Autenticação e autorização: antigas demandas, novos desafios e tecnologias emergentes

Emerson Ribeiro de Mello

Minicurso do SBSeg 2022

12 de setembro 2022

XXII
SBSeg
2022
Santa Maria - RS

Autores deste minicurso

- Prof. Emerson Ribeiro de Mello, Dr. (IFSC)
- Shirlei Aparecida de Chaves, doutoranda (IFSC)
- Prof. Carlos Eduardo da Silva, Dr. (Sheffield Hallam University, UK)
- Profa. Michelle Silva Wangham, Dra. (Univali e RNP)
- Prof. Andrey Brito, Dr. (UFCG)
- Prof. Marco Aurélio Amaral Henriques, Dr. (Unicamp)

Licenciamento

Agenda

1. Introdução
2. Demandas, desafios e tecnologias
3. Considerações finais

Introdução

Objetivo geral deste minicurso

Apresentar demandas, desafios e tecnologias que permeiam a gestão de identidade e de acesso

- Definição de modelos de gestão identidade e suas tecnologias
- Usabilidade, privacidade e os novos padrões para aplicações *web*
- Robustez da autenticação de usuários e autenticação dinâmica
- Identidades de software e modelos de confiança zero

Identidade digital

- Representação única de uma entidade usada para identifica-lá em uma transação *online*
- Não necessariamente revela a identidade física de seu detentor
- Deve ser única no contexto de um serviço *online*, porém não deve identificar de forma única uma entidade em diferentes contextos

Prova de identidade e autenticação

- A **autenticação digital** determina que o sujeito controla um ou mais **autenticadores** que estão associados à sua identidade digital
  - Ex: senha, chave privada etc.
- A **prova de identidade** determina que um sujeito é quem ele diz ser, sendo esta uma atividade desafiadora
  - Ocorre de forma remota e por meio de redes abertas
  - Ataques de personificação

Prova de identidade e autenticação

- A **autenticação digital** determina que o sujeito controla um ou mais **autenticadores** que estão associados à sua identidade digital
  - Ex: senha, chave privada etc.
- A **prova de identidade** determina que um sujeito é quem ele diz ser, sendo esta uma atividade desafiadora
  - Ocorre de forma remota e por meio de redes abertas
  - Ataques de personificação

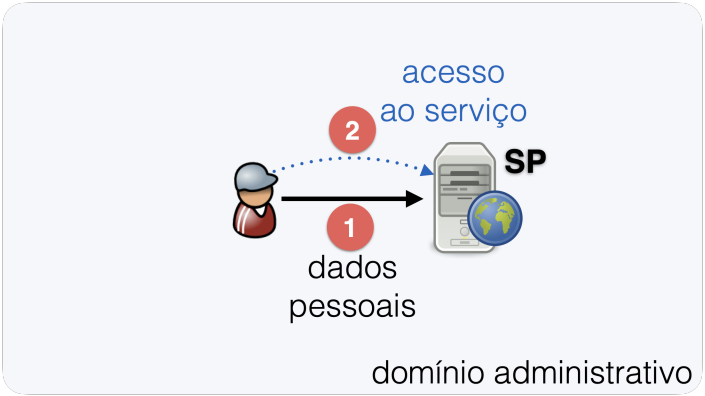
Gestão de identidade e de acesso (*Identity And Access Management* – IAM)

Conjunto de processos e tecnologias que visa garantir a identidade de uma entidade e prover procedimentos de autenticação, autorização e auditoria

- **Relatório anual sobre violação de dados da IBM (2022)**
  - O uso de credenciais roubadas ou comprometidas é o **principal vetor de ataque** (19%)
  - 243 dias para identificar a violação e outros 84 dias para conter a violação
  - Uso de IAM: redução de custos com a violação de dados em 224 mil dólares
  - Uso de MFA: redução de custos com a violação de dados em 187 mil dólares
- **Pesquisa Global de Identidade e Fraude 20211 da Serasa (2021)**
  - 33% dos consumidores disseram estar preocupados com roubo de identidade
  - Os consumidores apontaram os três métodos mais seguros para autenticação:
    - 74% indicaram biometria física em dispositivos móveis
    - 72%indicaram senhas de uso único (One-Time Password – OTP) enviados para dispositivos móveis
    - 66% dos consumidores disseram análise comportamental

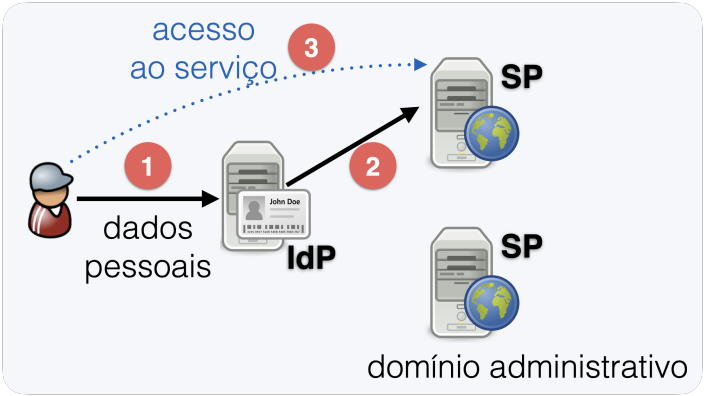
- **Usuário**
  - Entidade que participa de transações *online*
- **Provedor de identidade** (IdP)
  - Emite identidades digitais (conjunto de atributos) para seus usuários
  - Implementa métodos próprios para comprovar que o usuário é detentor de tais atributos
- **Provedor de serviços** (SP)
  - Oferta serviços para usuários autorizados, os quais passaram por um processo de autenticação que baseou-se na identidade fornecida pelo usuário
  - Estabelece relação de confiança com IdPs

Modelo baseado em silo ou tradicional



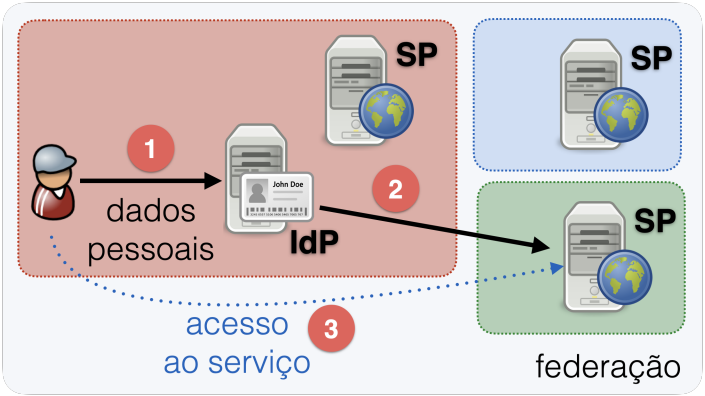
- Cada SP possui base própria de usuários
- Usuário possui uma conta por SP

Modelo centralizado



- Usuário possui uma única conta, cujos dados podem ser compartilhados por todos SPs do domínio
- *Central Authentication Service* (CAS) protocol pode ser usado para implementar este modelo

Modelo federado



- Usuário possui uma única conta, cujos dados podem ser compartilhados por todos SPs da federação
- IdP sempre intermedeia a interação entre usuário e SP
- Framework Shibboleth e protocolo SAML podem ser usados para implementar este modelo

Modelo federado

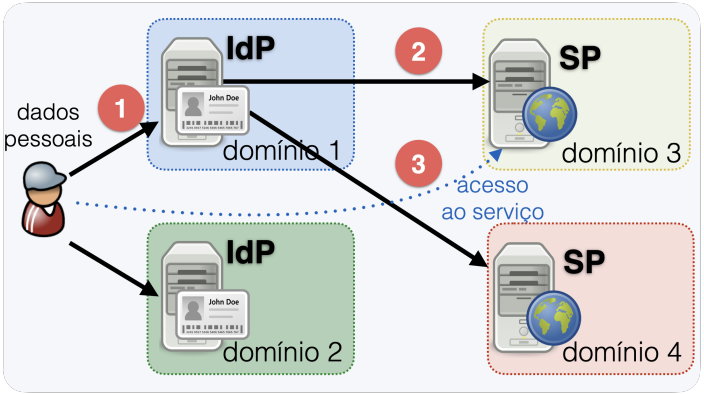
o possui uma única
cujos dados podem ser
rtilhados por todos SPs
eração

mpre intermedeia a
ção entre usuário e SP

work Shibboleth e
olo SAML podem ser
s para implementar este
o

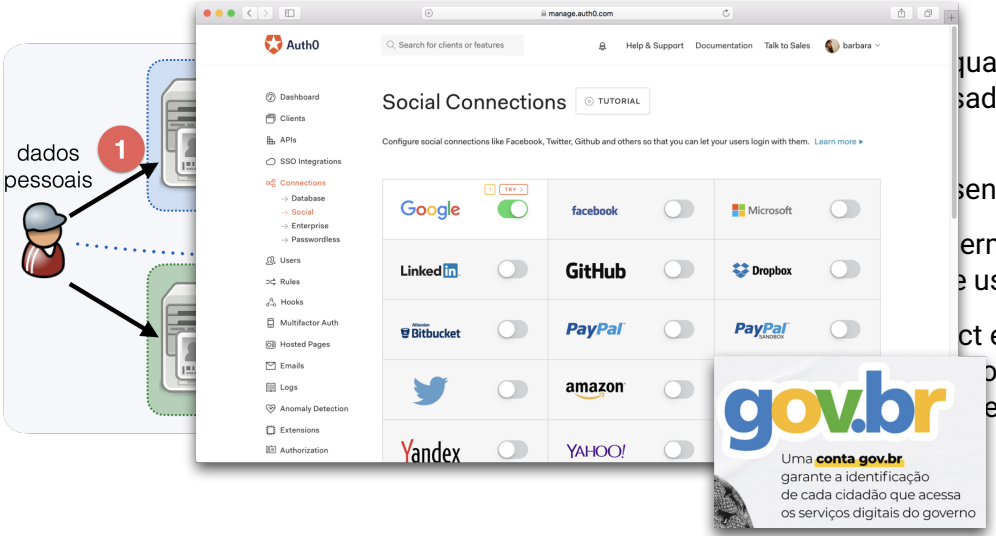
Fonte: Escola Superior de Redes – RNP

Modelo centrado no usuário



- SP escolhem quais IdPs poderão ser usados pelos usuários
- Termo de consentimento
- IdP sempre intermedeia a interação entre usuário e SP
- OpenID Connect e OAuth2 podem ser usados para implementar este modelo

