RNP Educação, Pesquisa e Inovação em Rede

Relatório de Visão de Futuro

Comitê Técnico de Gestão de Identidade

maio de 2023

Coordenador do CT-GId

Emerson Ribeiro de Mello, Dr. (IFSC)

Assistente Técnica do CT-GId

Shirlei Aparecida de Chaves, Ma. (IFSC)

Coordenador da RNP para o CT-GId

Clayton Reis da Silva, Me. (RNP)

Diretor Adjunto de e-Ciência e Ciberinfraestrutura Avançada

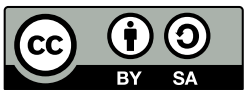
Leandro Neumann Ciuffo, Me. (RNP)

Diretora de Pesquisa e Desenvolvimento

Iara Machado, Ma. (RNP)

Autores

Emerson Ribeiro de Mello, Dr. (IFSC)
Andrey Elísio Monteiro Brito, Dr. (UFCG)
Antônio Tadeu Azevedo Gomes, Dr. (LNCC)
Frederico Schardong, Me. (IFRS)
Marco Aurélio Amaral Henriques (Unicamp)
Michelle Silva Wangham, Dra. (RNP/UNIVALI)
Shirlei Aparecida de Chaves, Ma. (IFSC)
Edelberto Franco Silva, Dr. (UFJF)



SUMÁRIO

Lista de abreviaturas e siglas

AARC *Authentication and Authorisation for Research and Collaboration*.

CA-GId Comitê Assessor de Gestão de Identidade.

CAFe Comunidade Acadêmica Federada.

CT-GId Comitê Técnico de Gestão de Identidade.

DC4EU *Digital Credentials for Europe*.

DID Identificadores Descentralizados (*Decentralized Identifier*).

EDIW Carteira de Identidade Digital Europeia (*European Digital Identity Wallet*).

EIDAS2 *Electronic IDentification, Authentication and trust Services 2*.

FedCM *Federated Credential Management API*.

GId Gestão de Identidades.

GIdLab Laboratório para Experimentação em Gestão de Identidade.

HSM *Hardware Security Module*.

IAA Infraestrutura de Autenticação e de Autorização.

IAM gestão de identidade e de acesso (*Identity and Access Management*).

ICP Infraestrutura de Chave Pública.

ICPEdu Infraestrutura de Chaves Públicas para Ensino e Pesquisa.

IDD Identidade Digital Descentralizada.

IdP Provedor de Identidade (*Identity Provider*).

MFA autenticação multifator (*Multi-Factor Authentication*).

MVNO Operadora Virtual de Rede Móvel (*Mobile Virtual Network Operator*).

NISO *National Information Standards Organization*.

NIST *National Institute of Standards and Technology*.

NREN *National Research and Education Network*.

NSF *National Science Foundation*.

OTP senha de uso único (*One Time Password*).

OV Organização Virtual.

P2P *Peer-to-Peer*.

PD&I Pesquisa, Desenvolvimento e Inovação.

PGId Programa de Gestão de Identidade.

REFEDS *Research and Education FEDerations group*.

RNP Rede Nacional de Ensino e Pesquisa.

RSA Rivest-Shamir-Adleman.

SAML *Security Assertion Markup Language*.

SBC Sociedade Brasileira de Computação.

SBSeg Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais.

SLSA *Supply-chain Levels for Software Artifacts*.

SP Provedor de Serviço (*Service Provider*).

SSI *Self-Sovereign Identity*.

SSO *Single Sign-On*.

STM *International Association of STM Publishers*.

VC Credenciais Verificáveis (*Verifiable Credentials*).

WGID Workshop de Gestão de Identidades Digitais.

1 Introdução

A Gestão de Identidades (GId), como apresentado em ITU (2009), ou a gestão de identidade e de acesso (IAM, *Identity and Access Management*), conforme em Allan (2020), consiste em um conjunto de processos e tecnologias para gerenciar identidades de pessoas, serviços e coisas, bem como o relacionamento e a confiança entre essas. Ou seja, a GId pode ser usada para garantir a identidade de uma entidade e para prover procedimentos de autenticação, autorização, responsabilização e auditoria. Diante da transformação digital, que foi potencializada devido a pandemia de Covid-19, da constante evolução de tecnologias, das necessidades de usuários e de empresas por segurança, proteção de dados pessoais e usabilidade, a área de GId se mostra relevante e desperta interesse da academia, do governo e das empresas.

A Rede Nacional de Ensino e Pesquisa (RNP) oferece à comunidade acadêmica brasileira alguns serviços ligados a GId, sendo estes: Comunidade Acadêmica Federada (CAFe), a Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu) e o *eduroam*.

O Comitê Técnico de Gestão de Identidade (CT-GId)[1], criado pela RNP em 2010, consiste em um fórum de discussão aberto com a missão de realizar prospecção de soluções de gestão de identidade inovadoras e embasadas em pesquisas de médio e longo prazo para o sistema RNP, além de promover a cultura, conscientização no uso de identidades digitais no Brasil. A prospecção visa se tornar uma fonte de referência para apoiar as atividades do Comitê Assessor de Gestão de Identidade (CA-GId) da RNP, podendo assim gerar impacto direto para RNP e suas instituições usuárias. Entre as ações e projetos conduzidos pelo CT-GId, destacam-se:

- Criação do Laboratório para Experimentação em Gestão de Identidade (GIdLab)[2], um serviço da RNP que oferece consultoria especializada em GId e uma plataforma que permite realizar experimentos com diferentes Infraestruturas de Autenticação e de Autorização (IAAs), disponibilizada sob medida, conforme a demanda do solicitante;
- Execução do Programa de Gestão de Identidade (PGId), que objetiva fomentar projetos de PD&I na área;
- Realização de reuniões periódicas com apresentações técnicas conduzidas pelos membros ou por convidados externos;
- Apoio à participação no Workshop de Gestão de Identidades Digitais (WGID), realizado anualmente em conjunto com o Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg);
- Produção de documentos técnicos como recomendações, estudos, relatórios e o documento de visão de futuro.

