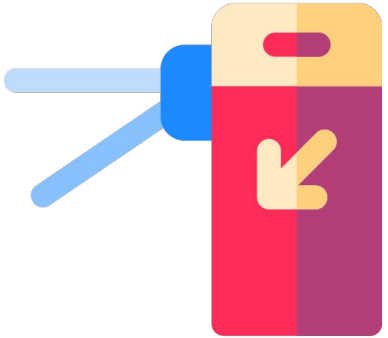
SAAS: uma Solução de Autenticação para Aplicativos de Smartphones

Rafael Fernandes

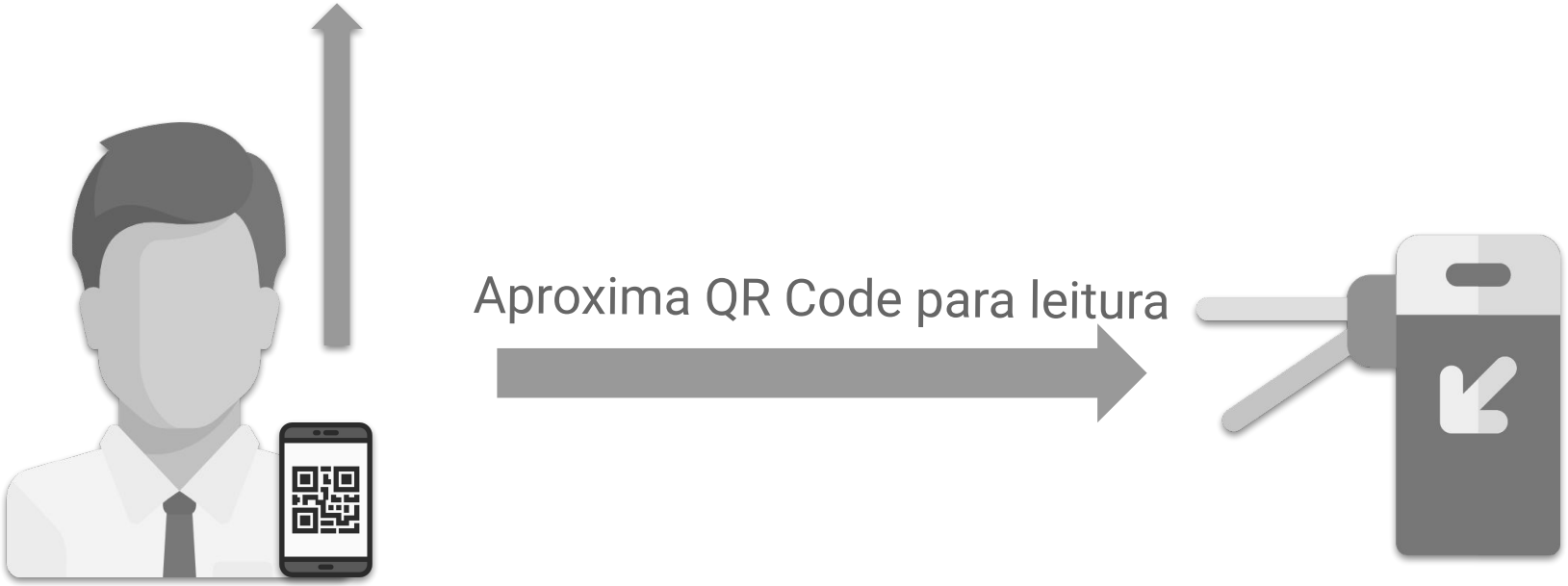
SESC-RS

Aproxima QR Code para leitura

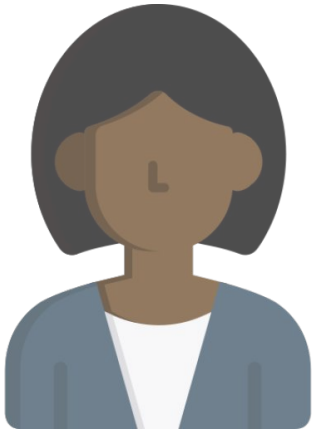


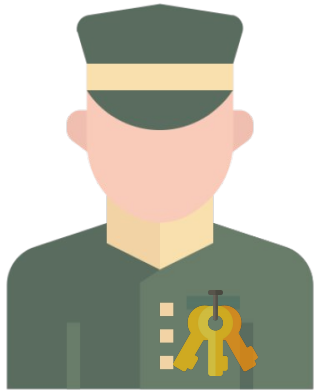
SESC-RS

Problema: O QR Code é estático. Apenas o CPF do usuário acrescido a dois zero ao final.



