



APRESENTAÇÃO

Segurança da Informação

Mecanismos de Autenticação

Elaboração: Jhonatan Geremias - jhonatan.geremias@pucpr.br

Revisão/Atualização: Gonzaga – luis.gonzaga@pucpr.br

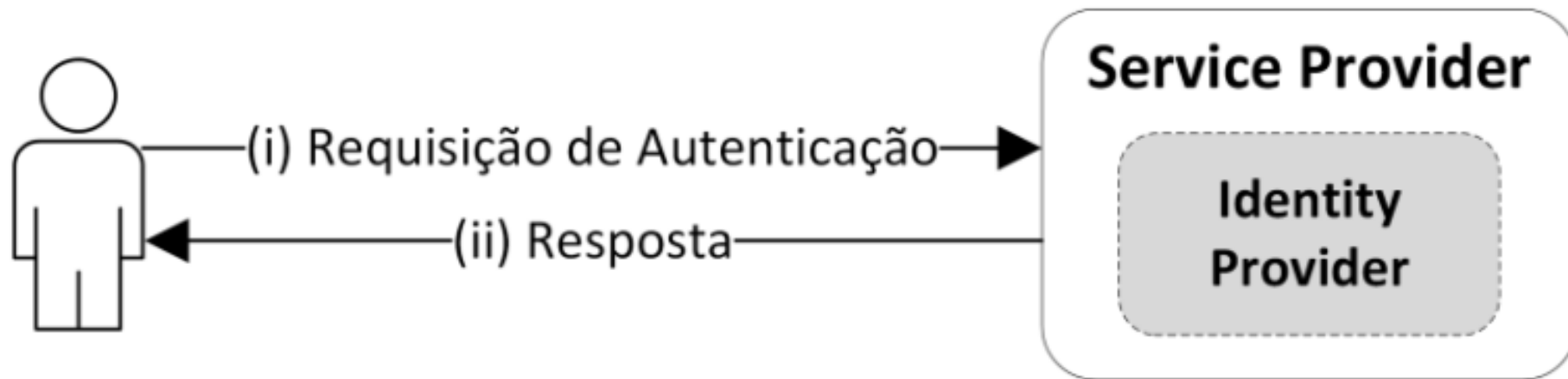


Modelos

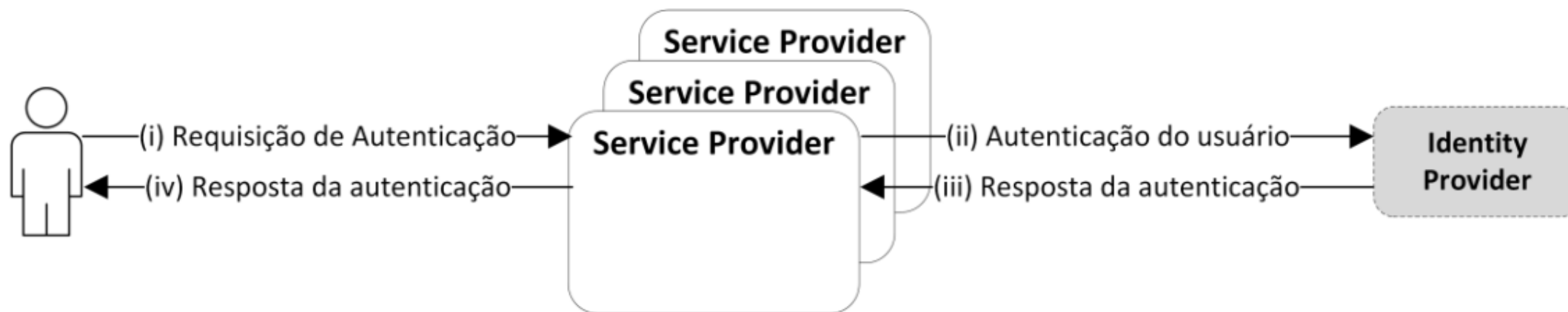
- Existem três modelos de IdM que determinam a relação entre SP e IdP:
- Tradicional;
- Centralizado;
- Federado.



