Aplicando segurança no código

Luiza <CODE>

Luizalabs Magalu

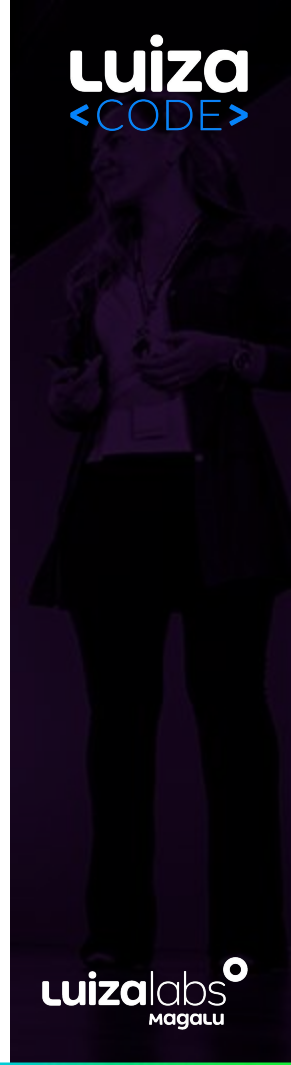
Ementa:

- **Pilares de segurança**
  - Confidencialidade
  - Integridade
  - Disponibilidade
- **Não repúdio**
- **Autenticidade**
- **Autenticação e Autorização**
- **Criptografia**
  - simétrica
  - assimétrica
- **Autenticação HTTP**
  - Basic
  - APIKey
  - Bearer


Pilares de segurança

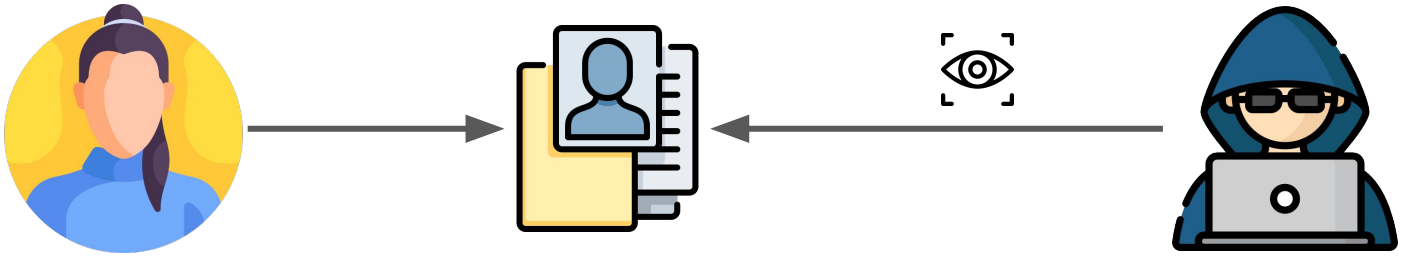
Pilares de segurança

Confidentiality	**C**onfidencialidade
Integrity	**I**ntegridade
Availability	**D**isponibilidade
---	---
CIA	CID



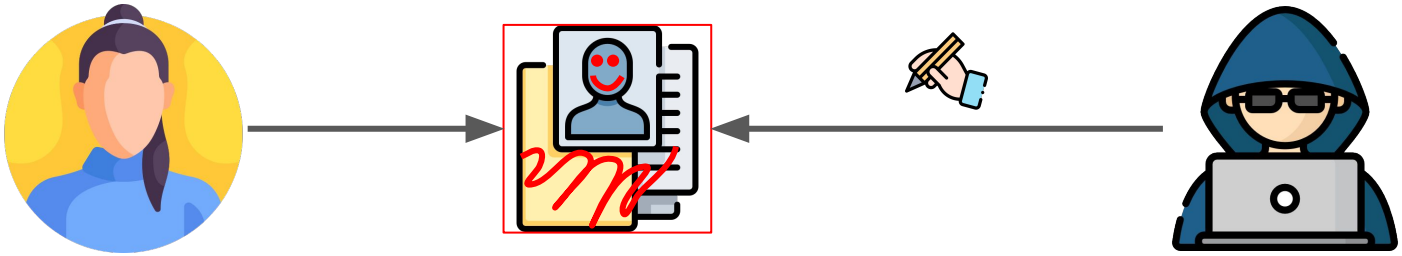
Confidencialidade

- Garantir que a informação não será divulgada ou disponibilizada para pessoas não autorizadas.