Gerenciamento de chaves da UNIPAMPA

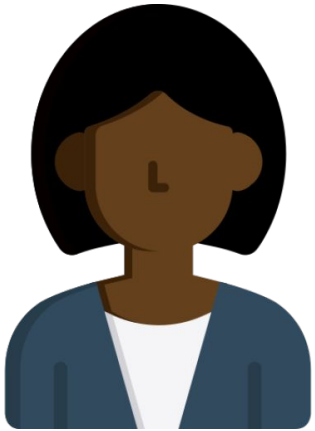


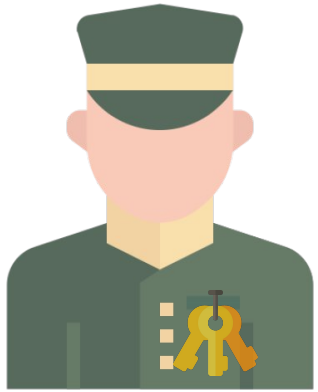


Gerenciamento de chaves da UNIPAMPA

Alice

Professora da UNIPAMPA

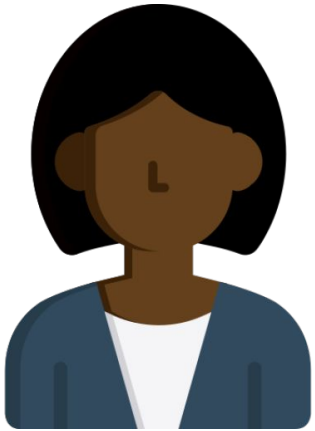




Gerenciamento de chaves da UNIPAMPA

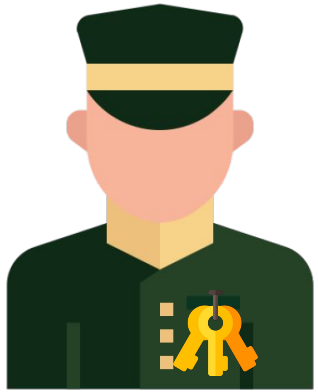
Alice

Professora da UNIPAMPA



Benedito

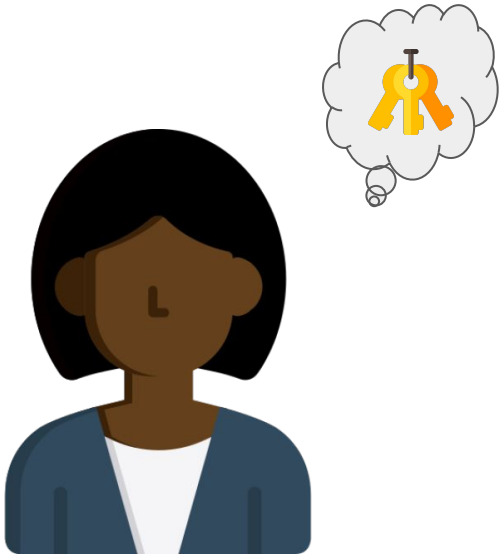
Porteiro da UNIPAMPA



Gerenciamento de chaves da UNIPAMPA

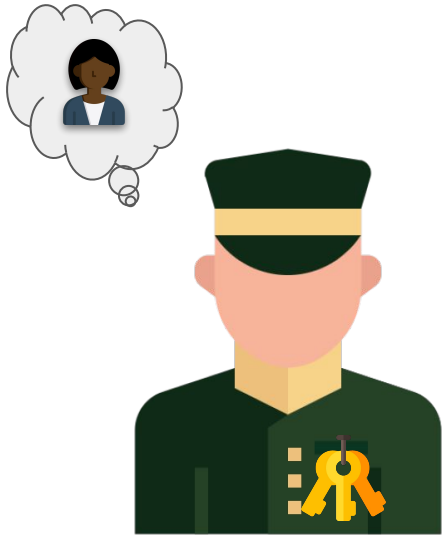
Alice

Professora da UNIPAMPA



Benedito

Porteiro da UNIPAMPA



Gerenciamento de chaves da UNIPAMPA

Alice

Professora da UNIPAMPA

Benedito

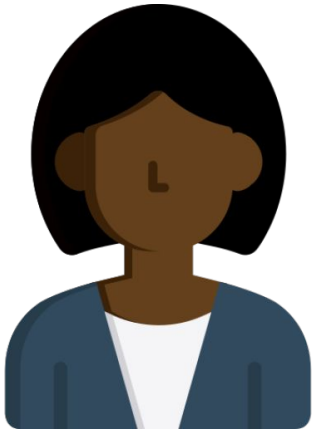
Porteiro da UNIPAMPA

Gerenciamento de chaves da UNIPAMPA

Alice

Professora da UNIPAMPA

:(

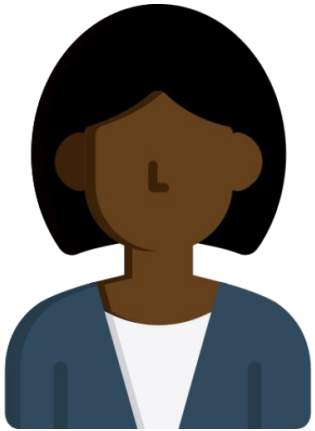


(:

Gerenciamento de chaves da UNIPAMPA

Alice

Professora da UNIPAMPA



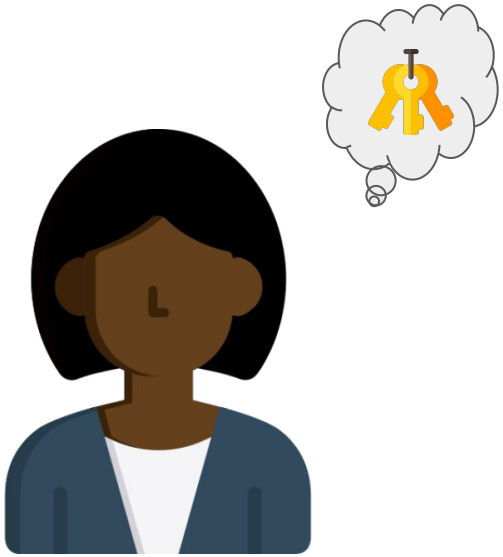
Cláudio (!Schepke)

Novo Porteiro da UNIPAMPA

Gerenciamento de chaves da UNIPAMPA

Alice

Professora da UNIPAMPA



Cláudio (!Schepke)

Novo Porteiro da UNIPAMPA

Gerenciamento de chaves da UNIPAMPA

Alice

Professora da UNIPAMPA

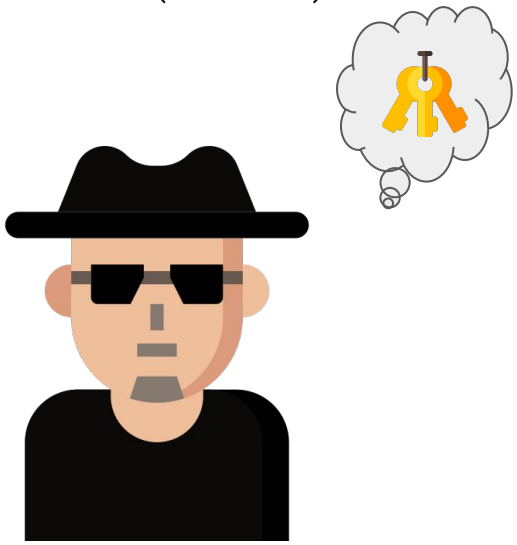
Cláudio (!Schepke)

Novo Porteiro da UNIPAMPA

Gerenciamento de chaves da UNIPAMPA

Diego

Atacante (assistente)



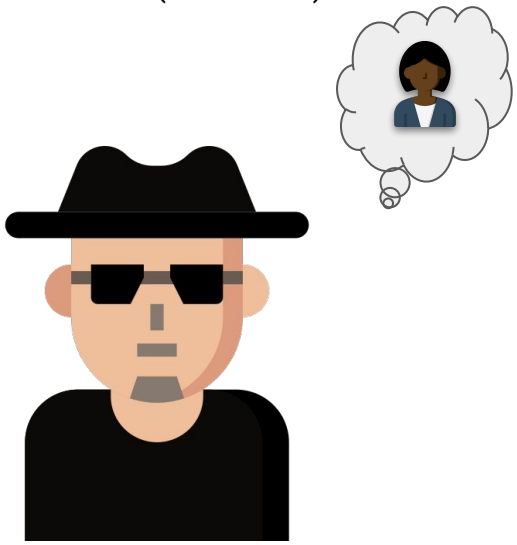
Cláudio (!Schepke)

Novo Porteiro da UNIPAMPA

Gerenciamento de chaves da UNIPAMPA

Diego

Atacante (assistente)



Cláudio (!Schepke)

Novo Porteiro da UNIPAMPA

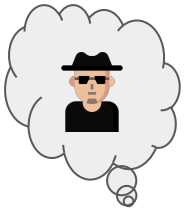
Gerenciamento de chaves da UNIPAMPA

Diego

Atacante (assistente)

Cláudio (!Schepke)

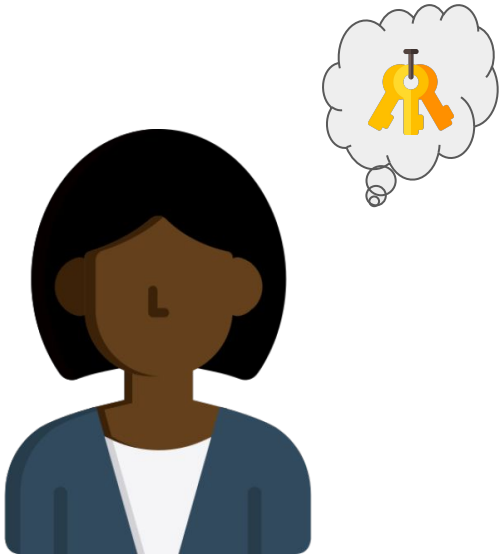
Novo Porteiro da UNIPAMPA



Gerenciamento de chaves da UNIPAMPA

Alice

Professora da UNIPAMPA



Cláudio (!Schepke)

Novo Porteiro da UNIPAMPA

Gerenciamento de chaves da UNIPAMPA

Alice

Professora da UNIPAMPA

Cláudio (!Schepke)

Novo Porteiro da UNIPAMPA

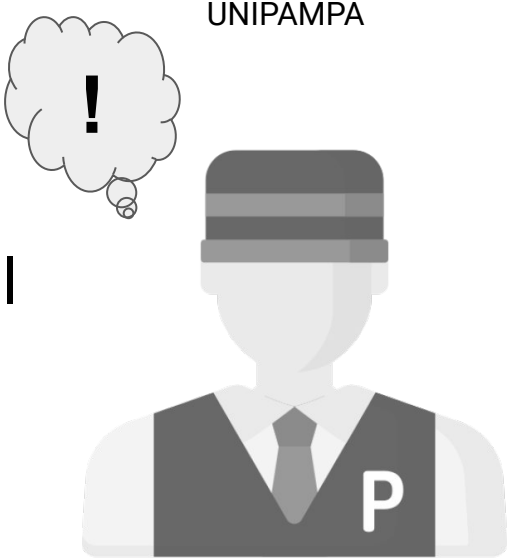
Gerenciamento de chaves da UNIPAMPA

Alice

Professora da UNIPAMPA

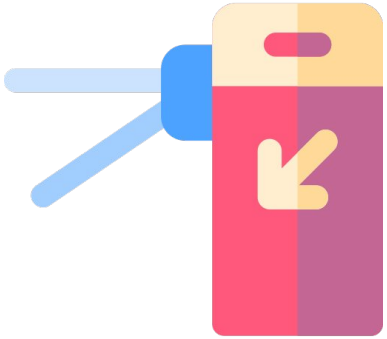
Cláudio (!Schepke)

Novo Porteiro da UNIPAMPA



Problema: engenharia social

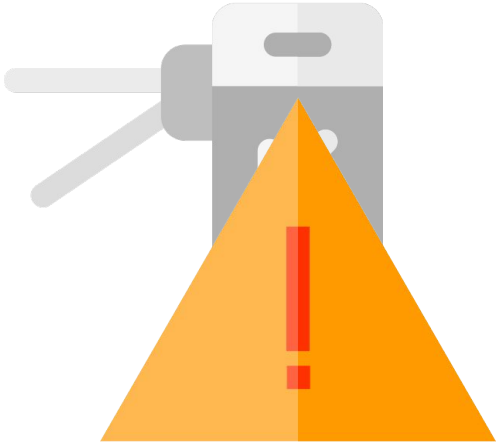
Problemas?