Modelo centrado no usuário



quais IdPs
sados pelos

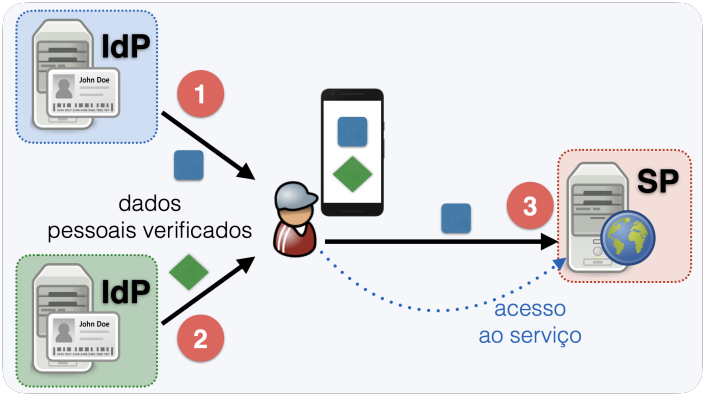
sentimento

ermedeia a
e usuário e SP

ct e OAuth2
os para
e modelo

Fonte: Adaptado de Auth0 e gov.br

Modelo descentralizado



- O usuário está no centro e o IdP não intermedeia a interação com SPs
- O usuário fica responsável por manter suas identidades (carteira digital)
- Atributos são atestados criptograficamente
- DID, VC e DLT podem ser usados para implementar este modelo

Modelos de gestão de identidade

- **Silo, centralizado, federado e centrado no usuário**
  - Relação de poder de forma que o usuário é a parte menos favorecida
  - Os dados pessoais do usuário não estão sob seu controle
  - O usuário não é de fato dono de sua identidade digital
- **Descentralizado**
  - Entidades que emitem as identidades não as controlam
  - O usuário (detentor) está no controle de sua identidade digital
  - Confiança é estabelecida entre emissores (IdPs) e verificadores (SPs)

- **Silo, centralizado, federado e centrado no usuário**
  - Relação de
  - Os dados p
  - O usuário n
- **Descentralizad**
  - Entidades c
  - O usuário (
  - Confiança é


The New York Times 21/08/2022

A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.

Google has an automated tool to detect abusive images of children. But the system can get it wrong, and the consequences are serious.

da

Ps)

1

[1] https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html

The New York Times 21/08/2022

A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.

Google has an automated tool to detect abusive images of children. But the system can get it wrong, and the consequences are serious.

- Perdeu acesso aos emails, contatos, documentos e fotos
- Perdeu sua conta Google Fi (seu número de telefone celular)
- Sem celular e sem email, não pode ter acesso as senhas de uso único (OTP) necessárias para acessar suas contas em outros provedores de serviço

Motivação

- Identificadores amplamente usados pelas pessoas na Internet não estão de fato sob seu controle
  - Controlador pode excluí-lo de acordo com sua política
- Alguns identificadores podem revelar mais informações do que o necessário para interação com o serviço (e.g. CPF, número do telefone)

Motivação

- Identificadores … estão de fato sob seu controle
  - Controlador
- Alguns identific… necessário para interação com

Motivação

- Identificadores amplamente usados pelas pessoas na Internet não estão de fato sob seu controle
  - Controlador pode excluí-lo de acordo com sua política
- Alguns identificadores podem revelar mais informações do que o necessário para interação com o serviço (e.g. CPF, número do telefone)

Endereço de email pode ser considerado como um identificador único global, porém não foi criado para ser identificador e não está sob o controle de seu detentor

DID

Identificador único global que possibilita uma identidade digital descentralizada e criptograficamente verificável

- Para identificar qualquer tipo de entidade (pessoa, serviço, etc.)
- Desacoplado de registros centralizados, IdPs e autoridades certificadoras
- Não há necessidade em ter organização mantenedora para que continue a existir
- Permite recuperar metadados associados (chamados de documentos DID)

Identificadores descentralizados

DID consiste de uma URI segmentada em três partes

Fonte: Adaptado de W3C

1. **Identificador do esquema**
   - Sempre será `did`
2. **Identificador do método DID**
   - Determinado pela especificação própria de cada método DID
3. **Identificador determinado pelo método DID**
   - Determinado pela especificação própria de cada método DID

Método DID	Registro	Contato
`bnb`	Binance Smart Chain	Ontology Foundation
`btcr`	Bitcoin	Christopher Allen
`dns`	Domain Name System	Danube Tech
`dual`	Ethereum	Smart ID Card Alliance
`hpass`	Hyperledger Fabric	IBM
`iota`	IOTA	IOTA Foundation
`jolo`	Ethereum	Jolocom
`web`	Web	Oliver Terbu

- Existem mais de 130 métodos DID sendo propostos

Método para ser usado em conjunto com DIDs baseados em *blockchain* de forma a permitir usar a reputação de domínios *web* como âncora de confiança para esses DIDs

- **Identificador do método** – `web`
- **Identificador determinado pelo método DID**
  - FQDN presente no CN de um certificado X.509 (TLS) para o domínio
  - Subdiretórios são opcionais e delimitados por `:` no lugar de `/`
  - Portas são opcionais e devem ser codificadas no formato URL (codificação com %)

```
did:web:w3c.github.io
did:web:w3c.github.io:user:alice
did:web:example.com%3A3000
```

- **Registro**
- **Resolução**
- **Atualização**
- **Revogação**

- **Registro**
- **Resolução**
- **Atualização**
- **Revogação**

- Criar documento DID `.well-known/did.json` (no formato JSON-LD) e disponibilizar na URL do identificador do método. Ex:
- `did:web:w3c.github.io` → https://w3c.github.io/.well-known/did.json

- **Registro**
- **Resolução**
- **Atualização**
- **Revogação**

- Substitua `:` por `/` para obter o FQDN
- Monte uma URL com o esquema HTTPS contendo com sufixo `.well-known/did.json`
- Faça um GET na URL gerada

- **Registro**
- **Resolução**
- **Atualização**
- **Revogação**

- O conteúdo do documento DID pode ser atualizado a qualquer momento.
- O DID não é alterado

- **Registro**
- **Resolução**
- **Atualização**
- **Revogação**
  - Exclua o documento DID `did.json`

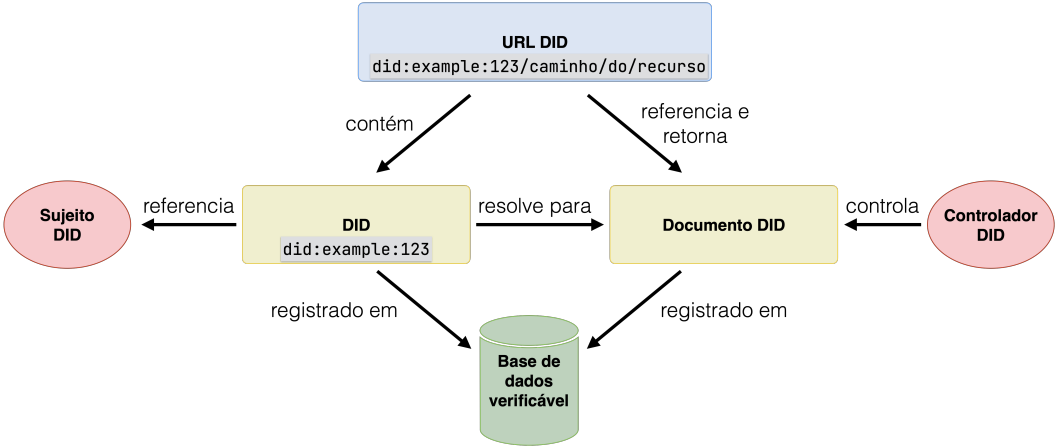
- Contém informações associadas ao sujeito identificado pelo DID
  - Ex: chaves públicas e outros metadados adicionais

```
{
    "@context": "https://www.w3.org/ns/did/v1",
    "id": "did:web:example.com",
    "verificationMethod": [
        {
            "id": "did:web:example.com#controller",
            "type": "Secp256k1VerificationKey2018",
            "controller": "did:web:example.com",
            "ethereumAddress": "0xb9c5714089478a327f09197987f16f9e5d936e8a"
        }
    ],
    "authentication": [
        "did:web:example.com#controller"
    ]
}
```

Fonte: W3C

- Contém informações associadas ao sujeito identificado pelo DID
  - Ex: chaves públicas e outros metadados adicionais


```
{
    "@context": [
        "https://www.w3.org/ns/did/v1",
        "https://gpg.jsld.org/contexts/lds-gpg2020-v0.0.jsonld"
    ],
    "id": "did:example:123",
    "verificationMethod": [
        {
            "id": "did:example:123#989ed1057a294c8a3665add842e784c4d08de1e2",
            "type": "PgpVerificationKey2021",
            "controller": "did:example:123",
            "publicKeyPgp": "-----BEGIN PGP PUBLIC KEY BLOCK-----\r\nVersion: OpenPGP.js v4.9.0\r\
    nComment: https://openpgpjs.org\r\n\r\
    nxjMEXkm5LRYJKwYBBAHaRw8BAQdASmfrjYr7vrjwHNiBsdcImK397Vc3t4BL\r\nE8rnN......v6\r\nDw==\r\n=
    wSoi\r\n-----END PGP PUBLIC KEY BLOCK-----\r\n"
        }
    ]
}
```



Fonte: Adaptado de W3C

Motivação

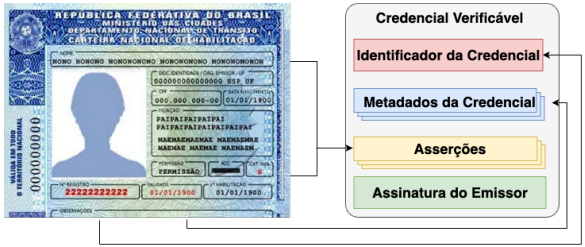
Dificuldade em expressar diplomas digitais, entre outros emitidos por terceiros na *Web* e que possam ser comprovados e interpretados por máquinas