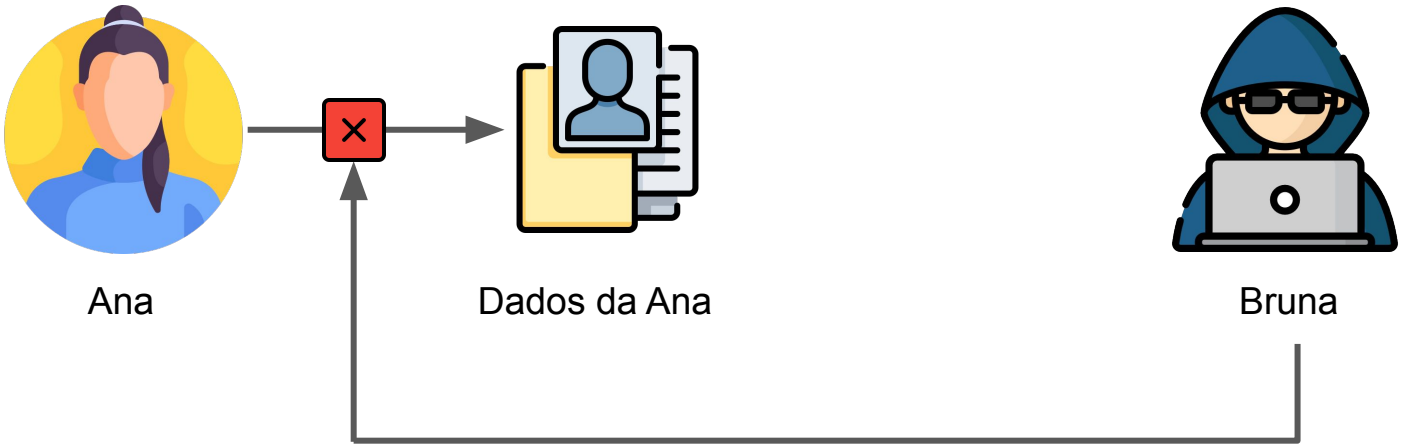
Integridade

- Garantir que a informação não será modificada por pessoas não autorizadas.



Disponibilidade

- Garantir que a informação estará disponível para as pessoas autorizadas.




Autenticidade

Autenticidade

- Garantir que a pessoa é quem ela diz ser.

Ana

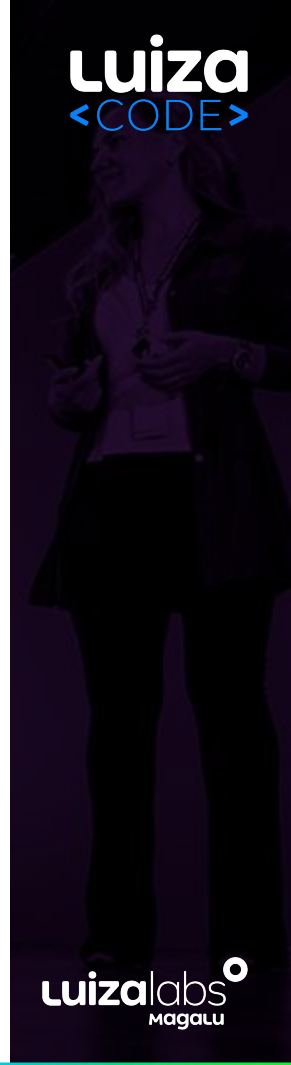
Bruna

Formas de aferir Autenticidade

- **Pelo o que a pessoa sabe**
  - Senha
  - Conhecimento
  - Passado da pessoa
- **Pelo o que a pessoa possui**
  - Documento
  - Token
  - Coroa de ouro do rei
- **Pelo o que a pessoa é**
  - Biometria facial
  - Digital
  - Personalidade

