RNP Educação, Pesquisa e Inovação em Rede

Relatório de Visão de Futuro

Comitê Técnico de Gestão de Identidade

fevereiro de 2025

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

Fiterlinge Sousa, Dr. (RNP)

Gerente da Secretaria de Apoio à Prospecção Tecnológica

José Ferreira de Rezende, Dr. (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)
Shirlei Aparecida de Chaves, Ma. (IFSC)
Andrey Elísio Monteiro Brito, Dr. (UFCG)
Caciano Machado, Dr. (UFRGS)
Frederico Schardong, Dr. (IFRS)
Edelberto Franco Silva, Dr. (UFJF)
Ioram Schechtman Sette, Dr.
Carla Merkle Westphall, Dra. (UFSC)

SUMÁRIO

Lista de abreviaturas e siglas

AARC *Authentication and Authorisation for Research and Collaboration*.

ANP provedores de acesso à rede (*Access Network Provider*).

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*.

DCC Digital Credentials Consortium.

DFP impressão digital do dispositivo (*Device Fingerprinting*).

DID Identificador Descentralizado (*Decentralized Identifier*).

EAP *Extensible Authentication Protocol*.

EBSI *European Blockchain Services Infrastructure*.

Eduroam *Education Roaming*.

EOSC *European Open Science Cloud*.

EUDI *European Digital Identity Wallet*.

FAIR *Findability, Accessibility, Interoperability, and Reusability*.

FedCM *Federated Credential Management API*.

FIM4R *Federated Identity Management for Research*.

FNDCT Fundo Nacional de Desenvolvimento Científico e Tecnológico.

GId Gestão de Identidades.

GIdLab Laboratório para Experimentação em Gestão de Identidade.

HSM *Hardware Security Module*.

IA Inteligência Artificial.

IAA Infraestrutura de Autenticação e de Autorização.

IAM *Identity and Access Management*.

ICPEdu Infraestrutura de Chaves Públicas para Ensino e Pesquisa.

IDD Identidade Digital Descentralizada.

IdP Provedor de Identidade (*Identity Provider*).

IETF *Internet Engineering Task Force*.

IMEI *International Mobile Equipment Identity*.

JSON *JavaScript Object Notation*.

MDL *Mobile Driver License*.

MFA *Multi-Factor Authentication*.

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

NREN *National Research and Education Network*.

OIDC *OpenID Connect*.

OV Organização Virtual.

OWASP *Open Worldwide Application Security Project*.

PD&I Pesquisa, Desenvolvimento e Inovação.

PGId Programa de Gestão de Identidade.

PoC Prova de Conceito (*Proof of Concept*).

PUF *Physical Unclonable Function*.

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.

SIRTFI *Security Incident Response Trust Framework for Federated Identity*.

SP Provedor de Serviço (*Service Provider*).

SSI Identidade Auto-Soberana (*Self-Sovereign Identity*).

TCB Base de Computação Confiável (*Trusted Computing Base*).

TEE *Trusted Execution Environment*.

TPM *Trusted Plataform Module*.

VC Credenciais Verificáveis (*Verifiable Credentials*).

VP Apresentação Verificável (*Verifiable Presentation*).

WGID Workshop de Gestão de Identidades Digitais.

WIMSE *Workload Identity in Multi System Environments*.

ZKP Prova de Conhecimento Zero (*Zero-Knowledge Proof*).

1 Introdução

A Gestão de Identidades (GId), conforme apresentada em ITU (2009), ou *Identity and Access Management* (IAM), como descrito em Allan (2020), refere-se a um conjunto de processos e tecnologias que visam gerenciar identidades de pessoas, serviços e objetos, além de estabelecer o relacionamento e a confiança entre essas entidades. Assim, a GId pode ser utilizada para garantir a identidade de uma entidade e para prover mecanismos de autenticação, autorização, responsabilização e auditoria.

A migração de muitos postos de trabalho para o ambiente remoto ampliou os perímetros de segurança das organizações, tornando a GId um componente ainda mais crucial para garantir a segurança e a autenticidade dos usuários. Esse cenário ganhou complexidade adicional com o crescimento de tecnologias de inteligência artificial cada vez mais sofisticadas, que vêm sendo utilizadas tanto para fortalecer mecanismos de segurança quanto para sofisticar ataques cibernéticos. Além disso, a descentralização da identidade digital é tendência para mitigar os riscos associados à dependência de sistemas centralizados, promovendo um modelo que prioriza a proteção de dados pessoais e a autonomia dos usuários. Esses fatores reafirmam a importância estratégica da GId em um cenário tecnológico cada vez mais dinâmico, exigindo que academia, empresas e governos permaneçam atualizados e invistam continuamente em prontidão tecnológica e inovação em GId.

A Rede Nacional de Ensino e Pesquisa (RNP) é uma organização cuja missão é promover o uso inovador de redes avançadas e fomentar a colaboração entre instituições de ensino e pesquisa no Brasil. A RNP disponibiliza à comunidade acadêmica e científica brasileira uma série de serviços avançados e dentro da área de gestão de identidade e de acesso, destacam-se os seguintes:

- **Comunidade Acadêmica Federada (CAFe)**: serviço de federação de identidades que permite o acesso a serviços e recursos digitais de forma segura e simplificada. A CAFe é utilizada por diversas instituições de ensino e pesquisa no Brasil, promovendo a colaboração acadêmica e científica, bem como a mobilidade de usuários entre diferentes instituições (RNP, 2024b);
- **Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu)**: solução de certificados digitais que assegura a autenticidade, integridade e confidencialidade de informações trocadas entre instituições de ensino e pesquisa. O ICPEdu é utilizado para a assinatura digital de documentos, a autenticação de servidores e a proteção de comunicações entre instituições (RNP, 2024d);
- ***Education Roaming* (eduroam)**: serviço de *roaming* acadêmico que permite que usuários de instituições de ensino e pesquisa acessem a rede sem fio de outras instituições, utilizando as credenciais de acesso de sua instituição de origem. O eduroam é utilizado em mais de 100 países, promovendo a mobilidade de usuários e a colaboração internacional (RNP, 2024c).

Além disso, o Comitê Técnico de Gestão de Identidade (CT-GId) (RNP, 2024a), estabelecido pela RNP em 2010, atua como um fórum de discussão aberto, com a missão de prospectar soluções inovadoras para gestão de identidade, fundamentadas em pesquisas de médio e longo prazo, e promover a conscientização e a cultura no uso de identidades digitais no Brasil. A prospecção visa tornar-se uma referência para apoiar as atividades do Comitê Assessor de Gestão de Identidade (CA-GId) da RNP, gerando, assim, impacto direto na organização e em suas instituições usuárias. Entre as principais ações e projetos conduzidos pelo CT-GId, destacam-se:

- **Laboratório para Experimentação em Gestão de Identidade (GIdLab)**: 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 (RNP, 2024e);

- **Programa de Gestão de Identidade (PGId)**: fomenta projetos de PD&I na área de GId, com o objetivo de desenvolver soluções inovadoras e promover a colaboração entre pesquisadores e instituições;
- **Reuniões técnicas e *workshops***: realização de reuniões periódicas para discutir temas relevantes na área de GId, com apresentações conduzidas por membros ou convidados externos; 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), para promover o intercâmbio de conhecimento e experiências entre os participantes daquele evento;
- **Documentação técnica**: produção de documentos técnicos como recomendações, estudos e relatórios, que fornecem diretrizes e visões de futuro para a área de GId.

As ações realizadas no CT-GId são colaborativas e voluntárias, abertas à participação de qualquer pessoa vinculada a uma instituição de ensino ou pesquisa brasileira e que atue na área de gestão de identidade. Periodicamente, convites e divulgações sobre essas ações são enviados para as principais listas de e-mail da Sociedade Brasileira de Computação (SBC), de modo que os membros dessas comunidades possam conhecer e integrar o CT-GId.

Escopo

O escopo deste documento é identificar tendências tecnológicas relacionadas à gestão de identidade e de acesso que possam ser exploradas em atividades de pesquisa e desenvolvimento no curto, médio ou longo prazo. O público-alvo deste documento é o sistema RNP e assim, foram consideradas tanto as tendências emergentes na academia quanto na indústria que possam promover melhorias nos serviços oferecidos pela RNP, além de possibilitar a criação de novos serviços ou modelos de negócio. Vale destacar que este documento não tem como objetivo ser uma revisão abrangente da literatura nem uma análise completa de todos os tópicos relacionados à gestão de identidade.