Escopo

O escopo desse documento se limita a identificar tendências tecnológicas relacionadas à gestão de identidade e de acesso e que possam ser exploradas em atividades de pesquisa e desenvolvimento de curto, médio ou longo prazo. O documento tem como público alvo o sistema RNP, sendo assim foram consideradas tendências na academia e na indústria que possam gerar evoluções para os serviços oferecidos pela RNP, além de vislumbrar novos serviços ou modelos de negócio. Desta forma, o presente documento não objetiva ser uma revisão ampla da literatura ou uma análise completa de todos os assuntos que permeiam a área de gestão de identidade.

[1] https://wiki.rnp.br/display/comitetgi/CT-GId
[2] https://www.rnp.br/servicos/testbeds/gidlab

2 Metodologia

A elaboração desse documento foi baseada em sua revisão anterior, publicada em Brito *et al.* (2021), e assim como naquela revisão, foi feito uso de método de visão qualitativo, do inglês *foresight*:

> Método de visão qualitativo consiste na antecipação de possibilidades futuras com base em percepções de especialistas, cada um deles apoiado exclusivamente em seus conhecimentos e subjetividades (TEIXEIRA, 2013).

Dessa forma, cada especialista seguiu o método baseado em pesquisa que analisou artigos publicados em periódicos e conferências, *whitepapers* e relatórios de tendências de organizações como Gartner e McKinsey, produtos, propostas e relatórios da indústria, bem como projetos e iniciativas de outras redes nacionais de ensino e pesquisa (NREN, *National Research and Education Network*).

O documento foi organizado tendo como base a estratégia de gestão chamada *Três Horizontes de Inovação*, elaborada pela consultoria McKinsey (BAGHAI; COLEY; WHITE, 2000). Nessa estratégia, a linha do tempo indica os ciclos pelos quais um produto ou serviço passa. No primeiro horizonte situam-se os produtos que atualmente geram receita para a organização. Os investimentos realizados no primeiro horizonte tendem a dar retorno ainda no mesmo ano. No segundo horizonte são apresentadas oportunidades para novos negócios, ou seja, produtos ou serviços que podem gerar retorno em um futuro breve. Por fim, no terceiro horizonte são colocadas hipóteses que precisam ser validadas para determinar se cabe investir em um determinado produto. Ou seja, o terceiro horizonte pode ser visto como um ambiente para experimentação, que busca inovação e que não há um retorno esperado. As ideias aqui experimentadas e validadas podem, em uma nova revisão do documento, migrar para o segundo horizonte ou mesmo serem descartadas.

Para a escrita do presente documento foram conduzidas discussões em reuniões *online* e por email. Foi feito uso de ferramentas para escrita colaborativa *online*, o que permitiu a cada autor trabalhar de forma assíncrona e acompanhar as atividades que estavam sendo conduzidas pelos demais autores. Por fim, foi realizada uma reunião final de alinhamento e revisão para entrega do texto consolidado.

As ações desenvolvidas dentro do CT-Gid são colaborativas e voluntárias, sendo aberta a participação para qualquer interessado que possua relação com alguma instituição de ensino ou pesquisa brasileira e que atue na área de gestão de identidade. Periodicamente são enviados convites e divulgadas ações para as principais listas de email da Sociedade Brasileira de Computação (SBC), de forma que os membros daquelas comunidades conheçam e façam parte do CT-GId.

Todos os membros do CT-GId foram consultados sobre o interesse e disponibilidade para participar da elaboração do presente documento. Dessa forma, este documento de visão de futuro é fruto do esforço coletivo de um subconjunto dos membros do CT-GId e nele está representada a visão de diferentes especialistas, mas não necessariamente representa a visão de suas instituições ou da própria RNP. Esse grupo de especialistas pode ser considerado como uma amostra dos pesquisadores que atuam com o tema gestão de identidade e de acesso no Brasil.

3 Panorama

O projeto *SeamlessAccess* (SEAMLESSACCESS, 2023) é uma iniciativa conjunta da GÉANT, Internet2, *National Information Standards Organization* (NISO) e *International Association of STM Publishers* (STM) com o objetivo de resolver os atuais problemas de usabilidade das federações acadêmicas baseadas em asserções *Security Assertion Markup Language* (SAML). Por meio do projeto SeamlessAccess é possível proporcionar uma experiência de *Single Sign-On* (SSO) verdadeira e transparente nas federações acadêmicas.

Desde a revisão de 2021 deste documento de visão de futuro, o projeto *SeamlessAccess* tem apresentado evoluções em sua implementação e documentação, e sua adoção tem aumentado entre Provedores de Identidade (IdPs, *Identity Provider*) e Provedores de Serviço (SPs, *Service Provider*).

Em 2021, informamos que os principais fabricantes de navegadores *web*, Apple, Google e Mozilla, iniciaram diversas frentes comuns para proteger a privacidade de seus usuários, sendo o bloqueio de *cookies* de terceiros a primeira que foi implantada. A *Federated Credential Management API* (FedCM) (W3C, 2023) busca ser uma API nativa dos navegadores *web* para fornecer suporte às aplicações que seguem o modelo federado, sem depender das primitivas de baixo nível, como *cookies*, redirecionamento HTTP e *link decoration*. A FedCM apesar de ainda ser um rascunho, seu desenvolvimento está ativo com participação de diferentes organizações. Alguns operadores de federações acadêmicas, como o grupo responsável pelo projeto *SeamlessAccess*, estão se apropriando e interagindo com o grupo responsável pela escrita da FedCM.

