



APRESENTAÇÃO

Segurança da Informação

Gestão de Identidades

Jhonatan Geremias (elaboração)

Jhonatan.geremias@pucpr.br

Gonzaga (revisão / atualização)

luis.gonzaga@pucpr.br



Identidade

- Uma identidade **representa** uma entidade em um contexto particular;
- Tipicamente, é formada por um **identificador** com credenciais e **atributos** que representam **características** da entidade;
 - Ex: Se for uma pessoa, seu identificador pode ser o CPF e seus atributos são informações pessoais **relevantes**;

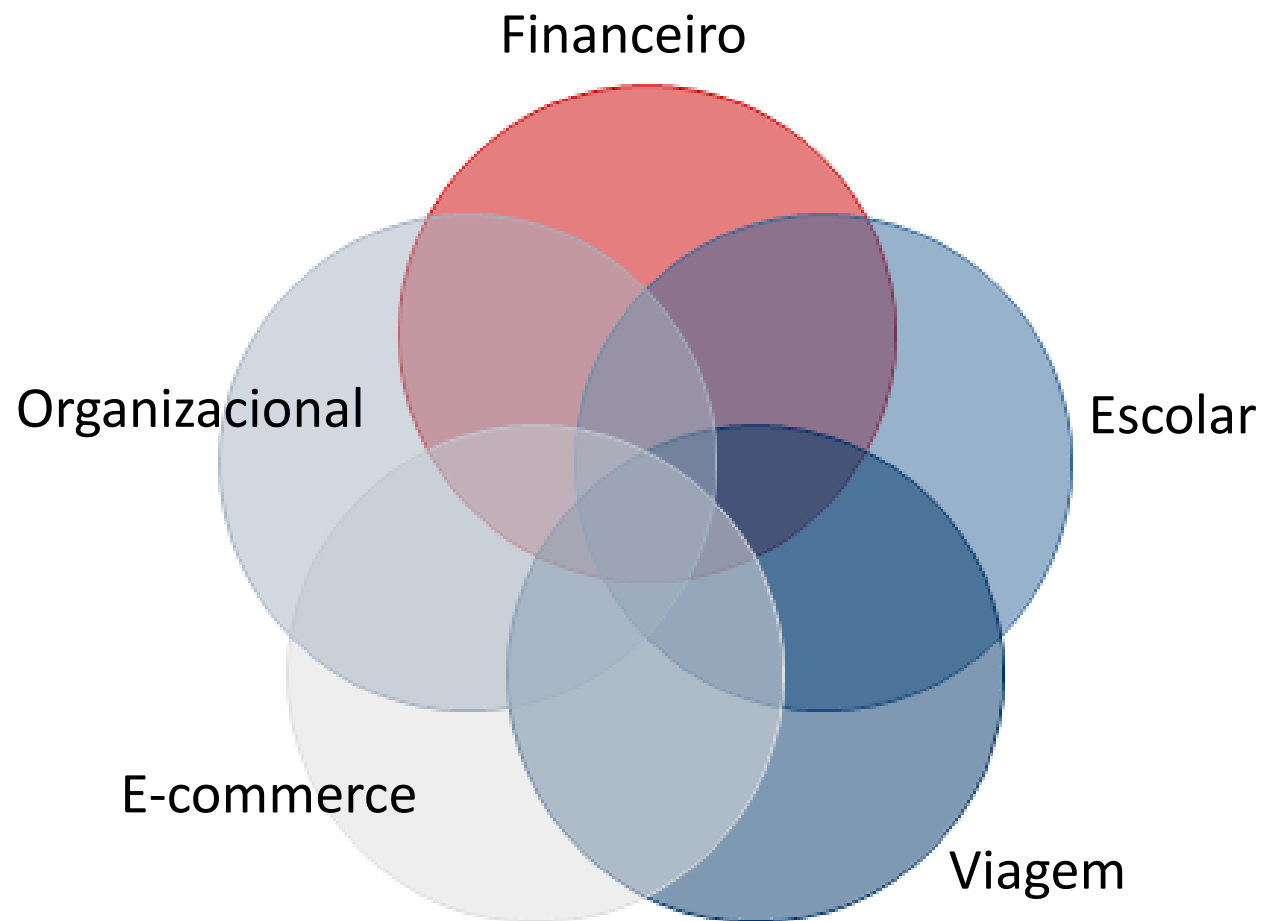


Identidade (cont.)