Exercícios

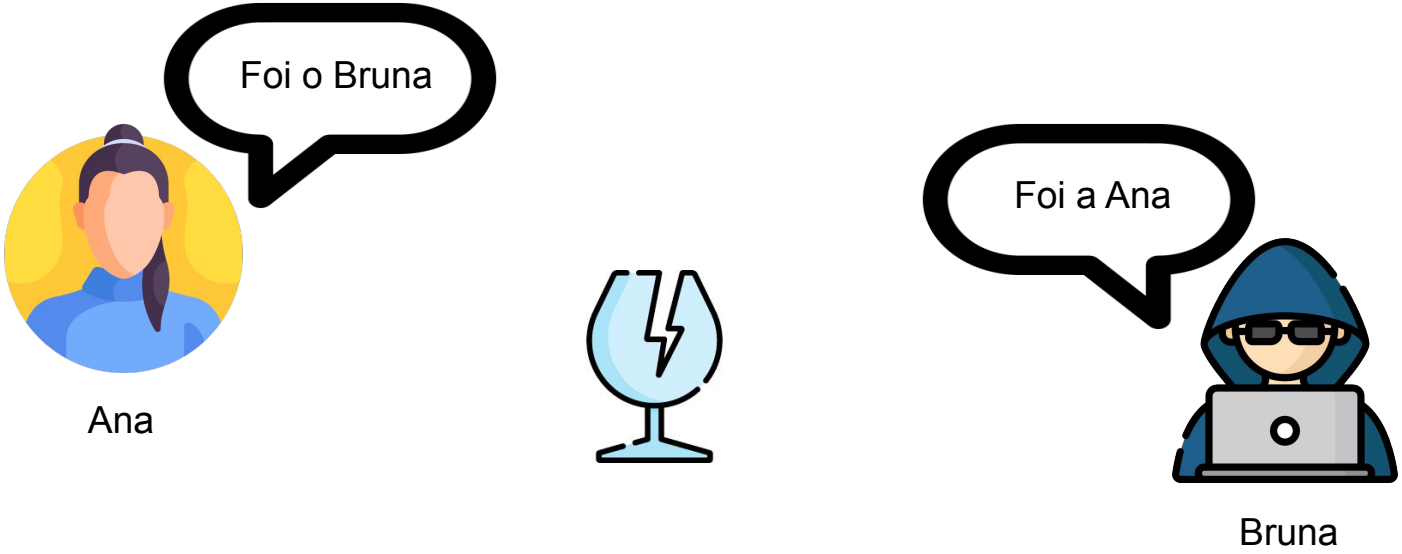
- **Pagar compras com o cartão de aproximação.**
- **Pagar compras com o cartão de crédito**
- **Destravar o seu celular.**
- **Entrar em um show de rock.**




Não Repúdio

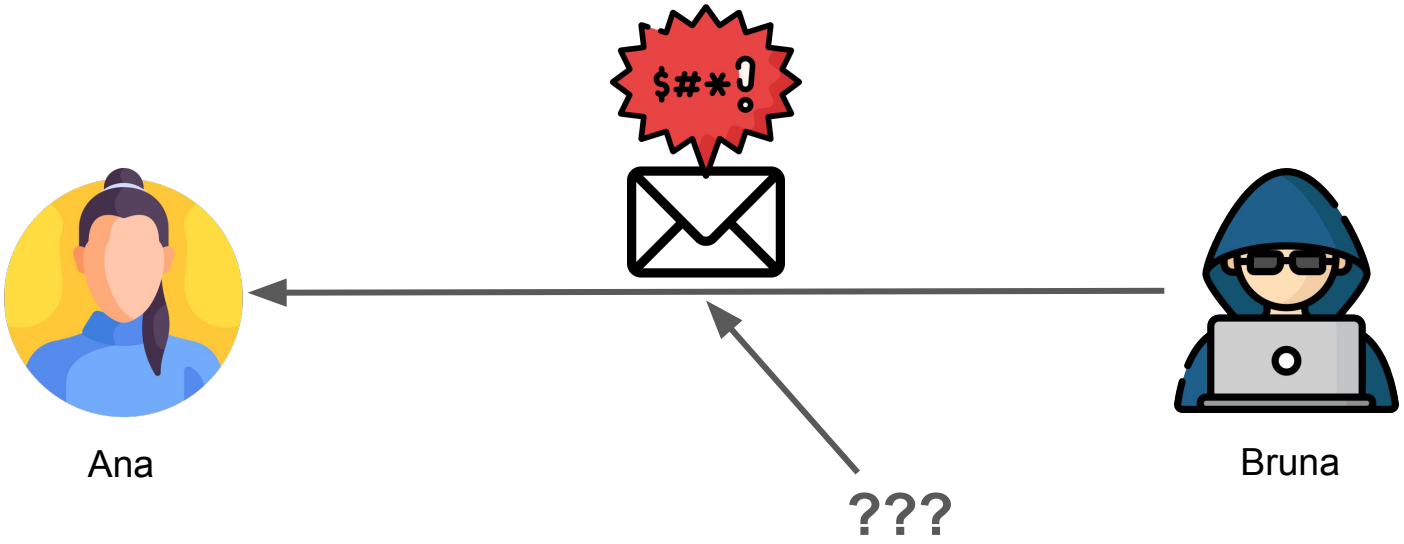
Não Repúdio

- Garantir que a pessoa não possa negar os seus atos.