A autenticação baseada em senhas possui diversas fragilidades, como senhas fracas, reuso de senhas, ataques de força bruta, *phishing* e vazamento de bases de senhas. Devido a isso, a autenticação multifator (MFA, *Multi-Factor Authentication*) tem se tornado cada vez mais popular e é frequentemente obrigatória em muitos serviços online. Segundo Grassi, Garcia e Fenton (2020) e o NIST (2017), a autenticação com dois fatores deve empregar pelo menos um fator que seja resistente a *phishing*, o que não é o caso da senha de uso único (OTP, *One Time Password*) (MICROSOFT, 2022; GRIMES, 2019), apesar de ser a solução mais comum entre provedores de serviços.

Desde 2014, a FIDO *Alliance* vem lançando padrões para aumentar a robustez da autenticação remota de usuários na *web* (MACHANI *et al.*, 2017; SRINIVAS *et al.*, 2017; LINDEMANN *et al.*, 2021; W3C, 2021). Entretanto, somente a partir de 2022 apresentaram o *passkeys* (ALLIANCE, 2022), que busca resolver os problemas de usabilidade para garantir sua adoção em massa, objetivando que os usuários não dependam mais de senhas para autenticação remota.

A revisão anterior deste documento destacava também a tendência de iniciativas relacionadas a Identidade Digital Descentralizadas (IDDs), muitas das quais usando *blockchain* por suas propriedades de descentralização, imutabilidade e transparência. Credenciais Verificáveis (VC, *Verifiable Credentials*) e Identificadores Descentralizados (DID, *Decentralized Identifier*), apontados na revisão anterior, são as tecnologias chave para identidades descentralizadas que se tornaram recomendações da W3C em 2022 e continuam em evidência, sem necessariamente implicar na utilização de *blockchain* para sua operacionalização.

Com relação à atribuição de identidades à componentes de software, podemos destacar o crescimento de ataques na cadeia de suprimento (*software supply chain*), chegando a um crescimento anual médio de 742% nos últimos três anos (SONATYPE, 2023). *Supply-chain Levels for Software Artifacts* (SLSA) é um arcabouço para a avaliação da segurança na cadeia de fornecimento de software. Esse arcabouço define termos e requisitos para atribuição de níveis de segurança. Em Abril de 2023 foi lançada a versão 1.0, que inclui definições estáveis para os níveis de 1 a 3 de segurança. Alguns gerenciadores de pacotes, como o NPM[3], já estão avaliando a integração com mecanismos de proveniência, permitindo que um pacote publicado possa ser vinculado ao código fonte e ao processo de compilação que o produziu. Desta forma, uma identidade a ser atribuída para um componente de software poderia também ser condicionada à evidências de integridade da cadeia de suprimento deste componente.

Considerando a abrangência do *eduroam* atualmente, presente em mais de 100 países ao redor do mundo, e seu avanço contínuo de cobertura para acadêmicos e pesquisadores, podemos citar grandes evoluções no panorama atual, o Hotspot2.0, o Passpoint, e o consórcio OpenRoaming. Podemos considerar o Passpoint e o Hotspot 2.0 como um padrão de associação à rede sem fio que permite que os dispositivos se conectem automaticamente a redes Wi-Fi parceiras. Esses protocolos permitem que a autenticação seja contínua e transparente, através da descoberta de rede,

[3] https://github.com/npm/rfcs/blob/main/accepted/0049-link-packages-to-source-and-build.md

e auxiliando na extensão da cobertura. No cenário Passpoint, o usuário *eduroam* pode se conectar a uma rede Wi-Fi de outro provedor de serviço de acesso à Internet, mesmo que seu nome de rede seja diferente. O suporte a esta tecnologia já está disponível em versão preliminar em parte do consórcio *eduroam*, como pode ser visto em Winter (2022).

Destacamos que, enquanto o Passpoint está focado em *roaming* local e parcerias de rede direta entre provedores, *e.g., eduroam* e um provedor Wi-Fi *XYZ*, o OpenRoaming[4] tem como alvo uma área geográfica mais ampla. No OpenRoaming são utilizados conceitos próximos ao *eduroam*, uma vez que diretórios federados das diversas empresas parceiras do consórcio permitem que o usuário seja autenticado localmente em seu provedor de identidades. OpenRoaming e Passpoint trabalham em conjunto e têm o suporte para a expansão do *eduroam* no ambiente Wi-Fi, possibilitando um roaming diferente do tradicionalmente utilizado por redes puramente "*eduroam*", mas que integram academia e mercado, expandindo ainda mais a sua cobertura. O consórcio *eduroam* global aderiu ao OpenRoaming em 2020[5], e atualmente está em avaliação e implantação em alguns ambientes[6].

Sendo assim, é interessante adquirir conhecimento, avaliar e propor a utilização da Gestão de Identidade em redes móveis de nova geração, como o 5G. Esta tecnologia se apoia em uma arquitetura baseada em serviços, que oferece suporte à *software* para componentes antes monolíticos e proprietários. Um tópico de relevância é verificar a viabilidade da autenticação e autorização com bases de usuários existentes. O cenário que se destaca nesse ponto é a integração eduroam e 5G, algo que já está sendo trabalhado em algumas iniciativas em outras NRENs[7] e projetos de pesquisa internacionais[8]. Essa integração possibilita diversos desdobramentos, desde a expansão do sinal de cobertura da rede até benefícios ao usuário eduroam em redes móveis 5G parceiras. Alguns caminhos nestes cenários são possíveis, desde a criação de uma rede privada 5G com autenticação eduroam, onde a ampliação da cobertura depende da colocação de equipamentos próprios, e os benefícios são todos aqueles voltados aos clientes que utilizam essa nova tecnologia, como ampliação da cobertura, baixa latência, alta disponibilidade e largura de banda.