Motivação

Dificuldade em exp erceiros na *Web* e
que possam ser co

Fonte: Luis Fortanell - Wikimedia.org

Credenciais verificáveis



- Para expressar credenciais digitais de forma similar às credenciais físicas
- Metadados – emissor, data de expiração, chave pública para verificação
- Conjunto de afirmações sobre a entidade
- Criptograficamente segura, respeita a privacidade (e.g. provas de conhecimento zero – ZKP) e pode ser interpretadas por máquinas

Formatos

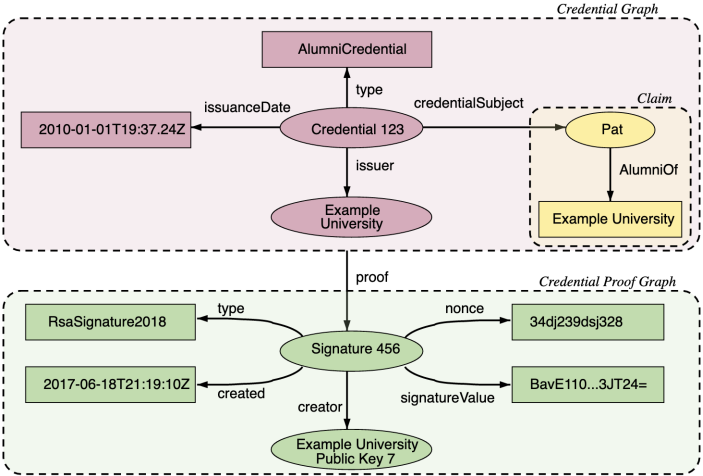
JSON-LD, JSON Web Token (JWT) ou ZKP com Camenisch-Lysyanskaya Signatures (ZKP-CL)

Credenciais verificáveis

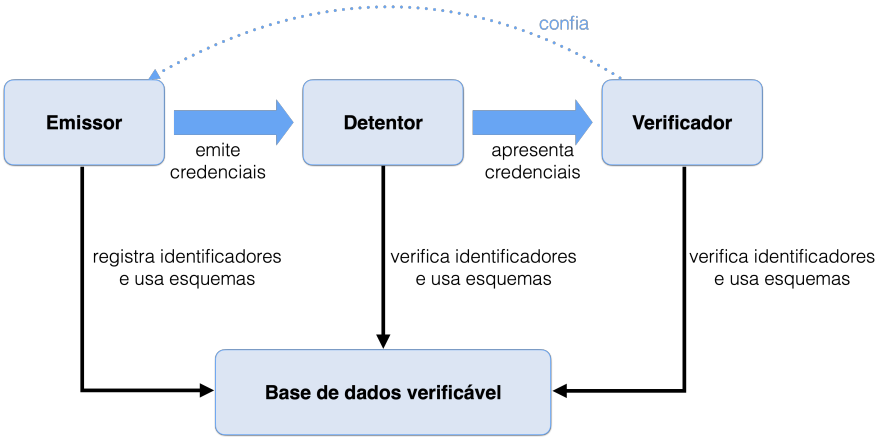
JSON-LD

```
{
    "@context": ["https://www.w3.org/2018/credentials/v1",
      "https://www.w3.org/2018/credentials/examples/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": "RsaSignature2018",
        "created": "2017-06-18T21:19:10Z",
        "proofPurpose": "assertionMethod",
        "verificationMethod": "https://example.edu/issuers/565049#key-1",
        "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19...."
    }
}
```

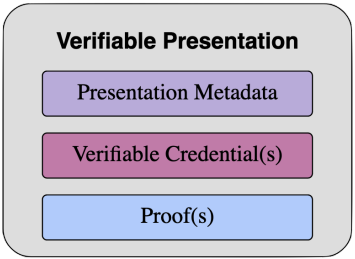
Credenciais verificáveis



Fonte: W3C

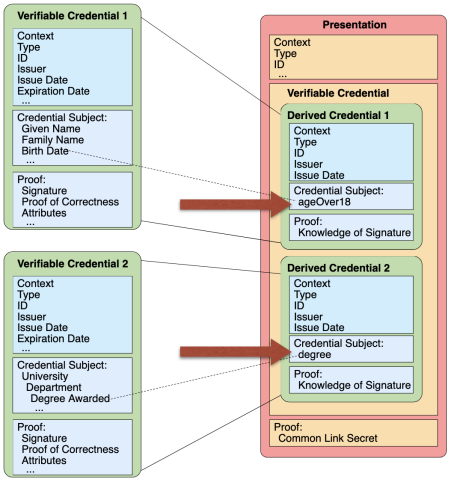

confia
Emissor
emite
credenciais
Detentor
apresenta
credenciais
Verificador
registra identificadores
e usa esquemas
verifica identificadores
e usa esquemas
verifica identificadores
e usa esquemas
Base de dados verificável

Fonte: W3C



Fonte: W3C

- **Apresentação Verificável** (VP) representa dados de uma ou mais VC de forma que a autoria continua podendo ser verificada
- Detentor pode **apresentar somente parte dos dados em uma VC** que julgar necessário para cada interação



Fonte: W3C

Prova de conhecimento zero

Método criptográfico que permite a uma entidade provar para uma outra que conhece um determinado valor sem ter a necessidade de revelar tal valor

- VC deve ser emitida de forma a permitir ao detentor derivar uma prova sobre ela
- VP deve conter todas informações necessárias para verificar a VC
- VP não deve vazar qualquer informação que permita ao verificador identificar o detentor por meio do correlacionamento de múltiplas VP

- A propriedade `id` pode ter um único valor associado e deve ser obrigatoriamente uma URI (neste exemplo: URL HTTP e DID)

```
{
    "@context": ["https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/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"
}
```

- VC não depende de DID e vice-versa, porém o uso combinado destes é considerado como um dos pilares para soluções de identidade digital descentralizada (IDD)

- **Permite** que ao usuário, o **dententor** da identidade, também **seja o controlador** e evita a dependência em IdPs
- Usuários ficam como responsáveis em armazenar suas identidades, geralmente com aplicativos de carteiras digitais
- Diversas tecnologias estão sendo propostas, muitas baseadas em livro razão distribuído

- **Permite** que ao usuário, o **dententor** da identidade, também **seja o controlador** e evita a dependência em IdPs
- Usuários ficam como responsáveis em armazenar suas identidades, geralmente com aplicativos de carteiras digitais
- Diversas tecnologias estão sendo propostas, muitas baseadas em livro razão distribuído

Conference Book Demo[a] consiste em uma aplicação para demonstrar o uso do DID e VC. É necessário ter uma carteira[b] no celular

[a] https://digital.gov.bc.ca/digital-trust/projects-and-initiatives/conference-book-demo
[b] https://digital.gov.bc.ca/digital-trust/tools/how-to-get-a-mobile-wallet

- **Autorização**
  - **Especificação** de políticas de acesso, as quais indicam quais recursos um sujeito pode ter acesso
- **Controle de acesso**
  - **Aplicação** das políticas de acesso, decidindo se um sujeito pode ou não acessar um determinado recurso ou realizar uma determinada operação (permissões ou privilégios)

Modelos de controle de acesso

- **Discricionário (DAC)**
- **Obrigatório (MAC)**
- **Baseado em papéis (RBAC)**
- **Baseado em atributos (ABAC)**

- **Discricionário (DAC)**
- **Obrigatório (MAC)**
- **Baseado em papéis (RBAC)**
- **Baseado em atributos (ABAC)**

- Dono do recurso indica quais permissões um sujeito possui sobre o recurso
- É dito discricionário, pois o próprio dono do recurso pode manipulá-lo
- Pode ser implementado por meio de Listas de Controle de Acesso (ACL)
- Adequado para sistemas de arquivos, mas teria dificuldade em ambientes distribuídos, dinâmicos e de larga escala

- **Discricionário (DAC)**
- **Obrigatório (MAC)**
- **Baseado em papéis (RBAC)**
- **Baseado em atributos (ABAC)**

- Restringe o acesso a um recurso considerando o nível de sensibilidade da informação e da autorização que o sujeito possui
- Difere do discricionário de forma que o sujeito não consegue alterá-lo ou contorná-lo
- Em sistemas operacionais, os sujeitos podem ser processos e os recursos podem ser arquivos

Modelos de controle de acesso

- **Discricionário (DAC)**
- **Obrigatório (MAC)**
- **Baseado em papéis (RBAC)**
- **Baseado em atributos (ABAC)**

- Privilégios são associados a um papel e o papel é associado ao sujeito
- Sujeito pode ter mais de um papel e um mesmo privilégio pode ser associado a mais de um papel
- Hierárquico – papel herda privilégios de outro
- Separação de responsabilidades (SOD)
  - Diversos papéis a um mesmo sujeito
  - Diversos privilégios a um mesmo papel
  - Quando um papel pode ser ativado (e.g. hora do dia)

- **Discricionário (DAC)**
- **Obrigatório (MAC)**
- **Baseado em papéis (RBAC)**
- **Baseado em atributos (ABAC)**

- Dificuldade: “engenharia de papéis”
- Como definir todos os possíveis papéis e seus respectivos privilégios
- Facilidade de administração *versus* políticas de segurança mais rígidas
  - Resulta em uma maior quantidade de papéis

- **Discricionário (DAC)**
- **Obrigatório (MAC)**
- **Baseado em papéis (RBAC)**
- **Baseado em atributos (ABAC)**

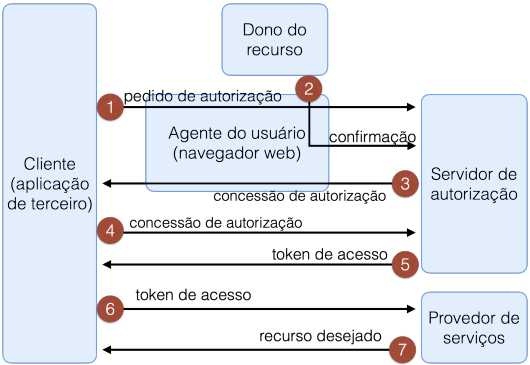
- Decisões de acesso são sobre os valores de atributos associados aos sujeitos, recursos, operação solicitada e condições ambientais (e.g. hora do acesso)
- Dinâmico, flexível e adequado para soluções de larga escala
- XACML implementa este modelo

