

# Desafios do gerenciamento de identidade digital pelo usuário

Do uso inadequado de senhas à identidade digital descentralizada

Shirlei Chaves - 08/11/2023

5a. Semana Acadêmica do Curso de Redes de Computadores - SARC 2023

Universidade Federal de Santa Maria - UFSM

# Agenda

- Contextualização
- Tecnologias Emergentes
  - Passkeys
  - Identidade Descentralizada
- Considerações Finais

# Contextualização

# O que é uma identidade digital?

- Para o NIST (National Institute of Standards and Technology):

“A **representação única** de um sujeito envolvido em uma transação online. Uma identidade digital é sempre única no **contexto** de um serviço digital, mas **não** precisa **necessariamente** ser **rastreável** até um **sujeito específico da vida real**” [1]

# O que é uma identidade digital?

- Para o NIST (National Institute of Standards and Technology):

“A **representação única** de um sujeito envolvido em uma transação online. Uma identidade digital é sempre única no **contexto** de um serviço digital, mas **não** precisa **necessariamente** ser **rastreável** até um **sujeito específico da vida real**” [1]

“Na Internet, ninguém sabe  
que você é um cachorro”

(Peter Steiner, 1993)



[1] NIST SP 800-63-3 - <https://pages.nist.gov/800-63-3/sp800-63-3.html>

**“A internet foi construída  
sem uma camada nativa  
de identidade”**

**(Kim Cameron, 2005)[2]**

# Gerenciamento de Usuários - Autenticação

## Fatores de autenticação

Incluem [3]:

- **Alguma coisa que você sabe**
  - Senha, número de identificação pessoal (PIN - Personal Identification Number), etc
- **Alguma coisa que você tem**
  - Token criptográfico
- **Alguma coisa que você é**
  - Biometria

*Algum lugar em que você está:* serviços e aplicações disponíveis apenas dentro de uma localização geográfica.

[3] Veja mais em <https://doi.org/10.5753/sbc.10710.3>, Capítulo 1, página 24.

# Autenticação

## Senha

- Par usuário e senha (ainda) amplamente adotado
  - Ataque de força bruta, *phishing*
- As pessoas normalmente não sabem criar uma boa senha
  - Carga cognitiva
- As empresas nem sempre empregam as melhores técnicas para evitar vazamento de senhas e auxiliar os usuários a manterem suas identidades seguras

Top 5 senhas mais utilizadas no mundo de 2019 à 2022			
2019	2020	2021	2022
12345	123456	123456	password
123456	123456789	123456789	123456
123456789	picture1	12345	123456789
test1	password	querty	guest
password	12345678	password	12345678

Senhas comuns [4]

**No Brasil em 2022:** 123456, Brasil, 123456789, 12345, 12345678

...

Em 21o. lugar: 123mudar

Please choose a password

- ✗ Rule 5  
The digits in your password must add up to 25.
- ✓ Rule 4  
Your password must include a special character.
- ✓ Rule 3  
Your password must include an uppercase letter.
- ✓ Rule 2  
Your password must include a number.
- ✓ Rule 1  
Your password must be at least 5 characters.

Jogo da senha [5]

[4] Top 200 most common passwords - Nord Security Research - <https://nordpass.com/most-common-passwords-list/>