O que há de comum?

Problema de autenticação!

Problemas?



Como resolver?

Tecnologias

Algoritmos similares

SAAS

Considerações Finais

Cronograma

Autenticação por Múltiplos Fatores

O que é autenticação digital?

Fatores de Autenticação

O que é autenticação de múltiplos fatores?

O que é autenticação digital?

O que é autenticação digital?

Autenticação por Múltiplos Fatores

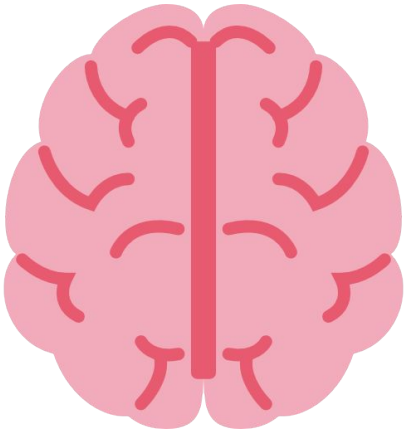
O que é autenticação digital?

Fatores de Autenticação

O que é autenticação de múltiplos fatores?

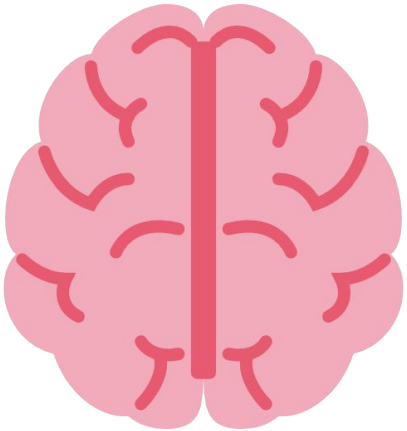
Fatores de autenticação

Conhecimento

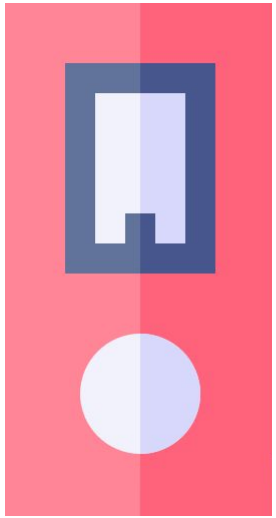


Fatores de autenticação

Conhecimento

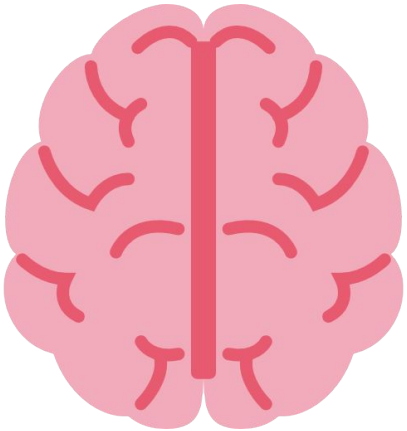


Posse

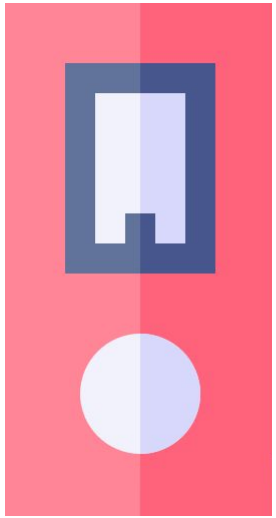


Fatores de autenticação

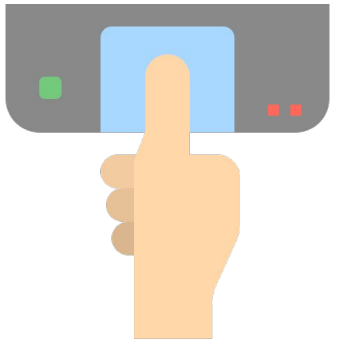
Conhecimento



Posse



Identidade / Biometria



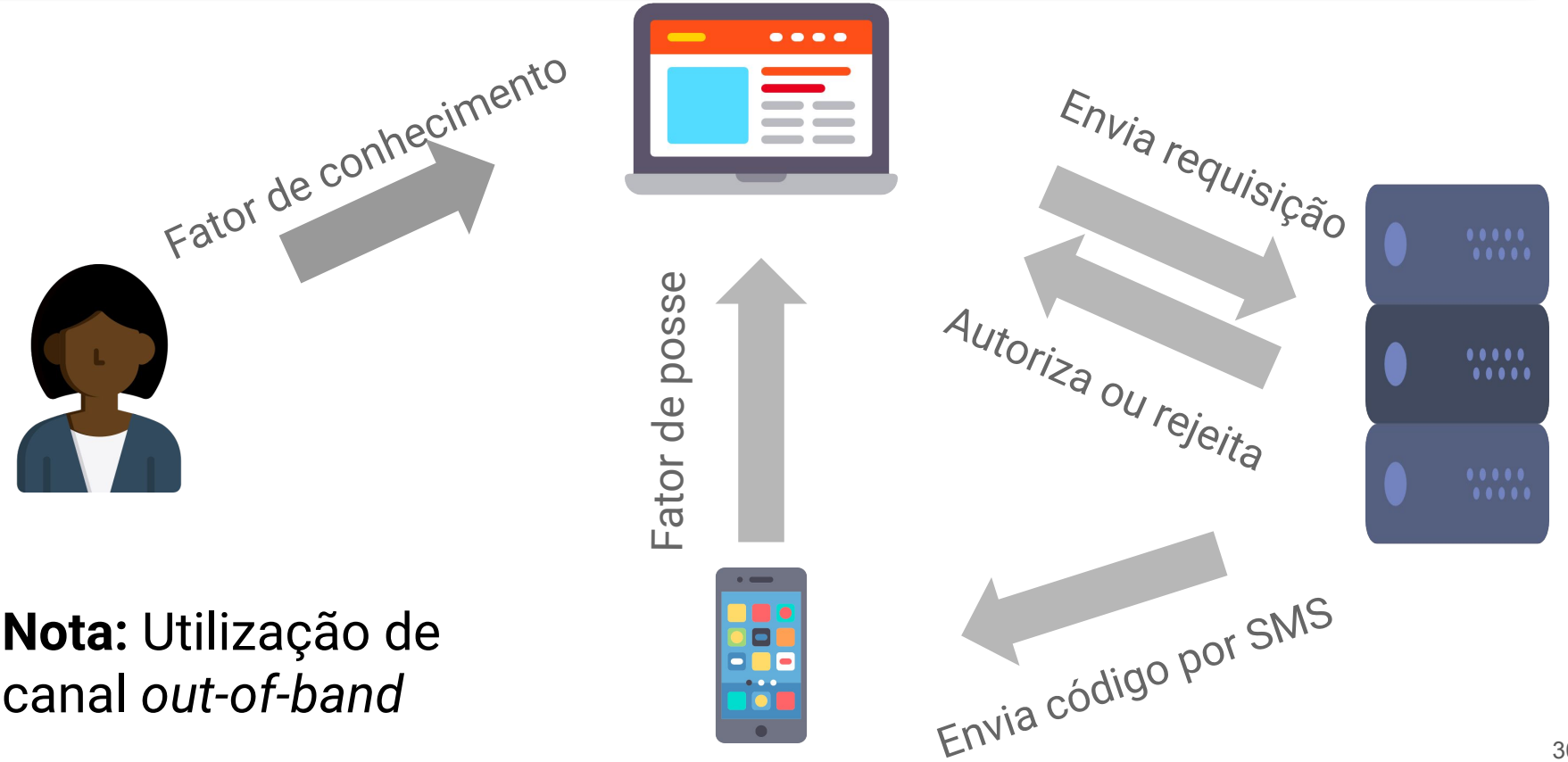
Autenticação por Múltiplos Fatores

O que é autenticação digital?