- A relevância das informações depende do contexto da aplicação, por exemplo, os atributos exigidos em uma **transação bancária** são diferentes dos atributos exigidos para **ouvir música** online;
- Usuários tem uma identidade para cada sistema que utiliza;



Muitas identidades



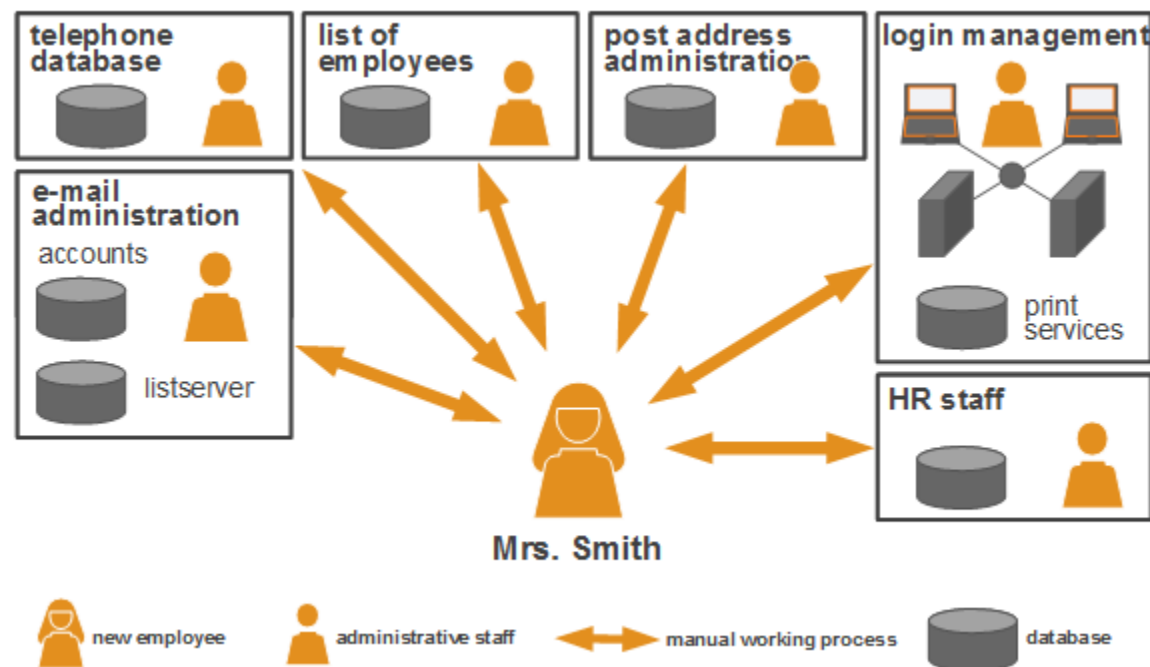
Problemas

1. Roubo de identidades;
2. Exposição de informações confidenciais;
3. Custo de manutenção;
4. Muitas identidades = muitas senhas;
5. Tempo para acesso as aplicações: realizar a autenticação em cada aplicação;
6. Problemas de sincronização de contas;

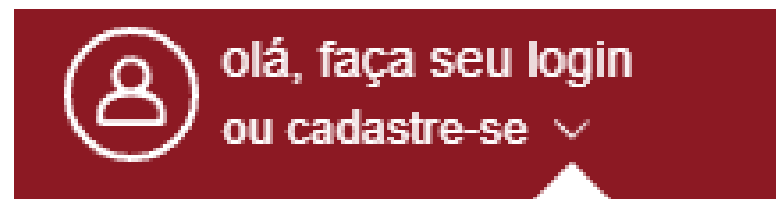


Gestão de Identidades - Definição

Responsável por gerenciar o relacionamento entre uma pessoa e os recursos computacionais que essa pessoa precisa para realizar seu trabalho.