[5] The Password Game - <https://neal.fun/password-game>

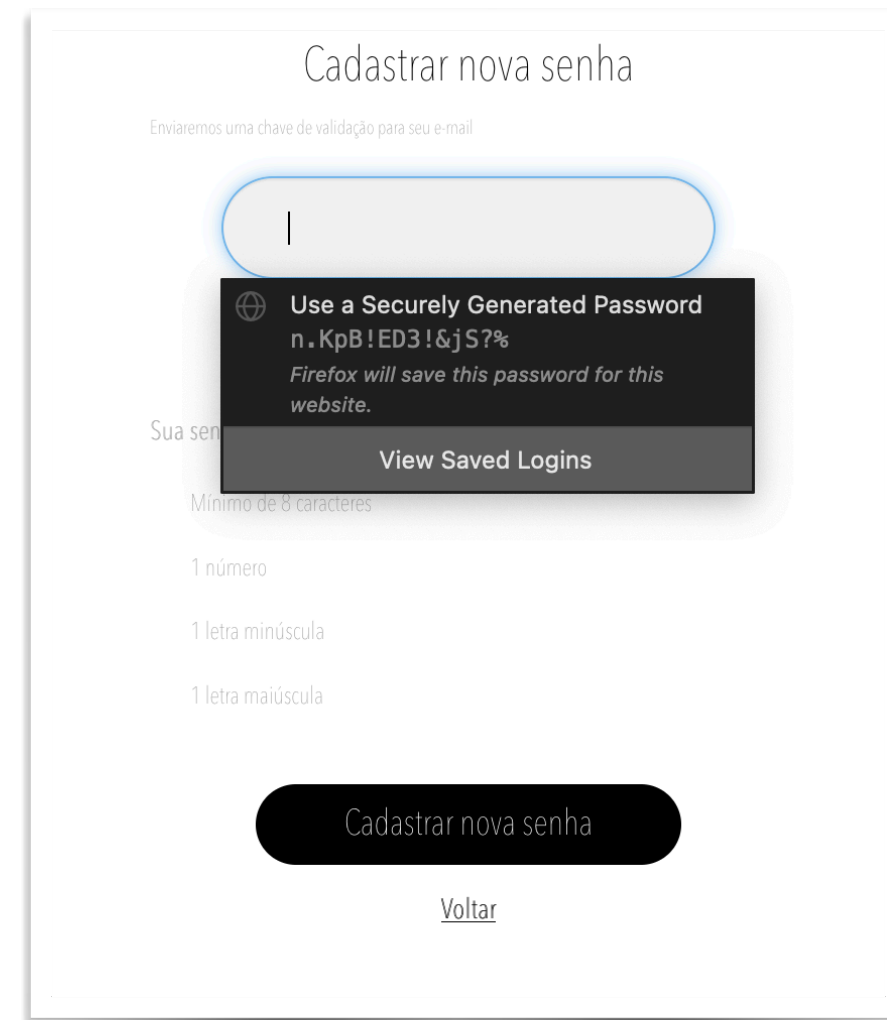


# Autenticação

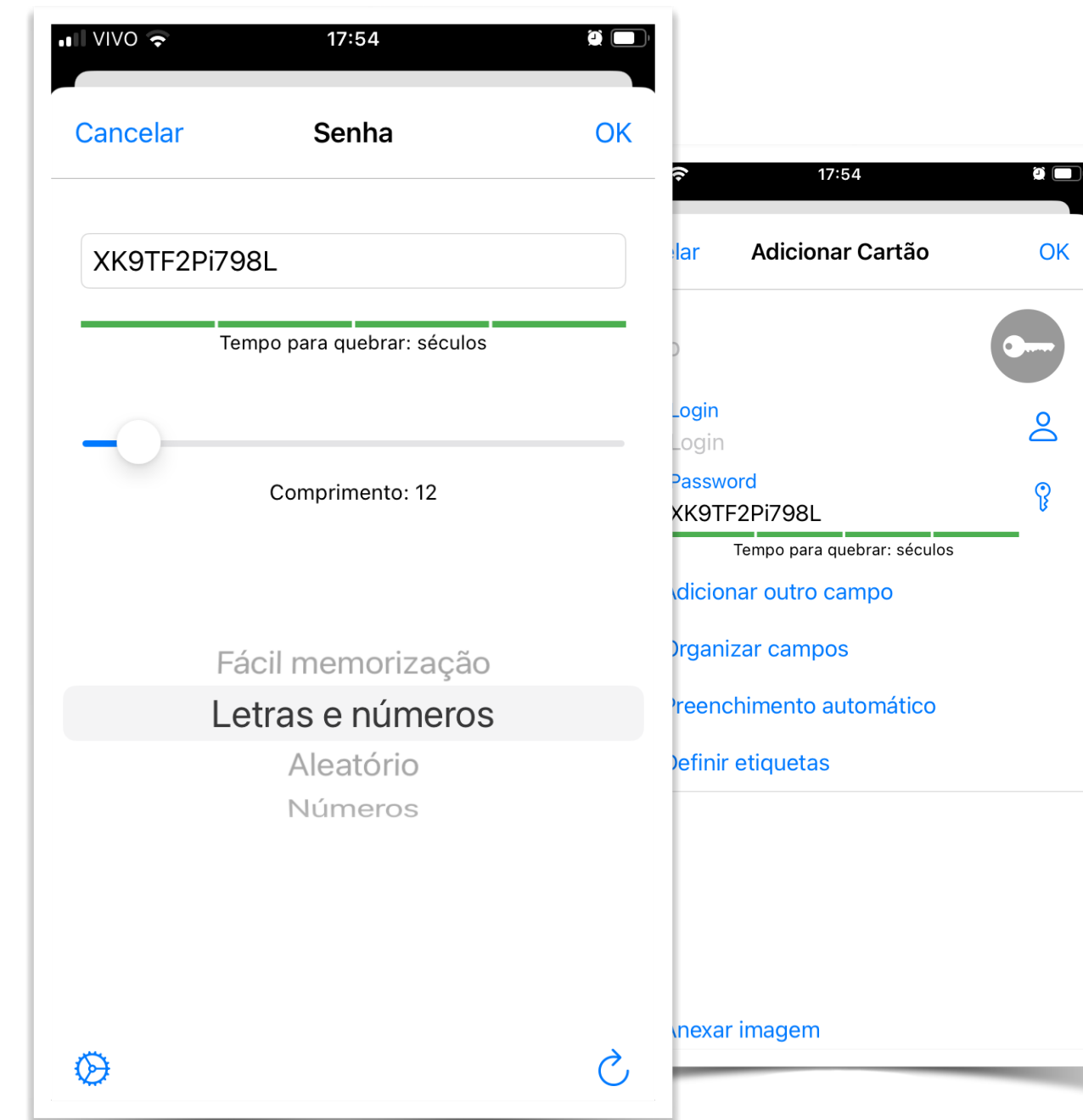
## Fatores de autenticação

- Gerenciadores de senhas

- Amplamente recomendado por especialistas em segurança
- Permitem que o usuário terceirize a tarefa de lembrar senhas
- Auxiliam a criar senhas mais fortes
- Diversas opções disponíveis no mercado
- Adoção continua aquém do esperado [6][7]



Mozilla - gerenciador de senhas - <https://www.mozilla.org/en-US/firefox/features/password-manager/>



SafeInCloud - gerenciador de senhas - <https://www.safe-in-cloud.com/en/index.html>

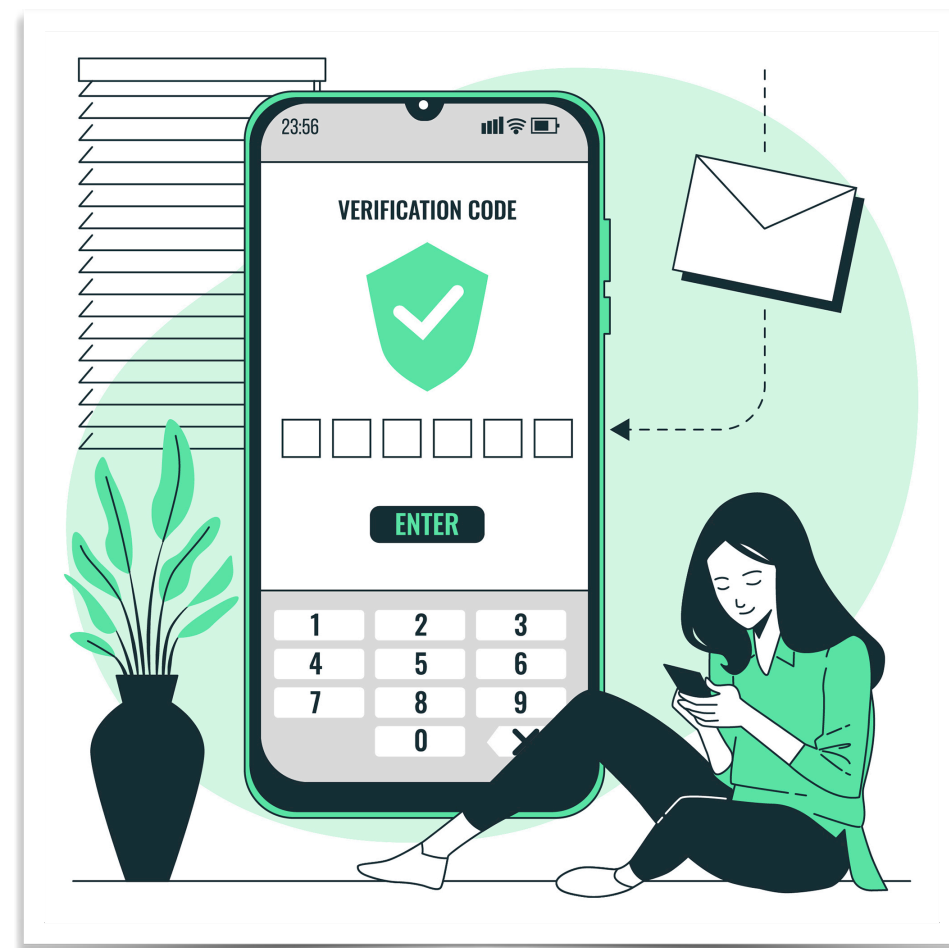
[6] Pearman et al (2019). Why people (don't) use password managers effectively. Disponível em: <https://www.usenix.org/conference/soups2019/presentation/pearman>

[7] Ray et al (2021). Why Older Adults (Don't) Use Password Managers. Disponível em: <https://www.usenix.org/conference/usenixsecurity21/presentation/ray>

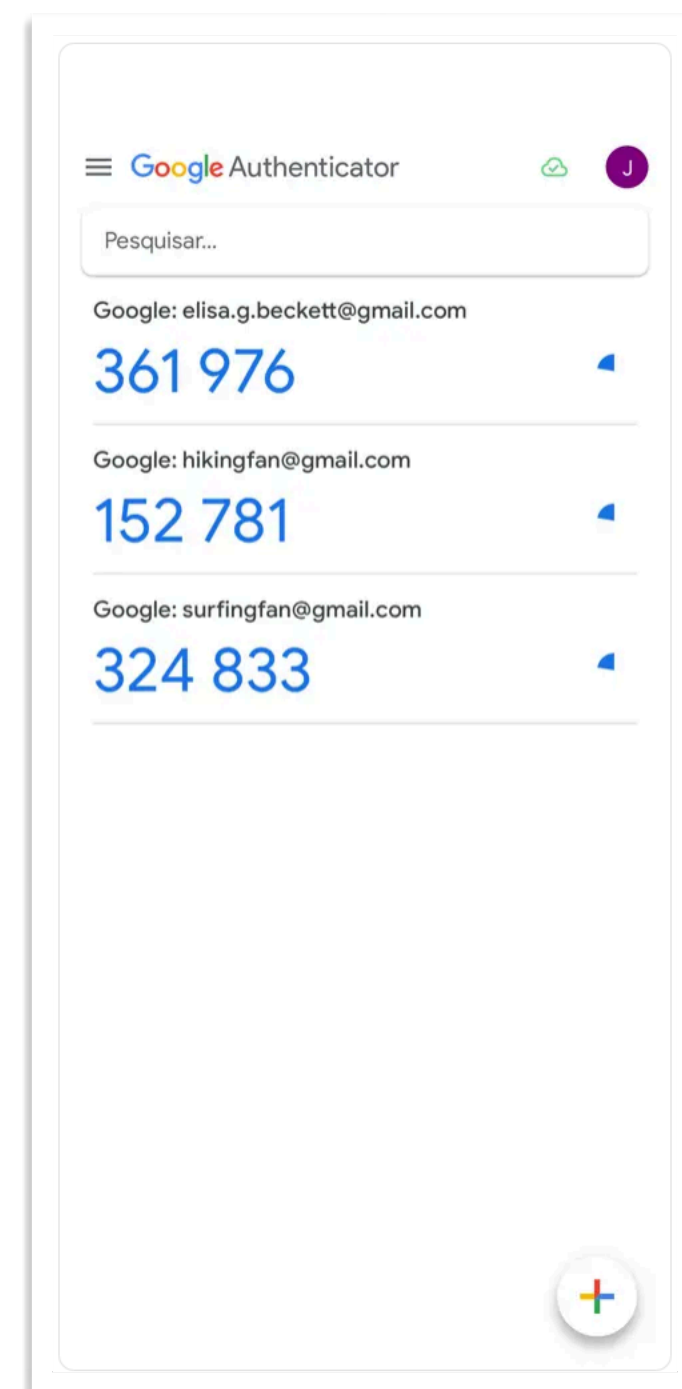
# Autenticação

## Segundo (ou múltiplos) fator(es)

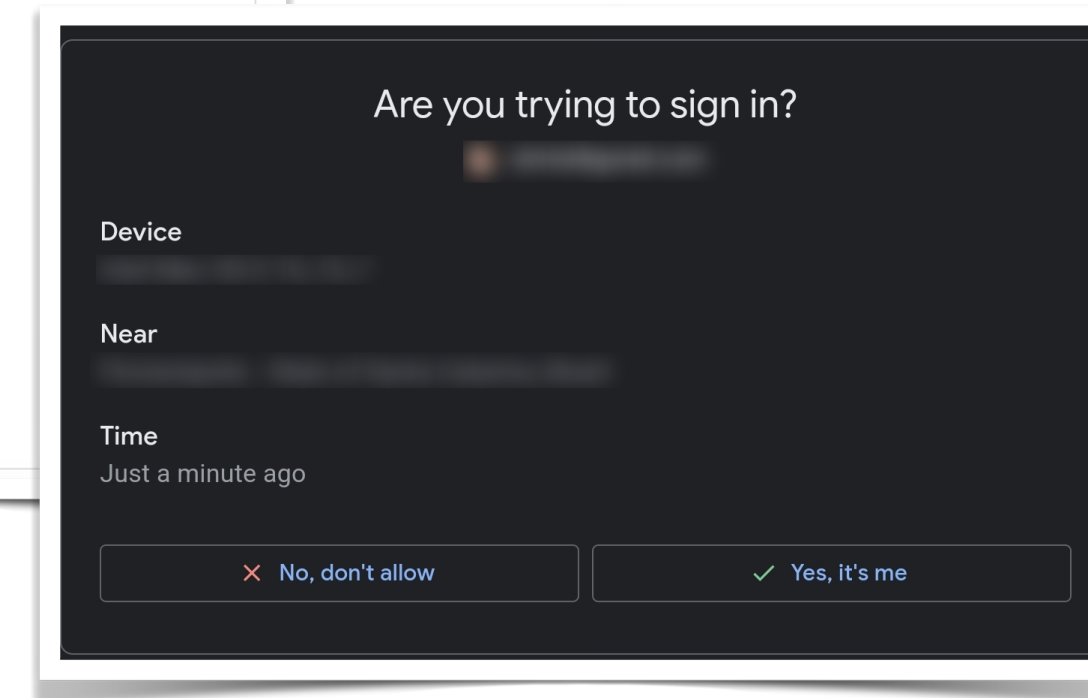
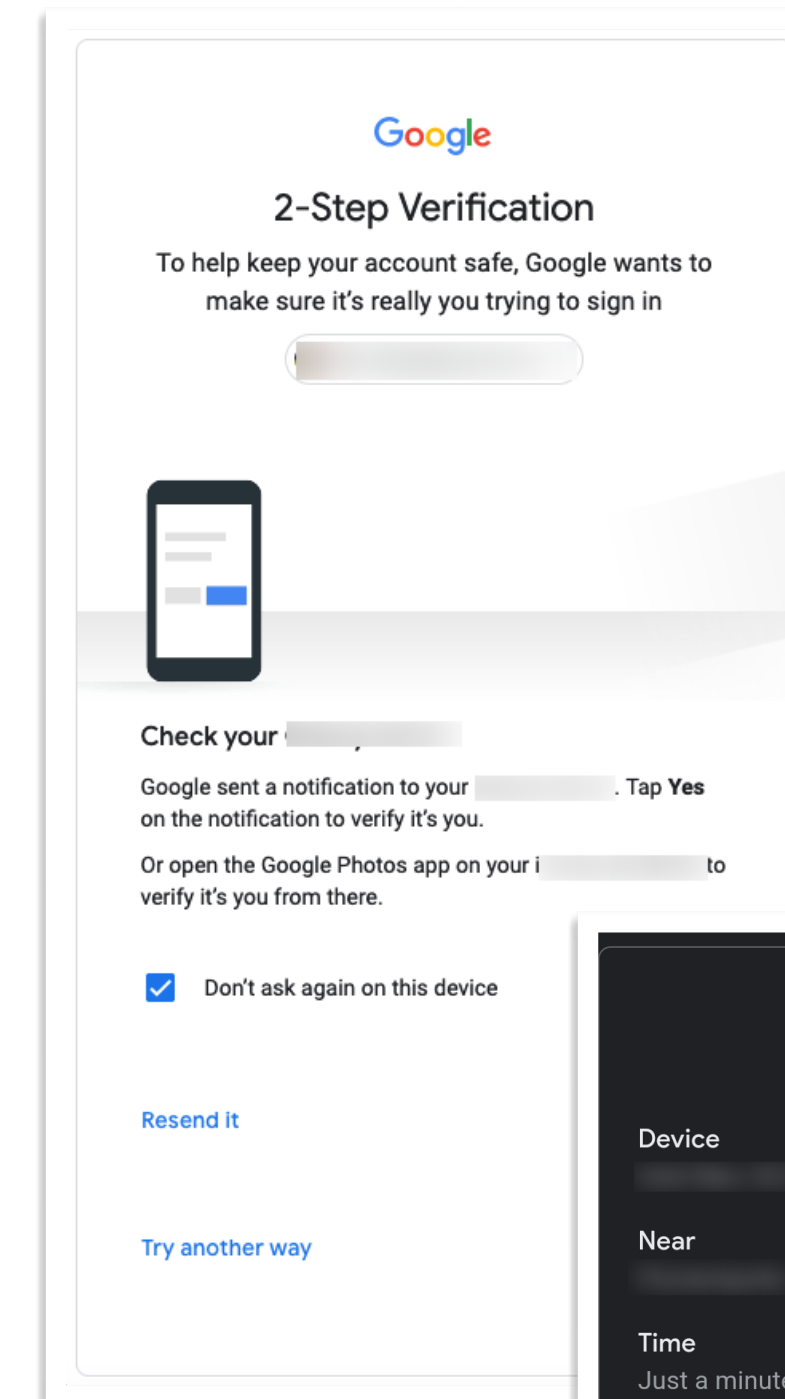
- Solução (ainda) não amplamente adotada
- Bastante esforço de pesquisa, com diversas implementações em uso
- Diversas opções de segundo fator
- Primeiro fator geralmente é usuário e senha



[https://br.freepik.com/vetores-gratis/digite-a-ilustracao-do-conceito-de-otp\\_20602806.htm](https://br.freepik.com/vetores-gratis/digite-a-ilustracao-do-conceito-de-otp_20602806.htm)



<https://apps.apple.com/br/app/google-authenticator/id388497605>



# Dificuldades de adoção de autenticação multi-fator

## •Principais dificuldades [8][9]

- Ainda existe um comprometimento (*tradeoff*) significativo entre funcionalidade e complexidade
  - Passo extra
  - Backup e migração
  - Dependência de dispositivo extra ou opções consideradas inseguras como SMS
- Expectativa de que o usuário faça adesão por conta própria
- Ambiguidade de terminologia
  - Verificação em 2 etapas (*2-step verification*)
  - Autenticação em dois fatores (*two-factor authentication* - 2FA)
  - Autenticação multi-fator (*multi-factor authentication* - MFA)
- ...

[8] Why You Should Ditch SMS as an Auth Factor - <https://www.okta.com/blog/2020/05/why-you-should-ditch-sms-as-an-auth-factor/>

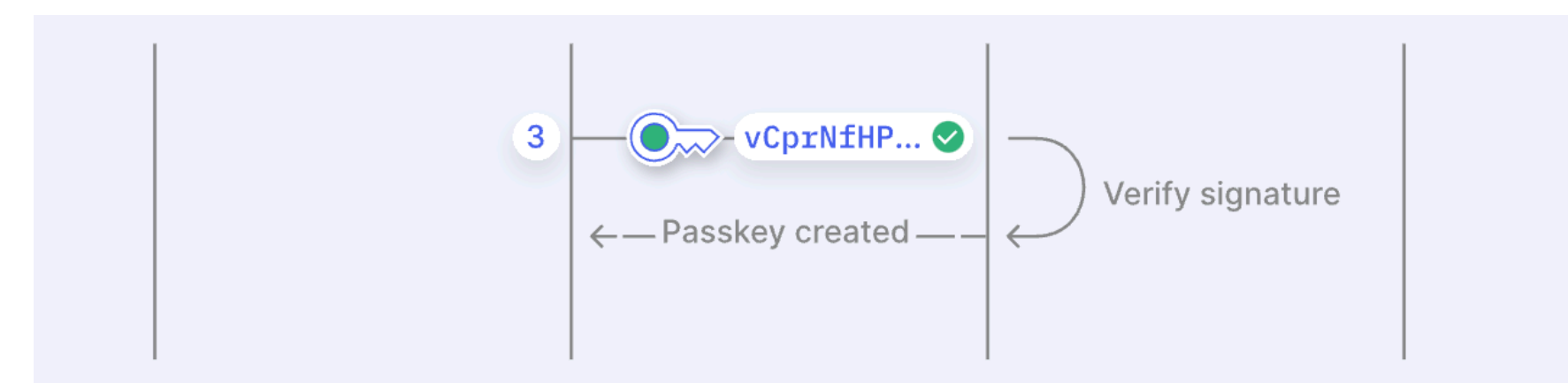
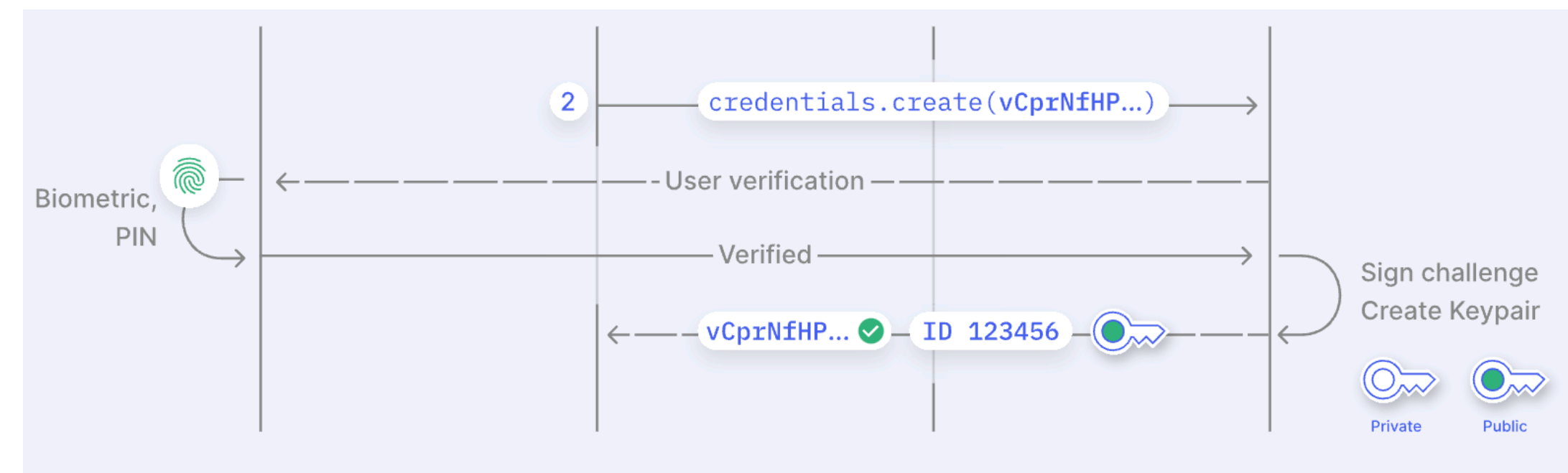
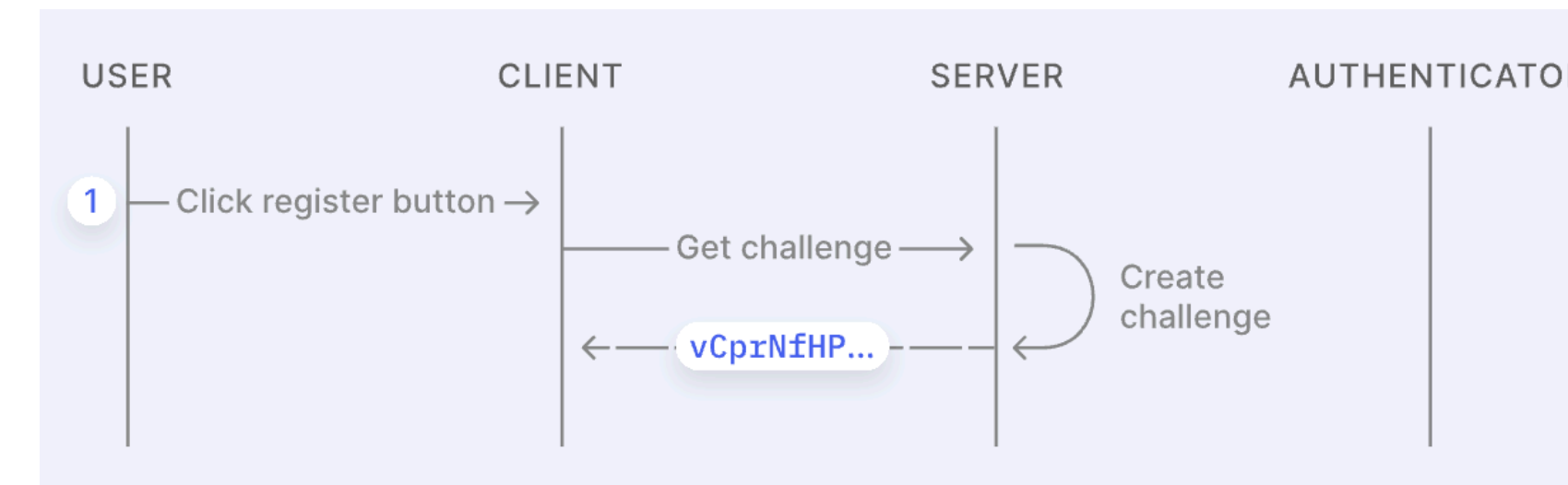
[9] NSA and ESF Report on MFA and SSO Challenges - <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3547453/nsa-and-esf-partners-release-report-on-mfa-and-sso-challenges/>

# Tecnologias Emergentes

# Autenticação

## FIDO passkeys ou chaves de acesso

- Credencial baseada em **par de chaves público-privada**
  - Chave pública é enviada pro serviço
  - Chave privada fica no dispositivo do usuário
- Usa API **WebAuthn** (especificação WebAuthn/FIDO2) disponível nos navegadores [10]
- Pode ser descoberta (**discoverable**) - usuário não precisa digitar um usuário
- Na fase atual, normalmente sincronizável entre **dispositivos da mesma plataforma**



Registro de conta usando passkeys [11]

*Não há segredo compartilhado entre servidor e usuário*

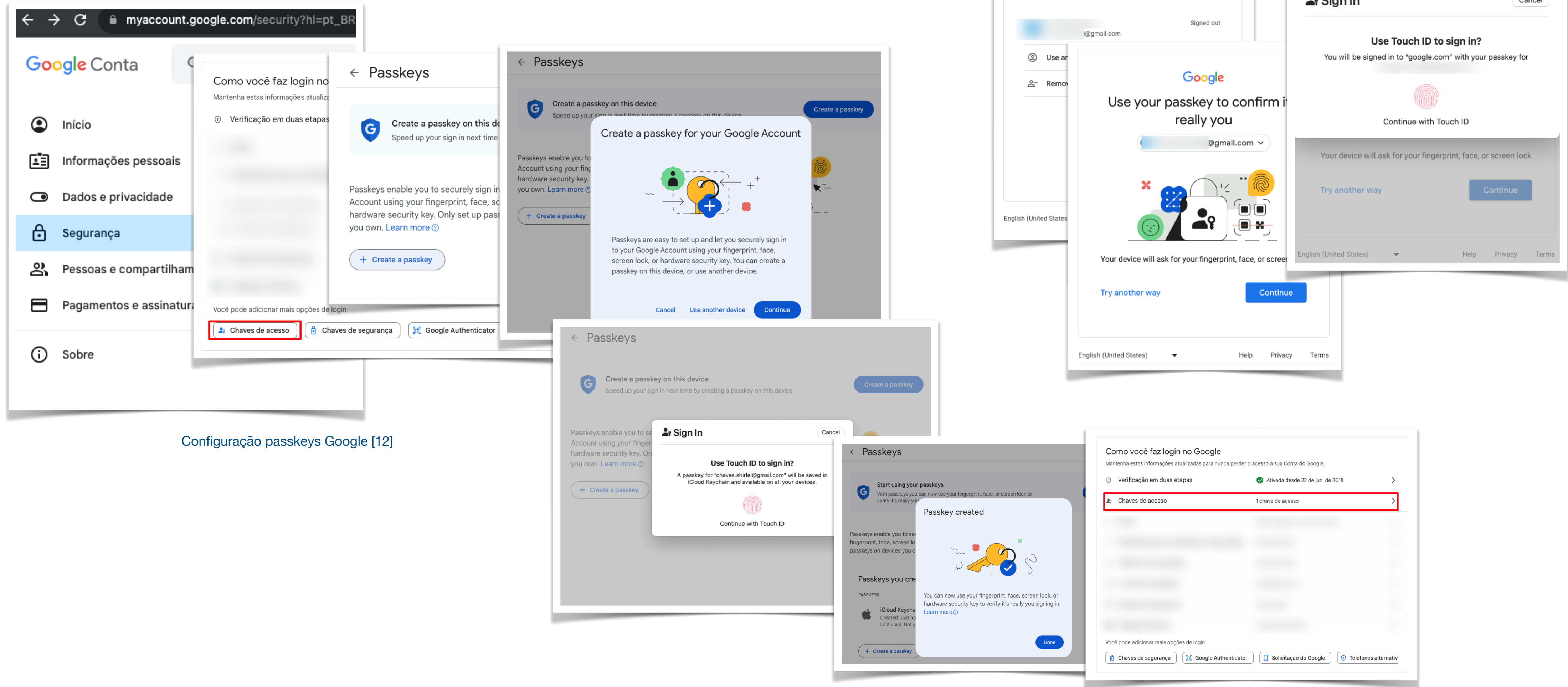
[10] Creating a passkey - <https://www.passkeys.io/technical-details>

[11] WebAuthn - <https://www.w3.org/TR/webauthn-2/>

**Demo**

# Autenticação

## FIDO passkeys ou chaves de acesso



Configuração passkeys Google [12]

# Gerenciamento de Identidade

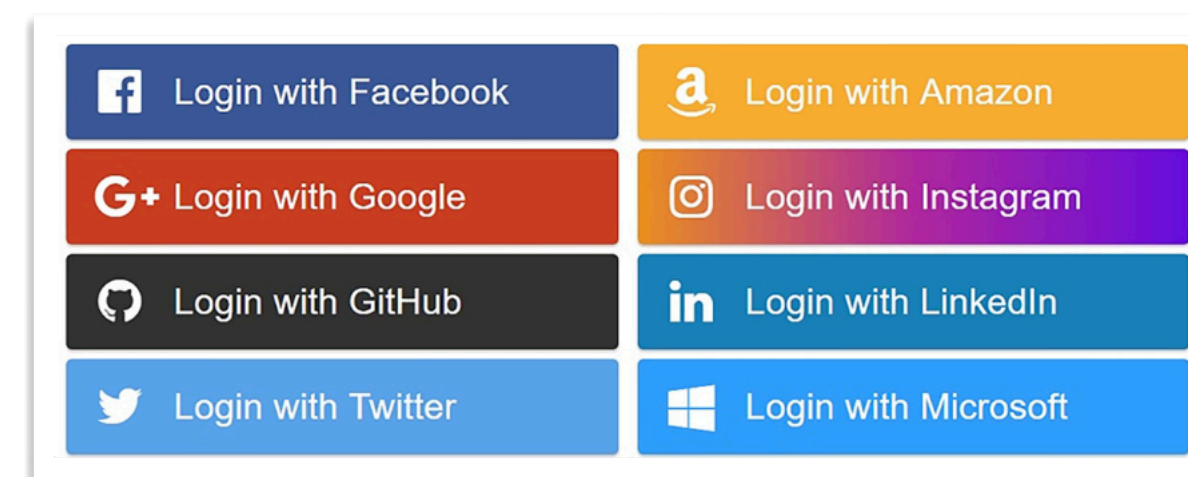
## Identidade descentralizada

- Modelos de gestão de identidade amplamente em uso na atualidade são centralizados em relação ao **controle de dados** da identidade do usuário

### Web 1.0 - Gestão de Identidade Centralizada

A screenshot of a centralized identity management form. It features several input fields: 'Nome Completo \*', 'Data de Nascimento \*' (with a placeholder '00/00/0000'), 'Email \*', 'Senha \*', 'Endereço \*', 'Complemento', and 'Cidade \*'. A 'Cadastrar' button is at the bottom left. A modal window is overlaid on the form, containing 'Usuário' and 'Senha' fields, a 'Conectar' button, and a link 'Esqueci minha senha'. At the bottom of the modal, it says 'Não possui uma conta? Clique aqui para criar'.

### Web 2.0 - Gestão de Identidade Federada / Login Social

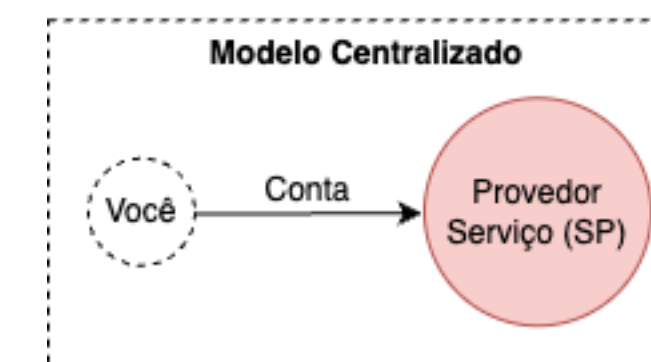


Exemplo de proliferação de login social [10]

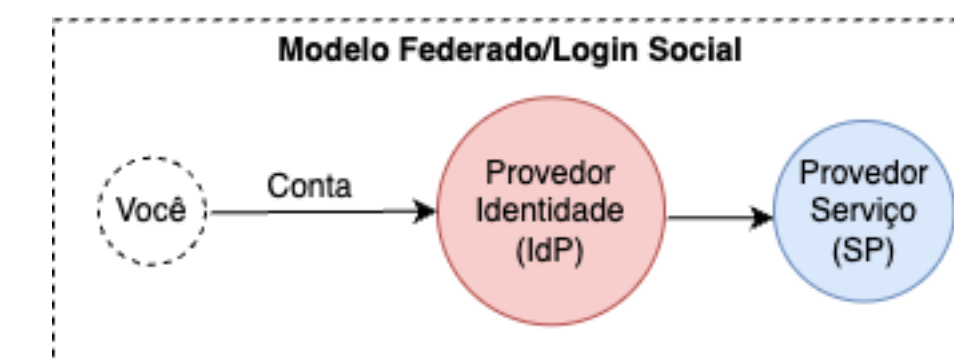
A screenshot of the CAFE login page. It features the CAFE logo (a blue mug with a yellow handle) and the text 'cafe comunidade acadêmica federada'. Below the logo is a dropdown menu labeled 'Selecione uma instituição' and an 'Enviar' button.

Login CAFE

### Controle da Identidade pelo Usuário



Modelo centralizado adaptado de [10]

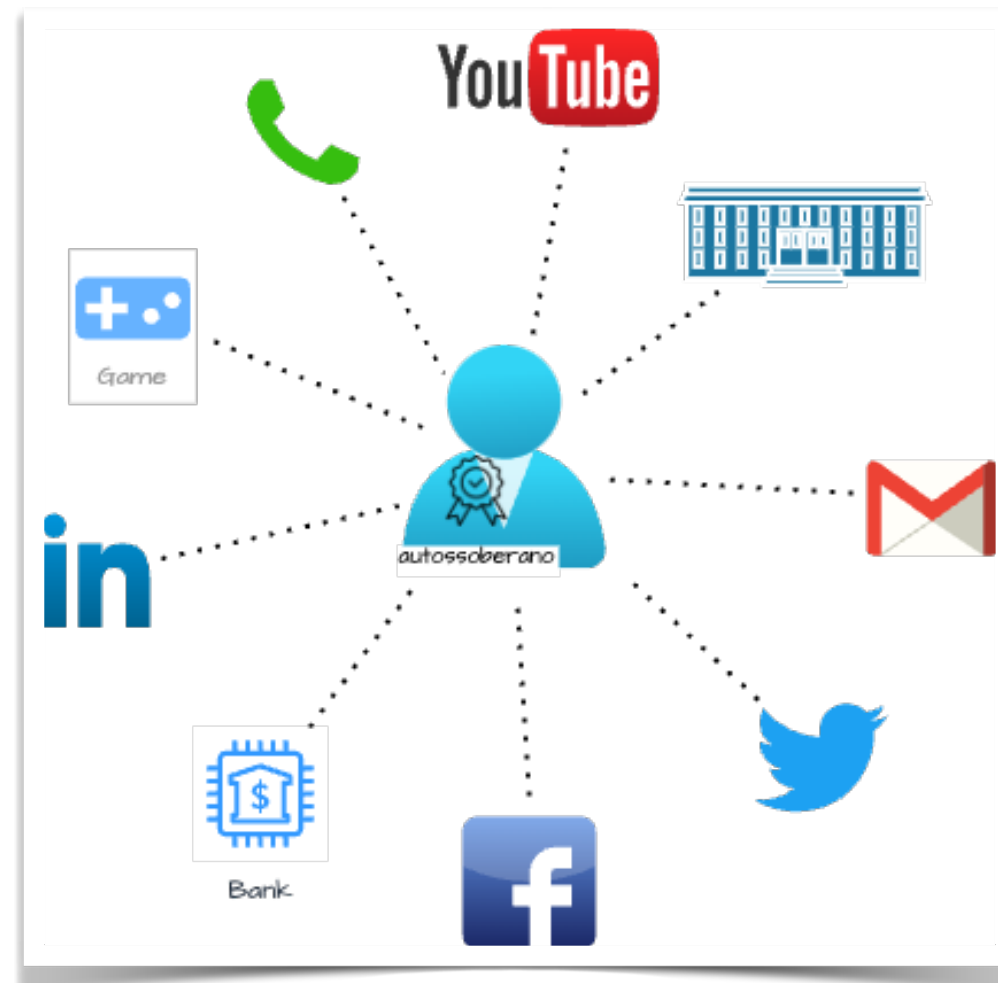


Modelo federado/login social adaptado de [13]

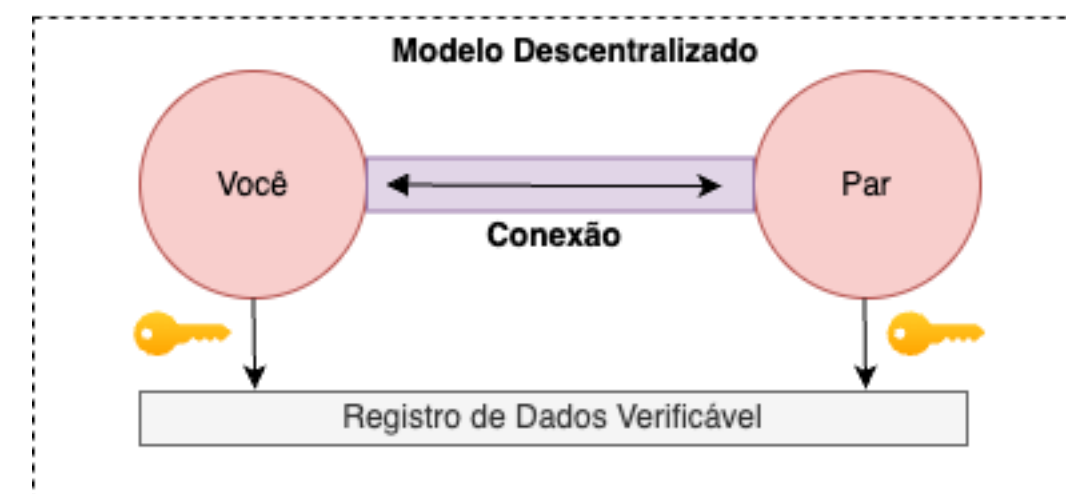


# Identidade descentralizada

- **Centrado no usuário**
  - Paradigma emergente
  - Mudança de controle
  - Sem provedor de identidade (IdP) intermediando
  - Também chamada de identidade autossobrerana (*Self-Sovereign Identity - SSI*)



## Controle da Identidade pelo Usuário



Modelo descentralizado adaptado de [14]


# Identidade descentralizada

## Web 3.0 - Gestão de Identidade Descentralizada

**Connect with BestBC College**


Imagine, as Alice, you are logged into the BestBC College website (see below). They want to offer you a Digital Student Card. Use your BC Wallet to scan the QR code from the website.

Scan the QR Code below with your digital wallet.