Fatores de Autenticação

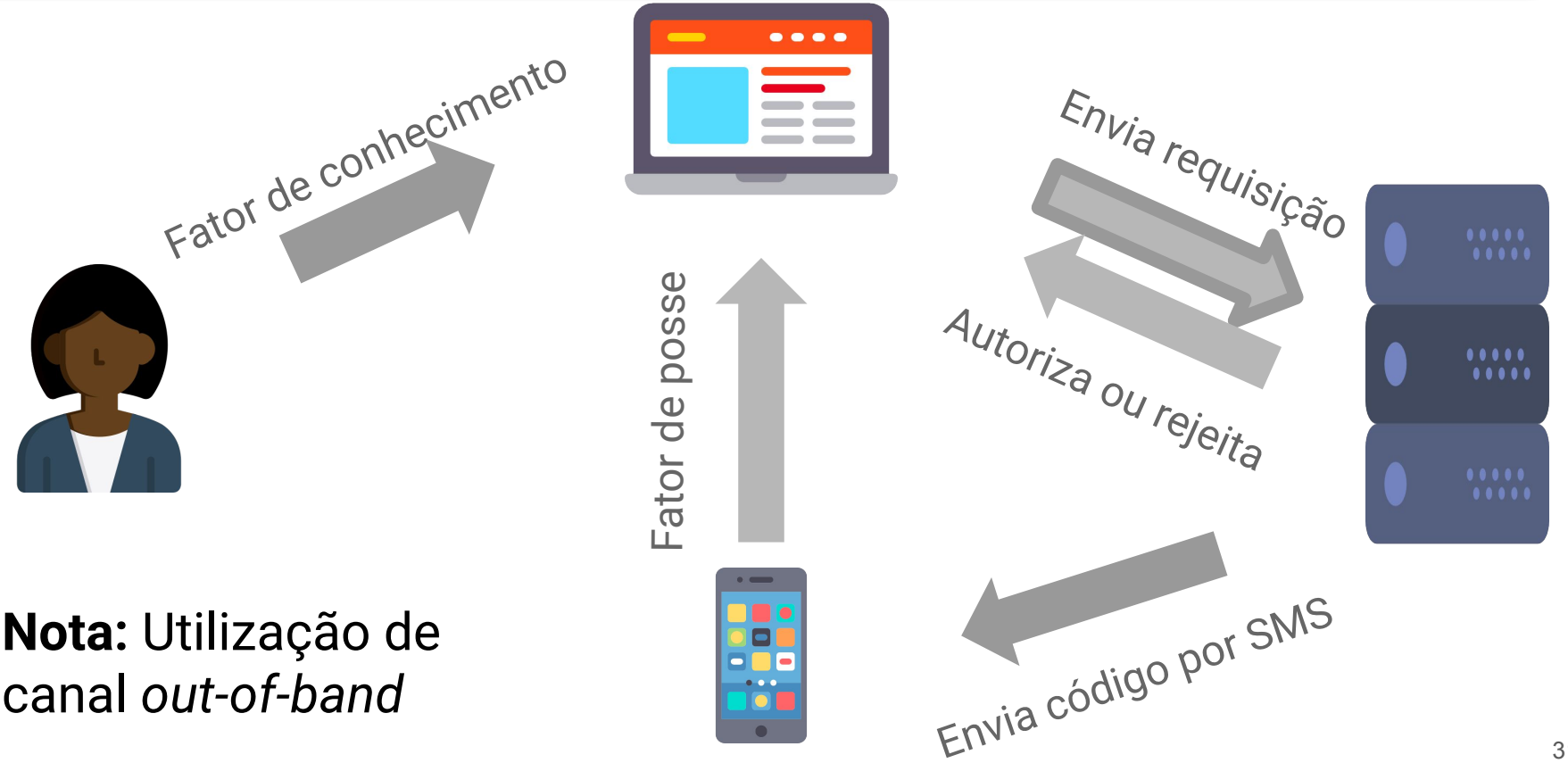
O que é autenticação de múltiplos fatores?

O que é autenticação de múltiplos fatores?



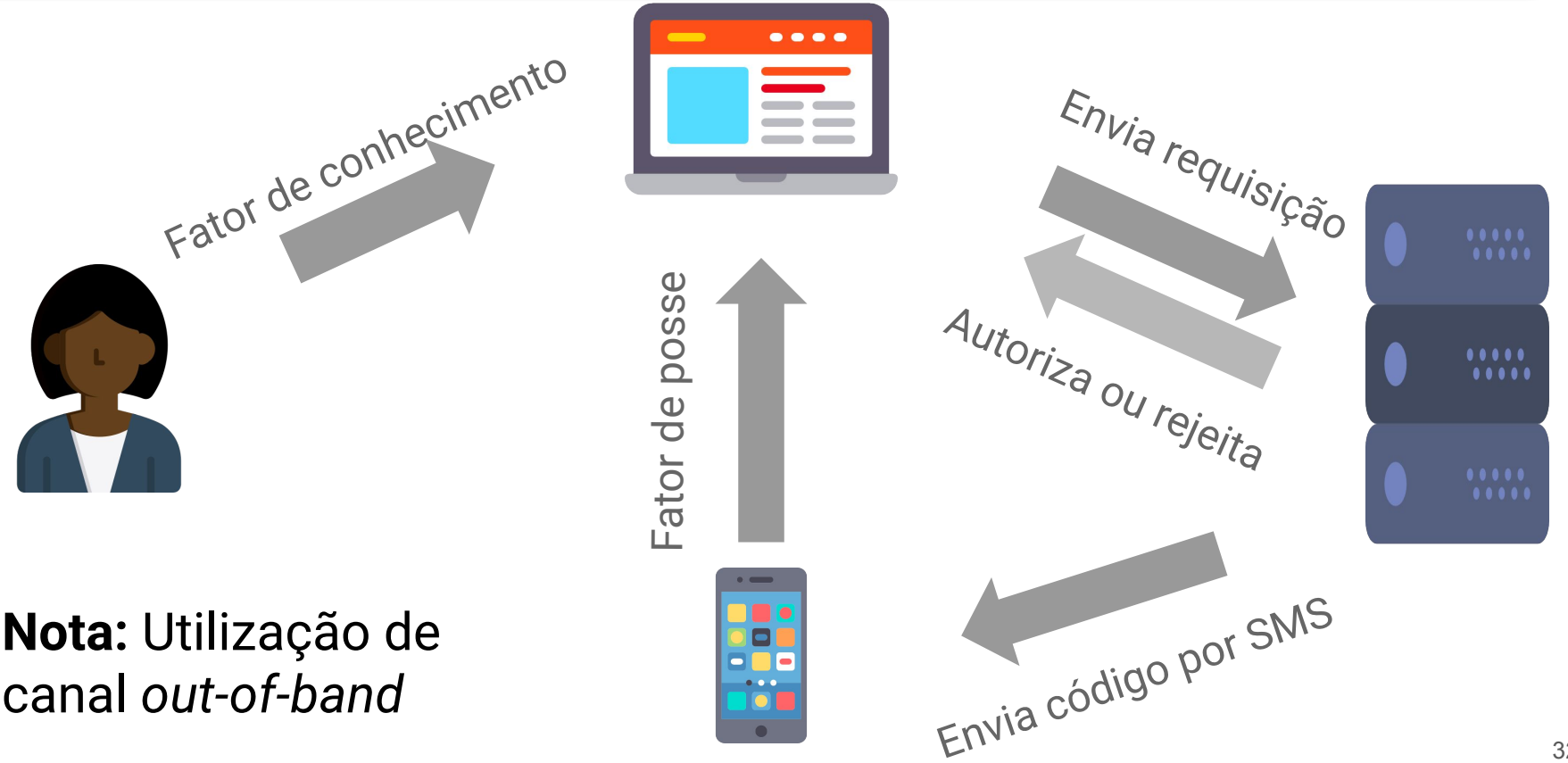
Nota: Utilização de canal *out-of-band*

O que é autenticação de múltiplos fatores?