Outro ponto possível é a parceria em consórcios para autenticação por meio de redes públicas 5G, onde o usuário, identificado como parte do consórcio eduroam, teria benefícios associados ao seu perfil acadêmico, como descontos em franquia, por exemplo, além de ampliar significativamente a cobertura do serviço eduroam. A utilização do eduroam como uma das bases de usuário 5G viabiliza ainda uma possível expansão da RNP como uma Operadora Virtual de Rede Móvel (MVNO, *Mobile Virtual Network Operator*) no futuro. Exemplos de cenários que se beneficiariam dessa integração em um rede pública 5G, ou por meio de uma MVNO, seriam de projetos como o Internet Brasil[9], no qual a RNP é executora. No cenário de redes privadas 5G, os benefícios podem ser ilustrados quando da utilização em campus acadêmicos ou centros de pesquisa com grandes áreas de extensão.

Por fim, ressaltamos a importância da gestão de identidade federada e de acesso às infraestruturas de pesquisa[10], normalmente ligadas a projetos científicos de grande porte. Esses projetos geralmente envolvem colaborações entre pesquisadores e instituições de diferentes organizações e países. Essas colaborações formam Organizações Virtuais (OVs), Organizações colaborativas ou times virtuais, cujo ciclo de vida é em geral bem mais dinâmico que o de organizações físicas. O crescimento das federações acadêmicas em nível nacional e internacional provou ser um modelo de sucesso para aumentar de forma eficiente a colaboração científica. No entanto, o serviço interfederado *eduGAIN* não foi projetado para ambientes abertos e dinâmicos que os membros de uma OV necessitam. Os membros das OV precisam gerenciar e acessar infraestruturas de pesquisas e ainda compartilhar

[4] https://wballiance.com/openroaming/
[5] https://eduroam.org/eduroam-is-proud-to-be-a-founding-member-of-the-wireless-broadband-alliance...
[6] https://wiki.geant.org/pages/viewpage.action?pageId=133763844
[7] https://beta.jisc.ac.uk/innovation/projects/edubox-delivering-eduroam-through-4g-and-5g-cellular-connectivity...
[8] https://www.fudge-5g.eu/en/use-cases/5g-eduroam
[9] https://www.gov.br/mcom/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e...
[10] Infraestruturas de pesquisa são instalações físicas ou virtuais que fornecem à comunidade científica insumos, equipamentos e serviços para realizar atividades de pesquisa e desenvolvimento experimental (P&D) e fomentar a inovação.

recursos com base em suas funções nessas colaborações. Diante da diversidade de mecanismos de autenticação e autorização destas infraestruturas, é comum que pesquisadores precisem gerenciar diversas credenciais de acesso e usá-las em sistemas de controle de acesso de forma desarticulada, gerando assim uma dificuldade para colaborações em e-science.

Desde que foi lançado, o modelo de arquitetura do projeto *Authentication and Authorisation for Research and Collaboration* (AARC)[11] é fortemente recomendado pela *Research and Education FEDerations group* (REFEDS) e, baseada neste modelo, a GÉANT desenvolveu o serviço eduTEAMS[12], o qual expande a eduGAIN. O eduTEAMS permite que pesquisadores e outros membros da comunidade de pesquisa possam criar e gerenciar times virtuais, utilizando provedores de identidade da eduGAIN e outros provedores de identidades confiáveis. As comunidades de pesquisa podem gerenciar seus usuários, organizá-los em grupos, atribuir papéis a eles e gerenciar de forma centralizada os direitos de acesso aos recursos.

Como a pesquisa não se limita apenas as instituições de pesquisa e universidades, eduTEAMS atende também usuários vindos da indústria ou cientistas que não tenham acesso a eduGAIN, por meio de um *proxy* que integra provedores de logins sociais (p.ex. Google, Facebook), provedor ORCID e outros provedores comerciais. Importante ressaltar que o eduTEAMS é operado pela GEÁNT e, atualmente, oferecido somente para usuários e comunidades de pesquisa na Europa. Outra solução de destaque no cenário internacional e que habilita o acesso as infraestruturas financiadas pela *National Science Foundation* (NSF)[13] é o CILogon. Com base em soluções de código aberto de IAM existentes, como o Shibboleth[14] e COManage[15] desenvolvidos pela Internet2, o CILogon habilita uma plataforma integrada *multi-tenant* de IAM para infraestruturas de pesquisa baseada na arquitetura de referência AARC. A plataforma oferece suporte a várias interfaces de autenticação e autorização e vários fluxos para registro, provisionamento, vinculação de identidade (p.ex. com ORCID) e gerenciamento de grupo (BASNEY *et al.*, 2019).

4 Visão de futuro

Nessa seção são apresentadas as tendências na área de gestão de identidade e de acesso conforme metodologia descrita na Seção 2. As tendências são apresentadas de forma sintética e estão distribuídas pelos três horizontes de acordo com o impacto e oportunidades que poderiam gerar nos serviços atuais ou que permitirão gerar novos negócios ou inovações em produtos disruptivos.

4.1 Primeiro horizonte

Tendências que podem impactar os atuais serviços da RNP no próximo biênio.

4.1.1 Adoção de mecanismo de autenticação sem senha

O FIDO *passkeys* (ALLIANCE, 2022) faz uso de criptografia de chave pública sem necessitar de uma ICP, é resistente a *phishing*, de fácil adoção pelos usuários, pois permite que as chaves criptográficas sejam sincronizadas por todos seus dispositivos (*i.e.* telefones inteligentes, *laptops*), semelhante aos gerenciadores de senhas tradicionais, e a autenticação do usuário, para que possa usar a chave privada, acontece localmente usando o mecanismo de desbloqueio do dispositivo (*i.e.* biometria).