Você já utilizou?



ou



Cliente novo? [Cadastrar](#)



Passo 1

- O Site/App deve se cadastrar no Facebook;
- Informações:
 - Descrição do Site/App
 - Endereço do site (URL)
 - Endereço de retorno (Callback URL)
- Após o cadastro, o Facebook informa o token de aplicação:
 - Utilizado para comprovar a autenticidade do Site/App.



Passo 2

- O usuário escolhe que deseja se autenticar utilizando sua conta do Facebook.



olá, faça seu login
ou cadastre-se

Entrar

ou

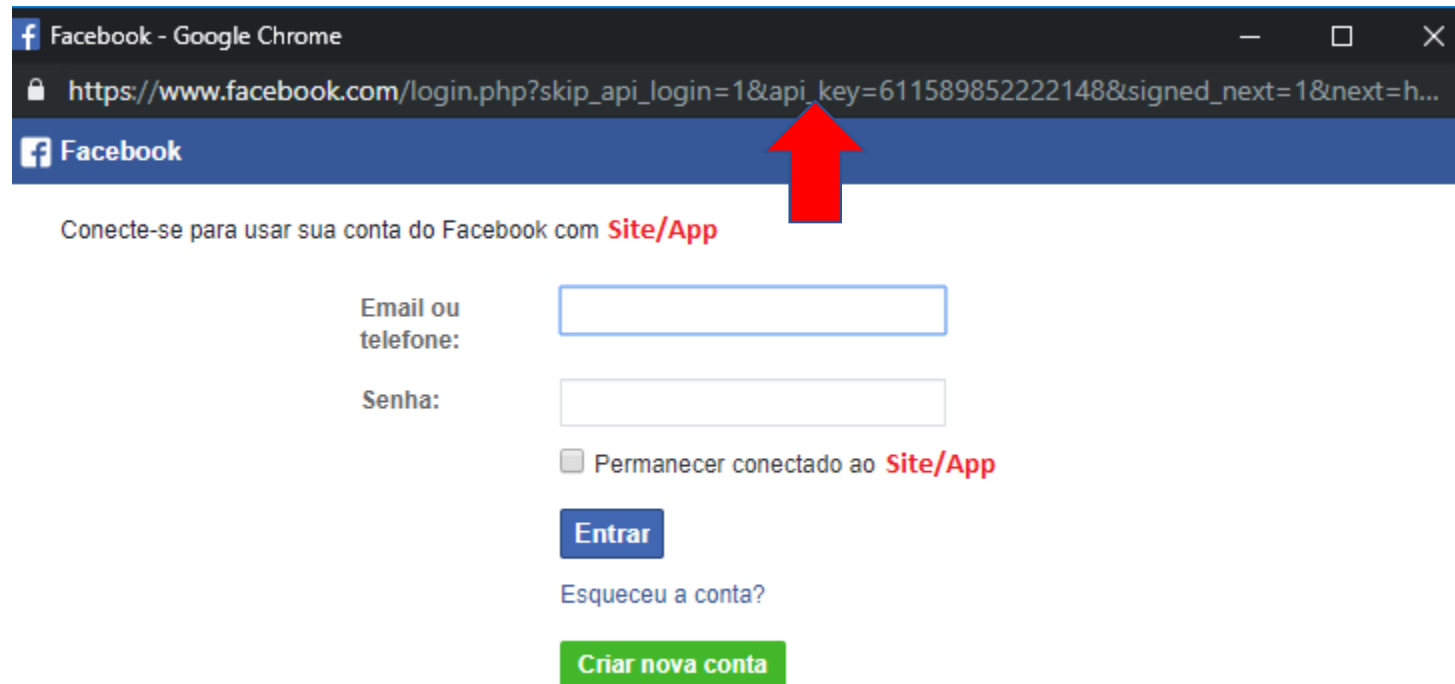
Entrar com Facebook

Cliente novo? Cadastrar



Passo 3

- O usuário é redirecionado para a página do Facebook;