Não Repúdio

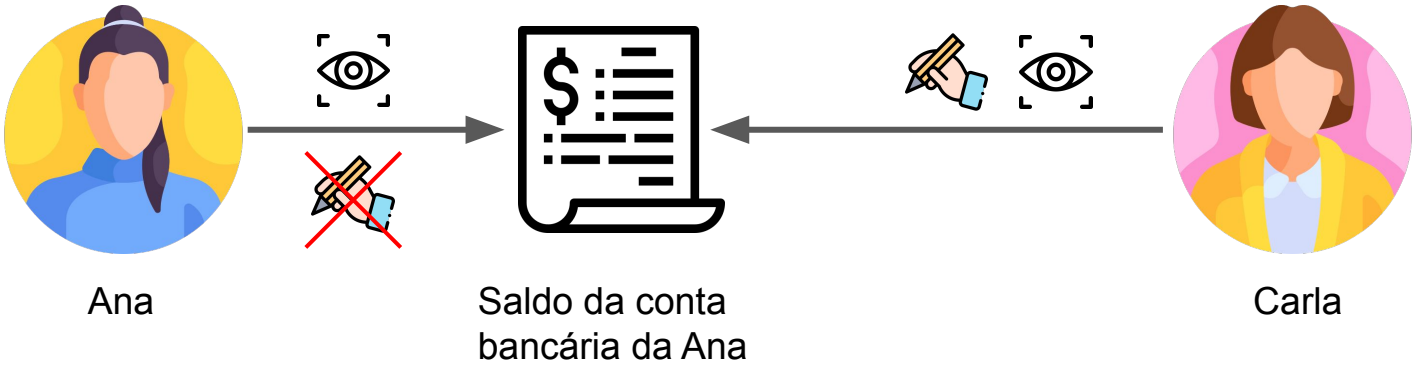
- Associado a integridade do dado e sua origem.




Autenticação
e
Autorização

Papéis e responsabilidades

- Diferentes usuários podem precisar de diferentes permissões dentro do sistema.

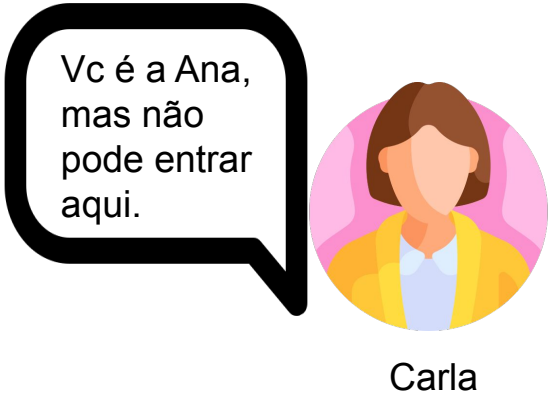


Autenticação

- Garantir que a pessoa é quem ela diz ser.