[11] https://aarc-project.eu
[12] https://www.eduteams.org
[13] O programa *Advanced Cyberinfrastructure Coordination Ecosystem: Services & Support*(ACCESS) da NSF habilita o acesso a diferentes infraestruturas de pesquisa nos EUA
[14] https://www.shibboleth.net/
[15] https://www.incommon.org/software/comanage/

Em 2022, Apple[16], Google[17] e Microsoft[18] iniciaram o suporte[19] a *passkeys* e atualmente diversos serviços comerciais já permitem a autenticação sem senha usando FIDO *passkeys*. Em 2021 a REFEDS definiu os requisitos para uma base comum de confiança para participantes das federações acadêmicas (AXELSSON; BUXEY, 2021) e o *MFA Profile* (REFEDS, 2017) está sendo revisado[20].

- Soluções que realizam autenticação remota de usuários, como os IdPs da CAFe, devem oferecer suporte a *passkeys* de forma que possam ser usadas como o único ou como segundo fator de autenticação.

4.1.2 Arquitetura de confiança zero e integração com soluções de nuvem

Adoção de serviços de nuvem e da migração da força de trabalho para fora dos limites físicos das organizações requer uma abordagem de gestão de identidade e acesso em que a premissa é de que nenhuma das partes é confiável.

- A gestão de identidade e de acesso é o ponto crucial para o sucesso da estratégia de confiança zero. Os mecanismos de autenticação e controle de acesso devem fazer uso de soluções de análise de risco e confiança de forma de dinâmica e contínua;
- Gestão de identidades de usuários com privilégios administrativos em diferentes soluções de nuvem. Garantir que nessas contas os mecanismos robustos de autenticação sejam obrigatórios, além da facilidade de propagação e revogação de direitos de forma granular e automática, por meio de mecanismos de análise dinâmica de riscos.

4.1.3 Ecossistema para identidade descentralizada

O ecossistema para identidade descentralizada engloba tecnologias como VCs e DIDs e também aplicações comumente chamadas de carteiras digitais, utilizadas para, entre outras coisas, armazenar e apresentar tais credenciais. O modelo de dados para VCs definidas pela recomendação da W3C (W3C, 2022) são amplamente citados, mas existem outras propostas de modelo de dados, como a ISO/IEC 18013-5 mDL[21]. Também há diversos escopos para essa descentralização, que podem ser da perspectiva de localização, do próprio usuário trazer seu identificador, da capacidade do usuário apresentar credenciais ao verificador sem contatar o provedor de identidade, e da perspectiva de controle do ecossistema (YASUDA *et al.*, 2022).

A Regulamentação *Electronic IDentification, Authentication and trust Services 2* (eIDAS2), publicada em 2021, estende a regulamentação original (REGULAMENTO..., 2014), e propõe um arcabouço legal e técnico para implementação de carteira de identidade digital que estará sob controle dos cidadãos através do uso de uma Carteira de Identidade Digital Europeia (EDIW, *European Digital Identity Wallet*). O projeto *Digital Credentials for Europe* (DC4EU)[22] busca usar o arcabouço de confiança do eIDAS2 nas áreas de educação e seguridade social, como para emissão de credenciais educacionais ou qualificações profissionais na área da educação.

- Permitir que soluções que realizam autenticação remota de usuários, como os IdPs da CAFe, ofereçam suporte a emissão de VCs. SPs devem ser capazes de verificarem essas apresentações de credenciais sem necessidade de contato com os IdPs;

[16] https://developer.apple.com/passkeys
[17] https://developers.google.com/identity/passkeys
[18] https://www.microsoft.com/en-us/security/blog/2022/05/05/this-world-password-day-consider-ditching-passwords...
[19] https://passkeys.dev/device-support
[20] https://wiki.refeds.org/display/GROUPS/MFA+Subgroup
[21] https://www.iso.org/standard/69084.html
[22] https://www.dc4eu.eu

- Acompanhar os padrões legais e técnicos para carteiras de identidades digitais descentralizadas com potencial de consolidação para criar um ecossistema de uso na academia e indústria;
- Prover *testbeds* para promover a experimentação e avaliação de diferentes soluções tecnológicas para gestão de identidades descentralizadas e para incentivar o desenvolvimento e avaliação de aplicações ou serviços que façam uso das VCs.

4.1.4 Certificados de assinatura única

O certificado de assinatura única (MAYR; SCHARDONG; CUSTÓDIO, 2022) é um certificado digital associado a um único documento. Baseia-se na premissa de que um IdP autentica o usuário e fornece ao assinador os atributos deste usuário, que então são usados para criar um certificado digital associado ao documento que o usuário está assinando. Este conceito permite a criação de certificados que não são revogados, pois os atributos são sempre atuais e a chave privada é destruída após seu primeiro e único uso. Desta forma, remove-se a necessidade de gerir listas de certificados revogados em uma ICP, bem como permite que assinadores não solicitem senha/PIN de desbloqueio de certificado em nuvem, simplificando as interações com os usuários.

- Certificados pessoais ICPEdu carecem de serviços que alavanquem seu uso. Soluções *web* de assinaturas digitais de documentos requerem que o certificado, bem como o *PIN code*, sejam fornecidos pelo usuário. Certificados de assinatura única, combinado com um serviço de assinatura digital provido pelo emissor dos certificados ICPEdu, mitigam as fragilidades das soluções atuais que fazem uso desses certificados.

4.1.5 O *eduroam*, suporte ao Hotspot2.0/Passpoint e integração ao OpenRoaming

O suporte ao Hotspot 2.0/Passpoint é uma realidade na comunidade *eduroam*, e tende a ser adotada em maior escala pelas federações acadêmicas. Desta forma, é importante a RNP procurar alinhamento com outras federações acadêmicas que têm demonstrado *expertise* no assunto, a fim realizar as etapas necessárias para utilização da tecnologia e o ingresso no OpenRoaming. Como destacado neste documento, a inclusão do suporte a essa tecnologia pelo eduroam no Brasil permitirá a ampliação da abrangência da cobertura do serviço e benefícios aos usuários.