- Como uma aplicação de terceiro conseguiria acessar um recurso, em nome de um usuário, em outra aplicação?
  - O usuário poderia fornecer suas credenciais de acesso (e.g. *username/password*) a essa aplicação

- Como uma aplicação de terceiro conseguiria acessar um recurso, em nome de um usuário, em outra aplicação?
  - O usuário poderia fornecer suas credenciais de acesso (e.g. *username/password*) a essa aplicação
- **Quais seriam os riscos associados a esta abordagem?**
  - Aplicação de terceiro teria armazenar as credenciais deste usuário para futuras requisições
  - Não há como revogar as credenciais concedidas para uma aplicação específica
  - Não teria como limitar quais recursos do usuário a aplicação teria acesso

OAuth2 – Framework de autorização (RFC6749)

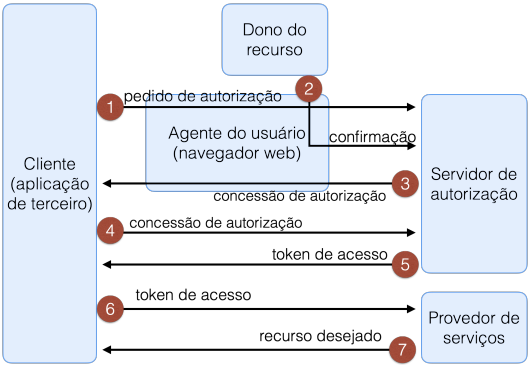
- Permite a aplicações de terceiros obterem acesso limitado, e por um período, aos recursos disponíveis a usuário em uma outra aplicação HTTP (*desktop*, *web* ou *mobile*)



Fonte: Adaptado de RFC6749

- Fundamentado sobre **redirecionamentos HTTP** e obrigatoriamente sobre o TLS

- Permite a aplicações de terceiros obterem acesso limitado, e por um período, aos recursos disponíveis a usuário em uma outra aplicação HTTP (*desktop*, *web* ou *mobile*)



Fonte: Adaptado de RFC6749

- Fundamentado sobre **redirecionamentos HTTP** e obrigatoriamente sobre o TLS

OpenID Connect é uma camada de autenticação feita sobre o OAuth2

Privacy by Design

Privacidade do usuário deve estar em foco desde a concepção do sistema e deve ser mantida durante todo o seu ciclo de vida

- Sistemas devem ser projetados para minimizar a quantidade de informação pessoal de seus usuários
- Sistemas devem fazer uso de mecanismos de segurança para proteger os dados de seus usuários
- Tais conceitos também estão presentes na LGPD e GPDR Europeia

Usabilidade

Requisito de qualidade, que define com que facilidade os usuários podem usar um *software* para realizar uma tarefa específica

- **Usabilidade da segurança** deve-se considerar que a **carga física e cognitiva** para tomada de decisões, mesmo que repetitivas, deve ser **tolerável**

Privacidade e usabilidade

1. Qual modelo de GId dá ao usuário maior poder sobre a gestão de seus dados pessoais?
2. Qual modelo de GId gera menor carga cognitiva para os usuários?
3. Pessoas com pouca afinidade em TI estariam na melhor posição para tomar decisões que impactam na proteção de seus dados pessoais?
4. As leis que obrigam o consentimento do usuário para uso de *cookies* (entre outros) ajudam na privacidade do usuário ou são apenas um passo extra entre o usuário e o recurso desejado?
5. Interfaces de consentimento do usuário impactam na usabilidade ao mesmo tempo que dão ao usuário controle sobre seus dados?

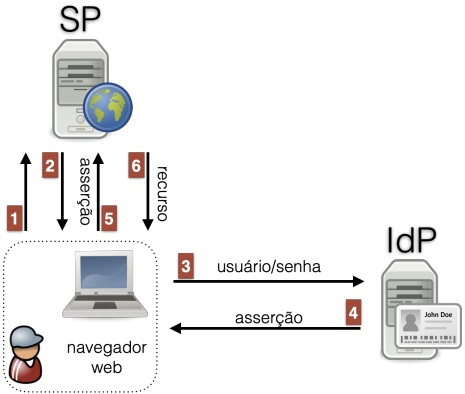
Demandas, desafios e tecnologias

Demandas, desafios e tecnologias

- Demandas sociais e regulatórias
- Novas formas de integração de serviços e diversidade de dispositivos usados
- Aumento da robustez e impacto na usabilidade dos processos de autenticação
- Dispositivos que atuam em nome do usuário
- Identidade de software e modelos de confiança zero

- Redirecionamentos HTTP
- Parâmetros de URL
- *Link decoration*
- *Cookies*

- **Código de resposta HTTP da classe** `3XX` indica ao agente do usuário (navegador *web*) que este precisa tomar alguma ação para que o pedido possa ser atendido



- Formato da URI: `scheme://host:port/path?queryString#fragment`
  - **scheme** – HTTP, HTTPS etc.
  - **host** – nome ou IP
  - **port** – implícito ao esquema (80 para http) ou explícito
  - **path** – segmentos de texto delimitados por /
  - **queryString** – lista de parâmetros (nome=valor) delimitados por &
  - **fragment** – ponto particular dentro um documento

- **Agente de usuário indica ao *site* como deseja receber a lista de produtos ordenada**
  - https://www.example.com/produtos?ordem=maior-valor
- **Campanha de *marketing*, para saber de onde um usuário veio**
  - https://www.example.com/?utm_source=twitter&utm_medium=tweet&utm_campaign=summer-sale

- **Agente de usuário indica ao *site* como deseja receber a lista de produtos ordenada**
  - https://www.example.com/produtos?ordem=maior-valor
- **Campanha de *marketing*, para saber de onde um usuário veio**
  - https://www.example.com/?utm_source=twitter&utm_medium=tweet&utm_campaign=summer-sale

Usuário da CAFe tentando acessar o SP da CAPES

https://www.periodicos.capes.gov.br/Shibboleth.sso/Login?target=https://www.periodicos.capes.gov.br/secure&entityID=https://shibboleth.ifsc.edu.br/idp/shibboleth

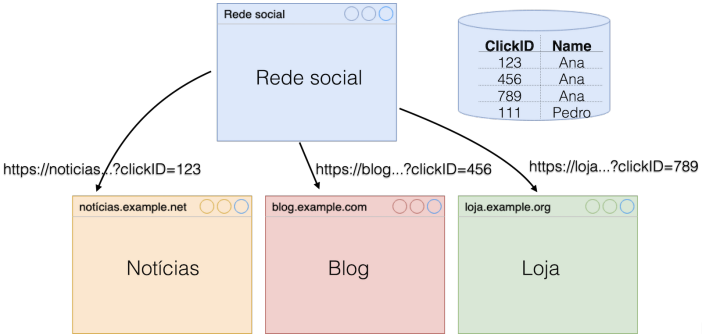
- **Agente de usuário indica ao *site* como deseja receber a lista de produtos ordenada**
  - https://www.example.com/produtos?ordem=maior-valor
- **Campanha de *marketing*, para saber de onde um usuário veio**
  - https://www.example.com/?utm_source=twitter&utm_medium=tweet&utm_campaign=summer-sale

Usuário da CAFe tentando acessar o SP da CAPES

https://www.periodicos.capes.gov.br/Shibboleth.sso/Login?target=https://www.periodicos.capes.gov.br/secure&entityID=https://shibboleth.ifsc.edu.br/idp/shibboleth

Casos de propósito geral *versus* caso de uso específico

- Parâmetros de URL, adicionados dinamicamente com Javascript, com o objetivo de rastrear o usuário
- Rotinas de terceiros embutidas em diferentes *sites* e não são impactadas pelo bloqueio de *cookies* de terceiros



Fonte: Wilander (2019)

- Fragmento de dados enviado pelo servidor HTTP ao navegador *web*, o qual pode armazenar e enviá-lo de volta ao servidor nos pedidos subsequentes
- Conjunto de pares (`chave=valor`) para permitir ao agente de usuário manter o estado da aplicação na interação com servidor HTTP

Servidor

```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: simposio=sbseg22
Set-Cookie: minicurso=mc01

[conteúdo da página]
```

Navegador *web*

```
GET /conteudo_minicurso.html HTTP/1.1
Host: www.example.com
Cookie: simposio=sbseg22; minicurso=mc01
```

- *Cookie* de **sessão** é excluído quando o cliente fecha a sessão
  - Navegadores *web* podem ser configurados para sempre restaurar sessão
- *Cookie* **permanente** é excluído de acordo com as diretivas `Expires` ou `Max-Age`

```
Set-Cookie: simposio=sbseg22; Expires=Thu, 15 Sep 2022 21:30:00 UTC
```

- Podem ter o escopo definido com a diretiva `SameSite`[1] para proteção contra ataques de requisição forjada entre sites (CSRF)
  - Exemplo: Estar com *cookies* válidos em uma sessão com o banco e acessar uma página *web* de terceiro que induza a executar uma operação no banco

```
<img src="http://bank.example.com/withdraw?account=bob&amount=1000000&for=mallory">
```

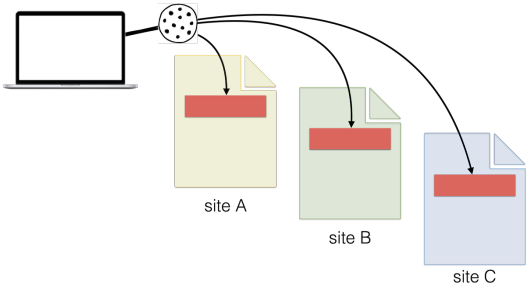
Fonte: Wikipedia

[1] Draft IETF

Cookies são usados para

- Gerenciamento de sessão
- Personalização da aplicação feita pelo usuário
- Rastreamento do usuário

- **Cookie primário** é criado e gerenciado pelo servidor HTTP responsável pelo domínio *web* que o usuário acesso diretamente
- **Cookie de terceiros** são criados para outros domínios, cujo conteúdo destes domínios é acessado de forma indireta pelo usuário



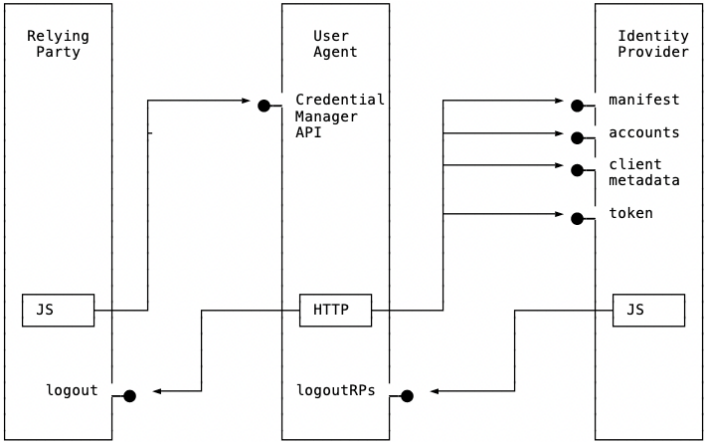
Fonte: Merewood (2020)

- Banner de propaganda do domínio example.net presente em diferentes *sites*
- Cada *site* que o usuário visitar o *cookie* é enviado ao example.net, permitindo assim rastrear a navegação

Como manter o funcionamento da autenticação federada diante de mecanismos mais restritivos, com foco na privacidade, impostos pelos navegadores *web*?