2 Metodologia

Esse documento consiste em uma revisão da visão de futuro da gestão de identidade e de acesso, elaborada pelo CT-GId em 2023 (MELLO; BRITO et al., 2023) 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).

Todos os membros do CT-GId foram consultados sobre seu interesse e disponibilidade para contribuir na elaboração deste documento. Assim, este documento de visão de futuro é resultado do esforço coletivo de um subconjunto dos integrantes do CT-GId, refletindo as perspectivas de diferentes especialistas. No entanto, as opiniões apresentadas aqui não representam necessariamente as visões de suas instituições ou da própria RNP. Esse grupo de especialistas pode ser considerado uma amostra representativa dos pesquisadores que atuam na área de gestão de identidade e de acesso no Brasil.

Durante o WGID, realizado em conjunto com o SBSeg[1] de 2024, em São José dos Campos - SP, ocorreu uma reunião presencial com a participação de 30 pessoas. Nessa ocasião, foram discutidas

[1] https://sbseg2024.ita.br

as principais soluções, ameaças e oportunidades relacionadas aos serviços de gestão de identidade e acesso oferecidos pela RNP. Também foram debatidas as tendências emergentes na área de gestão de identidade e acesso, com foco em seu impacto sobre os serviços atuais e no potencial de criação de novos negócios ou inovações disruptivas.

Com o objetivo de aprofundar a análise e tornar este documento mais substancial e relevante, em 2024 a RNP lançou uma chamada pública para trabalhos de prospecção tecnológica destinados ao CT-GId e ao recém-criado Comitê Técnico de Cibersegurança. No âmbito do CT-GId, foram financiados três pesquisadores para a elaboração de relatórios de prospecção tecnológica sobre um dos seguintes temas: gestão de identidade e de acesso na nuvem; arquitetura de confiança zero e gestão de identidades para IoT; e integração de gestão de identidade com inteligência artificial e aprendizado de máquina. Os resultados gerados com essa prospecção também foram incorporados no presente documento.

Por fim, as tendências foram organizadas com base no conceito dos Três Horizontes de Inovação, proposto pela McKinsey (BAGHAI; COLEY; WHITE, 2000), que divide o processo de inovação em três estágios distintos: o presente (Horizonte 1); o futuro próximo (Horizonte 2); e as visões disruptivas para um futuro mais distante (Horizonte 3). Nesse conceito, a linha do tempo reflete o ciclo de vida pelo qual um produto ou serviço passa.

No Horizonte 1, encontram-se os produtos que atualmente geram receita para a organização, e os investimentos realizados tendem a proporcionar retorno dentro do mesmo ano. O Horizonte 2 apresenta oportunidades para novos negócios, com produtos ou serviços que podem gerar retorno em um futuro próximo. O Horizonte 3 abrange hipóteses que ainda precisam ser validadas para determinar se vale a pena investir em um determinado produto. Esse horizonte funciona como um espaço de experimentação, focado na busca por inovações, sem uma expectativa imediata de retorno. As ideias experimentadas e validadas podem, em uma futura revisão do documento, ser realocadas para o Horizonte 2, ou até mesmo descartadas, dependendo dos resultados.

Para facilitar a escrita de forma colaborativa e assíncrona, foram utilizadas ferramentas que permitiram uma interação mais eficiente entre os participantes. Após uma reunião inicial de alinhamento, foi criado um documento compartilhado, no qual cada especialista ficou responsável por redigir uma parte específica, além de acompanhar o progresso das atividades conduzidas pelos demais autores. Por fim, uma reunião final foi realizada para alinhar os pontos pendentes e revisar o conteúdo, resultando na entrega do texto consolidado.

3 Panorama

Desde a revisão de 2023 (MELLO; BRITO et al., 2023), a atenção dedicada à gestão de identidade e de acesso tem se intensificado. Esse crescimento decorre de múltiplos fatores, incluindo a migração de serviços para a nuvem, o rigor crescente na conformidade regulatória e os avanços das tecnologias de inteligência artificial e aprendizado de máquina. Grande parte dos aspectos abordados na revisão anterior já vem sendo endereçada pela RNP, tanto na esfera da Pesquisa, Desenvolvimento e Inovação (PD&I) quanto na operação dos serviços, cabendo citar: adoção de mecanismo de autenticação sem senha; ecossistema para identidade descentralizada; e gestão de identidade e de acesso para ambientes colaborativos de e-Ciência.

Na reunião presencial do CT-GId que ocorreu no WGID, foi realizada uma dinâmica para levantar ameaças, oportunidades e tendências em GId para a RNP. Entre as ameaças, evidencia-se a crescente adoção da solução da Conta GOV.BR por instituições acadêmicas e de pesquisa, em detrimento do serviço CAFe, o que reforça a necessidade de comunicar de forma mais efetiva os benefícios do modelo federado. Além disso, a oferta de provedores de serviços por essas instituições configura uma oportunidade para que a RNP expanda seus serviços de autenticação e autorização. Quanto ao serviço ICPEdu, constatou-se que muitas regulamentações governamentais referenciam

unicamente a ICP Brasil, evidenciando a necessidade de esforços para que a ICPEdu seja mais reconhecida como uma opção viável no meio acadêmico.

Na reunião, foram expostos os seguintes temas como tendências emergentes na área de gestão de identidade e de acesso, sendo esses parte integrante deste documento: a aplicação de aprendizado de máquina para aprimorar sistemas de GId; o desenvolvimento de soluções para identidade digital descentralizada; a implementação de credenciais verificáveis; a integração do Eduroam com redes 5G; a autenticação sem senha por meio de chaves de acesso (*passkeys*); a preservação do sigilo de documentos assinados digitalmente por soluções de assinaturas baseadas na *web*; a autenticação federada para aplicações não *web* ou para o consumo de APIs de *Web Services*; bem como a resiliência dos serviços de GId mantidos pela RNP e pelas instituições usuárias.

3.1 Autenticação sem senha

No relatório da Gartner, *Hype Cycle Digital Identity* de 2024 (HARRIS; ALLAN, 2024), é indicado que a autenticação sem senha vem ganhando tração, devido à necessidade de simplificar o processo de autenticação e aumentar a segurança dos sistemas de informação. Consideram que as chaves de acesso (*passkeys*) vinculadas a dispositivos móveis estarão em ampla adoção em menos de dois anos, e as chaves de acesso multidispositivo em menos de cinco anos. As chaves de acesso multidispositivo ainda esbarram na fragmentação dos ecossistemas Apple, Google e Microsoft, uma vez que o sincronismo entre dispositivos de diferentes plataformas ainda é um desafio que precisa ser superado.

Nos documentos de visão de futuro de 2021 e 2023 (MELLO; BRITO et al., 2023; BRITO et al., 2021) foram feitas recomendações sobre a adoção de autenticação sem senha, e a tendência apontada pela Gartner reforça a importância de continuar investindo nessa direção. A RNP já vem trabalhando nesse sentido, com a implementação de autenticação sem senha para o serviço CAFe, por exemplo.

3.2 Identidade descentralizada

Em 2016 Christopher Allen publicou um artigo intitulado *The Path to Self-Sovereign Identity* (ALLEN, 2016), no qual são apresentados os princípios fundamentais da Identidade Auto-Soberana (SSI, *Self-Sovereign Identity*), onde diz que: "*uma identidade auto-soberana é criada, gerenciada e utilizada por um indivíduo. Ela é auto-soberana no sentido de que o indivíduo é o único que a controla. A identidade auto-soberana é descentralizada e não depende de uma autoridade central para ser criada, gerenciada ou utilizada*". Assim, entende-se que o termo SSI está mais relacionado a um conceito do que a uma tecnologia específica.

A Identidade Digital Descentralizada (IDD) é o nome geralmente usado para descrever a tecnologia que viabiliza a implementação da SSI, como *blockchain*, Identificador Descentralizado (DID, *Decentralized Identifier*), Credenciais Verificáveis (VC, *Verifiable Credentials*) e Prova de Conhecimento Zero (ZKP, *Zero-Knowledge Proof*). Segundo Allen (2024), a tecnologia que está sendo empregada na Identidade Digital Descentralizada (IDD) não está permanecendo fiel aos princípios da SSI, como a autonomia, a descentralização e a privacidade.