- Identificar os requisitos de tecnologias de equipamentos associados ao Hotspot2.0/Passpoint e testes;
- Criar corpo técnico capacitado para configuração da nova tecnologia através de contato com o padrão e integração com a rede *eduroam* no Brasil;
- Criar ambiente para validação da integração *eduroam* com Hotspot2.0/Passpoint e OpenRoaming;
- Avaliar e implementar o suporte para a tecnologia na federação do Brasil.

4.2 Segundo horizonte

Tendências que podem resultar em novos produtos ou serviços que possam explorados dentro do intervalo de 2 a 3 anos.

4.2.1 Automação e Inteligência Artificial

Soluções para a gestão de identidades combinada com inteligência artificial generativa, adequada para detecção e resposta a ataques de personificação como os baseados em *deep fakes*.

- Automatização de processos para criação de contas e autenticação, mitigando personificação e garantindo uma experiência de uso personalizada e segura com base no contexto e comportamento do usuário;
- Manutenção de contas que estejam sem uso por um longo período ou que possam acumular um grande nível de privilégios.

4.2.2 Integração do *eduroam* com redes 5G

A integração à redes móveis 5G e o *eduroam* é um tópico extremamente relevante. Além de aumentar ainda mais a possibilidade do incremento da cobertura da rede de acesso *eduroam*, há outros benefícios transversais em unir academia e redes móveis, como já exposto neste documento.

- Investigação e desenvolvimento de soluções para redes móveis 5G com autenticação federada baseada no *eduroam*;
- Validar ou propor modelos de autenticação que sejam suportados pelo *eduroam* e pelo ambiente 5G;
- Propor soluções, políticas e diretrizes relacionados ao *eduroam* em ambiente cooperativo da academia com a indústria, principalmente empresas de telecomunicações.

4.2.3 Atribuição de identidades de software

Componentes de software também precisam de identidades para acessar sistemas e serviços. A geração dessas identidades exige uma verificação e deve considerar não segredos embutidos no código ou arquivos de configuração, mas sim propriedades do próprio software e do ambiente onde ele executa.

- Automatizar a geração das identidades para componentes software de modo a condicionar a entrega destas identidades as propriedades do código e do ambiente onde ele está sendo executado;
- Criar sistemas de geração de imagens de contêineres ou máquinas virtuais com mecanismos de proveniência alinhados com o arcabouço SLSA, utilizando estas informações de proveniência no processo de provisionamento de identidades;
- Prover ambientes de execução que permitam a derivação de propriedades confiáveis sobre o software e a base de confiança. Por exemplo, máquinas virtuais com suporte a Intel SGX[23], AMD SEV-SNP[24] ou Intel TDX[25].

[23] https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html
[24] https://www.amd.com/en/processors/amd-secure-encrypted-virtualization
[25] https://www.intel.com/content/www/us/en/developer/articles/technical/intel-trust-domain-extensions.html

4.2.4 ICPEdu com suporte a algoritmos pós-quânticos

Considerando que temos grandes avanços na computação quântica, e estes têm sido anunciados com grande frequência, tanto RSA como as Curvas Elípticas perderão a credibilidade assim que um computador quântico prático seja anunciado. Há muitas discussões na comunidade internacional sugerindo que não se gaste tempo e esforço para a transição para Curvas Elípticas, já que a criptografia pós-quântica está cada vez mais próxima de nós, tendo o *National Institute of Standards and Technology* (NIST) afunilado a escolha a poucos algoritmos agora.

Muito tem se falado em certificados híbridos, os quais têm chaves clássicas (RSA ou Curvas Elípticas) e pós-quânticas para dar suporte a essa transição para um mundo seguro após o advento do computador quântico prático. Existe um grande desafio para implementar-se tal solução, mas grandes centros de pesquisa estão avançando e fabricantes de *hardware* seguro (como a Kryptus) estão desenvolvendo novos *Hardware Security Module* (HSM) com suporte a certificados híbridos. Desta forma recomenda-se que a RNP encaminhe a discussão acerca desse problema para que a solução esteja disponível com a tempestividade requerida.

- Buscar familiarização com as novas bibliotecas com suporte à criptografia de chave pública convencional e pós-quântica (criptografia híbrida), como as providas pelo projeto *Open Quantum Safe*[26];
- Considerar a viabilidade da criação de projeto piloto, em parceria com fornecedoras de HSM baseados em criptografia híbrida, para emissão de certificados digitais híbridos ICPEdu pessoal por meio da ferramenta OQS-OpenSSL, bem como entender quais aplicações estão aptas para usar tais certificados;
- Promover ações educativas para os participantes do sistema RNP a respeito da ameaça quântica e da necessidade de migrar aplicações para algoritmos resistentes a atacantes quânticos.

4.2.5 Modelo de confiança para credenciais verificáveis

O ecossistema de VCs prevê que as credenciais emitidas possam ser verificadas e que o verificador confie no emissor. Para que essa verificação seja automatizada e escalável, de acordo com a W3C (w3c, 2022), é necessária a manutenção de uma Base de Dados Verificável (*Verifiable Data Registry*), a qual permite a criação, verificação, atualização e desativação de DID e documentos DID, além da manutenção dos esquemas das VCs. Para essa base, apesar de geralmente ser considerado o uso de livro razão distribuído (normalmente *blockchains*), também podem ser considerado o uso de redes P2P, sistemas de arquivos distribuído, etc.

- Verificar como a RNP, possivelmente por meio da CAFe, poderia ser usada como uma Base de Dados Verificável e ofertar uma API comum e única que possa ser usada para verificar credenciais emitidas pelas instituições participantes da federação.