**Book a study room**

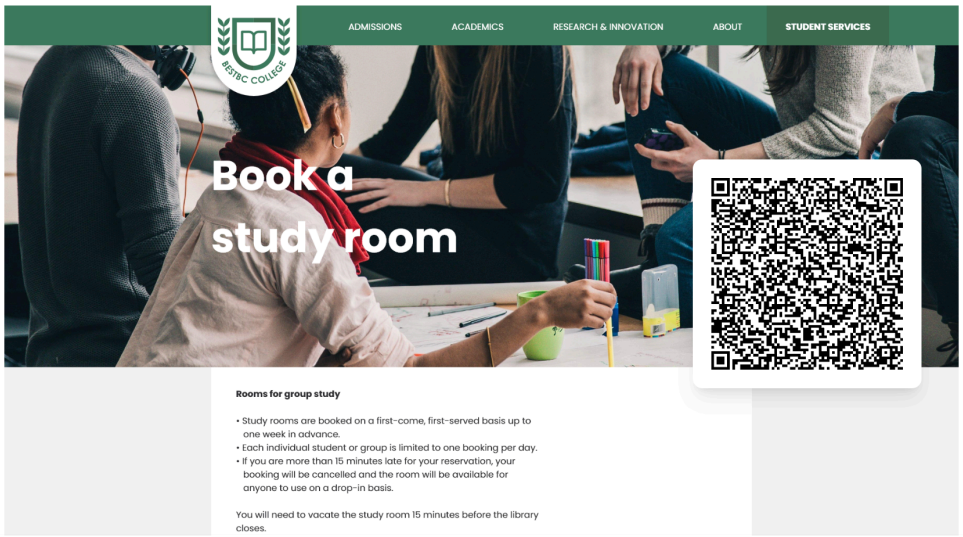
You're connecting with

 Best BC College

**START**

**Start booking the room**

Scan the QR code to continue.



**Rooms for group study**

- Study rooms are booked on a first-come, first-served basis up to one week in advance.
- Each individual student or group is limited to one booking per day.
- If you are more than 15 minutes late for your reservation, your booking will be cancelled and the room will be available for anyone to use on a drop-in basis.

You will need to vacate the study room 15 minutes before the library closes.

Exemplo oferta de credencial verificável de aluno [15]

 **Authentication Required** 

Please provide your Verifiable Credentials



 [Open in a Trusted Digital Wallet](#)

Exemplo autenticação com VC [16]

[15] BC Wallet Showcase - <https://digital.gov.bc.ca/digital-trust/showcase/>

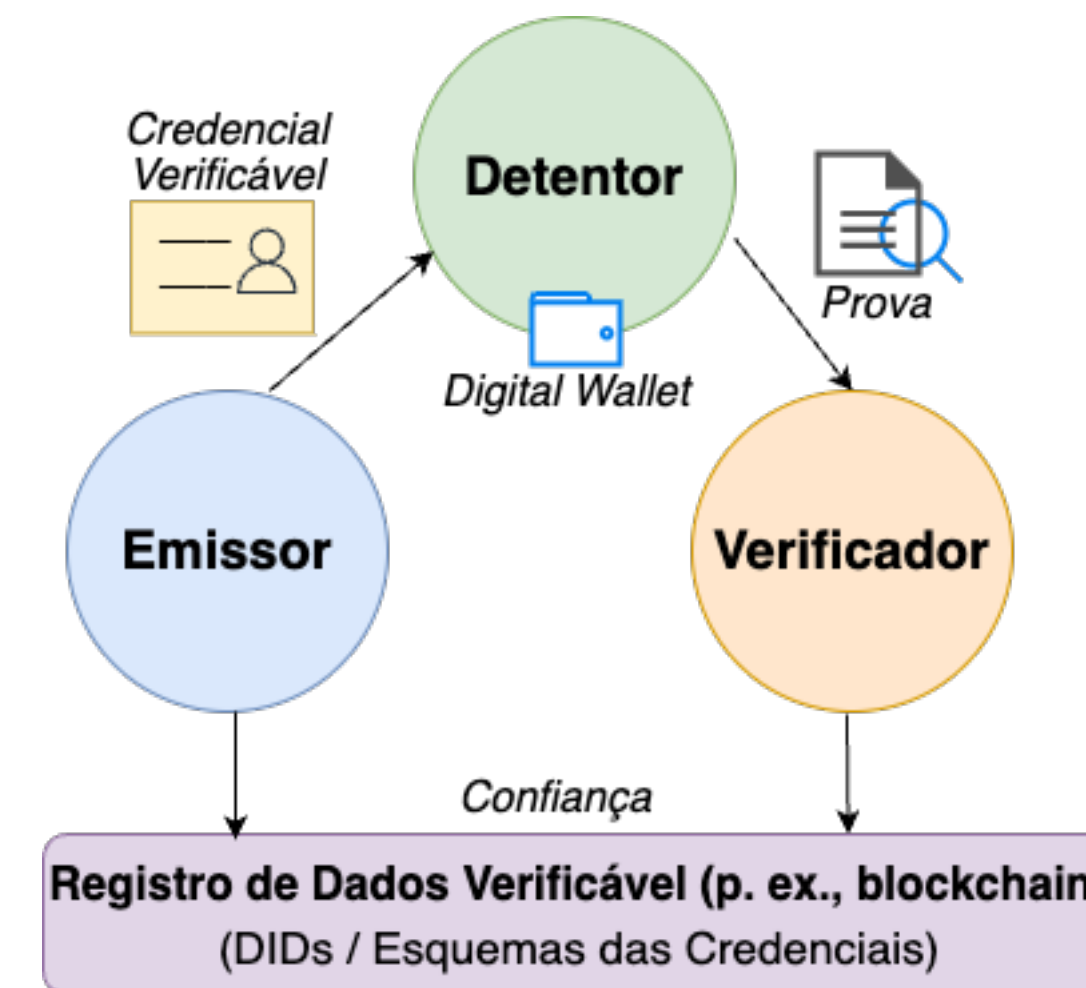
[16] Verified Email Authentication - <https://verified-email-authentication.vonx.io/>

**Demo**

# Identidade descentralizada

- **Pilares:**

- Credenciais Verificáveis (*Verifiable Credentials - VCs*) [17]
- Identificadores descentralizados (*Decentralised Identifiers - DIDs*) [18]



Triângulo de confiança modelo descentralizado, adaptado de [19]

[17] Verifiable Credential Data Model V1.1 - <https://www.w3.org/TR/vc-data-model/>

[18] Decentralised Identifiers (DIDs) V1.0 - <https://www.w3.org/TR/did-core/>

[19] PREUKSCHAT, A.; REED, D. Self-sovereign identity. [S.I.]: Manning Publications, 2021. ISBN 9781617296598.

# Considerações Finais

# Concluindo

## **Chaves de acesso ou *passkeys*:**

- Podem substituir o uso de senhas e serem utilizadas como único fator de autenticação
- Impulsionam a adoção de autenticação forte
- Permite escalabilidade e uso em massa
- ...

## **Identidade descentralizada:**

- Paradigma emergente
- Baseado em especificações/tecnologias que impulsionam uso de criptografia de chave pública
- Alavanca uso de registros distribuídos verificáveis, normalmente implementado com uso de blockchain
- Remove o terceiro confiável no processo de autenticação
- Traz para o usuário responsabilidades como segurança e backup em relação ao gerenciamento de seus dados de identidade
- ...

# Discussão / Dúvidas





[shirlei@gmail.com](mailto:shirlei@gmail.com)

<https://shirlei.me>