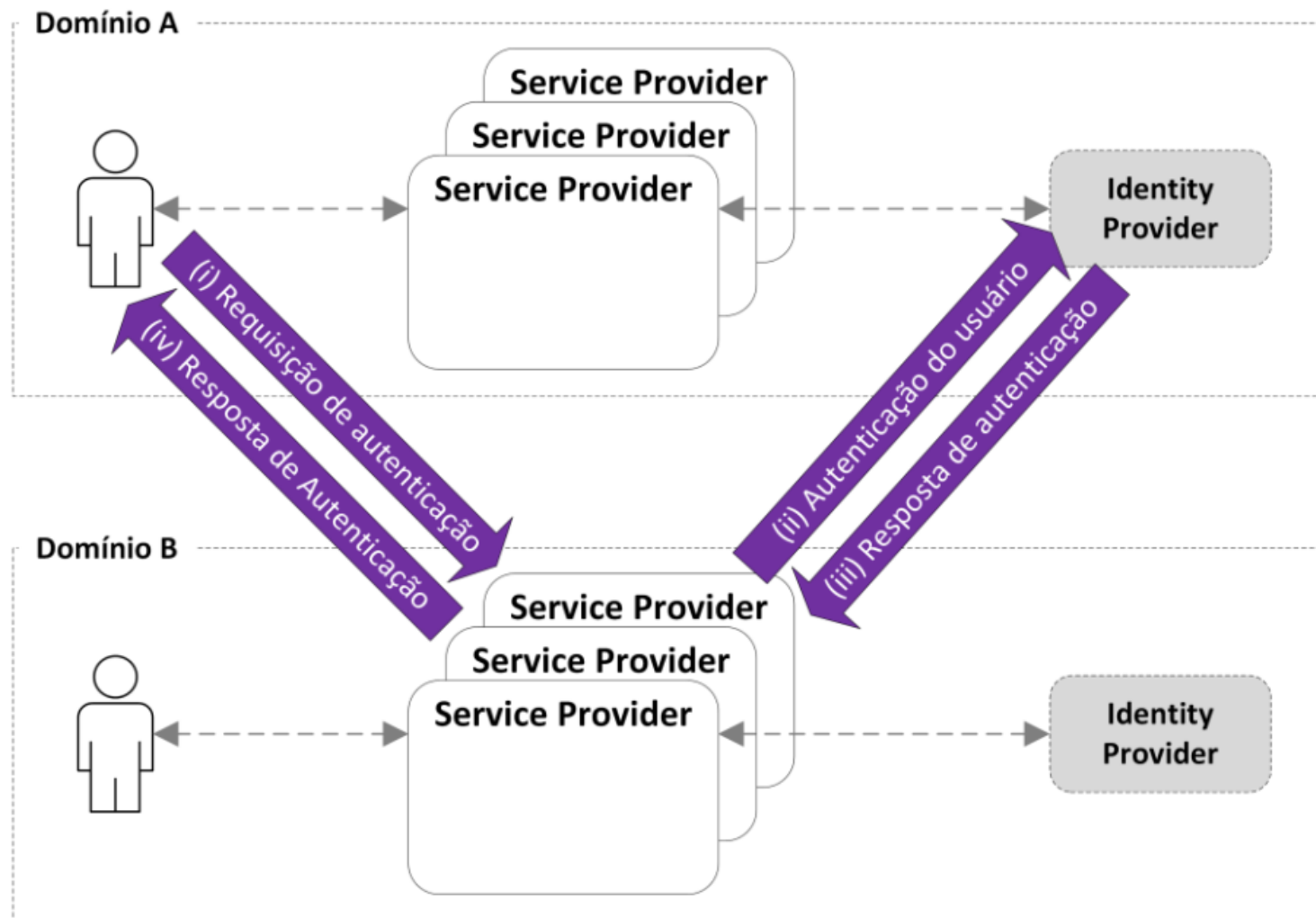
Tradicional



Centralizado



Federado



Norma ISO 27002 - identificação e autenticação

- A norma ISO 27002 fornece algumas diretrizes para orientar o processo de identificação e autenticação:
 - Todos os usuários devem ter um identificador único de **uso pessoal e exclusivo**, convém que uma técnica adequada de autenticação seja selecionada para validar a identidade dos usuários;
 - O controle de autenticação deve ser aplicado para **todos os tipos de usuários**, inclusive administradores do sistema e diretoria;
 - Os identificadores dos usuários devem ser utilizados para **rastrear as atividades** dos indivíduos. Como boas práticas as atividades regulares dos usuários não devem ser realizadas por meio de contas privilegiadas;



Norma ISO 27002 - identificação e autenticação

- Convém documentar qualquer tipo de circunstância excepcional que exija a utilização de **identificador** de usuário **compartilhado** por um grupo de pessoas;
 - Controles adicionais podem ser necessários para manter as responsabilidades dos indivíduos que vão utilizar este identificador;
- **Identificadores genéricos** para uso de um indivíduo só devem ser autorizados onde as ações executadas pelo usuário não precisam ser rastreadas, ou quando existem outros controles implementados para tal;
- Onde existe a necessidade de uma autenticação mais robusta **métodos adicionais** de autenticação são necessários;
 - Meios criptográficos, smart cards, tokens e mecanismos para autenticação biométrica.



Norma ISO 27002 - identificação e autenticação

- Convém que a força dos processos de identificação e autenticação sejam **proporcionais a sensibilidade da informação** que deve ser acessada.
 - Ideal que as senhas sejam protegidas utilizando meios criptográficos e protocolos de autenticação;
- Objetos como **tokens** podem ser utilizados para **identificação** e **autenticação**;
- Tecnologias de **autenticação biométricas** que usam características únicas de um indivíduo podem ser utilizadas para autenticar a identidade de um usuário;