4.2.6 Gestão de identidade e de acesso para ambientes colaborativos de *e-science*

Para viabilizar pesquisas colaborativas nacionais e internacionais (Organizações Virtuais - OVs) e o acesso seguro às infraestruturas de pesquisas[27], o uso de infraestruturas de autenticação e autorização interoperáveis e flexíveis são essenciais. Existem problemas a serem resolvidos quando

[26] https://openquantumsafe.org/applications/tls.html

[27] São exemplos de infraestruturas de pesquisa: grandes instalações de pesquisa, laboratórios, plantas piloto, biotérios, salas limpas, redes de informática de alto desempenho, bases de dados, coleções, observatórios, telescópios, navios de pesquisa, reservas e estações experimentais, entre outras.

um usuário precisa colaborar em um ambiente no qual mais de uma federação está envolvida ou quando este não pertence a nenhuma federação. Esta colaboração não deve tratar apenas dos aspectos tecnológicos, mas também das políticas organizacionais. Outro desafio relacionado são os diversos atributos exigidos pelos diferentes provedores de serviços de *e-science*. A decisão de acesso a um serviço em uma OV depende não apenas dos atributos definidos pelo provedor de identidade do usuário, mas também dos atributos definidos na própria OV. A falta de um padrão para expressar o pertencimento a uma OV e os papéis e atributos dos seus membros nas federações acadêmicas e na eduGAIN estreita o potencial dos sistemas federados para pesquisas colaborativas para o acesso às infraestruturas de pesquisa. Em ambientes de compartilhamento de recursos computacionais, como os de supercomputação, muitos usuários demandam acesso de terminal remoto seguro (SSH), devido às facilidades de automação (*scripting*) de processos e *pipelines* de execução. Prover a autenticação federada nesse tipo de ambiente (não Web) ainda precisa de soluções mais flexíveis e com boa experiência para os usuários.

- A oferta pela RNP de um serviço semelhante ao eduTEAMS ou CILogon, que possibilite a criação e gerenciamento das OVs, pode contribuir para criação de times virtuais nas comunidades de pesquisa brasileiras e viabilizar a cooperação internacional;
- Identificar os requisitos comuns para gestão de identidade e de acesso das comunidades de *e-science* brasileiras e suas infraestruturas de pesquisa para alavancar o uso do modelo federado e para desenvolver um serviço de gestão de times aderente à realidade brasileira, ou seja, que considere também o acesso não Web às infraestruturas de pesquisa.

4.3 Terceiro horizonte

Hipóteses sobre tendências que precisam ser validadas, semeando iniciativas para futuros negócios que possam ser explorados em 5 anos ou mais.

4.3.1 Identidade baseada em consentimento

Embora o modelo SSI ofereça várias vantagens em relação aos modelos de identidade anteriores, ele ainda enfrenta desafios e limitações. Ele exige que os usuários gerenciem suas credenciais, o que pode ser um desafio para indivíduos com conhecimento técnico limitado. Os usuários podem precisar de ajuda para entender todas as implicações do que aceitam compartilhar e são propensos a SPs abusivos que podem exigir informações excessivas.

No modelo de *identidade digital baseada em consentimento* o usuário fornece e revoga no passado, presente ou futuro o seu consentimento sobre o uso de sua identidade digital para quem gerencia sua identidade digital. Esse modelo permite aos usuários definirem regras que norteiam a decisão de seus representantes sobre onde os programas que operam sobre os dados do usuário podem ser executados. Por exemplo, um usuário pode não confiar em nenhum SP para receber sua data de nascimento, mas pode concordar em executar o algoritmo do SP em seu ambiente computacional de confiança para garantir que o SP não possa acessar sua data de nascimento. Nesse modelo, tanto o usuário (através de seus representantes) quanto os SPs possuem seus próprios dispositivos de computação, que podem ser usados de forma independente ou em conjunto para executar algoritmos que utilizam os dados do usuário.

- Fomentar PD&I de projetos que investiguem a viabilidade e as implicações técnicas e legais de dispositivos decidirem e executarem o compartilhamento de informações de usuários, bem como as implicações técnicas e legais de usuários explicitamente não consentirem a respeito de decisões já tomadas por seus representantes;

- Fomentar PD&I de projetos que envolvam carteiras digitais inteligentes capazes de tomarem decisões de forma autônoma com base em conjuntos de regras explícitas ou implícitas pelo dono da identidade.

4.3.2 Atribuição de identidades de software baseado em SLSA

O uso de informações da cadeia de suprimento de software ajuda a mitigar ameaças de comprometimento de componentes de software e a detectar componentes que usam dependências vulneráveis. *Supply-chain Levels for Software Artifacts* (SLSA) parece estar se tornando um padrão popular para especificação do processo de construção de software. Atualmente, a versão 1 do SLSA foca na especificação do sistema de geração ou compilação de artefatos (*build*) e em três níveis de segurança. Futuras versões do padrão devem considerar aspectos adicionais, como fatores relacionados com a gerência do código fonte, e níveis mais altos de segurança para a geração dos componentes (por exemplo, compilações reprodutíveis).

- Fomentar PD&I de projetos que investiguem o uso de SLSA e mecanismos de proveniência de software para aumentar a segurança no processo de geração de imagens de serviços (gerando *builds* com proveniência, lista de dependências, e assinaturas);
- Fomentar PD&I para a geração de serviços ou ferramentas de *trusted build*. Por exemplo, de modo que a RNP hospede um *pipeline* de integração contínua para geração de imagens confiáveis para serviços dos usuários da RNP. Neste caso, repositórios de projetos dentro ou fora da RNP poderiam ser beneficiado em ter uma imagem de contêiner gerada (e assinada) por um *pipeline* que segue boas práticas de geração e proveniência.

Referências

ALLAN, Ant. *Hype Cycle for Identity and Access Management Technologies*. Gartner, jul. 2020. Disponível em: https://www.gartner.com/en/documents/3987655/hype-cycle-for-identity-and-access-management-technologi. Acesso em: 5 maio 2021.

ALLIANCE, FIDO. *How FIDO address a full range of use cases*. Mar. 2022. Disponível em: https://fidoalliance.org/white-paper-multi-device-fido-credentials. Acesso em: 13 abr. 2023.