The screenshot shows a Google Chrome browser window with the Facebook login page. The address bar displays the URL: `https://www.facebook.com/login.php?skip_api_login=1&api_key=611589852222148&signed_next=1&next=h...`. A red arrow points to the URL bar. Below the address bar, the Facebook logo is visible. The main content area contains the text "Conecte-se para usar sua conta do Facebook com Site/App". Below this, there are input fields for "Email ou telefone:" and "Senha:". A checkbox labeled "Permanecer conectado ao Site/App" is present. Below the input fields, there is a blue "Entrar" button, a link "Esqueceu a conta?", and a green "Criar nova conta" button.

Facebook - Google Chrome

`https://www.facebook.com/login.php?skip_api_login=1&api_key=611589852222148&signed_next=1&next=h...`

Facebook

Conecte-se para usar sua conta do Facebook com Site/App

Email ou telefone:

Senha:

☐ Permanecer conectado ao Site/App

Entrar

[Esqueceu a conta?](#)

[Criar nova conta](#)



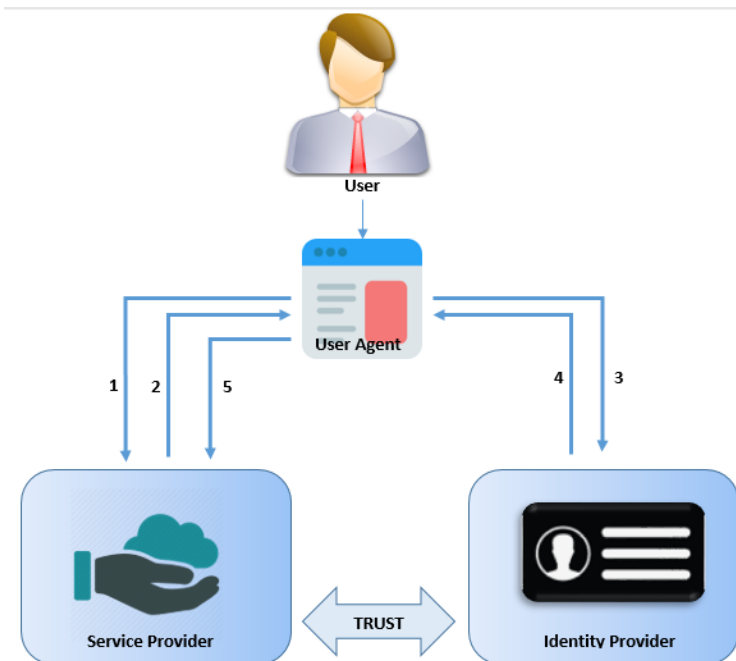
Passo 4

- O usuário consente o acesso do Site/App a conta



Passo 5

- O Site/App recebe um token de acesso que permite acessar informações confidenciais do usuário sem acessar suas credenciais.



Elementos (1/3)

Provedor de Serviço (SP, *Service Provider*):

- Provê serviços ao usuário, como:
 - Serviço bancário, e-commerce, rede social;



Elementos (2/3)

Provedor de Identidade (IdP, *Identity Provider*):

- Provê identidade ao usuário para utilização dos serviços (SP).
- É responsável pela autenticação do usuário e pelo processamento das requisições dos SP;



Elementos (3/3)

Usuário:

- É um cliente do SP e IdP que necessariamente precisa de uma identidade para utilizar os serviços.
- Na prática, um usuário pode ser uma pessoa, organização, entidade virtual etc.