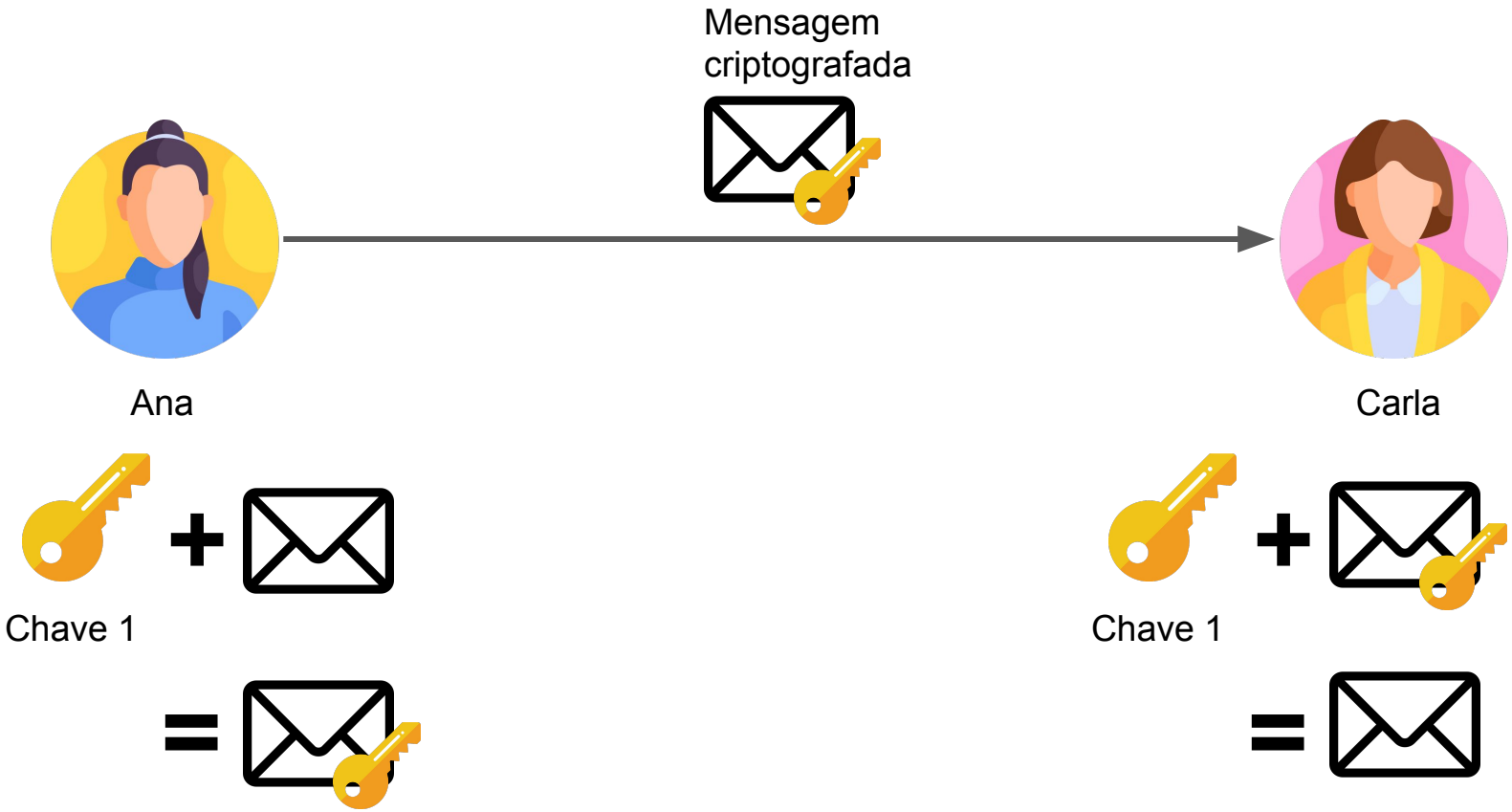
Autorização

- A autorização é o conjunto de permissões disponíveis para a pessoa.

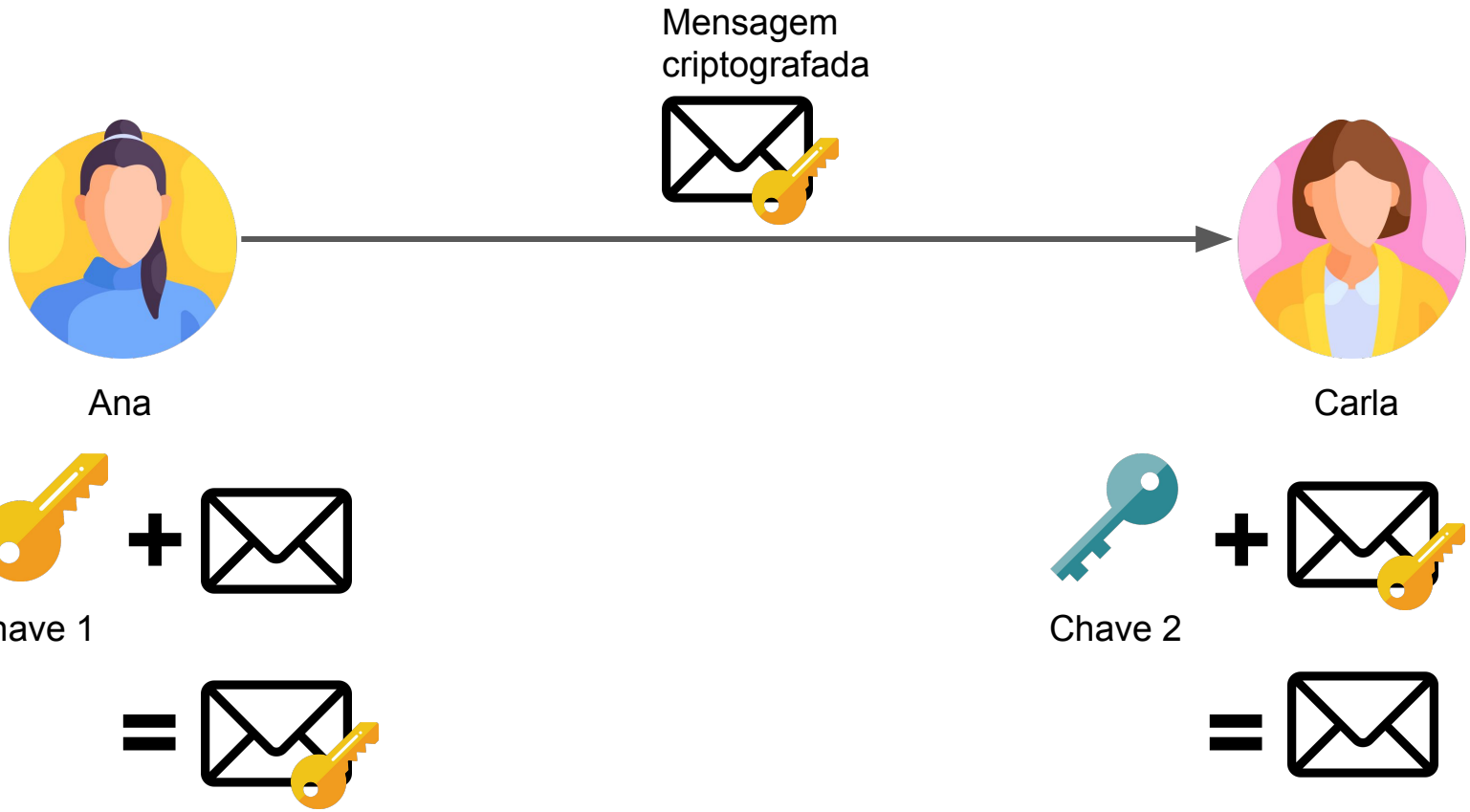


Criptografia: simétrica e assimétrica

Criptografia simétrica

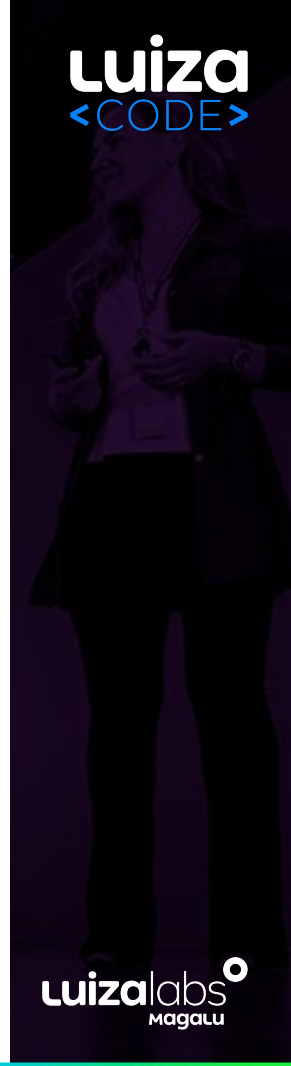


Criptografia assimétrica



Criptografia assimétrica

- Têm duas funções:
  - Criptografar a mensagem de forma que só o destinatário possa ler.
  - Assinar digitalmente a mensagem provando que foi você que escreveu aquela mensagem.

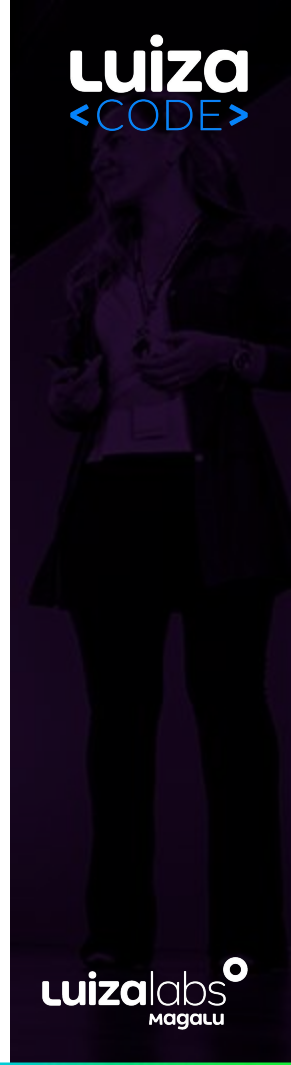



Autenticação HTTP

Autenticação HTTP

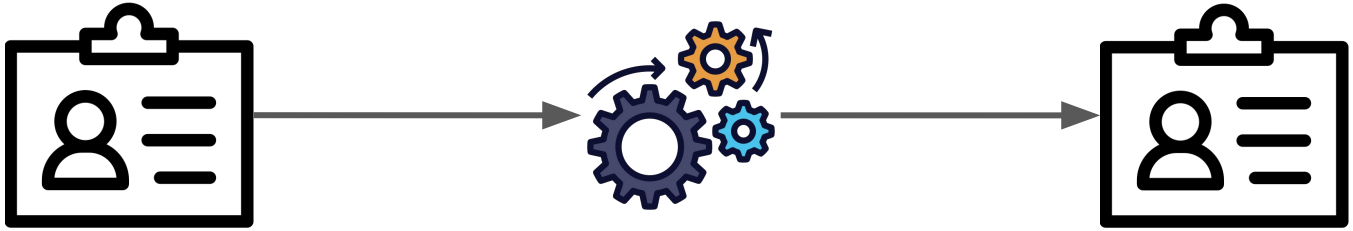
- **Basic:** credenciais (usuário e senha).
- **APIKey**: Criptografia simétrica.
- **Bearer:** tokens bearer (de portador) para acessar recursos protegidos por OAuth 2.0. Criptografia assimétrica.

https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Authentication



Basic

- Credencial (usuário:senha) -> Base64 -> HTTP Header Authorization

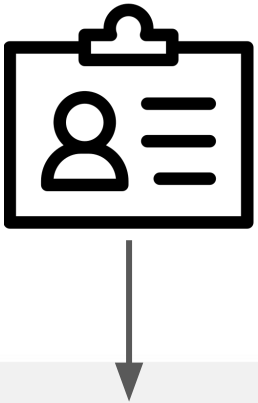


Credencial (usuário:senha)

Base64

Credencial em base64

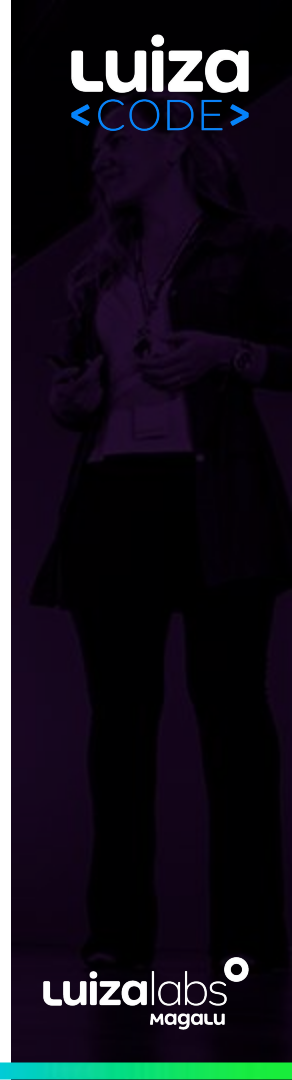
Basic



Credencial em base64

HTTP Header

```
Authorization: Basic <credentials>
```

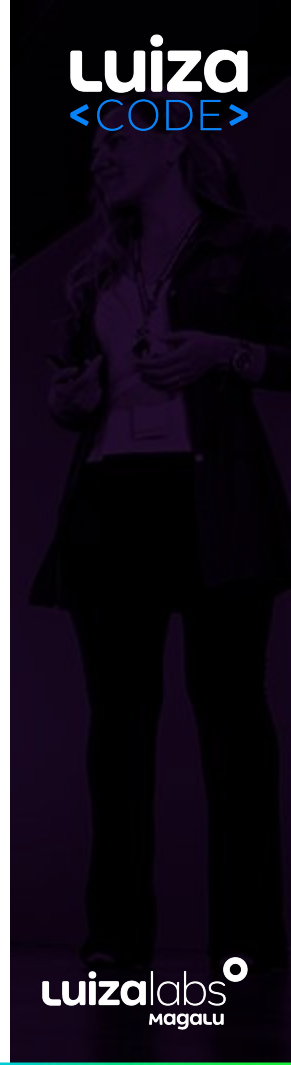


APIKey

- Envia uma chave simétrica no:
  - Header
  - Body
  - URL <- Não recomendado, pois a URL é logada em muitos sistemas.

Exemplo de Apikey na URL:

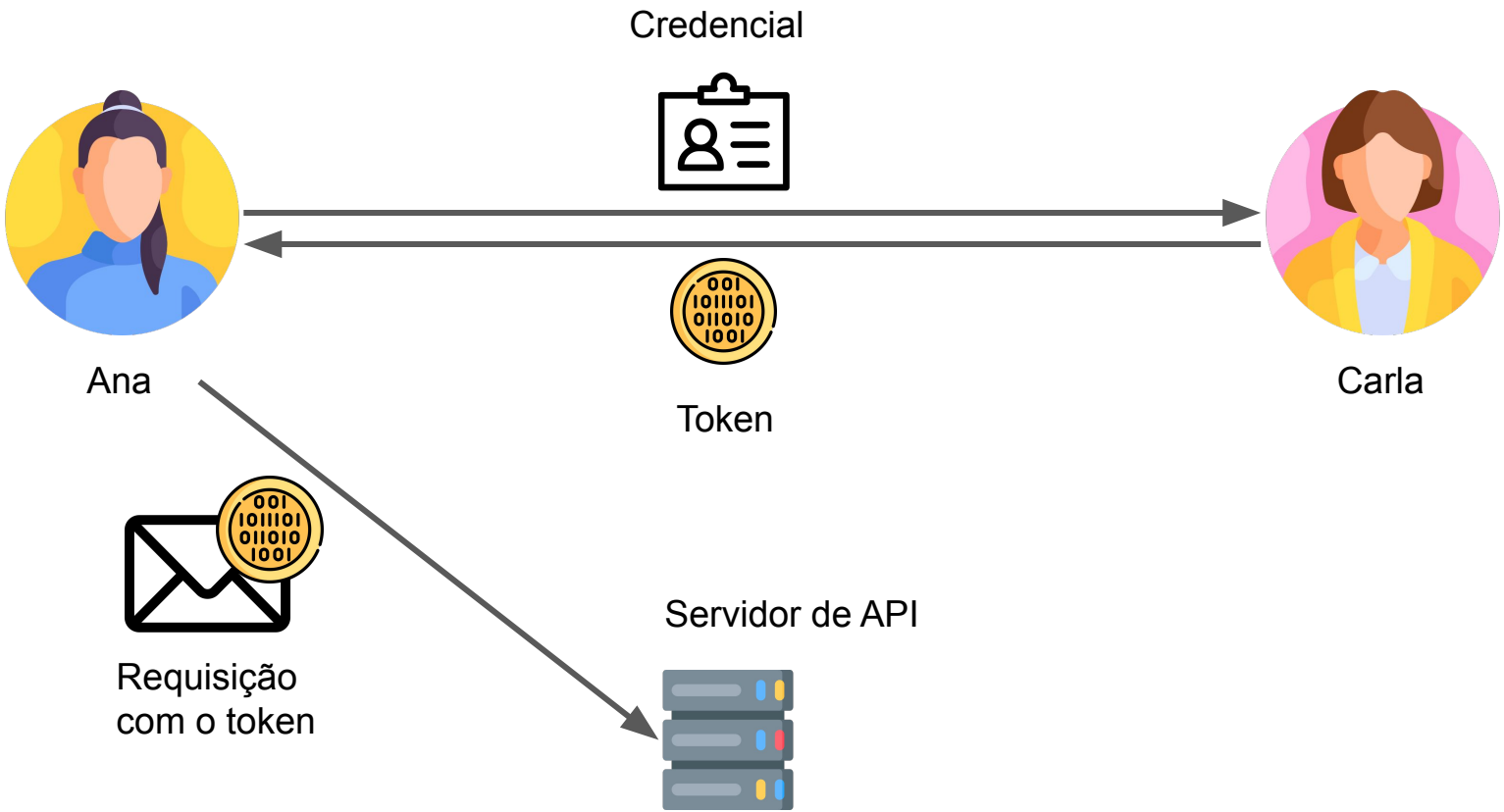
www.exemplo.com/recurso?**apikey=YhYUeCKeBmAQumKapJ**



Bearer

- Funciona por autenticações do OAuth 2.0. No curso utilizaremos autenticação por credenciais (usuário e senha).
- Alinhado com arquiteturas distribuídas como a de micro-seviços.
- Ao invés de confiar sua senha a cada API ou criar milhares de senhas para todas as APIs. Você confia em um único serviço que te fornece um token para acessar as outras APIs.
- Atualmente, a maioria dos sistemas usam o token no formato JWT.
- O token não é criptografado, mas sim assinado, o que garante que foi aquele servidor que o emitiu.

Exemplo usando o Bearer



Perguntas?


magalu
#VemSerFeliz