Segundo Harris e Allan (2024), as Credenciais Verificáveis (VC, *Verifiable Credentials*) devem ser adotadas amplamente até 2026, gerando um benefício que irá transformar a experiência do usuário e a confiança nas transações digitais. Por outro lado, a expectativa com relação à ZKP é baixa, e tornou-se obsoleta antes de atingir o platô de produtividade, conforme a classificação do ciclo de vida de tecnologias da Gartner, mas ainda assim, a ZKP é uma tecnologia promissora com grande valor para a segurança e privacidade dos usuários. Já Hughes (2024) afirma que a única forma das VCs serem adotadas em larga escala é por meio de uma obrigação regulatória, um ajuste no produto ou uma mudança no mercado. A interoperabilidade, uma das principais premissas para a existência das

VCs, ainda não pode ser observada na prática.

Como apresentado em Mello, Brito et al. (2023), o modelo de dados para as VCs (W3C, 2022, 2025b) não é a única iniciativa voltada para a descentralização da identidade digital. O *Mobile Driver License* (mDL) (ISO/IEC, 2021) é um padrão que vem sendo adotado por diversos estados norte-americanos para a emissão de carteiras de motorista digitais, com suporte integrado às carteiras digitais nativas dos dispositivos móveis com iOS e Android.

Uma Apresentação Verificável (VP, *Verifiable Presentation*) (W3C, 2022) é uma estrutura de dados que contém uma ou mais VCs e é assinada pelo detentor da VC. Uma VP pode ser usada por seu detentor como ZKP para provar a posse de uma ou mais VCs para um verificador. No modelo de dados v1.1 (W3C, 2022), e no *draft* do modelo v2.0 (W3C, 2025b), não está previsto como o detentor poderia delegar uma VP para um terceiro. Em Flamini et al. (2025) é proposto um esquema para representar a delegação de uma VP de forma a ser usada no *framework* da arquitetura de referência para *European Digital Identity Wallet* (EUDI), onde também apresentam uma discussão sobre o uso deste esquema no contexto da *European Blockchain Services Infrastructure* (EBSI).

3.3 Modelo fiduciário de gestão de identidade

Embora o modelo IDD ofereça vantagens em relação aos modelos de gestão 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. O Modelo Fiduciário (SCHARDONG; CUSTÓDIO, 2024) pode ser uma alternativa equilibrada entre o controle de dados pessoais, hoje fortemente centralizado em grandes Provedores de Identidade (IdPs, *Identity Provider*), e a autonomia muitas vezes complexa dos modelos de IDD.

O modelo fiduciário propõe uma nova abordagem para a gestão de identidades digitais, na qual um agente de confiança, denominado fiduciário, assume a responsabilidade pela administração desses dados. Esse agente estabelece um vínculo de confiança e obrigações legais e éticas com o indivíduo, garantindo que suas decisões sejam sempre tomadas no melhor interesse do titular dos dados. Esse tipo de relação é amplamente adotado em diferentes domínios, como direito, governança corporativa e gestão de ativos.

Todas as ações do fiduciário devem estar alinhadas com os consentimentos previamente fornecidos pelo usuário. Para garantir essa conformidade, é utilizado um mecanismo chamado Política de Consentimento, que consiste em um conjunto de regras definidas pelo próprio titular sobre como seus dados podem ser coletados, armazenados e compartilhados. Esse sistema permite que o fiduciário selecione as credenciais mais apropriadas para cada situação, respeitando as preferências do indivíduo sobre a sensibilidade de suas informações. Assim, o usuário mantém controle sobre sua identidade digital, podendo definir suas preferências com antecedência ou no momento da interação, caso surjam situações que exijam uma decisão contextualizada.

Embora a introdução de um intermediário na gestão de credenciais possa inicialmente sugerir uma limitação ao controle dos indivíduos sobre seus próprios dados, o propósito do fiduciário é justamente oferecer suporte para aqueles que desejam assistência na proteção de suas informações. A Política de Consentimento permite que os usuários definam com flexibilidade os limites de atuação do fiduciário, garantindo que ele opere conforme suas preferências. Dessa forma, o fiduciário pode desempenhar tanto o papel de uma carteira digital, como no modelo de IDD, quanto atuar como um agente responsável por tomar decisões em nome do titular dos dados, sempre pautado por seus deveres e obrigações.

3.4 Modelo federado e as novas premissas de privacidade dos navegadores

A preocupação com a privacidade dos usuários tem ganhado crescente relevância entre os fabricantes de navegadores. Assim, iniciativas da Apple e da Fundação Mozilla, por exemplo, visam restringir o rastreamento na *web* por meio do bloqueio de *cookies* de terceiros[2,3]. Em contrapartida, embora a Google tenha planejado limitar o uso de *cookies* de terceiros no Chrome, após diversos adiamentos essa medida foi abandonada em 2024, optando por alternativas que protegem a privacidade dos usuários por meio do projeto *Privacy Sandbox*[4].

Dentro desse projeto, destaca-se a adoção da API para navegadores *web* denominada *Federated Credential Management API* (FedCM) (W3C, 2025a), que viabiliza a autenticação federada dos usuários sem a dependência de primitivas de baixo nível, como *cookies*, redirecionamentos HTTP e parâmetros de URL. Em 2023 (MELLO; BRITO et al., 2023) destacamos que o FedCM ainda estava em fase de desenvolvimento, mas já apresentava um grande potencial para aprimorar a experiência do usuário final nos processos de autenticação e uso de serviços. A Fundação Mozilla colocou o FedCM como tecnologia experimental no Firefox, mas ainda não está disponível para uso geral.

A FedCM constitui, assim, uma alternativa moderna e segura de autenticação federada, favorecendo a integração dos serviços de autenticação em aplicações *web* e proporcionando uma experiência mais transparente e segura para o usuário. É importante acompanhar o desenvolvimento dessa tecnologia e avaliar sua aplicabilidade e os impactos que poderá gerar na operação dos serviços de gestão de identidade da RNP.

3.5 Redes de e-Ciência

Segundo FAPESP (2015), a e-Ciência promove a colaboração entre pesquisadores de diferentes áreas do conhecimento e, por meio do uso intensivo de computação e de grandes volumes de dados, busca acelerar a descoberta científica e a inovação. Esse modelo exige a atuação de cientistas da computação no suporte a pesquisadores de outras áreas, fomentando, consequentemente, inovações na própria computação.

Em março de 2024, a RNP lançou uma iniciativa, financiada pelo Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT), para o estabelecimento da rede e-Ciência brasileira. Inicialmente, a proposta consiste na implementação de uma rede de conectividade física para estabelecer uma infraestrutura segura e de alto desempenho para a colaboração entre pesquisadores e centros de pesquisa nacionais, incluindo supercomputadores e outras infraestruturas científicas.

A implementação da rede de e-Ciência transcende a interconexão física. É necessário oferecer um ambiente que gerencie todo o ciclo de vida das Organizações Virtuais (OVs), as quais viabilizam a colaboração segura e eficiente entre usuários de diferentes instituições e domínios administrativos, compartilhando recursos e dados. Ao término de uma OV, é crucial desprovisionar os recursos utilizados e revogar os acessos concedidos, a fim de evitar vazamento de dados e garantir a segurança da rede.

Nesse contexto, o modelo de GId federada (MELLO; CHAVES et al., 2022) é essencial para viabilizar a colaboração eficiente e segura entre pesquisadores e instituições, independentemente de suas localizações ou afiliações. 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.

[2] https://webkit.org/tracking-prevention/
[3] https://blog.mozilla.org/en/products/firefox/firefox-tips/internet-safety-for-families-total-cookie-protection/
[4] https://developers.google.com/privacy-sandbox

Iniciativas como o *Federated Identity Management for Research* (FIM4R) e o *European Open Science Cloud* (EOSC) exemplificam esforços para promover a interoperabilidade entre centros de pesquisa científica. O FIM4R é um fórum internacional voltado para a discussão de desafios e soluções para a gestão federada de identidade, enquanto o EOSC, uma iniciativa da União Europeia, oferece uma infraestrutura integrada baseada nos princípios *Findability, Accessibility, Interoperability, and Reusability* (FAIR) (WILKINSON et al., 2016), disponibilizando serviços e ferramentas para facilitar a pesquisa interdisciplinar, com foco em interoperabilidade, acessibilidade e compartilhamento de dados entre instituições.