Principais objetivos

- **Fornecimento de Identidade:** baseado em um único registro no IdP, diversos SPs podem criar diferentes identidades para o mesmo usuário;
- **Autenticação única (SSO, *Single Sign-On*):** baseado em uma única autenticação em um SP, é possível acessar diversos SPs que partilham do mesmo IdP;



Principais objetivos (cont.)

- **Compartilhamento de atributos:** os atributos de identidade especificados em determinado SP podem ser reutilizados em outros SPs;
- **Autorização de acesso:** Restringe o acesso de um SP a um recurso sem precisar acessar as credenciais;

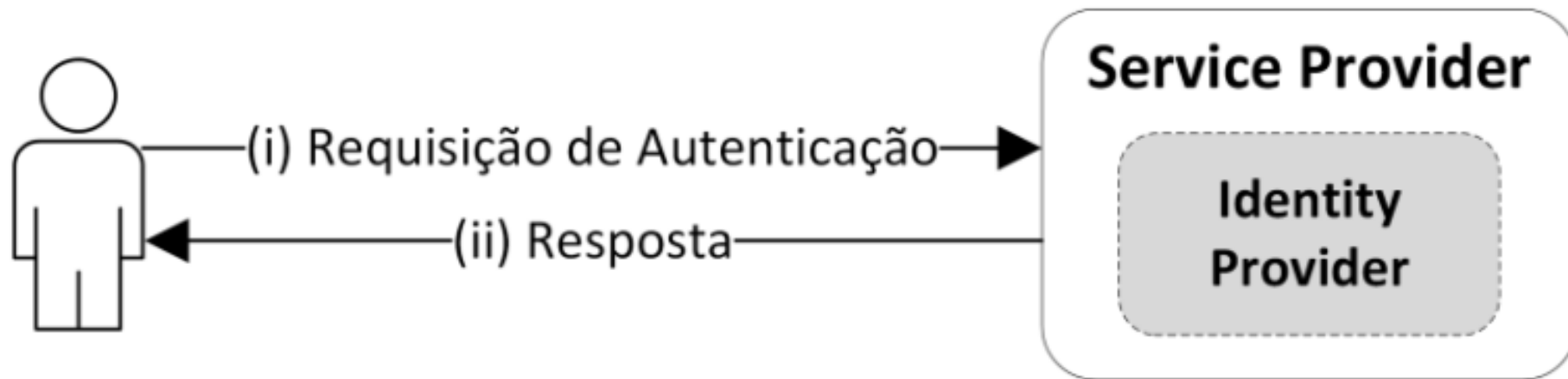


Modelos

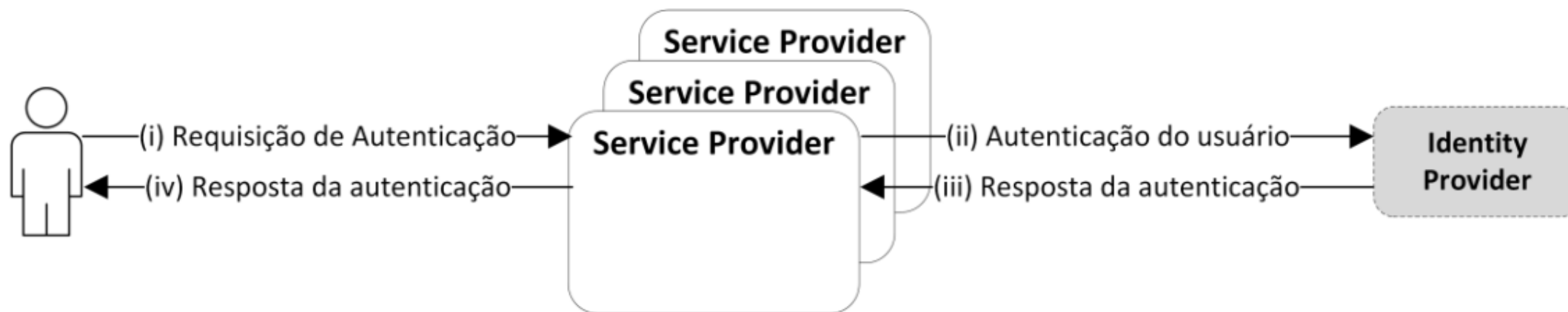
- Existem três modelos de IdM que determinam a relação entre SP e IdP, sendo eles o modelo tradicional, centralizado e federado.