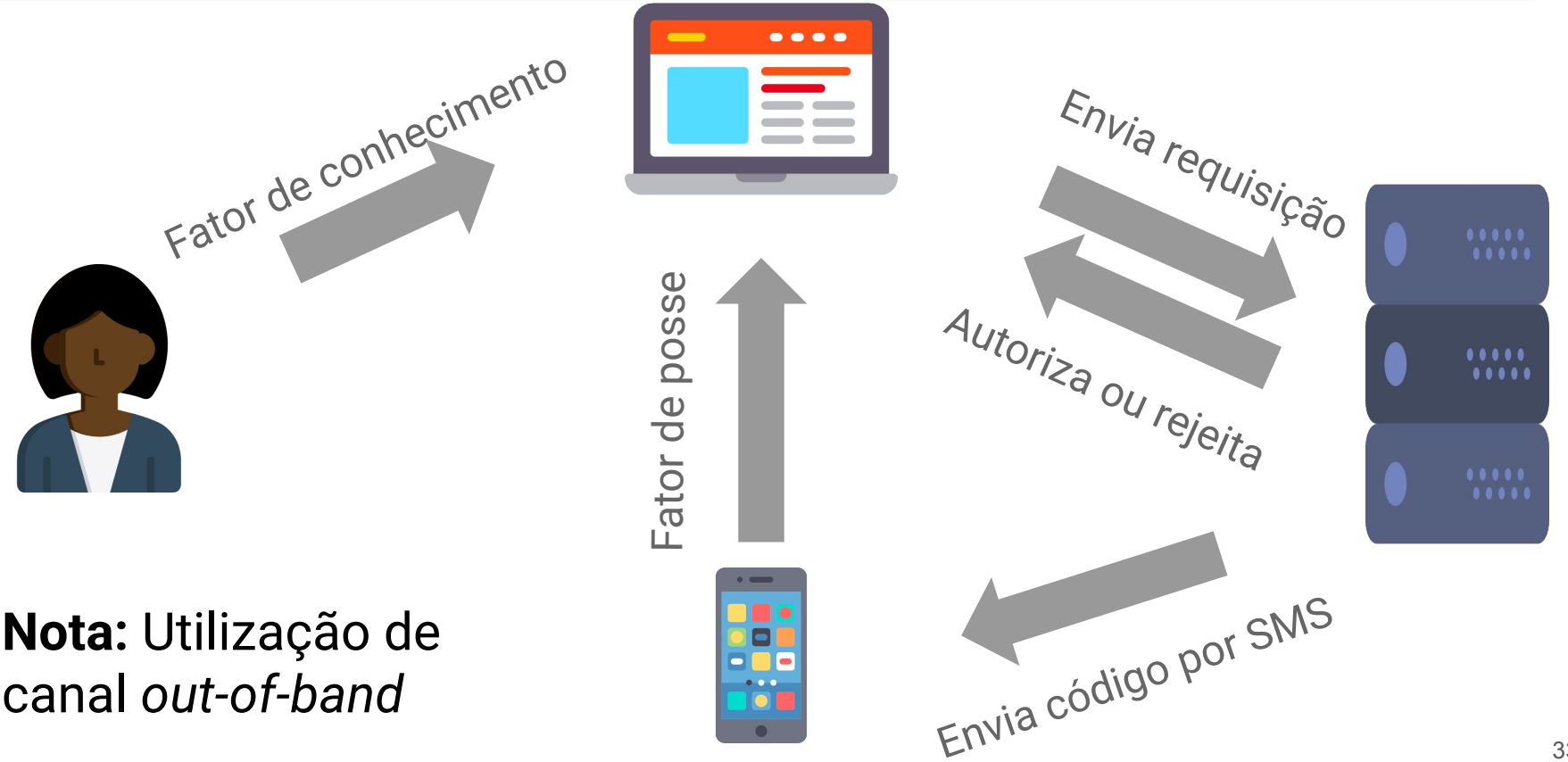
Nota: Utilização de canal *out-of-band*

O que é autenticação de múltiplos fatores?



Nota: Utilização de canal *out-of-band*

O que é autenticação de múltiplos fatores?



Nota: Utilização de canal *out-of-band*

Tecnologias

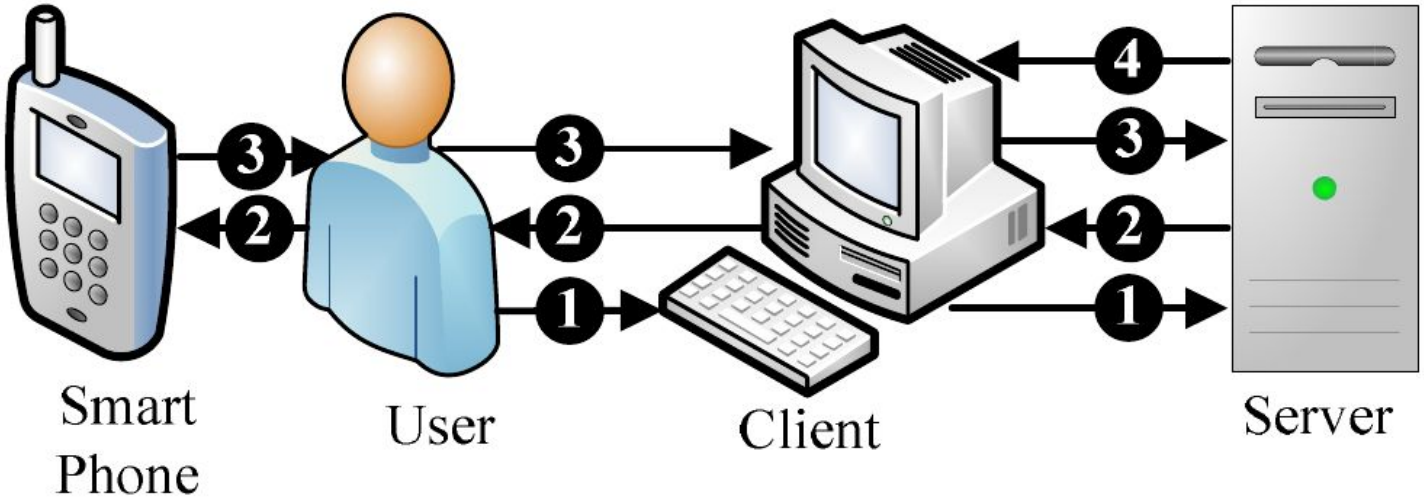
Algoritmos similares

SAAS

Considerações Finais

Cronograma

Algoritmos similares



“OTP-Based Two-Factor Authentication Using Mobile Phones”

Problemas em aberto

- Utilização de funções *hash* antigas como SHA-1 e MD5
- PKE depende da confiança das certificadoras
- Utilização de fatores de posse (*smart cards*)
- Custo de envio de SMS e cartas para enviar chaves e códigos