A comunidade acadêmica também tem se mobilizado para criar padrões e recomendações para a gestão de identidade federada para os ambientes de ciberinfraestrutura, como a *Authentication and Authorisation for Research and Collaboration* (AARC) *Blueprint Architecture* (GÉANT, 2024a). O projeto *AARC Technical Revision to Enhance Effectiveness (AARC TREE)* (GÉANT, 2024b), iniciado em março de 2024, acrescentará guias para: OpenID Federation (HEDBERG et al., 2024); autorização para recursos federados; IDD e carteiras digitais (GROEP, 2024).

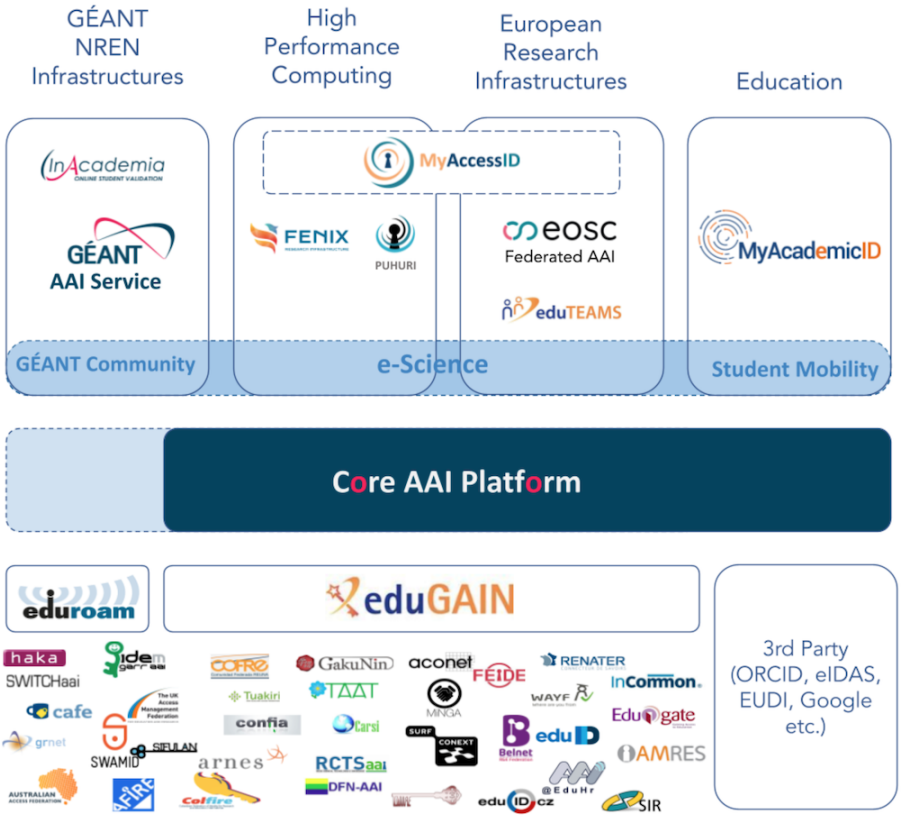


Figura 1: eduGAIN e a plataforma Core AAI. Fonte: (KANELLOPOULOS et al., 2023)

As redes de e-Ciência adotam o modelo federado de gestão de identidade para permitir que pesquisadores de diferentes instituições acessem recursos compartilhados de forma segura e eficiente. Para tal fazem uso de ferramentas que facilitam a integração das ciberinfraestruturas com as federações acadêmicas e de pesquisa, como *GÉANT Core AAI Plataform* (conhecido anteriormente por eduTEAMS) (GÉANT, 2024c), COmanage (INCOMMON, 2024), MyAccessID (GÉANT, 2022) e CILogon (BASNEY et al., 2019). Cabe ressaltar que a *GÉANT Core AAI Plataform* (Veja Figura 1) será o *backbone* dos serviços de identidade como MyAcademicID, MyAccessId e o EOSC AAI Federated AAI. Essa plataforma da GÉANT busca permitir as *National Research and Education Network*s (NRENs) propiciarem um ambiente seguro para a inovação e colaboração entre os setores educacional e de pesquisa científica.

O CILogon é um *proxy* de identidade que permite que provedores de serviços mediados se beneficiem da autenticação federada sem a necessidade de aderir diretamente à federação acadêmica.

Essa abordagem facilita a integração de serviços que não possuem suporte nativo para autenticação federada ou para os protocolos utilizados por essas federações. Porém, conforme apontado por Barton et al. (2023), diferentemente do propósito final do CILogon, outros *proxies* de identidade podem ter um interesse monetário e não há uma transparência quanto ao tratamento dos dados dos usuários e ao número de serviços operando por meio de um *proxy*.

Assim, a confiança entre as partes é um dos principais obstáculos para a adoção de *proxies* de identidade, pois a federação acadêmica não tem controle sobre a política de privacidade e segurança dos provedores de serviços mediados. Isso pode gerar riscos e custos para a federação acadêmica, incluindo a exposição de dados sensíveis dos usuários e possíveis responsabilidades legais decorrentes do uso indevido dessas informações.

3.6 Gestão de Identidade na Integração eduroam e 5G

Como continuidade aos esforços realizados pela RNP desde 2023 em chamada do PGId (RNP, 2023) para aquisição de conhecimento e investigação sobre a integração do serviço eduroam às redes móveis de nova geração, como o 5G, se mostra necessário o início da implantação de provas de conceito e de desenvolvimento de soluções. Tanto para ambiente de Operadora Virtual de Rede Móvel (MVNO, *Mobile Virtual Network Operator*) quanto para redes privativas, faz-se necessária a adaptação de componentes da arquitetura de autenticação do 5G. Os resultados previamente apresentados em iniciativas da RNP, como o PGId, demonstram a necessidade de utilização de métodos de autenticação comuns para o ambiente Wi-Fi e 5G, além de adaptações no núcleo do 5G (OLIVEIRA; SILVA, 2024b,a).

Neste contexto, a implantação da integração eduroam e 5G em redes privativas possibilita que instituições e centros de pesquisa parceiros expandam sua cobertura de rede e se beneficiem do *roaming*. Desta forma, é relevante a continuidade das investigações de validação das propostas de integração da base de dispositivos usuários 5G à CAFe. Além disso, deve-se verificar a viabilidade do desenvolvimento de um *proxy* de credenciais para interligação entre os ambientes 5G, eduroam e CAFe.

Destaca-se que não há solução disponível atualmente no mercado para essa funcionalidade, o que possibilita à RNP assumir um papel protagonista no cenário mundial das redes acadêmicas.

3.7 Gestão de identidade na integração eduroam e IDD

Redes federadas de *roaming*, como o eduroam e o OpenRoaming (OPENROAMING, 2025), permitem que usuários acessem a infraestrutura de diferentes provedores de acesso à rede (ANP, *Access Network Provider*) utilizando uma única credencial fornecida por um IdP. Essas arquiteturas dependem de uma infraestrutura distribuída e hierárquica de servidores RADIUS, que estão sujeitas a falhas. Os protocolos de autenticação comumente utilizados seguem o padrão 802.1x e empregam o *Extensible Authentication Protocol* (EAP). A adaptação dos métodos EAP ao modelo de IDD (veja Subseção 3.2) pode trazer diversos benefícios para a segurança e confiabilidade das redes federadas de *roaming* (METABLOX LABS, 2024; PETRLIC, 2024; HOFFMANN; WESTPHALL; MACHADO, 2025), destacando-se, entre eles:

a) Senhas: a autenticação em redes como eduroam geralmente depende de senhas (ex.: método PEAP/MSCHAPv2). No caso do IDD, um processo de autenticação utilizando VP eliminaria o problema de perda ou vazamento de senhas, além de evitar o armazenamento centralizado de credenciais;

b) Necessidade de autoridade certificadora desconhecida: O IDD elimina a necessidade do cliente ter que instalar certificados desconhecidos na primeira tentativa de associação à rede, algo ocorre hoje no eduroam;

c) Independência da federação RADIUS: A autenticação passaria a ser feita diretamente na própria ANP que o usuário deseja acessar a rede utilizando a blockchain subjacente ao sistema de IDD, que já conteria as informações necessárias para autenticar os usuários. O resultado seria a descentralização do processo de autenticação que eliminaria a necessidade de repasse de credenciais por meio da federação RADIUS, tornando o sistema menos suscetível a possíveis falhas na rede e em *proxies* RADIUS.