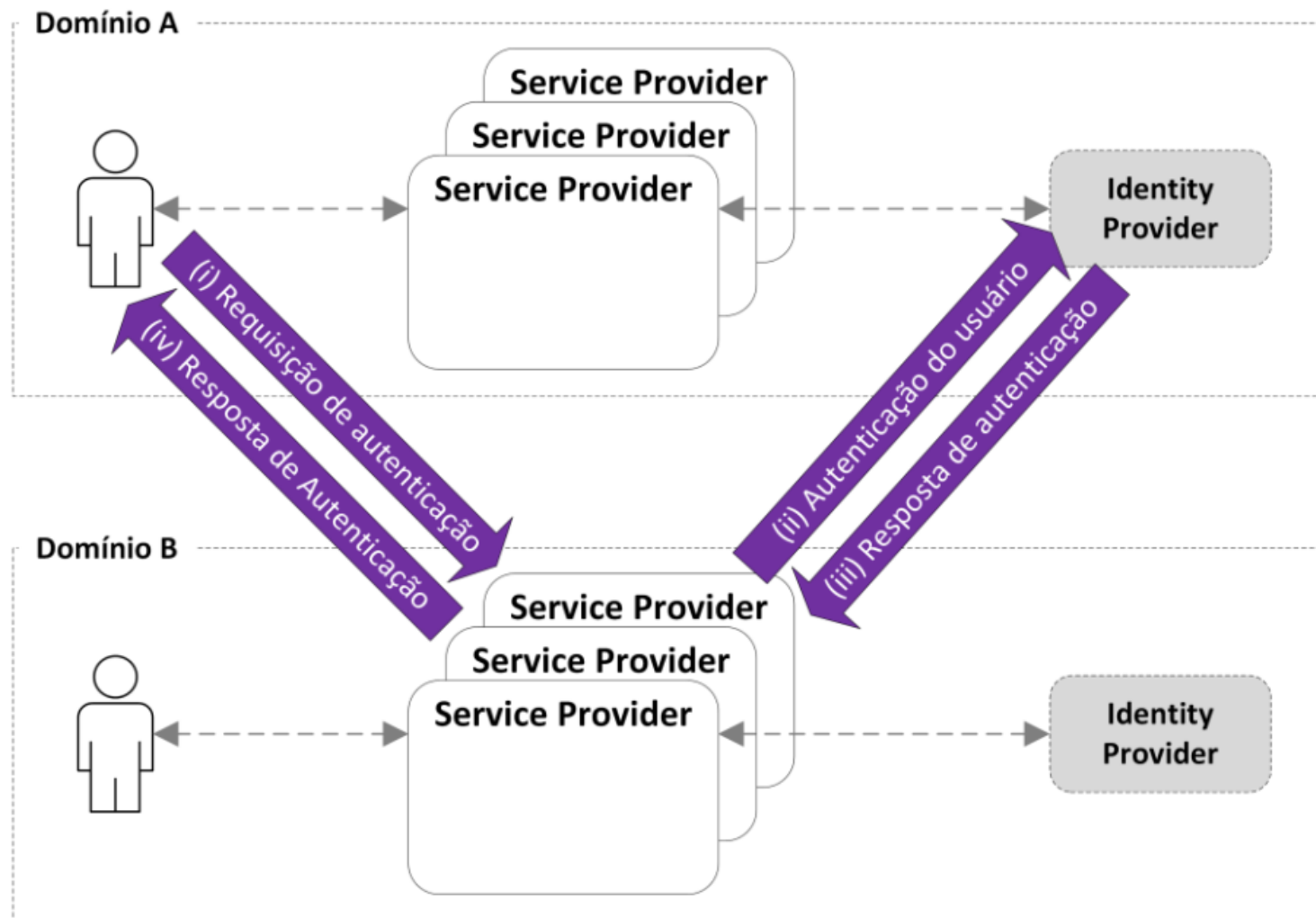
Tradicional



Centralizado



Federado



OpenID Connect

- OpenID Connect (OIDC) é um protocolo de gestão de identidades (IdM);
- Permite ao provedor de serviço (SP) a verificação da identidade e autorização de acesso de cada usuário;
- Provê um **token de identidade** (ID Token) e um **token de acesso**;



Token de Acesso

- O token de acesso define **parâmetros** para **restrição das ações** que o usuário é capaz de realizar;
 - Escopo de acesso;
 - Tipo do token;
 - Tempo de expiração;
 - Token de *refresh*;



Token de Acesso

Access token type	Bearer
Access token value	eyJhbGciOiJSUzI1NiIsImtpZCI6IjEifQ.eyJzY3AiOi0lsib3BlbmlkIiwicHJvZmlsZSI6InJiYWMTaG9tZS1mdWxsIiwicmJhYylyZWlvdGUTCmVhZCJleHAiOi0jE0NTQwOTcwNTcsInN1YiI6InZpbGlhc iIsImZlcyI6Imh0dHBz0lwvXC9sb2NhbgHvc3Q6ODQ0MlwvYzJpZCIsImVhdCI6MTQ1NDA5MTA1NywiY 2lkIjoiaMDAwMTIzIiwiaY2xtIjpbIm5pY2tuYWllIiwicHJvZmlsZSI6IjdfQ.I421xrtUf7mDqFuqU- -wTm VMrc_YBodwYdIyegR2ydpPHTZ0nvcyrZC-N1UQX4wdU9ePlaiaRT7rsFwTvalfd66fARIWiSiRfp0WfE 5pe8wx6vaphwjaVU7Mam5G2YwP7tiGwFgPbIfnPikeKkJtZK_ilXUwtSCJMWt53C4aX-c
Access token lifetime	6000 seconds
Access token scope	openid profile
Refresh token	dmlsbWFy.MDAwMTIz.2PvYUlcwUWiR_Sy_t1LoIg



Token de Acesso (cont.)

- Permite que uma **aplicação terceira confiável** (SP) tenha acesso restrito a um serviço no ambiente web, sem a necessidade de **compartilhamento de credenciais**;



Token de Identidade

- O token de identidade contém informações sobre a autenticação e atributos do usuário;



Token de Identidade (cont.)

Atributo	Descrição
sub	Identificador do usuário, deve ser único dentro do domínio.
iss	Identificador do CAM que deve ser único entre a federação.
aud	Identificador do SP que utilizará o <i>token de identidade</i> . Deve ser único dentro do domínio.
exp	Data e hora da expiração do <i>token de identidade</i> . Após essa data e hora, o <i>token de identidade</i> não deve ser aceito.
iat	Data e hora da emissão do <i>token de identidade</i> .
amr	Método de autenticação utilizado durante a autenticação. Esse atributo pode conter uma lista de valores, que são os possíveis fatores.