Tecnologias

Algoritmos similares

SAAS

Considerações Finais

Cronograma

Principais características da SAAS

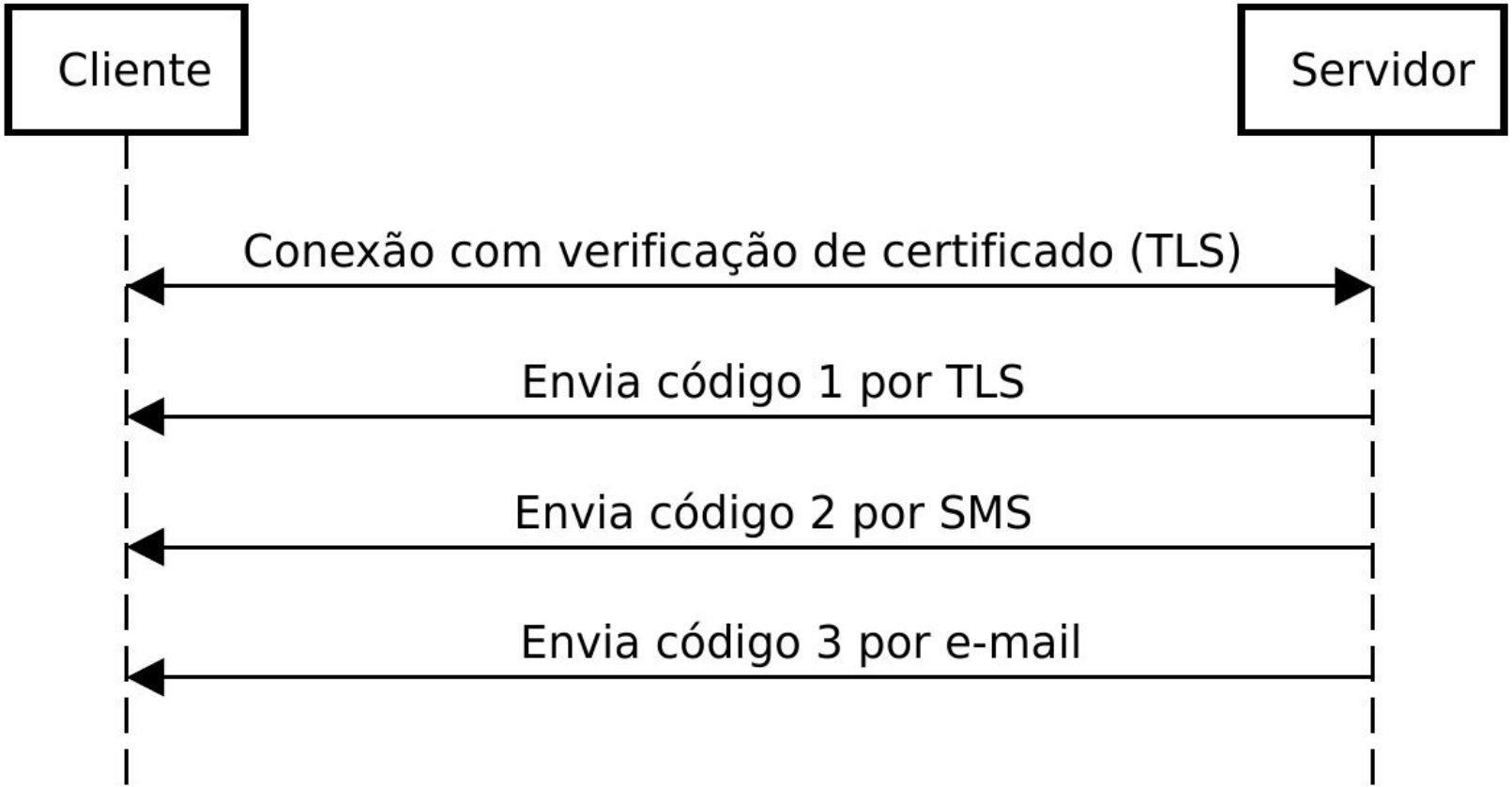
- **Proposta de protocolos de identificação e autenticação genéricos**
  - Uso canais *out-of-band* no processo de identificação

- Geração códigos únicos

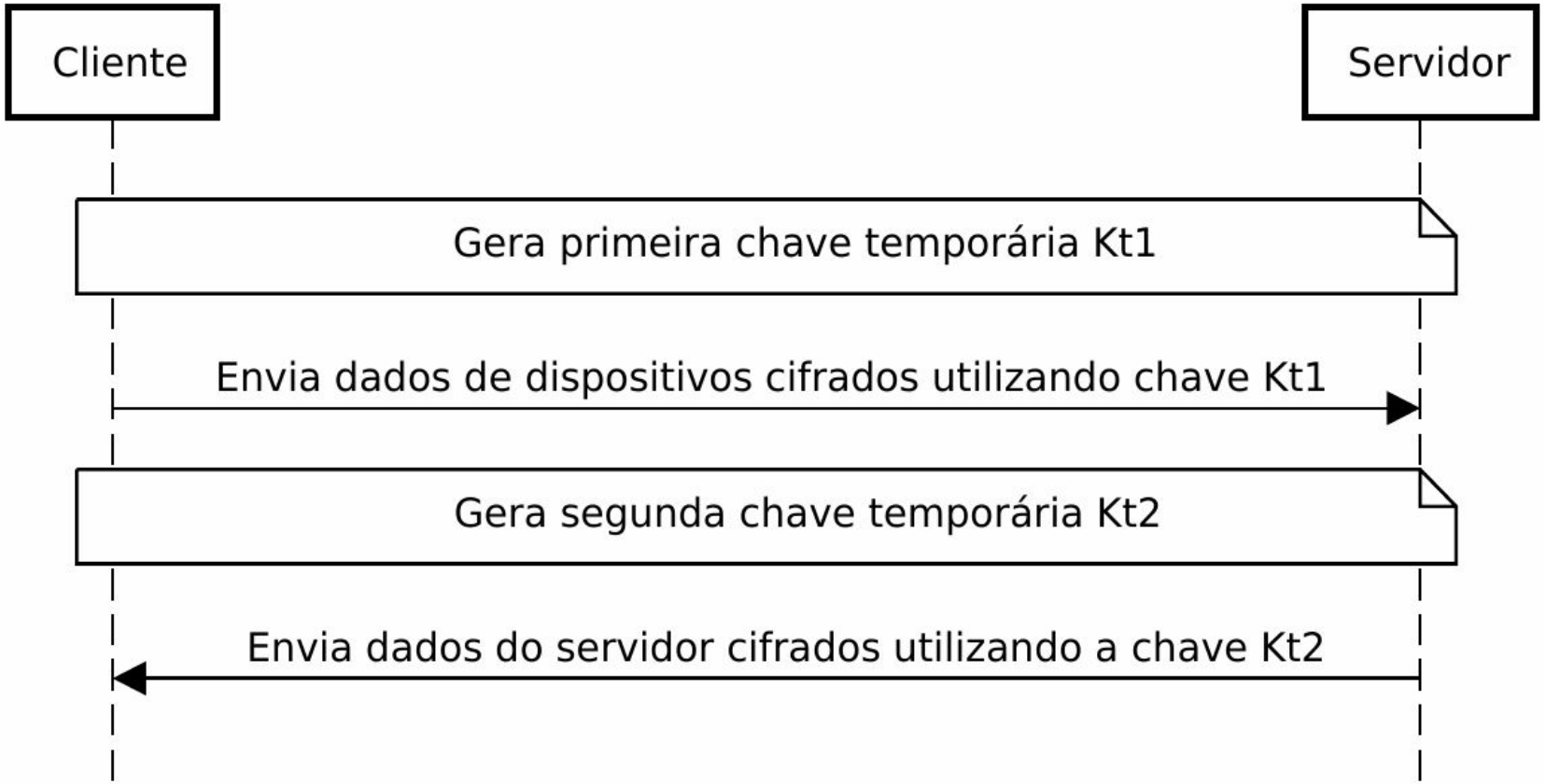
Protocolo de identificação

- Identificar usuários
- Vincular acesso de usuário do aplicativo ao dispositivo
- Gerar chave mestra

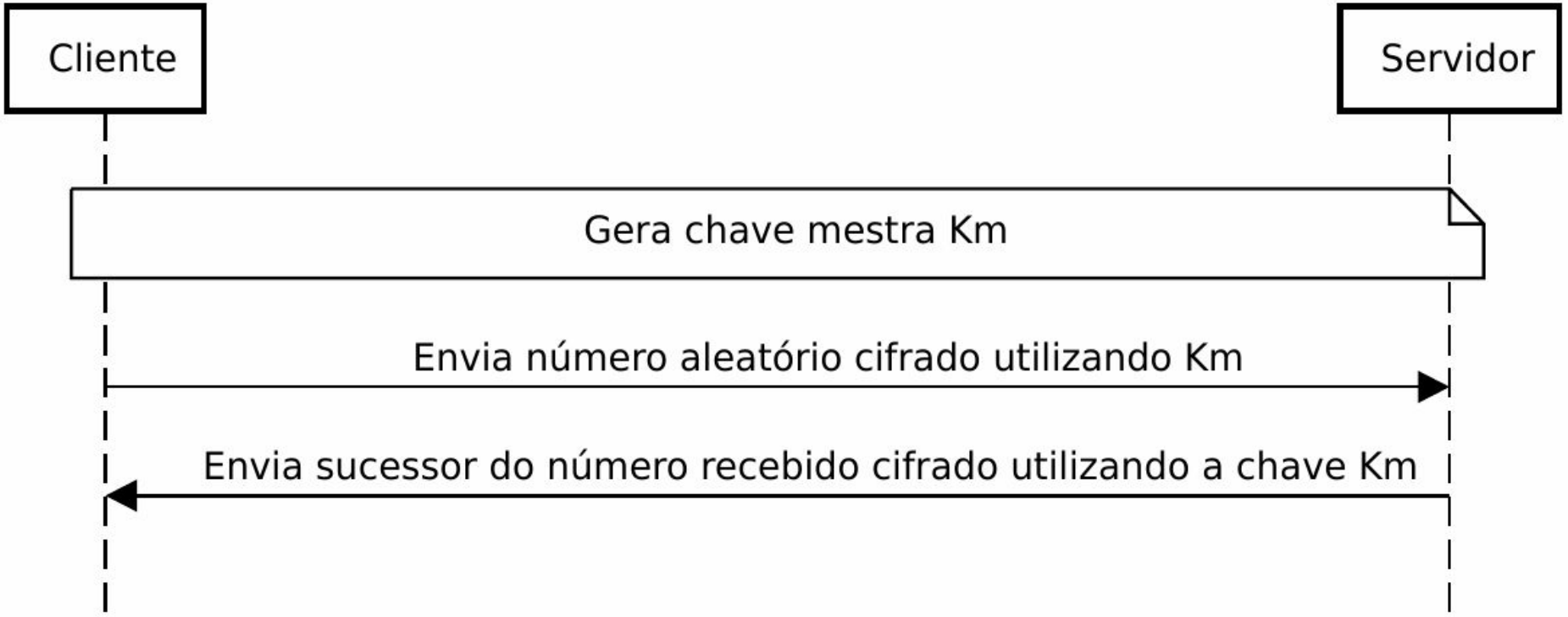
Protocolo de identificação - Diagrama 1/3