3.8 Gestão de Identidade e IA

Tanto no âmbito acadêmico (CREMONEZI et al., 2024) como em entidades de prestígio, como é o caso da Gartner em (GARTNER, 2024), vêm apontando a necessidade de atenção às soluções de Inteligência Artificial (IA) no âmbito da cibersegurança e GId. O relatório da Gartner (HARRIS; ALLAN, 2024) também destaca que a aplicação de IA na administração de acesso pode transformar a governança de identidade, reduzindo trabalho manual, acelerando a adaptação a mudanças organizacionais, assim como também melhorar simultaneamente segurança, conformidade e eficiência operacional. No entanto, há desafios envolvidos, como lidar com a qualidade e disponibilidade dos dados, pois políticas de acesso fragmentadas e registros inconsistentes podem comprometer a eficácia dos modelos de aprendizado. Outro desafio crítico é garantir a explicabilidade e transparência das decisões automatizadas, especialmente em contextos regulatórios que exigem auditoria e justificativa das permissões concedidas.

Como prova do avanço evidente da área, é possível listar soluções comerciais amplamente adotadas, como Okta [5], Auth0 [6] e Microsoft Entra ID [7], que oferecem ferramentas para a automatização de processos de criação de contas e autenticação, utilizando, por exemplo, biometria, *Multi-Factor Authentication* (MFA) e inteligência artificial, a fim de detectar possíveis tentativas de personificação e garantir uma experiência personalizada com base no comportamento do usuário. Outras soluções, como as plataformas SailPoint [8] e One Identity [9] possibilitam a gestão de contas inativas ou com privilégios excessivos, implementando políticas automatizadas de desativação, revalidação periódica de acessos e análise de risco baseada em comportamento, a fim de reduzir o risco de acessos indevidos.

Além disso, o avanço da IA também levanta preocupações sobre a autenticidade das identidades digitais, à medida que entidades controladas por IA se tornam cada vez mais sofisticadas. O estudo sobre *Personhood Credentials* (ADLER et al., 2025) ou credenciais de personalidade ou humanidade, numa tradução livre, propõe um modelo baseado em VC para permitir que indivíduos comprovem que são de fato pessoas e de uma forma que sua privacidade ainda seja garantida.

Já o documento NIST SP 800-63-4 (*draft*) (TEMOSHOK et al., 2024) orienta a prova e autenticação de identidade de usuários que interagem com sistemas de informação governamentais, sem tratar especificamente de IA. No entanto, ele levanta questões sobre a existência de métricas e metodologias de teste para avaliar o desempenho de tecnologias emergentes e compreender seus impactos em diferentes usuários, incluindo possíveis vieses aplicados a sistemas de IA. Além disso, o documento menciona a necessidade de pesquisas futuras sobre métodos emergentes, como análise de fraudes e pontuação de risco, que podem envolver o uso de IA para aprimorar a detecção e prevenção de fraudes em processos de identidade digital. O que evidencia a necessidade de aprofundamento no tema GId e IA e a sua relação.

Por fim, como resultado obtido pela *Chamada Pública de trabalhos de Prospecção Tecnológica para Comitês Técnicos 2024* da RNP no âmbito do projeto *Integração de GId com Inteligência Artificial*

[5] https://www.okta.com/
[6] https://auth0.com/
[7] https://www.microsoft.com/pt-br/security/business/identity-access/microsoft-entra-id
[8] https://www.sailpoint.com/
[9] https://www.oneidentity.com/

e aprendizado de máquina percebeu-se o impacto crescente da IA na segurança digital, mostrando-se essencial o acompanhamento das iniciativas e soluções comerciais.

Desta forma, a utilização de técnicas de IA integrada ao processo de análise de padrões de acesso, detecção de anomalias e gestão preditiva de identidade pode aumentar a segurança, tornando-se um diferencial estratégico para a RNP.

3.9 Evolução tecnológica nos protocolos base das federações acadêmicas

Atualmente, a CAFe encontra-se ancorada no protocolo *Security Assertion Markup Language* (SAML), que, embora consolidado, não é adequado para aplicações modernas, aplicativos móveis e dispositivos IoT. A crescente adoção de protocolos da família OAuth 2.0 (HARDT, 2012) e OpenID Connect (SAKIMURA et al., 2023) indica que as instituições já buscam soluções mais adaptadas a práticas modernas de desenvolvimento de software e às expectativas de seus usuários. Nos relatórios da Gartner de 2023 e 2024 (ALLAN; HARRIS, 2023; HARRIS; ALLAN, 2024), há recomendação para uso de OAuth 2.0 e OpenID Connect como padrões para autenticação e autorização em aplicações modernas em detrimento do SAML.

Desta forma, uma oportunidade que se desenha no ecossistema RNP está relacionada à transição para arquiteturas de confiança descentralizadas baseadas em protocolos modernos, como o *OpenID Federation* (HEDBERG et al., 2024), e à necessidade de aprimorar a experiência do usuário final nos processos de autenticação e uso de serviços. Esse cenário oferece um espaço promissor para inovar em processos de autenticação mais flexíveis e intuitivos, capazes de integrar diferentes tecnologias de forma ágil, minimizando barreiras de adoção e manutenção.

3.10 Arquitetura de confiança zero e gestão de identidades para IoT

Os temas “confiança zero” e “IoT” têm aparecido no documento de visão de futuro desde sua revisão de 2021 (BRITO et al., 2021). A motivação para a inclusão do tema confiança zero foi o aumento das aplicações envolvendo microsserviços e da implantação destes em infraestruturas distribuídas. Como consequência, os perímetros de rede precisavam ser mais flexíveis e dinâmicos e, assim, mais permeáveis e menos seguros. Desde então, o uso do modelo de confiança zero tem ganho força através de ações como a ordem executiva 14028 do governo americano (JR., 2021) que exige das agências federais um planejamento para a adoção de confiança zero, assim como determina a criação de um modelo de maturidade que possa avaliar a adoção dessas práticas.

A criação de estratégias para a adoção de princípios de confiança zero, assim como tecnologias de acesso à rede da organização usando tecnologias de confiança zero também aparecem com benefícios alto e moderado, respectivamente, no relatório de 2024 da Gartner para a área (LERNER; WATTS; BHOGAL, 2024) indicando um benefício claro na adoção das tecnologias. Esta versão do documento resgata a discussão sobre confiança zero, reforçando práticas que amadureceram neste período e destacando iniciativas que motivam a adoção dessas práticas.

Com relação à identidade para IoT, a edição de 2021 deste documento de visão de futuro, considerou o uso de certificados gerados por entidades certificadoras após a autenticação com segredos pré-provisionados. Esta ainda é a prática mais comum, no entanto, novas tendências incluem o uso de componentes de hardware seguro nos dispositivos para proteção desses segredos e estratégias de aprendizagem de máquina para a atestação dos dispositivos IoT. Desta forma, o provisionamento de identidades pode ser baseado em mais fatores, incluindo fatores que refletem o *status* de integridade do dispositivo ou seu comportamento de fato.

A necessidade de melhor suporte para identidades para IoT é destaque nos relatórios da Gartner de 2024 tanto para a área de redes de confiança zero (LERNER; WATTS; BHOGAL, 2024) como para a área de identidades digitais (HARRIS; ALLAN, 2024), uma vez que implementar segurança para

IoT requer boa autenticação para estes dispositivos, cuja gestão de identidades é mais complexa que para humanos devido à sua escala e à grande heterogeneidade de dispositivos. Além disso, na medida que a adoção de arquiteturas de confiança zero cresce, cresce também a necessidade de integrar os dispositivos de IoT nestas arquiteturas.

Por fim, o provisionamento de identidades desempenha um papel fundamental nos processos de autenticação e autorização. Para garantir sua robustez, é essencial considerar aspectos de segurança, tornando a fronteira entre provisionamento de identidades e cibersegurança menos definida. Diante disso, espera-se que futuras edições deste documento, assim como do documento de visão do futuro do Comitê Técnico de Cibersegurança da RNP (RNP, 2025), identifiquem ações que fortaleçam a conexão entre essas duas áreas.

3.10.1 Arquitetura de confiança zero

Segundo o NIST (ROSE et al., 2020), o modelo de confiança zero é uma coleção de conceitos e ideias que minimizam as incertezas no controle de acesso em sistemas de informação. As arquiteturas de confiança zero são consideradas extremamente importantes e, portanto, têm sido recomendadas por agências internacionais de segurança da informação como a ENISA (ENISA, 2024) e o ITU (HUANG et al., 2024), além de agências estadunidenses como o NIST (ROSE et al., 2020) e a CISA (CISA, 2023). Também usando iniciativas estadunidenses como referência, o uso de arquiteturas de confiança zero tem sido reforçado em memorandos do governo, como o Memorando 22-09 de janeiro de 2022, que exige que agências federais atinjam objetivos específicos de adoção de arquiteturas de confiança zero até o fim de 2024 (YOUNG, 2022).

Ainda segundo o NIST (ROSE et al., 2020), o modelo de confiança zero tem os seguintes pilares:

1. Todas as fontes de dados e serviços são recursos;
2. Toda comunicação é segura, independentemente da sua localização na rede;
3. O acesso aos recursos é dado por sessão (p. ex., por tarefa e não permanente para um componente);
4. O acesso aos recursos é determinado por uma política dinâmica;
5. A organização monitora a integridade e postura de segurança de seus ativos;
6. A autenticação e autorização é constante;
7. A organização coleta o máximo possível de informações sobre os ativos, rede e comunicações para melhorar a postura de segurança.

A aplicação destes fundamentos é avaliada por modelos de maturidade. Por exemplo, no caso do governo americano, a Agência de Cibersegurança e Segurança de Infraestrutura americana (CISA, *Cybersecurity and Infrastructure Security Agency*) desenvolveu um modelo de maturidade para confiança zero como parte das atividades previstas na ordem executiva 14028 (CISA, 2023). A lista de pilares do NIST deixa claro que identidades são essenciais em uma arquitetura zero, não somente para os usuários humanos envolvidos, mas também para os usuários não humanos, como serviços de software e dispositivos. Consequentemente, este papel da identidade está refletido também no modelo de maturidade. É importante destacar, no entanto, que o papel de identidade como definido aqui neste documento engloba mais que o pilar “Identidade” no modelo da CISA, mas está refletido em todos os pilares, uma vez que a atribuição de identidade é necessária para controle de acesso dos usuários, dispositivos, aplicações e serviços de software.

A academia também tem se debruçado sobre o uso de arquiteturas de confiança zero. A literatura científica recente inclui levantamentos amplos de trabalhos sobre ferramentas e estratégias de

confiança zero. Estes artigos exploram aspectos como os fatores críticos para o sucesso (YEOH et al., 2023; FERNANDEZ; BRAZHUK, 2024), modelos de maturidade (YEOH et al., 2023), arquiteturas de referência (SYED et al., 2022; HE et al., 2022) e aplicações em diferentes ambientes como IoT, computação na nuvem e sistemas de controle industrial (AZAD et al., 2024; HE et al., 2022; SYED et al., 2022). Os trabalhos também destacam desafios de implementação, a importância da gestão de identidades e as lacunas de pesquisa em áreas como avaliação de confiança, identificação de ameaças e criptografia pós-quântica.

Como a gestão de identidades é um dos pilares da implementação de arquiteturas de confiança zero, os componentes de software também precisam receber identidades e o provisionamento deve ser granular, evitando credenciais compartilhadas entre múltiplos serviços, ou pior, compartilhadas entre humanos e componentes de software.

As identidades para componentes de software têm sido objeto de estudo de diferentes organizações. Recentemente, em 2024, a *Internet Engineering Task Force* (IETF), organização internacional que desenvolve e promove padrões abertos para a Internet, criou o *Workload Identity in Multi System Environments* (WIMSE), um grupo de trabalho para identidades para cargas de trabalho (serviços ou aplicações que usam recursos do sistema computacional). Este grupo vem trabalhando na documentação de práticas existentes e na padronização de soluções, considerando padrões existentes como OAuth e SPIFFE (KASSELMAN; RICHER, 2024).

A relevância das identidades para componentes não humanos como cargas de trabalho, ou componentes de software, e dispositivos (p.ex., dispositivos IoT) também tem sido considerado por organizações tradicionais de segurança da informação, como a *Open Worldwide Application Security Project* (OWASP), que lançou em 2025 o projeto *Non-Human Identities Top 10*. Este projeto, que é semelhante a outros da OWASP, tem como objetivo chamar atenção para os desafios mais críticos da integração das identidades para não humanos no ciclo de desenvolvimento (OWASP, 2025).

Por fim, é importante destacar que o modelo de confiança zero e a implantação de uma arquitetura de confiança zero é um processo longo e complexo, até por ser um conjunto de boas práticas e não estar relacionado com tecnologias específicas, como destacado na ordem executiva 14144 do governo estadunidense (JR., 2025). No entanto, sua adoção passou a ser um requisito direto, como no exemplo das agências federais estadunidenses, ou um requisito indireto, como forma de atendimento a controles críticos de segurança cibernética como os definidos pelo *Center for Internet Security* (CIS, 2025). Este documento destaca então possíveis ações para a RNP que apoiem entidades do seu sistema na adoção deste modelo.

3.10.2 Identidade para Internet das Coisas

Embora a identificação de dispositivos IoT esteja frenquentemente associada a aspectos funcionais, como a rotulagem das informações coletadas, o provisionamento de identidades robustas é essencial para garantir a integridade dos dados, por exemplo, validando a origem das informações, e até para a negociação de chaves que assegurem sua confidencialidade.

O provisionamento de identidades robustas para dispositivos IoT não se restringe ao contexto de confiança zero. No entanto, como as arquiteturas de confiança zero também se aplicam a sistemas que envolvem IoT e dependem de uma gestão de identidade sólida, as identidades para IoT estão fortemente relacionadas à implementação deste modelo.

O provisionamento de identidades robustas para IoT impõe alguns requisitos (SYED et al., 2022):

- Identidades únicas para os dispositivos;
- Resistência contra adulterações e contra clonagem;
- Suporte a autenticação e controle de acesso adaptativos;

- Suporte a criptografia ponta-a-ponta;
- Escalabilidade.

As formas tradicionais de identificação de dispositivos são baseadas em informações pré-provisionadas, como considerado em edições anteriores deste documento (BRITO et al., 2021). Exemplos de tais mecanismos são o uso de atributos simples do dispositivos, chaves de criptografia simétrica ou *tokens* pré-configurados, ou de chaves privadas e certificados também configuradas antes da implantação do dispositivos. Assim, atributos como o *International Mobile Equipment Identity* (IMEI) , endereço MAC, endereço Bluetooth, ou LoRaWAN DevEUI, não são adequados pois podem ser inspecionados e clonados.

Novos mecanismos e tecnologias permitem melhorar tal processo de provisionamento. Um exemplo é o uso de uma raiz de confiança em *hardware* como um ambiente de execução confiável, *Trusted Execution Environment* (TEE), por exemplo, Intel TDX, AMD SEV-SNP, Intel SGX, ARM CCA, ARM TrustZone) ou um módulo *Trusted Plataform Module* (TPM) para armazenamento de um segredo pré-compartilhado que pode gerar identidades ou chaves efêmeras que podem ser vinculadas ao mesmo dispositivo de origem (ENISA, 2020).

Uma outra vertente se apoia no uso de atributos intrínsecos ao *hardware* de cada dispositivo, como *Physical Unclonable Function*s (PUFs). PUFs produzem respostas não clonáveis e imprevisíveis que podem ser utilizadas para identificar os dispositivos específicos. PUFs podem ser implementados em dispositivos mais complexos, usando TEEs, por exemplo, mas também podem depender de características mais simples como as imperfeições no processo de fabricação dos dispositivos e, assim, serem implementadas em dispositivos mais simples.

Finalmente, a identificação dos dispositivos pode ser feita com base em aspectos do contexto, como a associação com *gateways* ou o comportamento do dispositivo (SYED et al., 2022), incluindo o uso de inteligência artificial para correlacionar fatores dinâmicos e padrões, criando uma impressão digital do dispositivo (DFP, *Device Fingerprinting*) (ENISA, 2020).

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

Adaptações necessárias para garantir a continuidade, interoperabilidade e evolução dos serviços de identidade e acesso da RNP diante de novas demandas tecnológicas.