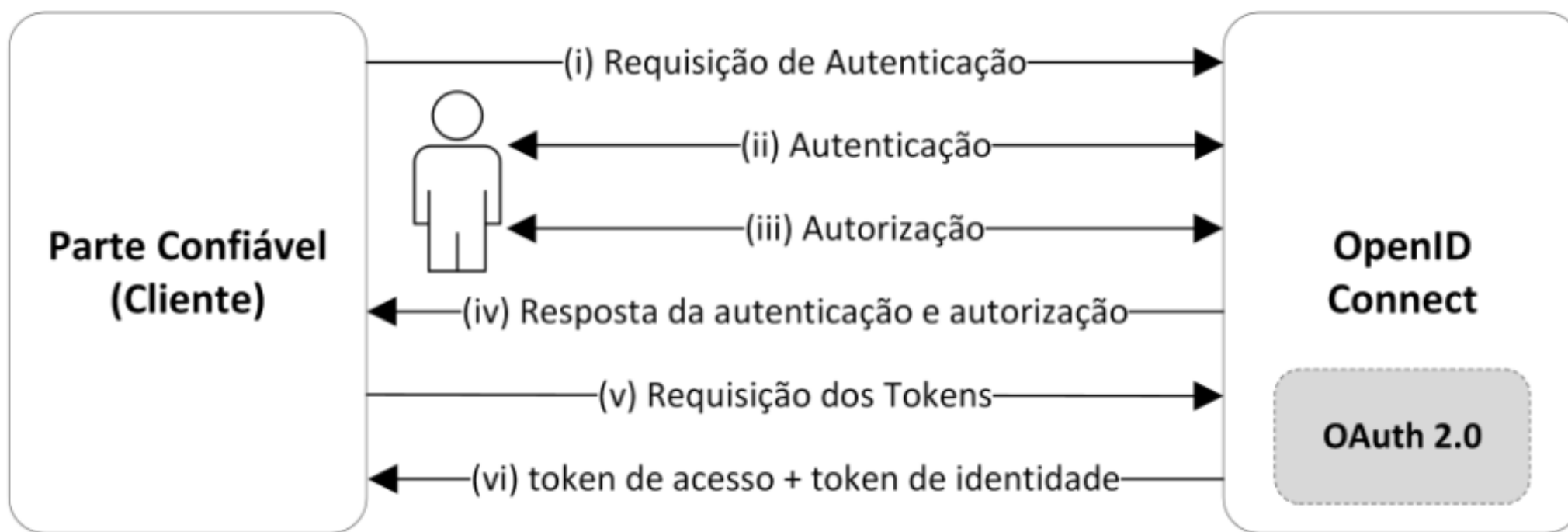


Fluxo do protocolo

1. Inicialmente a RP solicita a autenticação do usuário no OIDC;
2. O usuário fornece suas credenciais, caso sejam válidas, o mesmo será questionado se autoriza ou não que a RP acesse a suas informações definidas no escopo do token;
3. O OIDC responde ao RP sobre o processo de autenticação e consentimento de acesso do usuário;
4. Finalmente, o RP pode obter do OIDC o token de acesso e o token de identidade do usuário;



Fluxo do protocolo



Finalidade

- A autorização de acesso provida pelo OAuth limita o acesso a um recurso protegido, mas não suporta políticas que determinam as operações nos recursos;
- Dessa forma, não é possível obter um controle de granularidade fina, sendo necessário um controle de acesso adicional.



Bibliotecas que implementam OpenID Connect

1. WsO2 Identity Server (<https://wso2.com/identity-and-access-management>)
2. Connect2ID (<https://connect2id.com/>)
3. MITREid Connect (<https://github.com/mitreid-connect/>)
4. Firebase (<https://firebase.google.com/products/auth>)















Firebase

- Plataforma de desenvolvimento de Apps, que não exige a gerência da infraestrutura
- Produto do Google
- Principais funcionalidades: **Autenticação**, base de dados em tempo real, funções de aprendizagem de máquina, analítica etc.



Firebase Autenticação

Provedor	
	E-mail/senha
	Smartphone
	Google
	Play Games
	Game Center
	Facebook

	Twitter
	GitHub
	Yahoo
	Microsoft
	Apple
	Anônimo



Firestore no Python

1. Instalar o Pyrebase4
`pip install pyrebase4`
2. Configurar um projeto no firebase
3. Obter a base de configurações
4. Inicializar o app
5. Autenticar o app
6. Criar conta
7. Autenticar
8. Obter informações a partir do token





Obrigado!

Jhonatan Geremias (elaboração)

Jhonatan.geremias@pucpr.br

Gonzaga (revisão / atualização)

luis.gonzaga@pucpr.br

