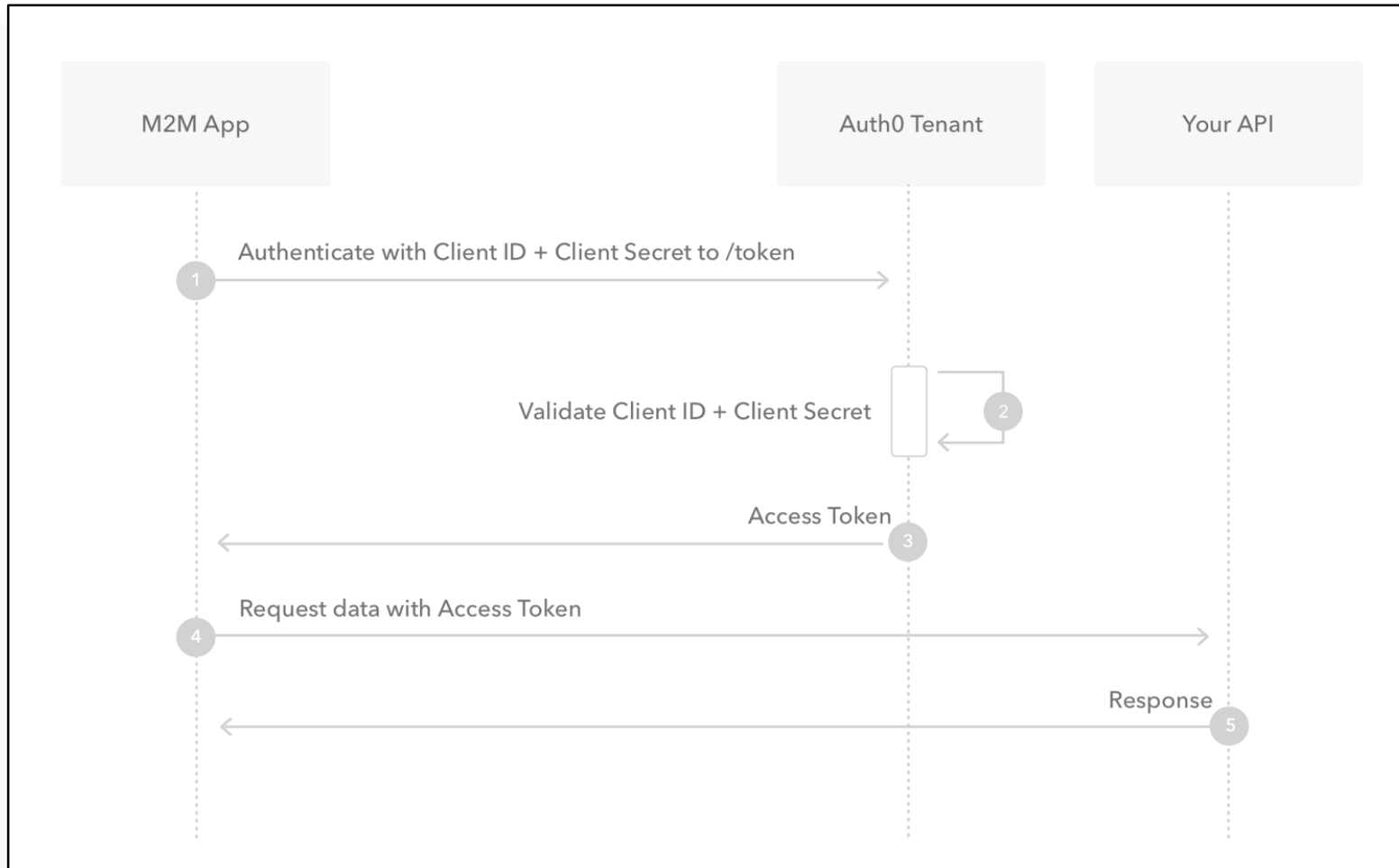


Resource Owner Password Flow



1. O usuário fornece usuário e senha na aplicação cliente;
2. A aplicação encaminha as credenciais para o Servidor de Autorização;
3. O Servidor de Autorização valida as credenciais;
4. O Servidor de Autorização responde com o Token de Acesso (Pode incluir também o Refresh Token).
5. A aplicação usa o token de acesso para acessar a API requisitando as informações;
6. A API responde com os dados requisitados.

Client Credentials Flow



Conclusão



- ✓ Authorization code grant flow:
 - Mais utilizado.
- ✓ Implicit grant flow:
 - Menos seguro, responsabilidade no cliente.
- ✓ Resource owner password credentials grant flow:
 - Login e senha são enviados pra obter o token;
 - Recomendado para clientes altamente confiáveis.
- ✓ Client credentials grant flow:
 - Útil para APIs;
 - Aplicação cliente requisita recursos próprios.