AXELSSON, Pal; BUXEY, Alan. *REFEDS Identity Federation Baseline Expectations*. Zenodo, abr. 2021. DOI: 10.5281/zenodo.4672083. Disponível em: https://doi.org/10.5281/zenodo.4672083.

BAGHAI, M; COLEY, S; WHITE, D. The Alchemy of Growth: Practical Insights for Building the Enduring Enterprise. McKinsey & Company. *Inc. United States. First Paperback Printing*, 2000.

BASNEY, Jim *et al.* CILogon: Enabling federated identity and access management for scientific collaborations. English (US). *Proceedings of Science*, Sissa Medialab Srl, v. 351, 2019. ISSN 1824-8039. DOI: 10.22323/1.351.0031.

BRITO, Andrey Elísio *et al. Relatório de visão de futuro em Gestão de Identidade*. Jul. 2021. Publicações técnicas do Comitê Técnico de Gestão de Identidade (CT-GId) da RNP. Disponível em: https://wiki.rnp.br/download/attachments/106895177/CT-GId-Vis%5C%C3%5C%A3o-de-Futuro-2021-07.pdf.

GRASSI, Paul; GARCIA, Michael; FENTON, James. *NIST Special Publication 800-63-3 Digital Identity Guidelines*. 2020. https://doi.org/10.6028/NIST.SP.800-63-3.

GRIMES, Roger. *12+ ways to hack multi-factor authentication*. KnowBe4, 2019. Disponível em: https://info.knowbe4.com/12-way-to-hack-two-factor-authentication. Acesso em: 3 ago. 2022.

ITU. *NGN identity management framework*. International Telecommunication Union (ITU), 2009. Recommendation Y.2720. Disponível em: https://www.itu.int/rec/T-REC-Y.2720-200901-I. Acesso em: 5 maio 2021.

LINDEMANN, R. *et al. Client to Authenticator Protocol "(CTAP)"*. Jun. 2021. Disponível em: https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html. Acesso em: 14 abr. 2023.

MACHANI, Salah *et al. FIDO UAF architectural Overview*. Fev. 2017. Disponível em: https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-uaf-overview-v1.1-ps-20170202.pdf.

MAYR, Lucas; SCHARDONG, Frederico; CUSTÓDIO, Ricardo. Simplifying Electronic Document Digital Signatures. *arXiv preprint arXiv:2208.03951*, 2022.

MICROSOFT. *From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud*. Jul. 2022. Disponível em: https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud. Acesso em: 3 ago. 2022.

NIST. *Digital Identity Guidelines: Authentication and Lifecycle Management*. National Institute of Standards e Technology, jun. 2017. NIST Special Publication 800-63B. DOI: https://doi.org/10.6028/NIST.SP.800-63b.

REFEDS. *REFEDS MFA Profile*. Jun. 2017. Disponível em: https://refeds.org/profile/mfa. Acesso em: 14 abr. 2023.

REGULAMENTO (UE) Nº 910/2014 do parlamento europeu e do conselho relativo à identificação eletrônica e aos serviços de confiança para as transações eletrônicas no mercado interno e que revoga a Diretiva 1999/93/CE. *Jornal Oficial da União Europeia*, v. L 257/73, jul. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32014R0910&from=EN. Acesso em: 30 jun. 2021.

SEAMLESSACCESS. *SeamlessAccess enables true Single Sign-On*. Disponível em: https://seamlessaccess.org. Acesso em: 14 abr. 2023.

SONATYPE (ed.). *8th Annual State of the Software Supply Chain*. 2023. Disponível em: https://www.sonatype.com/state-of-the-software-supply-chain/introduction. Acesso em: 4 maio 2023.

SRINIVAS, Sampath *et al. Universal 2nd Factor (U2F) Overview*. Abr. 2017. Disponível em: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.pdf.

TEIXEIRA, Luciene Pires. Prospecção tecnológica: importância, métodos e experiências da Embrapa Cerrados. *EMBRAPA Cerrados*, 2013. ISSN 2176-5081; 317.

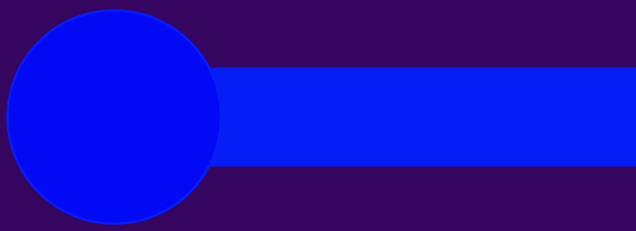
W3C. *Federated Credential Management API*. Mar. 2023. Disponível em: https://fedidcg.github.io/FedCM/. Acesso em: 14 abr. 2023.

W3C. *Verifiable Credentials Data Model 1.1*. Mar. 2022. Disponível em: https://www.w3.org/TR/vc-data-model/. Acesso em: 27 abr. 2023.

W3C. *Web Authentication: An API for accessing Public Key Credentials Level 2*. Mar. 2021. Disponível em: https://www.w3.org/TR/webauthn. Acesso em: 14 abr. 2023.

WINTER, Stefan. *Passpoint / Hotspot 2.0*. 2022. Disponível em: https://wiki.geant.org/pages/viewpage.action?pageId=121346191.

YASUDA, Kristina *et al.* (ed.). *OpenID for Verifiable Credentials*. 2022. Disponível em: https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf. Acesso em: 28 abr. 2023.



RNP

MINISTÉRIO DA **CULTURA**

MINISTÉRIO DA **DEFESA**

MINISTÉRIO DA **SAÚDE**

MINISTÉRIO DAS **COMUNICAÇÕES**

MINISTÉRIO DA **EDUCAÇÃO**

MINISTÉRIO DA **CIÊNCIA, TECNOLOGIA E INOVAÇÃO**

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO