Desafios do gerenciamento de identidade digital pelo usuário

Do uso inadequado de senhas à identidade digital descentralizada

Shirlei Chaves - 21/10/2024
Semana Acadêmica da Computação e Sistemas - SECCOM 2024
Universidade Federal de Santa Catarina - UFSC

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]

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

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)

“On the Internet, nobody knows you're a dog.”

[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]

[2] The Laws of Identity - https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

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

(Kim Cameron, 2005)[2]

Serviços online precisam gerenciar a identidade de seus usuários:

- Cada serviço na internet teve que criar sua própria solução para gerenciamento de seus usuários
  - Coleta de informações pessoais diversas para identificação
  - Existência de múltiplos sistemas isolados de identidade.
    - Políticas de segurança e privacidade diversas;
    - Dados da identidade do indivíduo normalmente não são portáveis ou reutilizáveis;
    - Grandes bases de dados centralizadas - atrativos de ataques e alvos de grandes vazamentos de dados.

[2] The Laws of Identity - https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

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.

Fatores de Autenticação

Alguma coisa que você sabe - 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

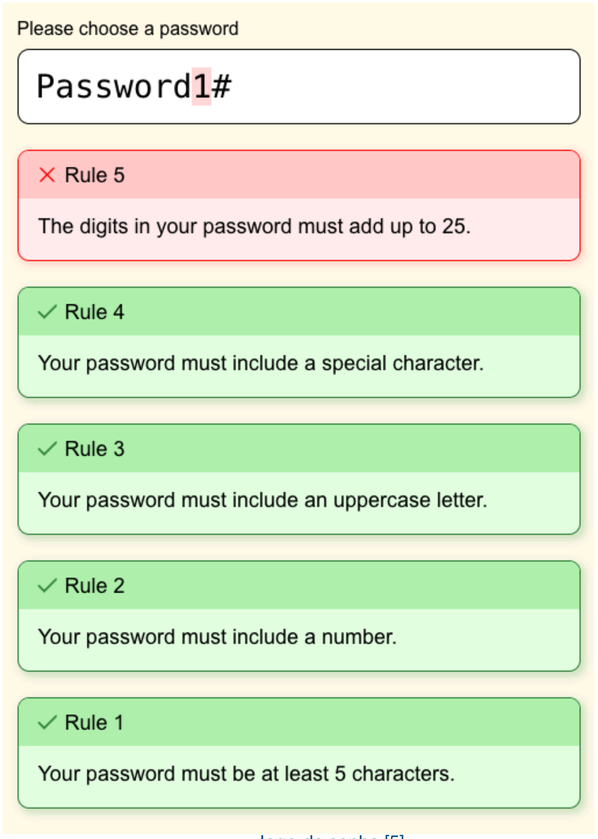
Top 5 senhas mais utilizadas no mundo de 2019 à 2023				
2019	**2020**	**2021**	**2022**	**2023**
12345	123456	123456	password	123456
123456	123456789	123456789	123456	admin
123456789	picture1	12345	123456789	12345678
test1	password	querty	guest	123456789
password	12345678	password	querty	1234

Senhas comuns [4]

No Brasil em 2023: admin, 123456, 12345678, 102030, 123456789

…

Em 11o. lugar: 123mudar



Jogo da senha [5]

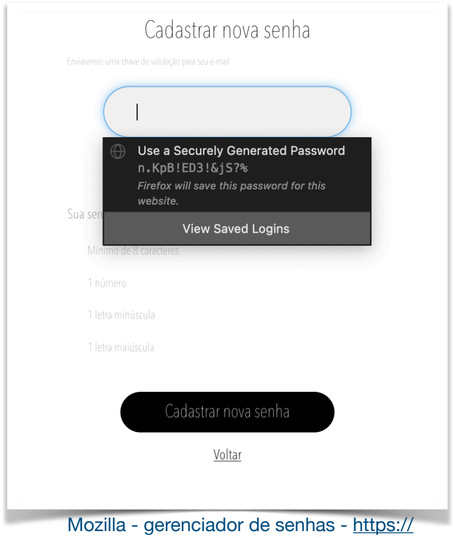
[4] Top 200 most common passwords - Nord Security Research - https://nordpass.com/most-common-passwords-list/

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

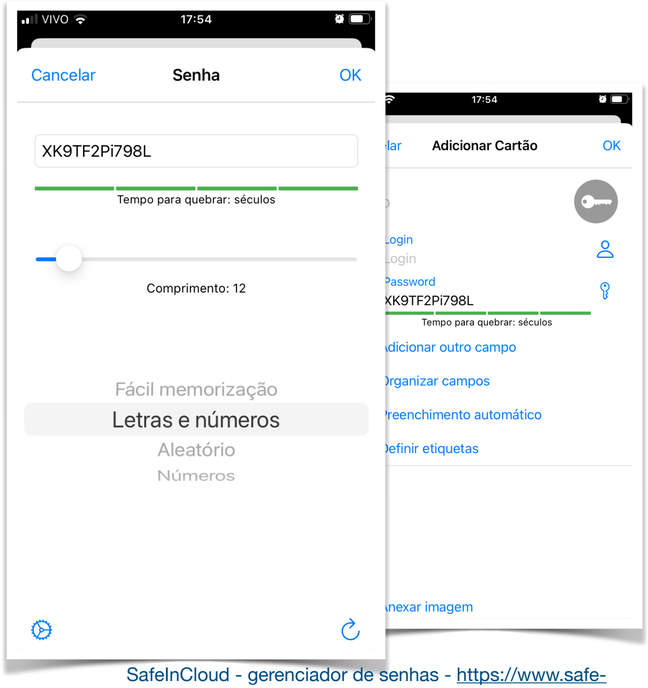
Fatores de Autenticação

Alguma coisa que você sabe - Senha

- **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

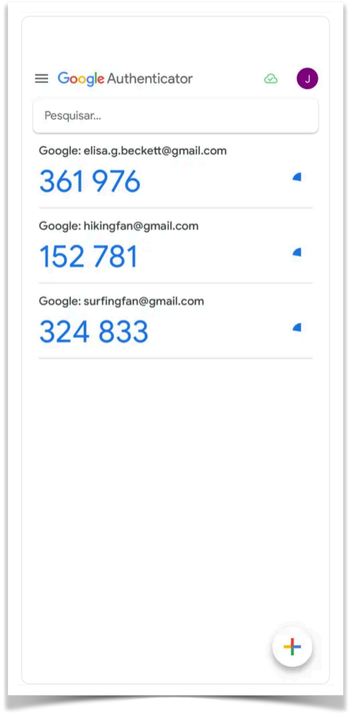
[7] Ray et al (2021). Why Older Adults (Don't) Use Password Managers. Disponível em: https://www.usenix.org/conference/usenixsecurity21/presentation/ray

Fatores de Autenticação

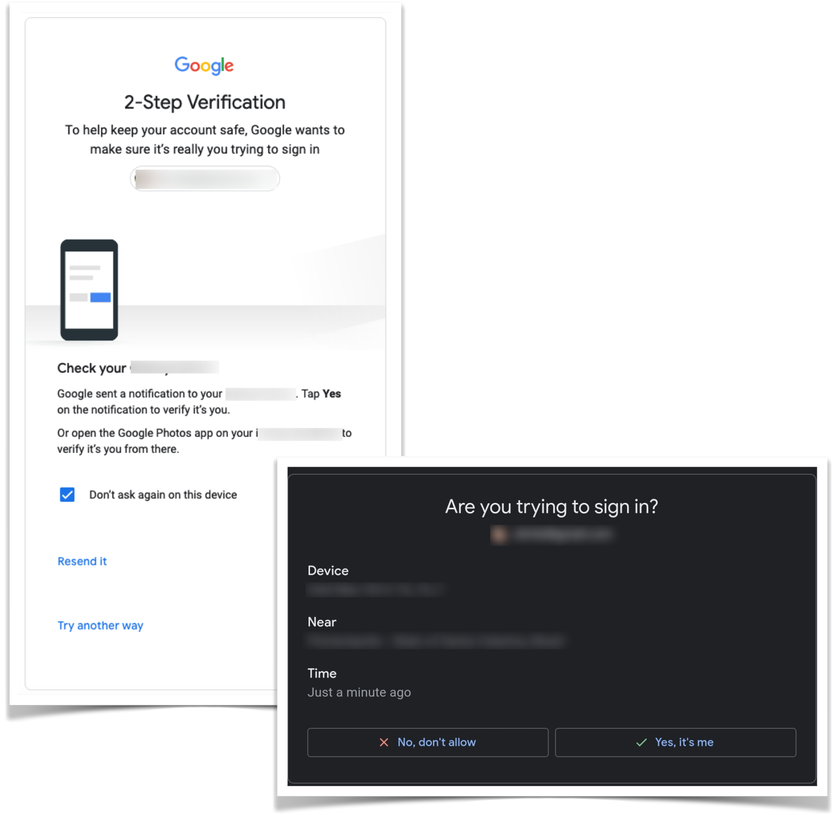
Segundo (ou múltiplos) fator(es)

- 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://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

Passkeys

Autenticação

FIDO *passkeys* ou chaves de acesso

•Credencial baseada em **par de chaves público-privada**

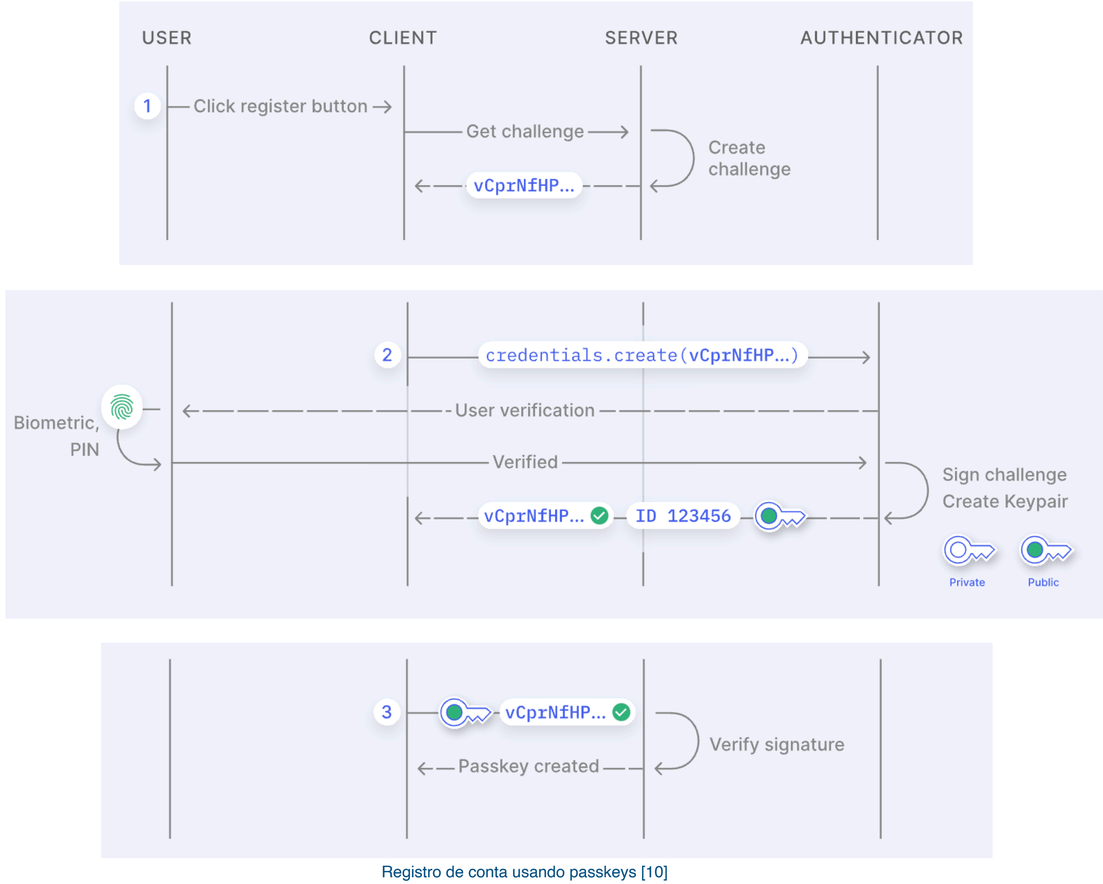
- Chave pública é enviada pro serviço
- Chave privada fica no dispositivo do usuário

• 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**

- Iniciativa da FIDO Alliance em andamento para criar padrões de transferência entre provedores de maneira segura [12]



Registro de conta usando passkeys [10]

Não há segredo compartilhado entre servidor e usuário

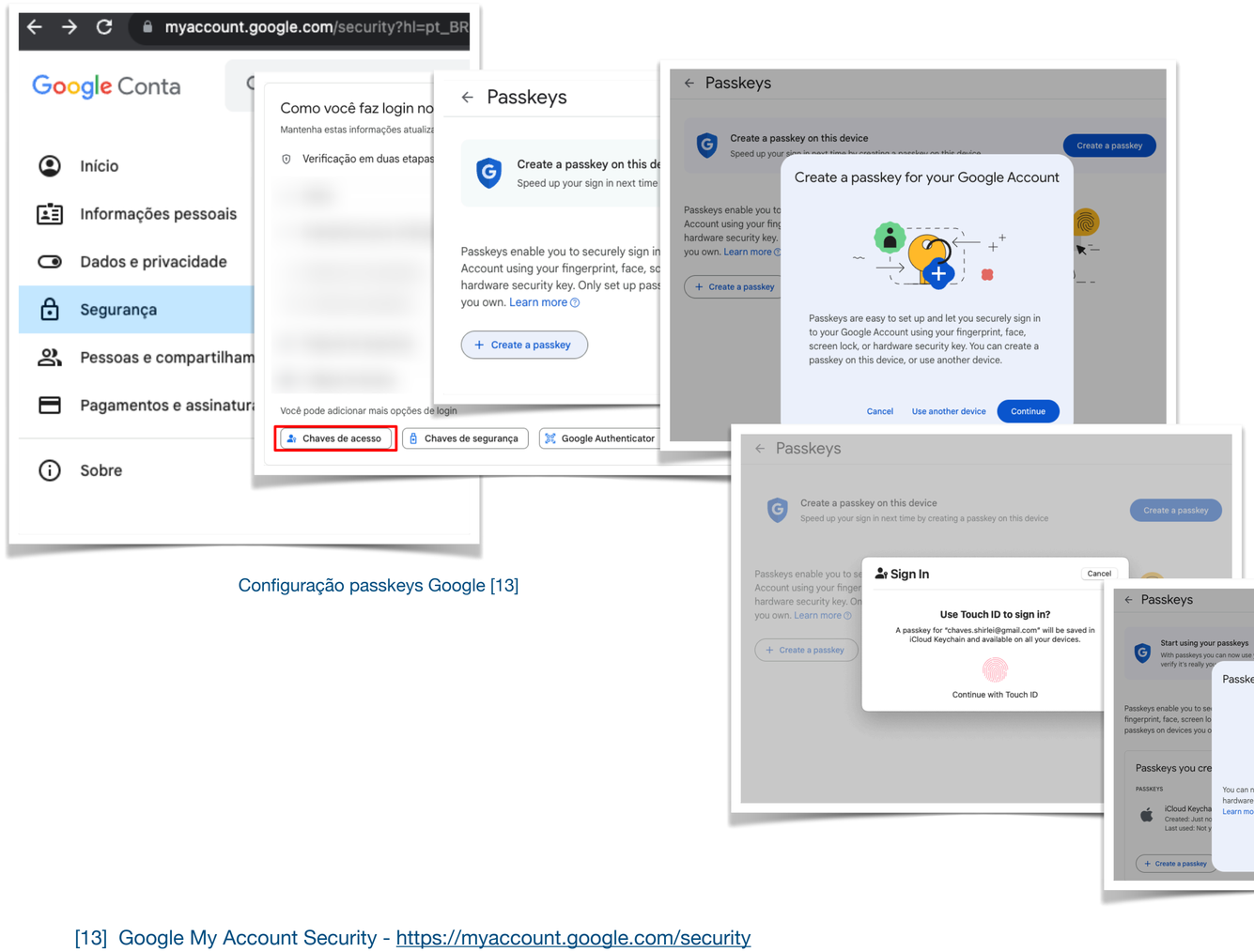
[10] WebAuthn - https://www.w3.org/TR/webauthn-2/

[11] Creating a passkey - https://www.passkeys.io/technical-details

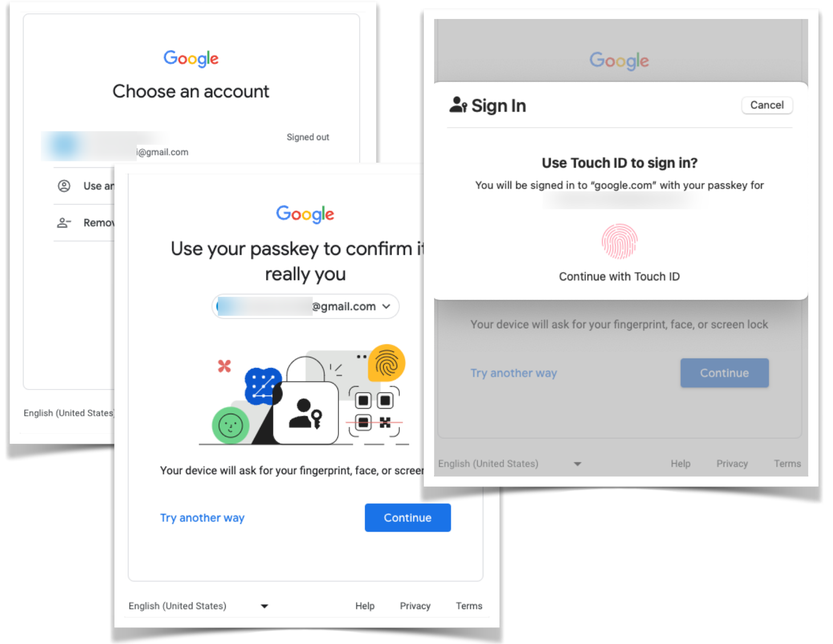
[12] https://fidoalliance.org/fido-alliance-publishes-new-specifications-to-promote-user-choice-and-enhanced-ux-for-passkeys/

Autenticação

FIDO *passkeys* ou chaves de acesso



Configuração passkeys Google [13]



Login Google usando passkeys

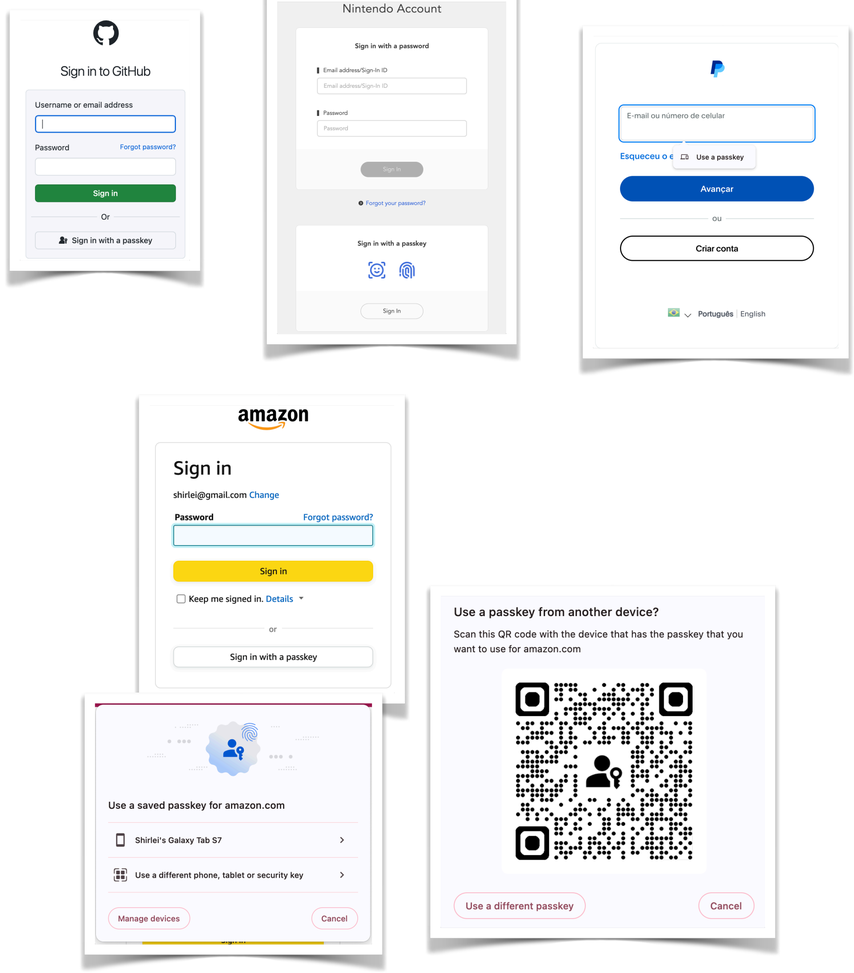
[13] Google My Account Security - https://myaccount.google.com/security

Autenticação

FIDO *passkeys* ou chaves de acesso

Sistema Operacional	Navegador/App	Status	Observações
iOS (16+)	Safari, Chrome, Brave, Edge	✔	
	Firefox	✔	
	Aplicativos iOS	✔	
macOS (13+)	Safari, Chrome, Brave, Edge	✔	Firefox adicionado na versão 122
	Firefox	✔	
	Aplicativos Mac	✔	
Android (9+)	Chrome, Brave, Edge, Firefox	✔	
	Samsung Internet	✔	
	Aplicativos Android	✔	
Windows (10/11)	Chrome, Brave, Edge, Firefox	✔	Suporte adicional na versão 11 23H2
Linux	Chrome, Firefox	⚠	Apenas chaves físicas e QR code são suportados

Passkeys - compatibilidade [14]



[14] Can I use passkeys on my devices? - https://www.passkeys.io/compatible-devices

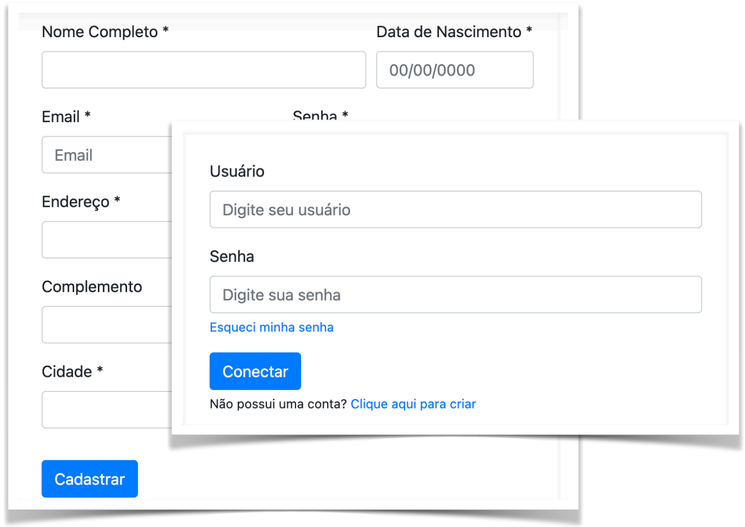
Gerenciamento de Identidade Descentralizado

Gerenciamento de Identidade

Modelos Tradicionais

- 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

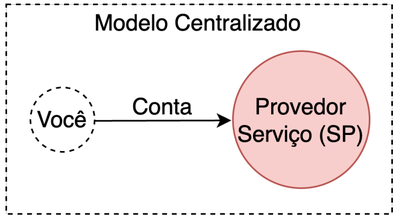


Web 2.0 - Gestão de Identidade Federada / Login Social

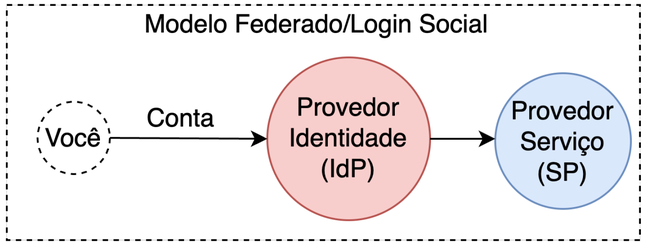
Exemplo de proliferação de login social [10]

Login CAFe

Controle da Identidade pelo Usuário



Modelo centralizado adaptado de [15]



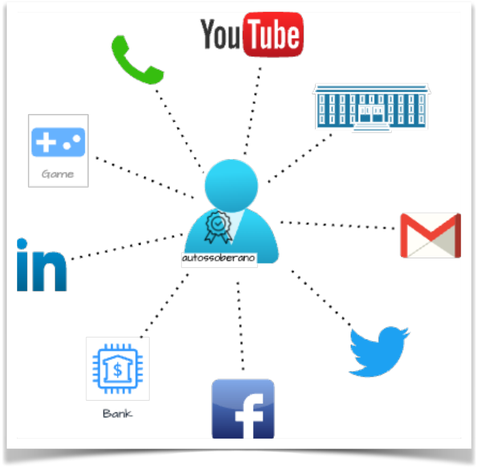
Modelo federado/login social adaptado de [15]

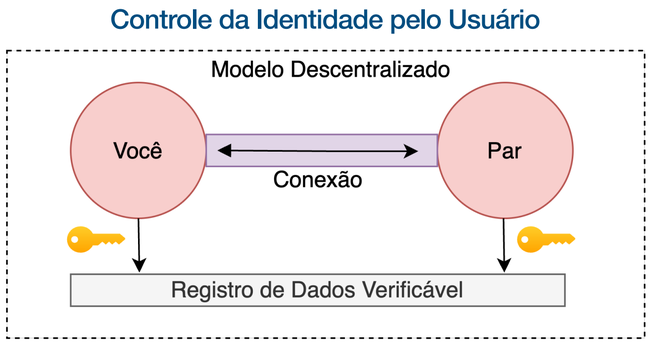
[15] PREUKSCHAT, A.; REED, D. Self-sovereign identity. [S.l.]: Manning Publications, 2021. ISBN 9781617296598.

Gerenciamento de Identidade

Modelo Descentralizado

- **Centrado no usuário**
  - Paradigma emergente
  - Mudança de controle
  - Sem provedor de identidade (IdP) intermediando
  - Também chamada de identidade autossoberana (*Self-Sovereign Identity* - SSI)
  - Baseada fortemente em Credenciais Verificáveis (*Verifiable Credentials* - VCs)



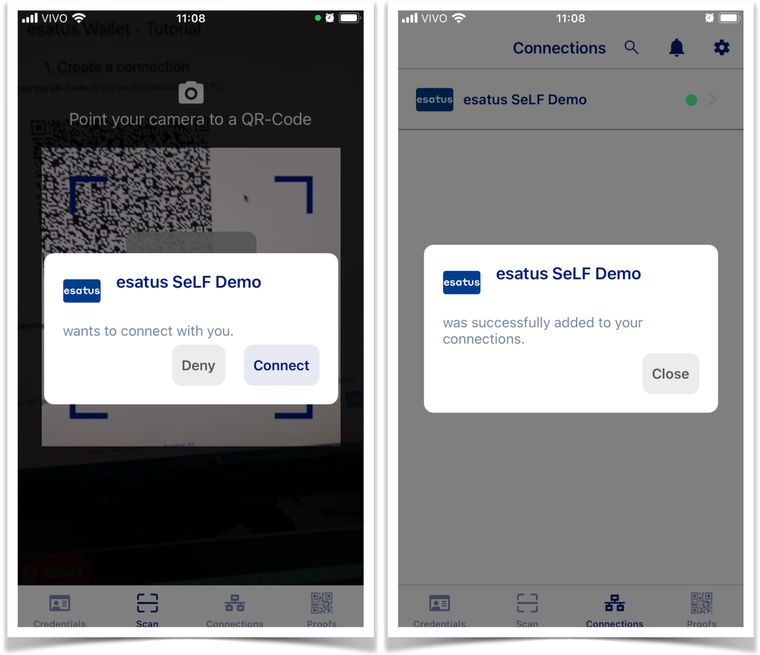


Modelo descentralizado adaptado de [16]

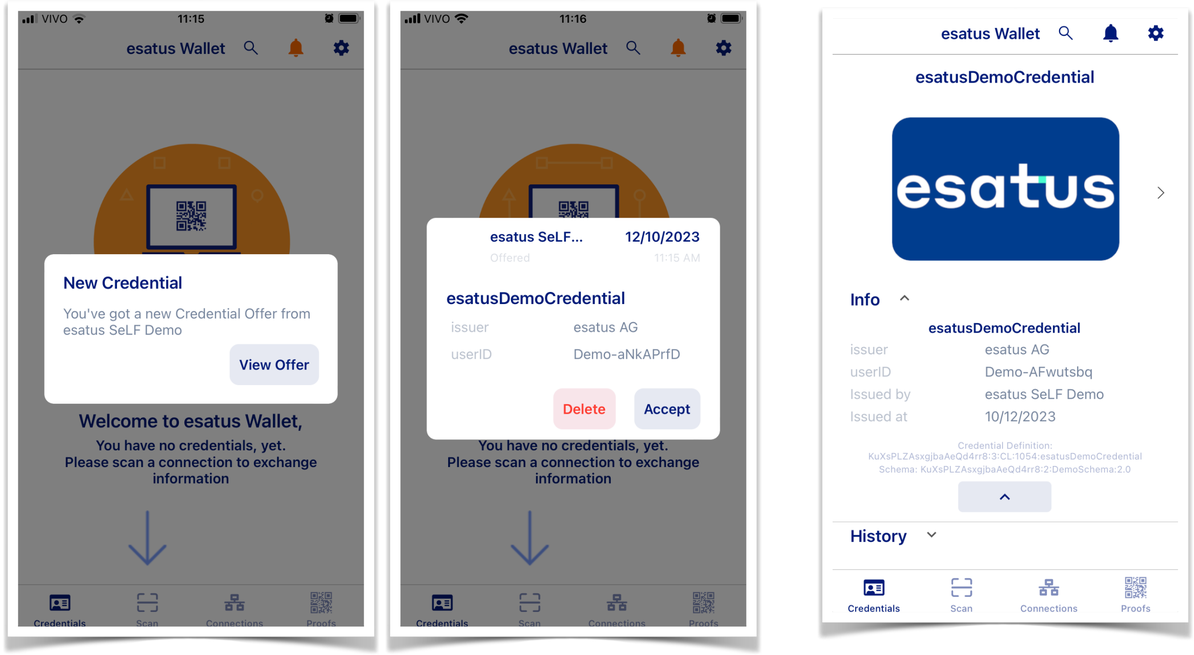
[16] PREUKSCHAT, A.; REED, D. Self-sovereign identity. [S.l.]: Manning Publications, 2021. ISBN 9781617296598.

Identidade descentralizada

Web 3.0 - Gestão de Identidade Descentralizada



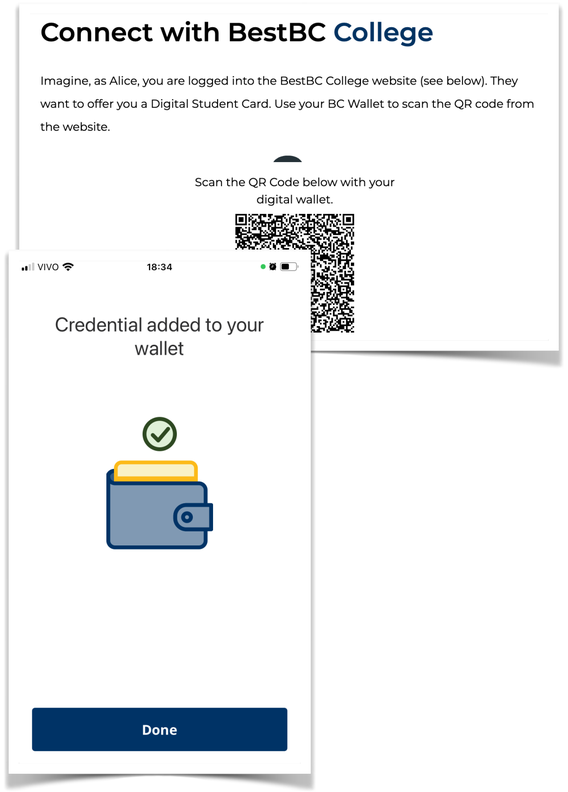
Estabelecendo conexão [17]



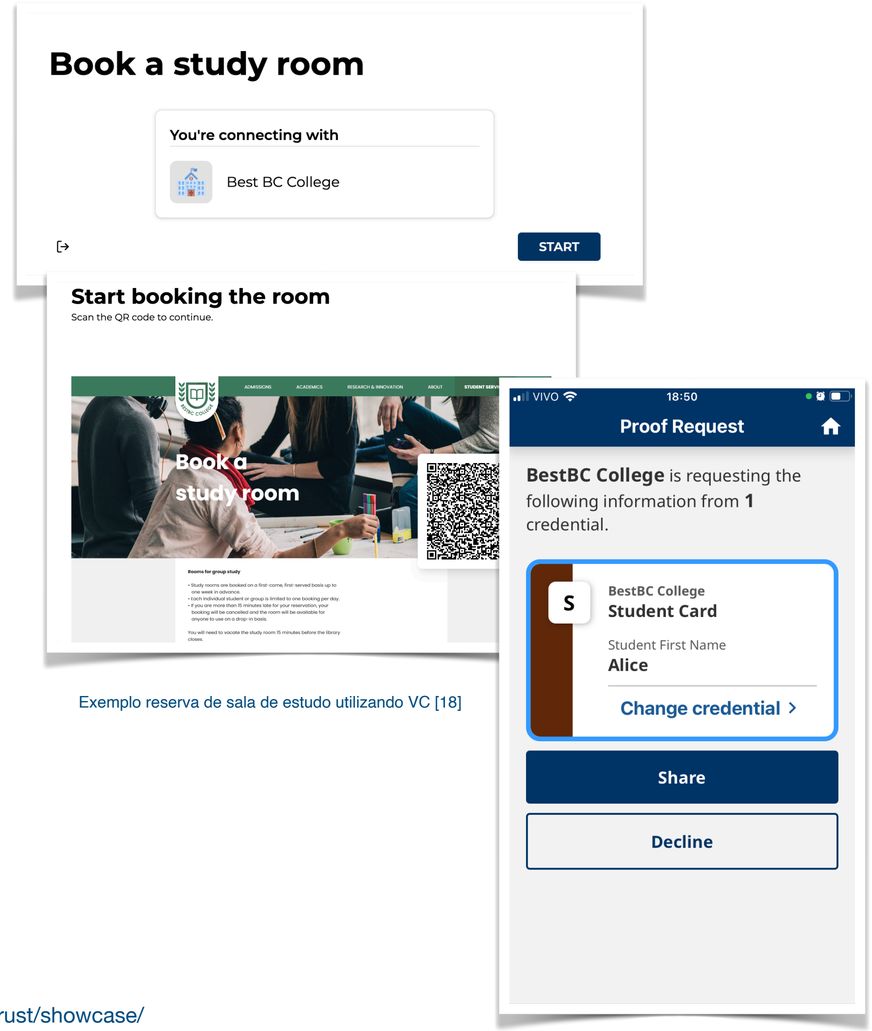
Recebendo credencial e armazenando na carteira [17]

[17] esatus Wallet - Tutorial - https://wallet-demo.esatus.com/

Identidade descentralizada



Exemplo oferta de VC de aluno [18]



Exemplo reserva de sala de estudo utilizando VC [18]

Exemplo autenticação com VC [19]

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

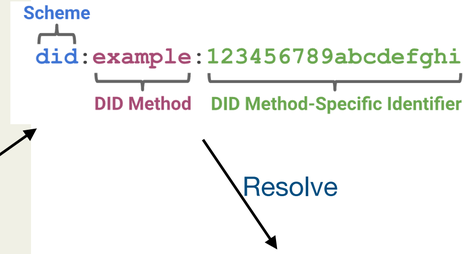
[19] Verified Email Authentication - https://verified-email-authentication.vonx.io/

Identidade descentralizada

- **Pilares:**
  - Credenciais Verificáveis (*Verifiable Credentials* - VCs) [20]
  - Identificadores descentralizados (*Decentralised Identifiers* - DIDs) [21]

Verifiable Credential (with proof)

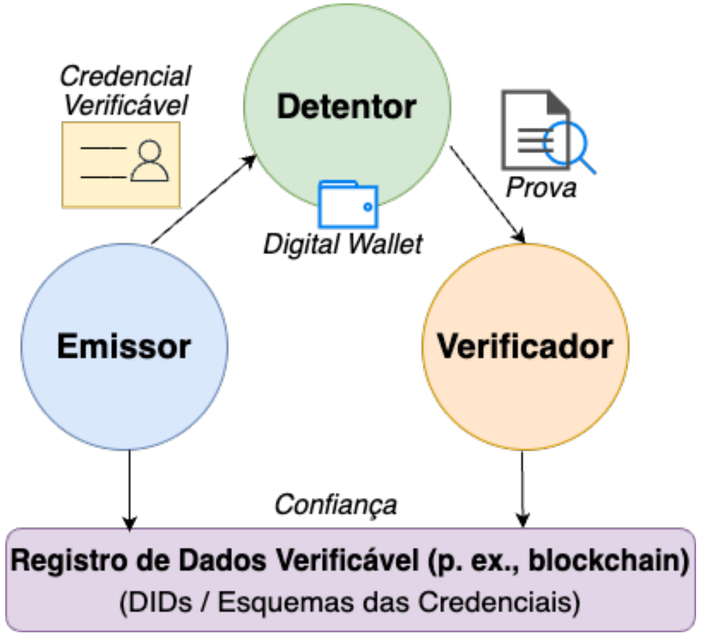

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "http://example.edu/credentials/3732",
  "type": [
    "VerifiableCredential",
    "UniversityDegreeCredential"
  ],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2010-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-02-25T14:58:42Z",
    "verificationMethod": "https://example.edu/issuers/565049#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z3FXQjecWufY46yg5abdVZsXqLhxhueuSoZgNSARiKBk9czhSePTFehP
8c3PGfb6a22gkfUKods5D2UAUL5n2Brbx"
  }
}
```

Resolve

A simple DID document


```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

Triângulo de confiança modelo descentralizado, adaptado de [22]

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

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

[22] PREUKSCHAT, A.; REED, D. Self-sovereign identity. [S.l.]: 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

Imagem de catalyststuf no Freepik

Imagem de storyset no Freepik

shirlei@gmail.com

https://shirlei.me