- **Federated Credential Management API**[2] – ainda é um rascunho W3C
- API para IdPs, SPs e navegador *web* que permita a autenticação federada sem impactar na privacidade dos usuários
- Alternativa para soluções federadas que dependem de *cookies* de terceiros para permitir o *Single Sign-On* (SSO) e *Single Logout* (SLO)

[2] https://fedidcg.github.io/FedCM/

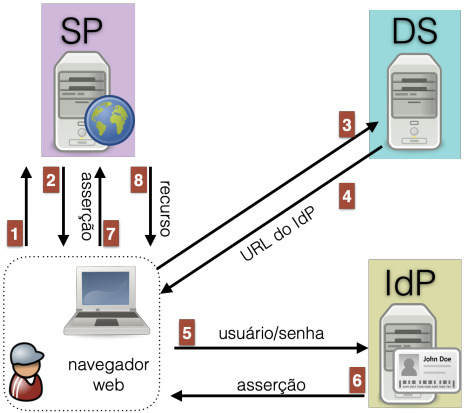


Fonte: Fedidcg

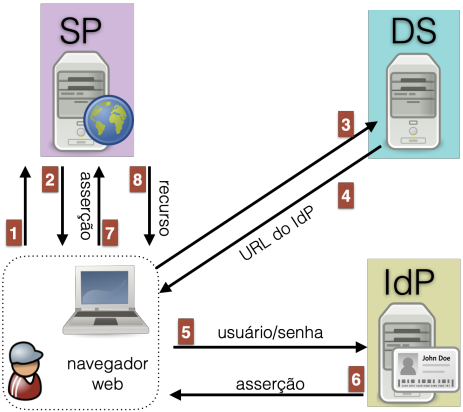
Federated Credential Management API

Exemplo

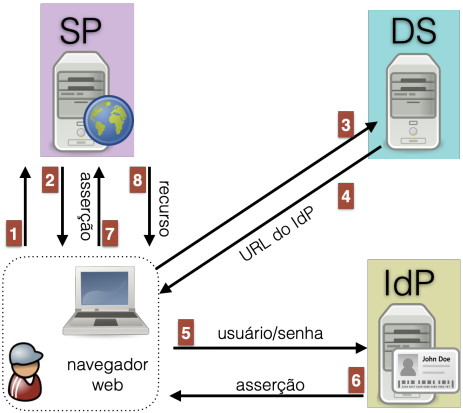
```
<html>
<body>
    <button onclick="login()">Login with idp.example</button>
    <script>
        let nonce;
        async function login() {
            nonce = random();
            return await navigator.credentials.get({
                mediation: "optional",
                identity: {
                    providers: [{
                        configURL: "https://idp.example/manifest.json",
                        clientId: "123",
                        nonce: nonce
                    }]
                }
            });
        }
    </script>
</body>
</html>
```


SP
DS
IdP
1
2
asserção
7
8
recurso
3
URL do IdP
4
5
usuário/senha
6
asserção
navegador
web
John Doe

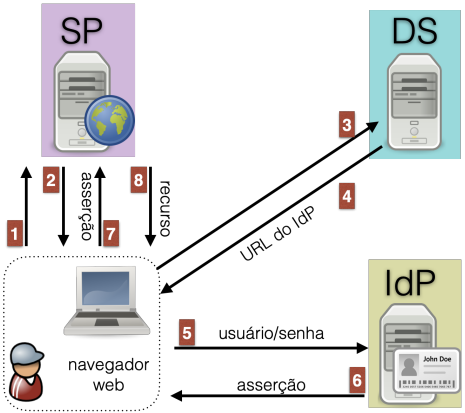

Bem vindo ao
SP 1
Entrar

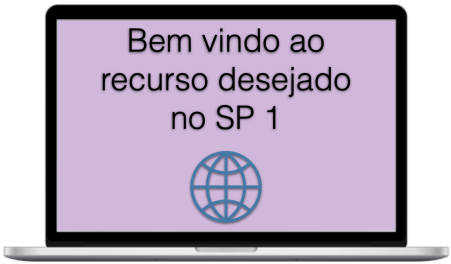

SP
DS
IdP
1
2
asserção
7
8
recurso
3
URL do IdP
4
5
usuário/senha
6
asserção
navegador
web
John Doe


Discovery Service
Qual é o teu IdP?
Entrar

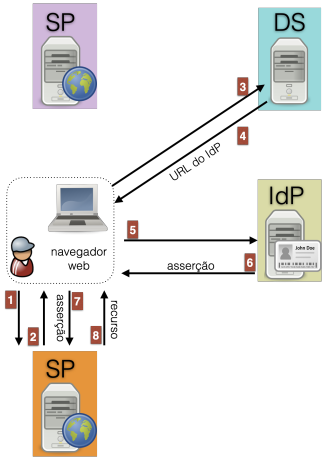

SP
DS
IdP
1
2
asserção
7
8
recurso
3
URL do IdP
4
5
usuário/senha
6
asserção
navegador
web
John Doe

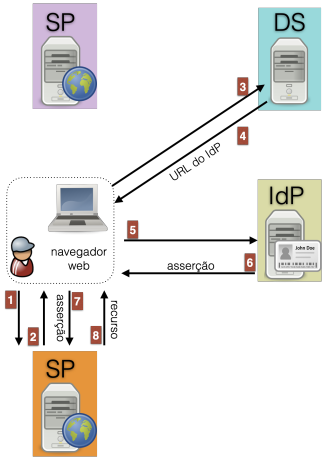

Meu IdP
fulano
Confirma


SP
DS
IdP
1
2
asserção
7
8
recurso
3
URL do IdP
4
5
usuário/senha
6
asserção
navegador
web
John Doe

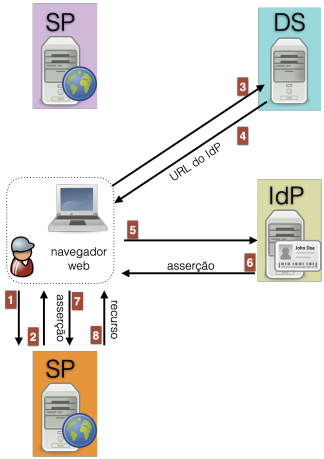

Bem vindo ao
recurso desejado
no SP 1

Redirecionamentos HTTP: *SP* → *DS* → *IdP* → *SP*




SP
DS
3
4
URL do IdP
IdP
5
navegador
web
asserção
6
1
2
asserção
7
8
recurso
SP

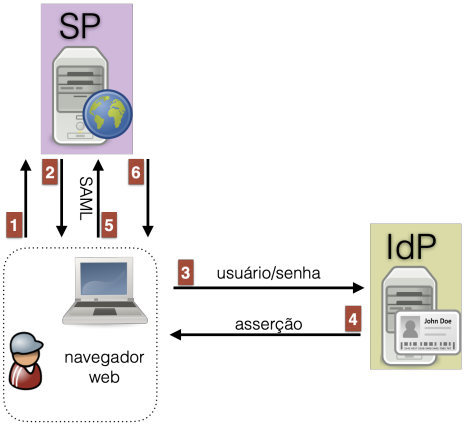

Discovery Service
Meu IdP
Entrar

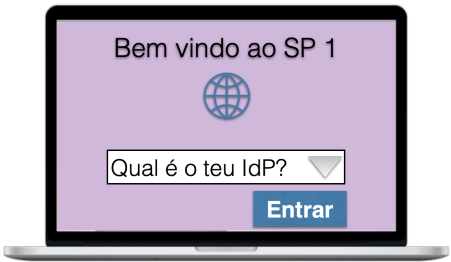

SP
DS
3
4
URL do IdP
IdP
navegador
web
5
6
asserção
1
2
asserção
7
8
recurso
SP


Bem vindo ao
recurso desejado
no SP 2

Autenticação federada, centrada no usuário e novos mecanismos de privacidade

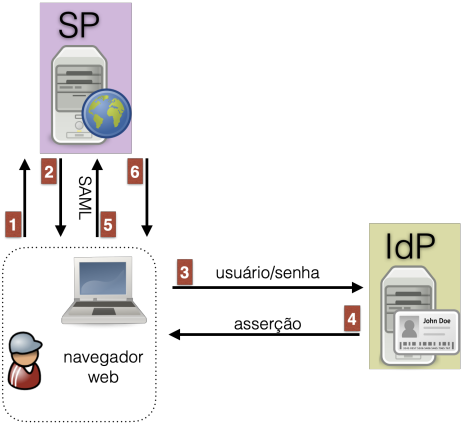
Redirecionamentos HTTP: *SP* → *IdP* → *SP* (DS embarcado no SP)

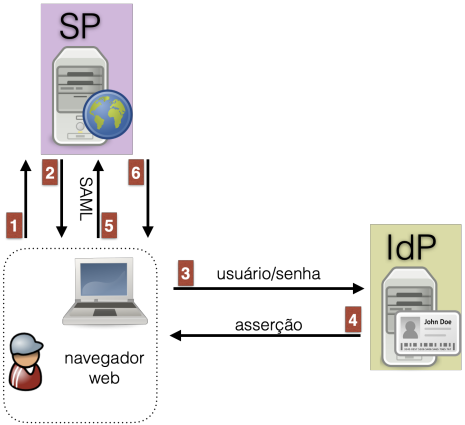


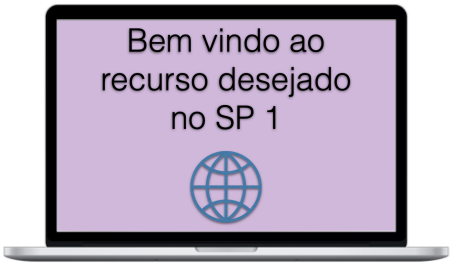


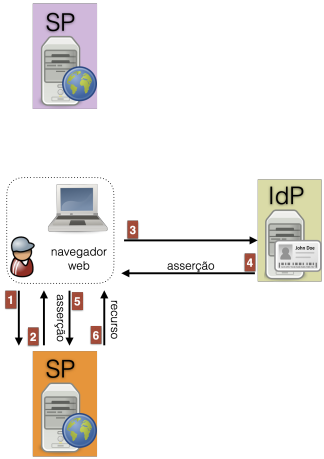
Autenticação federada, centrada no usuário e novos mecanismos de privacidade

Redirecionamentos HTTP: *SP* → *IdP* → *SP* (DS embarcado no SP)

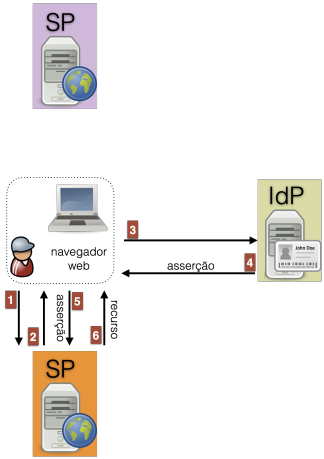



SP
1
2
SAML
5
6
3
usuário/senha
4
asserção
IdP
John Doe
navegador
web


Bem vindo ao
recurso desejado
no SP 1


SP
IdP
navegador
web
3
4
asserção
1
2
asserção
5
recurso
6
SP


Bem vindo ao SP 2
Qual é o teu IdP?
Entrar

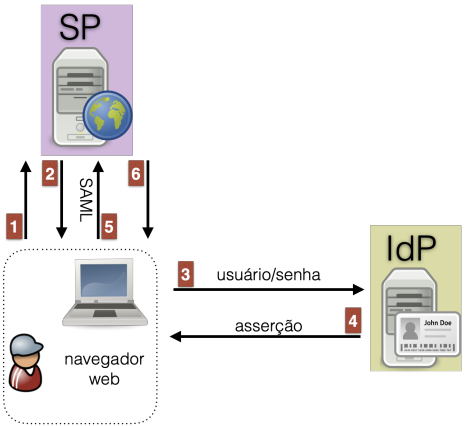

SP
IdP
navegador web
3
4
asserção
1
2
asserção
5
6
recurso
SP

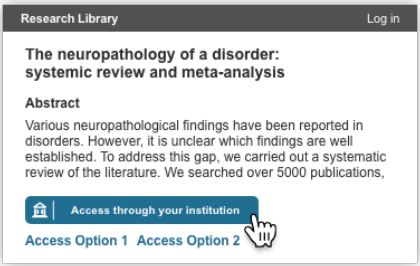

Bem vindo ao
recurso desejado
no SP 2

- Permitir o SSO verdadeiro e transparente nas federações acadêmicas
- O serviço de descoberta (DS) pode ser embarcado na página do SP, evitando um redirecionamento ao DS para escolha do IdP
- Se o usuário já estiver autenticado junto ao seu IdP, então o DS nem é apresentado
  - Faz uso da *Web storage API* dos navegadores *web* e não depende de *cookies* de terceiros
- Padroniza a forma de apresentar o botão para autenticação

Autenticação federada, centrada no usuário e novos mecanismos de privacidade

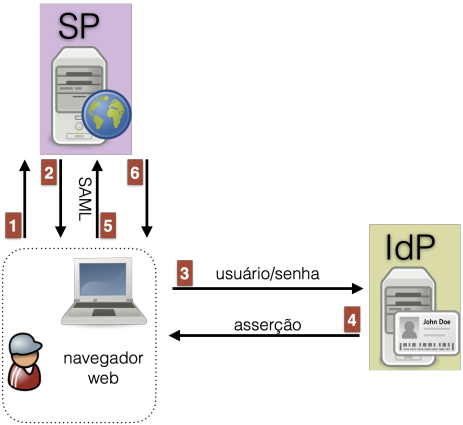
Projeto https://seamlessaccess.org

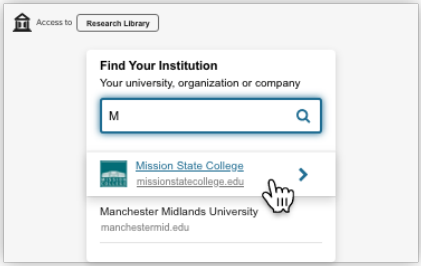




Autenticação federada, centrada no usuário e novos mecanismos de privacidade

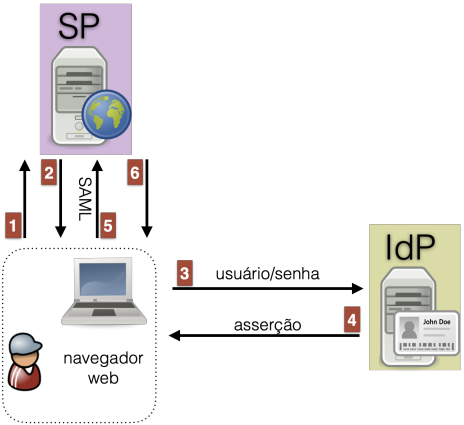
Projeto https://seamlessaccess.org

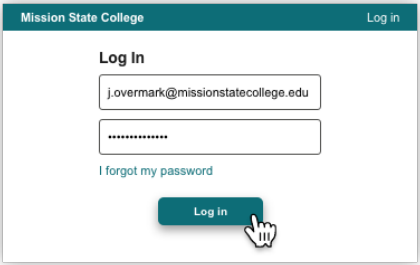


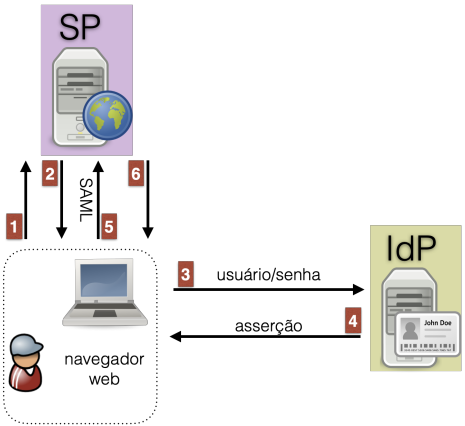


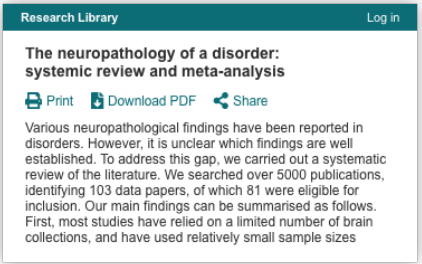
Autenticação federada, centrada no usuário e novos mecanismos de privacidade

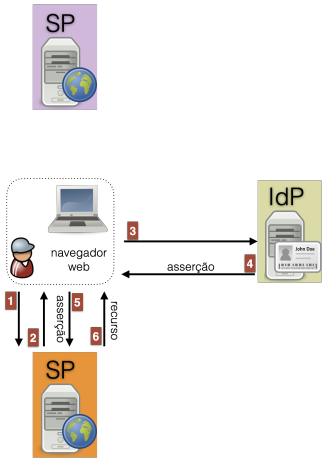
Projeto https://seamlessaccess.org

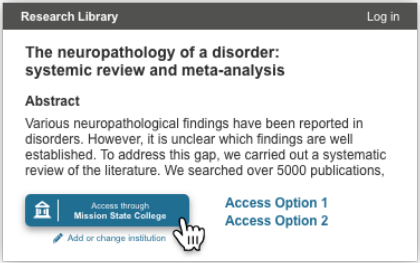




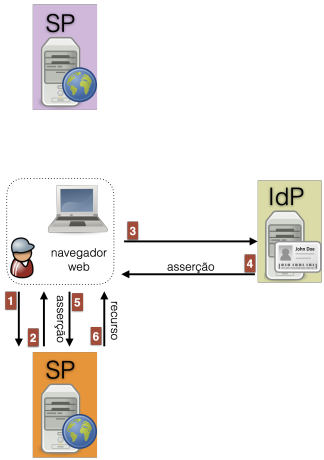

SP
2
SAML
6
1
5
3
usuário/senha
IdP
asserção
4
navegador
web
John Doe

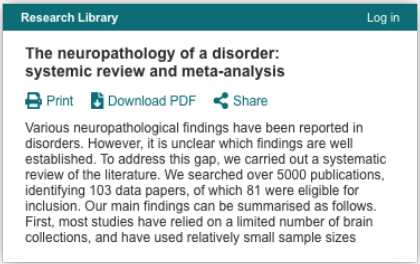

Research Library
Log in
The neuropathology of a disorder: systemic review and meta-analysis
Print
Download PDF
Share
Various neuropathological findings have been reported in disorders. However, it is unclear which findings are well established. To address this gap, we carried out a systematic review of the literature. We searched over 5000 publications, identifying 103 data papers, of which 81 were eligible for inclusion. Our main findings can be summarised as follows. First, most studies have relied on a limited number of brain collections, and have used relatively small sample sizes





O botão exibe o último IdP usado, informação obtida a partir do `localStorage` do navegador


SP
IdP
navegador web
3
asserção
4
1
2
asserção
5
6
recurso
SP


Research Library
Log in
The neuropathology of a disorder: systemic review and meta-analysis
Print
Download PDF
Share
Various neuropathological findings have been reported in disorders. However, it is unclear which findings are well established. To address this gap, we carried out a systematic review of the literature. We searched over 5000 publications, identifying 103 data papers, of which 81 were eligible for inclusion. Our main findings can be summarised as follows. First, most studies have relied on a limited number of brain collections, and have used relatively small sample sizes

Autenticação digital

Garantir que o sujeito possui controle sobre um ou mais autenticadores (senha, chave privada etc.) que estejam associados à sua identidade digital

- **Aquilo que você sabe**
  - senha, PIN
- **Aquilo que você possui**
  - chave privada, *token* criptográfico, *token* OTP
- **Aquilo que você é**
  - biometria

Wired[3]

- `123456` e `password` foram as senhas mais comuns na Internet por 7 anos seguidos
- **Gerenciadores de senhas** são "os vegetais da Internet". Sabemos que são bons para nós, mas a maioria de nós é bem mais feliz comendo *junk food* (senhas fáceis de lembrar e de quebrar)

[3] https://www.wired.com/story/best-password-managers

Wired[3]

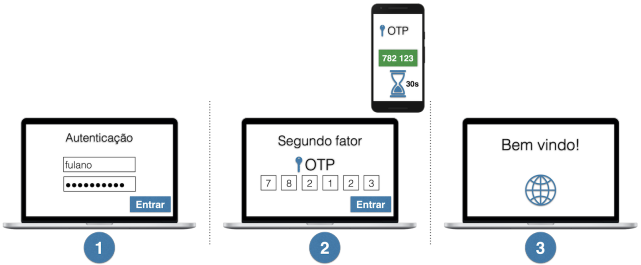
- `123456` e `password` foram as senhas mais comuns na Internet por 7 anos seguidos
- **Gerenciadores de senhas** são "os vegetais da Internet". Sabemos que são bons para nós, mas a maioria de nós é bem mais feliz comendo *junk food* (senhas fáceis de lembrar e de quebrar)

PEARMAN ET AL, ***WHY PEOPLE (DON'T) USE PASSWORD MANAGERS EFFECTIVELY***, SYMPOSIUM ON USABLE PRIVACY AND SECURITY, 2019.

RAY ET AL, ***WHY OLDER ADULTS (DON'T) USE PASSWORD MANAGERS***, USENIX SECURITY, 2021

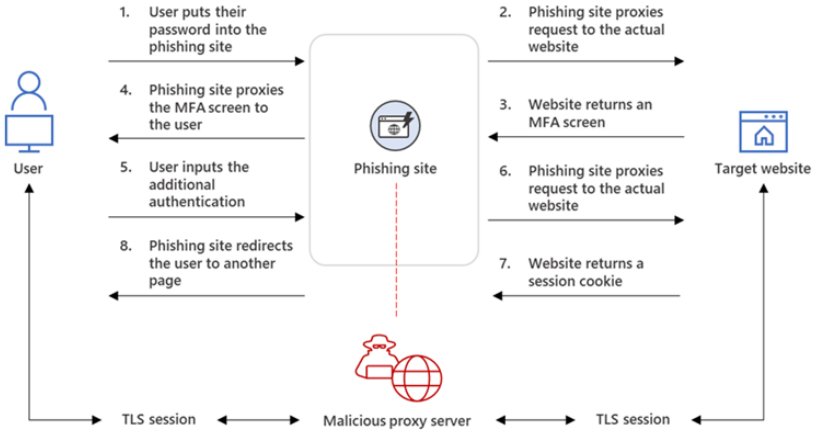
[3] https://www.wired.com/story/best-password-managers

- **Aquilo que você sabe** está suscetível a ataques de força bruta, *phishing*, *malwares* no dispositivo do usuário e *adversary-in-the-middle*
- **Autenticação multifator** combina fatores de diferentes categorias
  - Ex: (*username* & *password*) + senha de uso único (OTP)
  - OTP enviado por SMS, telefone, email, *token* criptográfico ou aplicativo



- **Aquilo que você sabe** está suscetível a ataques de força bruta, *phishing*, *malwares* no dispositivo do usuário e *adversary-in-the-middle*
- **Autenticação multifator** combina fatores de diferentes categorias
  - Ex: (*username* & *password*) + senha de uso único (OTP)
  - OTP enviado por SMS, telefone, email, *token* criptográfico ou aplicativo

OTP está suscetível a ataques de *phishing*, *malwares* no dispositivo do usuário e *adversary-in-the-middle*

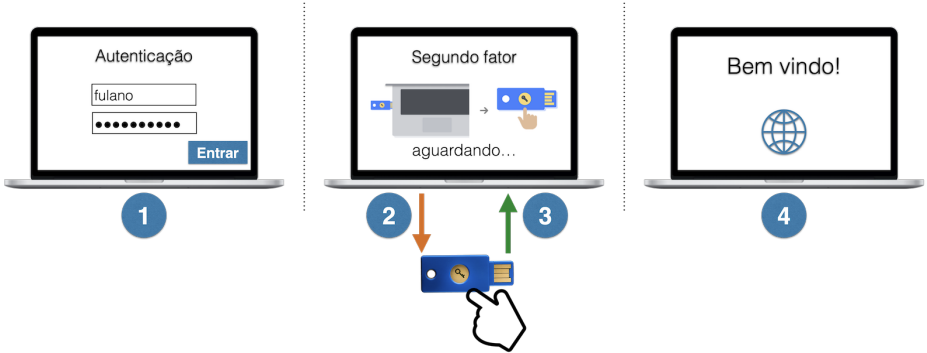


Fonte: Microsoft, 2022

- **FIDO UAF** foco na experiência sem senha (*smartphone*)
- **FIDO U2F** foco segundo fator de autenticação (chaves USB)
- **Chave de ateste** garante que é um dispositivo genuíno e certificado
  - *Basic, Self, CA, AnonCA, No attestation*
- Para cada SP é gerado um **par de chaves exclusivo** para o domínio *web* do SP
  - Não suscetível a ataques de força bruta, *phishing*, *malwares* no dispositivo do usuário e *adversary-in-the-middle*
  - Não compartilhar uma mesma chave privada por diferentes SPs restringe a possibilidade de rastreamento do usuário

Robustez do processo de autenticação

Processo de autenticação com FIDO como segundo fator



- API presente nos navegadores *web*[4]
- Pode-se usar **chaves USB** (autenticadores externos), **computadores ou telefones** (autenticadores de plataforma) com hardware seguro
  - Permite a experiência sem senha ou como segundo fator de autenticação
  - Comunicação via USB, BLE ou NFC

[4] https://webauthn.me/browser-support

- API presente nos navegadores *web*[4]
- Pode-se usar **chaves USB** (autenticadores externos), **computadores ou telefones** (autenticadores de plataforma) com hardware seguro
  - Permite a experiência sem senha ou como segundo fator de autenticação
  - Comunicação via USB, BLE ou NFC

Dificuldades

- Chaves USB são caras, disponíveis em poucos mercados e podem ser perdidas
- Computadores ou telefones podem ser trocados e assim, as chaves são perdidas

[4] https://webauthn.me/browser-support

Multi-device FIDO Credentials (chaves de acesso ou *passkeys*)

- Chaves sincronizadas entre múltiplos dispositivos, mesmo de diferentes fabricantes (e.g. Apple, Google, Microsoft)
- Experiência semelhante ao uso de **gerenciadores de senha**
  - Mantidas na conta Google ou iCloud do usuário
- Provedores de Serviço conseguem determinar se o usuário está usando um dispositivo conhecido

Multi-device FIDO Credentials (chaves de acesso ou *passkeys*)

- Chaves sincronizadas entre múltiplos dispositivos, mesmo de diferentes fabricantes (e.g. Apple, Google, Microsoft)
- Experiência semelhante ao uso de **gerenciadores de senha**
  - Mantidas na conta Google ou iCloud do usuário
- Provedores de Serviço conseguem determinar se o usuário está usando um dispositivo conhecido

Estará disponível a partir de 2023 nos sistemas operacionais e serviços da Apple, Google e Microsoft

- Sistemas adaptativos estão aptos a modificarem seu comportamento para escolha do(s) melhor(es) mecanismo(s) de autenticação em resposta a **fatores contextuais**
  - Recursos gerenciados: os autenticadores (nos dispositivos e em aplicativos do usuário)
  - Lógica de adaptação: pode ser executada no mesmo dispositivo da aplicação que deseja utilizar os autenticadores, ou em outro dispositivo

- Sistemas adaptativos estão aptos a modificarem seu comportamento para escolha do(s) melhor(es) mecanismo(s) de autenticação em resposta a **fatores contextuais**
  - Recursos gerenciados: os autenticadores (nos dispositivos e em aplicativos do usuário)
  - Lógica de adaptação: pode ser executada no mesmo dispositivo da aplicação que deseja utilizar os autenticadores, ou em outro dispositivo

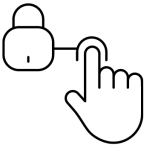
Exemplos

- um app que detecta quando o usuário está em casa e desativa a proteção por senha até que ele se mude para um local diferente
- sistema no qual um usuário se autentica com o leitor de impressão digital do smartphone para acessar seu laptop, quando os dois dispositivos estão próximos

Autenticação Contínua (Ativa)

- Monitoramento em tempo real de modo a validar o usuário durante a sessão estabelecida (biometria baseada em software)

Autenticação Explícita



Biometria digital

Reconhecimento facial

Reconhecimento voz

Autenticação Implícita

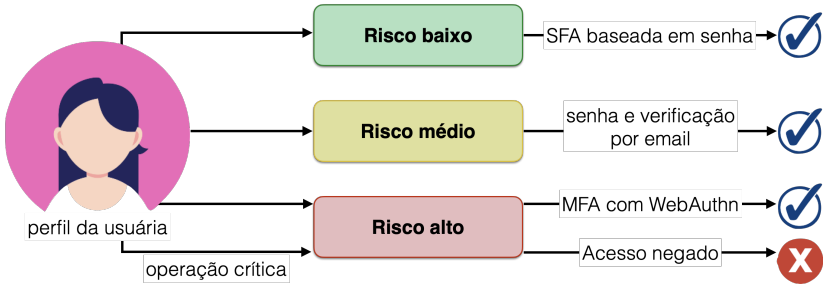
Atributos Comportamentais

Ex: movimento corporal do usuário, pressiona a tela, usa o mouse, velocidade de digitação

Comportamental baseado em localização

Autenticação baseada em risco
(*Risk- Based Authentication* - RBA)

- Sistema captura e armazena diferentes tipos de informações, a partir disso calcula uma pontuação e gera uma classificação de risco, e então decide o mecanismo ou fator de autenticação



Soluções Tecnológicas com Autenticação Dinâmica

- Plataformas de identidade (IAM) comerciais, como por exemplo a *OKTA*, a *Azure Active Directory* e *OneLogin*, possibilitam a criação de políticas de acesso contextual que avaliam fatores de risco
- O *framework Shibboleth* permite aos IdPs implementarem novos fluxos de autenticação
  - *MFA Flow* fornece uma maneira programável de combinar diferentes tipos de fluxos de autenticação, bem como orquestrar sequências de execução destes fluxos

Soluções Tecnológicas com Autenticação Dinâmica

- Plataformas de identidade (IAM) comerciais, como por exemplo a *OKTA*, a *Azure Active Directory* e *OneLogin*, possibilitam a criação de políticas de acesso contextual que avaliam fatores de risco
- O *framework Shibboleth* permite aos IdPs implementarem novos fluxos de autenticação
  - *MFA Flow* fornece uma maneira programável de combinar diferentes tipos de fluxos de autenticação, bem como orquestrar sequências de execução destes fluxos

A autenticação dinâmica, usando características comportamentais e contextuais, pode **aumentar a qualidade** do processo de autenticação e **a experiência do usuário**

Cenário internacional de federações acadêmicas

- **Serviço eduGAIN**: possibilita que pesquisadores possam usar seus logins institucionais para acessar inúmeros provedores de serviços na interfederação
- **Ciberinfraestruturas de e-Science**: colaboração global em determinadas áreas da ciência (formam as OVs)

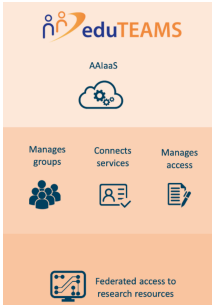
Cenário internacional de federações acadêmicas

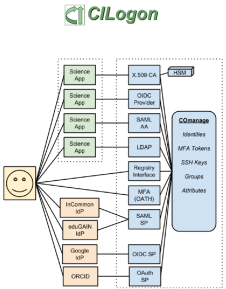
- **Serviço eduGAIN**: possibilita que pesquisadores possam usar seus logins institucionais para acessar inúmeros provedores de serviços na interfederação
- **Ciberinfraestruturas de e-Science**: colaboração global em determinadas áreas da ciência (formam as OVs)

Desafios que precisam ser enfrentados

- Sistemas de GId federada **não foram projetados** para serem usados em ambientes abertos e dinâmicos como as OVs
- Profissionais autônomos e empresas também colaboraram e eles utilizam **Login Social** ou OPs OpendId Connect
- Muitas decisões de acesso dependem de **atributos definidos na própria OV** (falta de padrão amplamente aceito)
  - Falta do atributo que identifica um usuário é **membro** de uma OV específica e o atributo que identifica o seu **papel** na OV

- O projeto **AARC**: definiu uma arquitetura de referencia (BPA)
  - Serviço **eduTEAMS**: solução AAIaaS da Gèant
  - Serviço **CILogon**: Shibboleth + COManage + BPA
  - Serviço **Unity**: SAML e OpenId Connect e gestão de grupos e atributos





Motivação

- Assim como no caso com humanos, componentes de software também precisam de identidades
  - Componentes de software precisam acessar outros componentes (e.g., BDs, APIs)
  - Identidades são fundamentais para o controle de acesso
- *Privacy by Design*
  - Cada entidade deve ter acesso apenas aos recursos necessários para o seu propósito
  - Em um contexto mais atual: se um micro-serviço tem uma responsabilidade específica, deve ter uma identidade específica

Motivação (cont.)

- *Zero-Trust*: identidades únicas, verificáveis e dinâmicas
  - Todos os recursos devem ter identidades
  - Todas as conexões devem ser autenticadas
  - Autenticação deve ser dinâmica (e não só baseada em uma credencial estática)

- Componentes de software podem ter ciclos de vida bastante dinâmicos (e.g., milhares de instâncias criadas/destruídas por dia)
- Quais atributos devem definir a identidade?

- Componentes de software podem ter ciclos de vida bastante dinâmicos (e.g., milhares de instâncias criadas/destruídas por dia)
- Quais atributos devem definir a identidade?
  - O que está executando? (e.g., qual código ou imagem de disco/contêiner)
  - Onde está executando? (e.g., em que hospedeiro, em que *namespace*)
  - Por que está executando? (e.g., modo de produção/teste, outros parâmetros)
  - Quem está executando? (e.g., usuário)

- Componentes de software podem ter ciclos de vida bastante dinâmicos (e.g., milhares de instâncias criadas/destruídas por dia)
- Quais atributos devem definir a identidade?
  - O que está executando? (e.g., qual código ou imagem de disco/contêiner)
  - Onde está executando? (e.g., em que hospedeiro, em que *namespace*)
  - Por que está executando? (e.g., modo de produção/teste, outros parâmetros)
  - Quem está executando? (e.g., usuário)
- Qual o formato desta identidade verificável?

- Componentes de software podem ter ciclos de vida bastante dinâmicos (e.g., milhares de instâncias criadas/destruídas por dia)
- Quais atributos devem definir a identidade?
  - O que está executando? (e.g., qual código ou imagem de disco/contêiner)
  - Onde está executando? (e.g., em que hospedeiro, em que *namespace*)
  - Por que está executando? (e.g., modo de produção/teste, outros parâmetros)
  - Quem está executando? (e.g., usuário)
- Qual o formato desta identidade verificável?
  - Certificados X.509: populares pois integram-se facilmente com aplicações existentes
  - *JSON Web Tokens* (JWT): mais simples se incorporados no desenvolvimento

Algumas alternativas para provisionamento de identidades de software

- **Kubernetes**
- **Google BeyondProd**
- **SPIFFE/SPIRE**

Algumas alternativas para provisionamento de identidades de software

- **Kubernetes**
- **Google BeyondProd**
- **SPIFFE/SPIRE**

- *Certificate API*: geração de certificados com aprovação automática ou manual
  - Usuário/componente gera um CSR e submete para API
  - Administrador ou controlador embutido no K8s aprova
  - Quando o status do objeto mudar, usuário/componente pode baixar certificado
- Mais utilizado para acesso a API do próprio K8s por usuários ou componentes do próprio K8s

- **Kubernetes**
- **Google BeyondProd**
- **SPIFFE/SPIRE**

- Outros controladores (e.g., *cert-manager*[a]) podem automatizar o provisionamento, incluindo outras fontes para assinatura
- Mas o provisionamento considera apenas informações estáticas nos manifestos

[a] https://cert-manager.io/

Algumas alternativas para provisionamento de identidades de software

- **Kubernetes**
- **Google BeyondProd**
- **SPIFFE/SPIRE**

- É um modelo de segurança para serviços baseado em princípios de **confiança zero**
  - Adapta o modelo BeyondCorp (que gere acesso de usuários individuais a serviços corporativos sem segurança baseada em perímetro, considerando autenticação baseada em risco e contexto)
  - Estende os atributos considerados na abordagem baseada no K8s para considerar contexto e gerar certificados X.509 que podem ser utilizados com conexões mTLS
- Provisionamento de identidades pode considerar local da execução e até detalhes da imagem de contêiner sendo executada e do processo de geração daquela imagem

Algumas alternativas para provisionamento de identidades de software

- **Kubernetes**
- **Google BeyondProd**
- **SPIFFE/SPIRE**

- SPIFFE é um conjunto de padrões para identificação de serviços
- Ids SPIFFE são URIs: `spiffe://example.com/database`
  - **spiffe** – Protocolo/padrão
  - **example.com** – nome ou IP representando o domínio administrativo
  - **database** – nome do componente de software

Algumas alternativas para provisionamento de identidades de software

- **Kubernetes**
- **Google BeyondProd**
- **SPIFFE/SPIRE**

- Outros exemplos de ids
  - `spiffe://example.com/database/client1` – o nome pode ser uma hierarquia de nomes amigáveis, autorização pode ser concendida para subárvores do caminho (`database/*`)
  - `spiffe://example.com/spire/agent/tpm/5ab45e...` – um *hash* de uma chave pública
- SVIDs (*SPIFFE Verifiable IDs*) são ids embutidas em certificados ou JWTs
  - Emitidos por sistemas como Istio, cert-manager e SPIRE
  - Consumidos por sistemas como Envoy, Ghostunnel e Kafka

Algumas alternativas para provisionamento de identidades de software

- **Kubernetes**
- **Google BeyondProd**
- **SPIFFE/SPIRE**

- SPIRE (*SPIFFE Runtime Environment*): implementação (projeto graduado CNCF) de emissor de identidades
- Identidades são registradas por operadores e vinculadas a atributos dos componentes de software
  - Unix: usuário, grupo, caminho do binário, hash do binário
  - Kubernetes: namespace, conta de serviço, imagem, rótulos
  - Docker: rótulos, variáveis de ambiente, id de imagem
- SVIDs (e certificados-mãe) são gerados automaticamente e recuperados pelos componentes ou pelos seus *proxies* em uma malha de comunicação

Considerações finais

Considerações finais

- **Como provar sua identidade *online* e garantir o acesso seguro aos recursos para os quais possui autorização?**
  - Diferentes modelos de IAM, com autenticação robusta, dinâmica e contínua
  - Controle de acesso baseado em atributos (ABAC)
- **Como colocar o ser humano no centro do controle sobre sua identidade digital?**
  - Estaria o usuário disposto e preparado para assumir essa responsabilidade?

Considerações finais

- **Processos de autenticação robustos terão a conveniência desejada pelos usuários?**
  - WebAuthN *passkeys* possui benefícios não observados por usuários leigos
- **Soluções de autenticação dinâmica e contínua serão fáceis de implantar e usar?**
  - Incluir novos autenticadores, novas estratégias de adaptação ou contextos
  - Carecem de mais estudos sobre usabilidade, viabilidade e aceitação dos usuários
- **Identidade de software permite o isolamento de serviços do ambiente e a integração de componentes de forma segura e transparente**

Referências

Todas as referências que aparecem nestes slides estão disponíveis no texto completo deste Minicurso do SBSeg 2022

Obrigado!

- Emerson Mello (IFSC)
- Shirlei Chaves (IFSC)
- Carlos Eduardo (Sheffield Hallam University, UK)
- Michelle Wangham (Univali e RNP)
- Andrey Brito (UFCG)
- Marco Henriques (Unicamp)

Slides disponíveis em

https://emersonmello.page/sbseg2022