Protocolo de identificação - Diagrama 2/3



Protocolo de identificação - Diagrama 3/3



Protocolo de identificação - Algoritmo

1. Cliente $\overset{\text{TLS}}{\longleftrightarrow}$ Servidor	Conexão com verificação do certificado do Servidor
2. Servidor $\rightarrow$ Cliente	[CODE_TLS, $code_1$]
3. Servidor $\rightarrow$ Cliente	[CODE_SMS, $code_2$]
4. Servidor $\rightarrow$ Cliente	[CODE_EMAIL, $code_3$]
5. Cliente, Servidor	$K_{T1} \leftarrow \text{H}(tls\_session\_key \| \| code_1 \| \| code_2 \| \| code_3)$
6. Cliente $\rightarrow$ Servidor	[SEND, *nonce*, $\text{E}_{K_{T1}}$(imei, app_rand1)], $\text{HMAC}_{K_{T1}}$
7. Cliente, Servidor	$K_{T2} \leftarrow \text{H}(imei \| \| app\_rand1 \| \| K_{T1})$
8. Servidor $\rightarrow$ Cliente	[SEND, *nonce*, $\text{E}_{K_{T2}}(server\_rand)$], $\text{HMAC}_{K_{T2}}$
9. Cliente, Servidor	$K_m \leftarrow \text{H}(K_{T1} \| \| K_{T2} \| \| imei \| \| app\_rand1 \| \| server\_rand)$
10. Cliente $\rightarrow$ Servidor	[V_MKEY, *nonce*, $\text{E}_{K_m}(app\_rand2)$], HMAC_{K_m}
11. Servidor $\rightarrow$ Cliente	[V_MKEY, *nonce*, $\text{E}_{K_m}(app\_rand2 + 1)$], HMAC_{K_m}

Protocolo de autenticação

O que é?

Como funciona?

Quais são as vantagens?

O que é?

- Esquema de autenticação simples
- Gerador de códigos únicos
- Protocolo genérico

Protocolo de autenticação

O que é?

Como funciona?

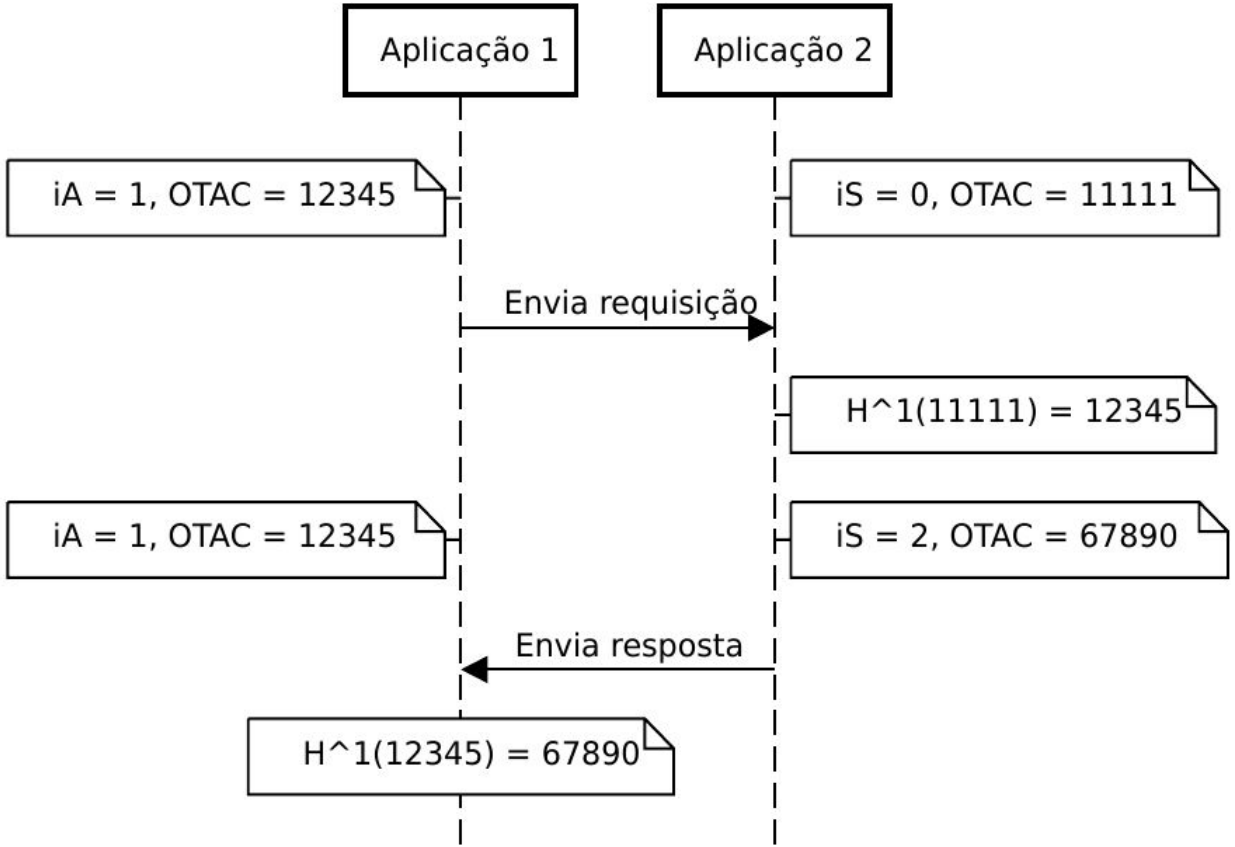
Quais são as vantagens?

Como funciona?

- Códigos de autenticação (OTAC):
  - K_c é a chave inicial ($K_c = H(K_m)$)
  - Primeiro código OTAC = K_c
  - Próximos códigos OTAC = H^N(OTAC)
  - **Utilizados como chave para HMAC**

- Índices:
  - Diferença entre índices (*iA - iS*)
  - Sincroniza OTAC
  - Verifica autenticidade OTAC

Como funciona?



Como funciona?

- Ciclos de atualizações:
  - Índices incrementados a cada troca de mensagens
  - Índices incrementados ao solicitar novo QR Code (aplicações móveis)
  - Índices incrementados a cada 60 segundos (aplicações móveis)
  - Código OTAC e índices sincronizados a cada troca de mensagens

Protocolo de autenticação

O que é?

Como funciona?

Quais são as vantagens?

Quais são as vantagens?

- Não utiliza senhas estáticas
- Códigos dinâmicos
- Não há necessidade de transmitir os códigos de autenticação
- Garante *Perfect Forward Secrecy*
- **Pode ser aplicado em casos de usos variados**

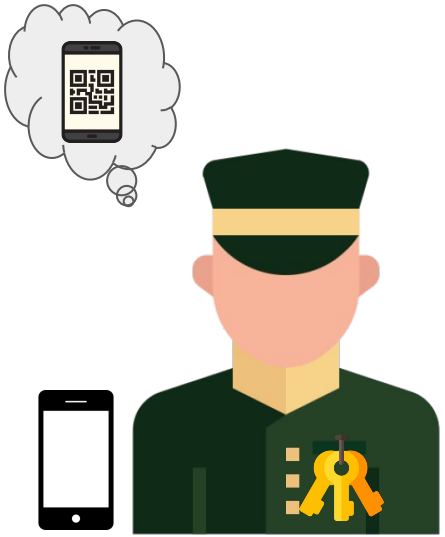
Caso de uso 2: gerenciamento de chaves

Alice

Professora da UNIPAMPA

Benedito

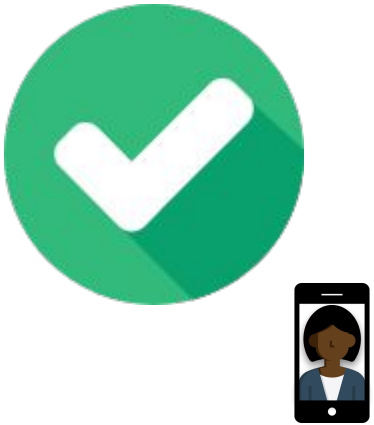
Porteiro da UNIPAMPA



Protocolo aplicado ao gerenciamento de chaves

Alice

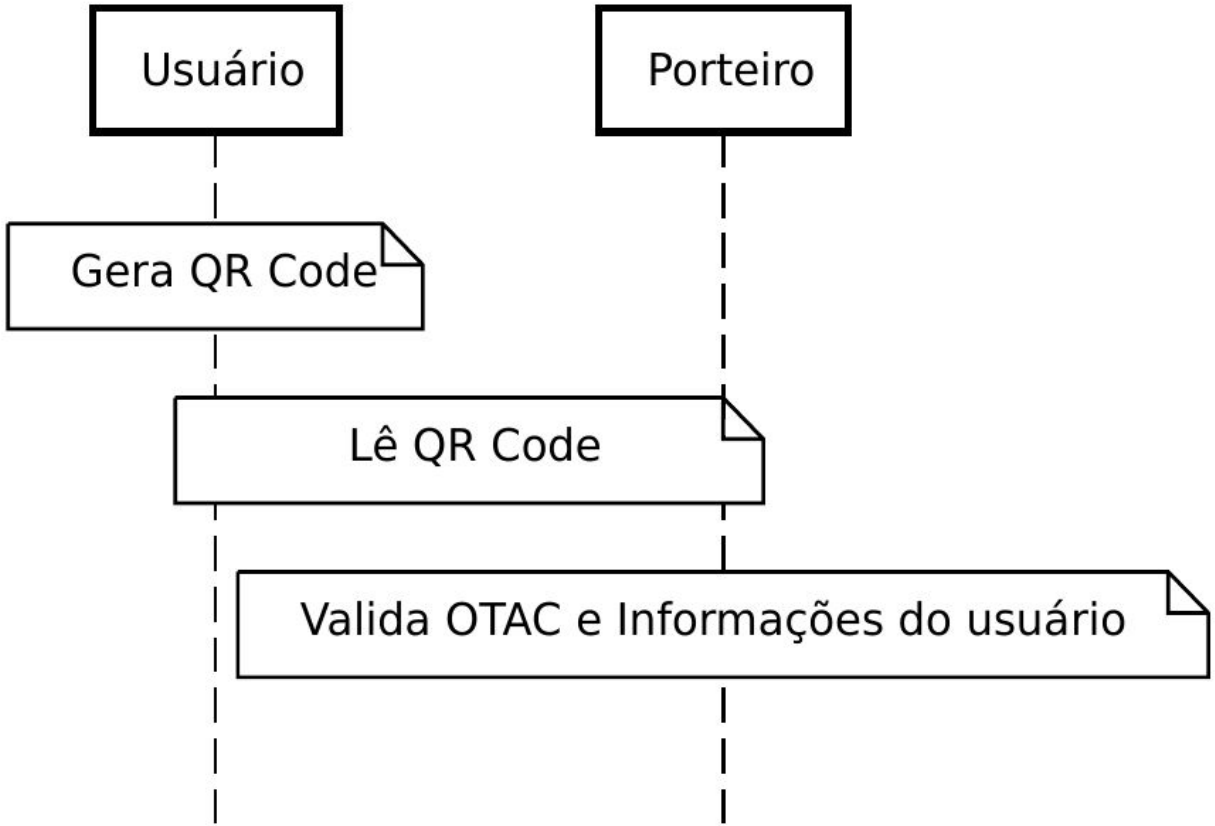
Professora da UNIPAMPA



Benedito

Porteiro da UNIPAMPA

Caso de uso 2: gerenciamento de chaves - Diagrama

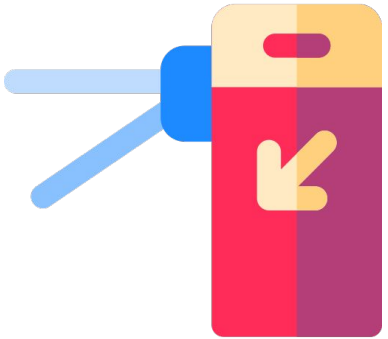


Caso de uso 2: gerenciamento de chaves - Algoritmo

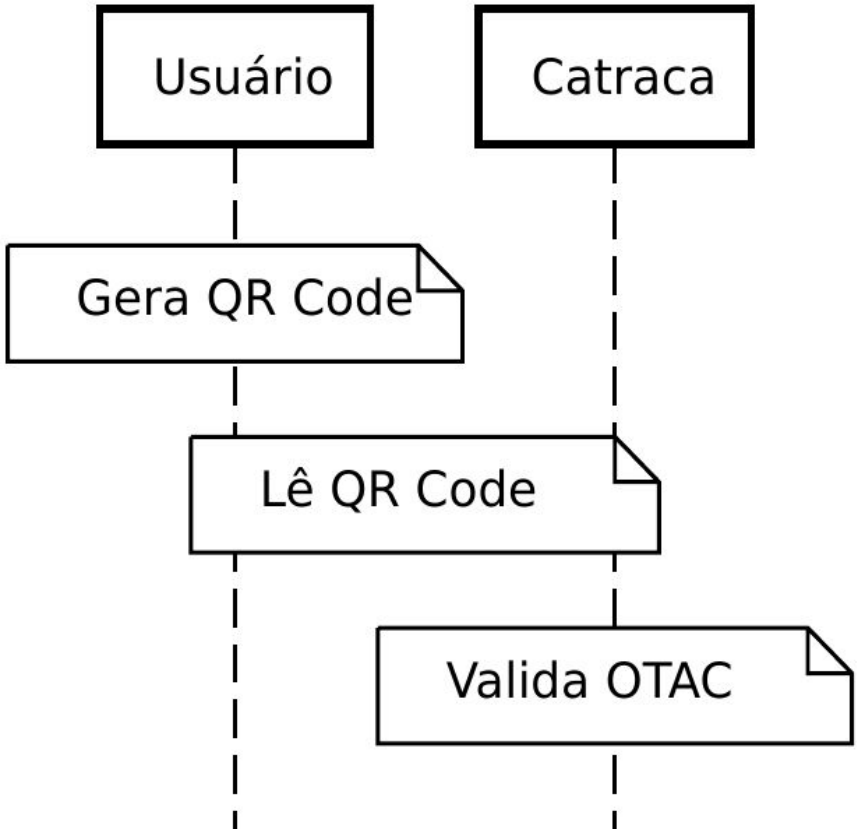
1. Usuário	Abre o aplicativo da carteirinha digital de identificação
2. Usuário	QR Code = [AUTH, nome, tipo, foto, iA], HMAC
3. Porteiro	Lê o QR Code
4. Porteiro	OTAC $\leftarrow$H^{iA-iS}(OTAC)
5. Porteiro	Verifica HMAC utilizando o OTAC como chave
6. Porteiro	Confere as informações do usuário (nome, tipo, foto, etc.)

Caso de uso 3: acesso em catracas digitais

Aproxima QR Code para leitura



Caso de uso 3: acesso em catracas digitais - Diagrama



Caso de uso 3: acesso em catracas digitais - Algoritmo

1. Usuário	Abre o aplicativo da carteirinha digital de identificação
2. Usuário	QR Code = [id, iA], HMAC
3. Usuário	Aproxima o QR Code do leitor da catraca
4. Catraca	Lê o QR Code
5. Catraca	Atualiza o OTAC $\leftarrow \mathrm{H}^{iA-iS}(\mathrm{OTAC})$
6. Catraca	Verifica HMAC utilizando o OTAC como chave

Tecnologias

Algoritmos similares

SAAS

Considerações Finais

Cronograma

Considerações finais

Protocolos genéricos

Independência de protocolos

Aplicação prática

unipampa

Universidade Federal do Pampa

Obrigado!

Contato:
faelsfernandes@gmail.com

SAAS: uma Solução de Autenticação para Aplicativos de Smartphones

Rafael Fernandes