- A **combinação** de diferentes tecnologias e mecanismos de segurança resulta em uma **autenticação mais forte**.



Fatores de Autenticação

- 1) **Algo que o indivíduo sabe:** baseado em algo que o usuário tem conhecimento;
 - Senhas;
 - Número de identificação pessoal (PIN);
 - Respostas a um conjunto de perguntas previamente arranjadas;
 - Desenhos e imagens;
- 2) **Algo que o indivíduo possui:** baseado em algo que o usuário tenha posse;
 - Cartões eletrônicos;
 - Smart Cards;
 - Chaves físicas;
 - Normalmente chamados de tokens;
 - Senhas descartável (OTP), por e-mail ou SMS.



Fatores de Autenticação

3. **Algo que o indivíduo é (biometria estática):** características físicas do indivíduo;
 - Impressão digital;
 - Leitura da Retina e Iris;
 - Reconhecimento Facial;
 - Geometria da palma da mão;
4. **Algo que o indivíduo é (biometria mecânica):** características comportamentais;
 - Padrão de voz;
 - Características de escrita;
 - Ritmo de digitação.



Autenticação Multifator

- A autenticação multifator é uma técnica onde o sistema pode implementar mais de um fator de autenticação para certificar as credenciais dos usuários;
- A combinação de diferentes tecnologias permite obter um mecanismo de autenticação mais robusto:
 - Para fortalecer o procedimento de autenticação podemos associar mais de um fator de autenticação.
 - Baseado nos quatro fatores básicos de autenticação:
 - O que o indivíduo sabe;
 - O que ele possui;
 - Características físicas;
 - Características comportamentais.















Firebase

- Plataforma de desenvolvimento de Apps: não exige a gerência da infraestrutura
- Produto do Google
- Principais funcionalidades:
 - **Autenticação;**
 - Base de dados em tempo real;
 - Funções de aprendizagem de máquina (ML);
 - Analytics;
 - 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!

Elaboração: Jhonatan Geremias - jhonatan.geremias@pucpr.br

Revisão/Atualização: Gonzaga – luis.gonzaga@pucpr.br