4.1.1 Prontidão tecnológica para a evolução dos protocolos em uso na federação

Atualmente, a CAFe encontra-se ancorada no protocolo SAML, que, embora consolidado, não é adequado para aplicações modernas, aplicativos móveis e dispositivos IoT. O SAML, inclusive, tem sido considerado um protocolo legado (FLANAGAN, 2024), uma vez que não tem sido mantido, especialmente para acompanhar evoluções como as VCs.

- Iniciar estudos técnicos detalhados sobre a transição de SAML para OpenID Federation (HEDBERG et al., 2024), conduzindo uma Prova de Conceito (PoC, *Proof of Concept*) baseada nas

experiências da GÉANT e outros projetos internacionais, focando na coexistência inicial dos dois protocolos, garantindo compatibilidade com os atuais IdP e Provedor de Serviço (SP, *Service Provider*) da federação.

- Acompanhar a evolução do *draft* OpenID Federation e monitorar PoCs, repositórios e configurações de iniciativas internacionais como o laboratório de interoperabilidade do projeto *Digital Credentials for Europe* (DC4EU) (SUNET, 2024) e o registro de emissores do Digital Credentials Consortium (DCC) (DCC, 2025).
- Estudar o *draft OpenID Federation Wallet Architectures* (MARCO et al., 2024) para entender como poderia ser integrado com a CAFe.
- Considerando que a CAFe e as instituições participantes não atuam, e possivelmente não atuarão, como provedores de carteiras digitais, analisar a necessidade de estabelecer políticas e parâmetros de confiança para a conformidade de carteiras externas que possam vir a ser adotadas pelos usuários da CAFe.

4.1.2 Credenciais Verificáveis

A adoção de Credenciais Verificáveis na CAFe requer adaptações para interoperar com a infraestrutura existente, incluindo a conversão de atributos SAML para *OpenID Connect* (OIDC), facilitando a integração com serviços federados e carteiras digitais que utilizam *JavaScript Object Notation* (JSON).

- Monitorar ativamente os trabalhos conduzidos pelo subcomitê na *Research and Education FEDerations group* (REFEDS) (REFEDS, 2025) para a definição de VCs alinhadas aos esquemas utilizados pela federação, como o brEduPerson, SCHAC e voPerson.
- Estudar a integração de VCs com a infraestrutura existente, garantindo interoperabilidade entre SAML, OIDC e carteiras de identidade digitais. Além disso, avaliar como os IdPs da CAFe podem oferecer suporte à emissão de VCs, permitindo que os SPs verifiquem essas credenciais sem necessidade de contato direto com os IdPs.

4.1.3 Autenticação federada utilizando FedCM

Atualmente, o suporte ao FedCM está restrito ao Google Chrome, sendo que a fundação Mozilla está na fase experimental, o que pode limitar sua adoção no curto prazo. No entanto, a API representa uma abordagem para a preservação da privacidade em protocolos de autenticação federada, como o SAML e o OIDC, que são amplamente utilizados nas federações acadêmicas e nos principais provedores de serviços comerciais na Internet. A abordagem do FedCM é promissora e pode ganhar tração à medida que outros navegadores considerem sua implementação, especialmente com o grupo de trabalho sendo conduzido na W3C (W3C, 2025a).

- Monitorar ativamente a evolução do FedCM e testar sua integração experimental com a infraestrutura atual de autenticação na CAFe, avaliando seu impacto na privacidade e usabilidade.

4.1.4 Integração do eduroam com redes 5G

A integração das redes móveis 5G com o *eduroam* continua sendo um tópico extremamente relevante. Além de aumentar as possibilidades de cobertura da rede de acesso *eduroam*, há outros benefícios transversais como já exposto neste documento.

- Realizar o desenvolvimento e validação por provas de conceito da integração entre as credenciais 5G e eduroam;
- Propor soluções, políticas e diretrizes relacionados ao *eduroam* no ambiente 5G de redes privativas e redes públicas.

4.1.5 Gestão de Identidade e Inteligência Artificial

A integração da inteligência artificial na gestão de identidade e acesso pode aumentar a segurança e a eficiência operacional, mas também exige uma infraestrutura preparada para lidar com desafios emergentes.

- Avaliar a necessidade de melhorias na infraestrutura de identidade digital existente, como conformidade com regulamentações iniciais, para enfrentar os desafios emergentes de modelos cada vez mais sofisticados.
- Avaliar o uso de soluções de gestão de identidade e acesso combinadas com IA, explorando sua aplicação para automação da gestão de permissões e detecção de anomalias em acessos, incluindo, por exemplo:
  - 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;
  - Implementar modelo de confiança zero, de forma que a identidade do usuário seria verificada de forma contínua e não apenas durante o processo de autenticação.

4.1.6 Gestão de identidade e de acesso para ambientes colaborativos de e-Ciência

Para viabilizar pesquisas colaborativas nacionais e internacionais, uso de OVs e o acesso seguro às ciberinfraestruturas de pesquisa, o uso de infraestruturas de autenticação e autorização interoperáveis e flexíveis são essenciais.

- **Padronização de atributos com *Research & Scholarship Entity Category*:** Incentivar que os provedores de identidade da CAFe adotem o *Research & Scholarship Entity Category* (REFEDS, 2016), garantindo que um conjunto mínimo de atributos seja disponibilizado de forma padronizada para os serviços de e-Ciência. Isso facilita o acesso de pesquisadores aos recursos, simplifica a integração e promove a interoperabilidade com federações internacionais, como a eduGAIN;
- **Adesão ao SIRTFI:** Diante da natureza dos serviços de e-Ciência, que envolvem o compartilhamento de grandes volumes de dados e o acesso a supercomputadores, é fundamental que as instituições estejam preparadas para responder a incidentes de segurança de forma rápida e eficiente. Assim, o *Security Incident Response Trust Framework for Federated Identity* (SIRTFI) deve ser adotado pelas instituições que fazem parte da rede de e-Ciência e também pelos provedores de identidade das federações acadêmicas;
- **Oferta de *proxies* para autenticação federada:** Soluções como o CILogon (BASNEY et al., 2019) ou o MyAccessID (GÉANT, 2022) devem ser exploradas para permitir que serviços de e-Ciência sejam integrados às federações acadêmicas. Esses *proxies* oferecem funcionalidades como a tradução de credenciais SAML em *tokens* OIDC e OAuth 2.0, viabilizando a autenticação em serviços que utilizam protocolos distintos;

- **Autenticação em aplicações não *web*:** O protocolo *OAuth 2.0 Device Authorization Grant* (DENNISS et al., 2019) possibilita que aplicações como serviços via SSH e APIs REST adotem autenticação federada. Ferramentas como o CILogon e o MyAccessID já oferecem suporte a esse protocolo e poderiam ser aproveitadas na rede de e-Ciência. As soluções *MyAccessID Federated SSH CA*[10] e (GUDU; HARDT; ZACHAMANN, 2022) são exemplos de formas para permitir a autenticação federada em serviços SSH.

4.1.7 Identidades para não humanos e arquiteturas de confiança zero

A adoção da abordagem de aplicações construídas com micro-serviços e de arquiteturas de confiança zero vai exigir mecanismos de provisionamento automatizado de identidades.

- Avaliar o uso de padrões abertos como o SPIFFE (SPIFFE PROJECT, 2025) para implementar hierarquias de atestação e atribuição de identidades para componentes de software e dispositivos de IoT.
- Avaliar mecanismos de monitoramento de riscos que viabilizem a implementação de autenticação e controle de acesso de forma contínua.

4.2 Segundo horizonte

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

4.2.1 Autenticação e governança de agentes de IA autônomos

Com o avanço da inteligência artificial, a presença de agentes autônomos nas interações digitais se tornará cada vez mais comum, exigindo novas abordagens para autenticação e governança. A distinção entre entidades humanas e agentes de IA será um fator crítico para a segurança, confiabilidade e transparência dos ecossistemas digitais.

- Explorar modelos de autenticação que diferenciem humanos de agentes de IA, garantindo que determinadas ações e acessos sejam restritos a indivíduos reais, quando necessário.
- Acompanhar a evolução de soluções como as *Personhood Credentials*, que propõem um modelo baseado em VCs para permitir a verificação da humanidade de forma a preservar a privacidade, contribuindo para um ecossistema digital mais confiável.
- Estabelecer diretrizes para a participação de agentes autônomos em serviços digitais, definindo níveis de acesso, transparência nas interações e mecanismos para auditoria e rastreabilidade de ações realizadas por IA.
- Considerar regulamentações emergentes sobre o uso de IA em identidade digital, incluindo padrões éticos e requisitos para que agentes autônomos possam interagir de maneira segura e responsável em federações de identidade.

4.2.2 Atestação para emissão de identidades para componentes de software e IoT

Como discutido na Subseção 3.10, o uso de raízes de confiança em hardware como base para emissão de identidades componentes de software e dispositivos IoT já é recomendado por agências de

[10] https://wiki.geant.org/display/MyAccessID/Federated+SSH+CA

padronização e relatórios da Gartner. No caso de componentes de software, os mesmos mecanismos que possibilitam identidades mais fortemente vinculadas aos componentes também trazem benefícios adicionais, como a criptografia dos dados em uso durante o processamento, sendo este um requisito para os mais altos níveis de maturidade em arquiteturas de confiança zero.

Como abordagem intermediária, o uso de contexto, combinando identidades pré-provisionadas com informações do ambiente de execução e localização, permite a geração de identidades de forma escalável e mais robusta do que o simples pré-provisionamento com certificados durante a configuração inicial dos componentes.

- Avaliar a utilização de mecanismos de atestação, preferencialmente usando raiz de confiança em hardware para o provisionamento de identidades para componentes de software e IoT.

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 Adoção ampla da Identidade Digital Descentralizada

Diferentes órgãos padronizadores, pesquisadores da academia e a indústria estão investindo na evolução no modelo de IDD, buscando assim encontrar uma solução que possa ser aceita como adequada e viável para garantir a privacidade dos usuários, dando poder a estes, e ao mesmo tempo economicamente viável. Nesta linha, seria interessante investigar os seguintes pontos, ainda em aberto nas especificações e soluções da indústria:

- **Delegação de autoridade sobre credenciais ou atributos de identidade a terceiros**: O modelo de dados da VC não prevê a delegação de autoridade sobre credenciais ou atributos de identidade a terceiros. É necessário investigar se iniciativas na literatura (FLAMINI et al., 2025) podem ser adotadas para resolver este problema mesmo sem uma padronização e mesmo assim se tenha garantido a interoperabilidade entre as soluções propostas.
- **Acesso à rede autenticado por IDD:** A autenticação utilizando IDD em redes federadas de *roaming* como o eduroam pode ser um grande impulsionador para a popularização das IDD. Pesquisas nessa linha (METABLOX LABS, 2024; PETRLIC, 2024; HOFFMANN; WESTPHALL; MACHADO, 2025) encontram desafios na integração aos padrões *de facto* de autenticação (802.1x e EAP) suportados atualmente pelos dispositivos finais e equipamentos de rede.

4.3.2 Identidade Fiduciária

Com a expansão do modelo fiduciário, a RNP tem a oportunidade de se posicionar na vanguarda de uma próxima geração de soluções para identidade digital, equilibrando privacidade, segurança e usabilidade de modo a atender às demandas acadêmicas e profissionais. Uma das principais oportunidades para o ecossistema RNP e para o cenário de gestão de identidades digitais é a exploração técnica e científica do modelo fiduciário (SCHARDONG; CUSTÓDIO, 2024).

- Experiência do usuário simplificada:
  - Desenvolvimento de políticas de consentimento que permitam aos usuários definir de modo prévio ou sob demanda como e quando suas informações podem ser compartilhadas;

  - Criação de interfaces de auditoria (evidências) que forneçam visibilidade sobre todas as ações do fiduciário, permitindo que os titulares entendam rapidamente quais dados foram utilizados, em que momento e para qual finalidade.

- Governança e transparência aprimoradas:

  - Implementação de mecanismos de rastreabilidade robustos, capazes de responsabilizar o fiduciário por qualquer uso indevido ou vazamento de dados;
  - Investigação de modelos regulatórios que estabeleçam claramente as obrigações do fiduciário, reforçando vínculos jurídicos e éticos que confiram maior credibilidade ao ecossistema.

- Protocolos seguros e flexíveis:

  - Definição de normas para trocas de informações entre o fiduciário, SPs e usuários, garantindo que os dados pessoais permaneçam sob controle dos titulares;
  - Exploração de tecnologias de computação multipartidária e provas de conhecimento zero, ampliando as possibilidades de verificação de informações sem revelar dados sensíveis.

4.3.3 Atestação com raiz de confiança em hardware para emissão de identidades

Assim como destacado na Subsubseção 4.2.2, a raiz de confiança em hardware é um mecanismo poderoso para a atribuição de identidades para componentes de software e IoT. Além disso, segundo Russinovich (RUSSINOVICH, 2023), em alguns anos, o que hoje é conhecido como “computação confidencial” será apenas “computação”, uma vez que os mecanismos de proteção de confidencialidade e integridade, associados à evolução das ferramentas de desenvolvimento e operação não só tornarão aplicações mais seguras como também viabilizarão aplicações com dados sensíveis através da redução da Base de Computação Confiável (TCB, *Trusted Computing Base*) e das superfícies de ataque.

- Acompanhar a evolução de mecanismos de verificação de identidade baseados em PUFs para dispositivos IoT, avaliando a implementação de sistemas de provisionamento de identidades e de autenticação baseados em tais tecnologias.
- Implementar suporte para mecanismos de atribuição de identidades para componentes de software e dispositivos de IoT considerando elementos seguros, como ambientes de computação confiáveis (TEE), máquinas virtuais e contêineres confidenciais.

4.3.4 ICPEdu com suporte a algoritmos pós-quânticos

A computação quântica representa uma séria ameaça à criptografia tradicional, tornando a migração para algoritmos pós-quânticos uma necessidade urgente. 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. Desta forma recomenda-se que a RNP encaminhe a discussão acerca desse problema para que a solução esteja disponível com a tempestividade requerida para uso na ICPEdu.

- 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*[11];

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

- Considerar a viabilidade da criação de projeto piloto, em parceria com fornecedoras de *Hardware Security Module* (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.

Referências

ADLER, Steven et al. *Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online*. 2025. arXiv: 2408.07892 [cs.CY]. Disponível em: <https://arxiv.org/abs/2408.07892>.

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.

ALLAN, Ant; HARRIS, Nathan. *Hype Cycle for Digital Identity, 2023*. Gartner, jul. 2023.

ALLEN, Christopher. *Musings of a Trust Architect: Has our SSI Ecosystem Become Morally Bankrupt?* 29 out. 2024. Disponível em: <https://www.blockchaincommons.com/musings/musings-ssi-bankruptcy>. Acesso em: 7 fev. 2025.

_____. *The Path to Self-Sovereign Identity*. 26 abr. 2016. Disponível em: <https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/>. Acesso em: 7 fev. 2025.

AZAD, Muhammad Ajmal et al. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, v. 27, p. 101227, 2024. ISSN 2542-6605. DOI: https://doi.org/10.1016/j.iot.2024.101227. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2542660524001689>.

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.

BARTON, Tom et al. *Formalizing the role of federation proxies within the InCommon Federation*. Jun. 2023. DOI: http://doi.org/10.26869/TI.169.1.

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.

CIS. *Center for Internet Security (CIS) - Critical Security Controls*. 2025. https://www.cisecurity.org/controls. Acessado em: 15 de fevereiro de 2025.

CISA. *Cybersecurity and Infrastructure Security Agency – Zero Trust Maturity Model Version 2.0*. Abr. 2023. Disponível em: <https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf>.

CREMONEZI, Bruno et al. Identity management for Internet of things: concepts, challenges and opportunities. *Computer communications*, Elsevier, 2024.

DCC. *Selecting the OpenID Federation specification for the DCC and Credential Engine Issuer Registry Project*. 2025. Disponível em: <https://blog.dcconsortium.org/selecting-the-openid-federation-specification-for-the-dcc-and-credential-engine-issuer-registry-f9079f620472>. Acesso em: 7 fev. 2025.

DENNISS, W. et al. *OAuth 2.0 Device Authorization Grant*. Ago. 2019.

ENISA. *European Union Agency for Cybersecurity – Guidelines for Securing the Internet of Things: Secure Supply Chain for IoT*. Nov. 2020. ISBN 978-92-9204-411-4. DOI: 10.2824/314452.

_____. *European Union Agency for Cybersecurity – Threat Landscape 2024*. Set. 2024. ISBN 978-92-9204-675-0. DOI: 10.2824/071088. Disponível em: <https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf>.

FAPESP. *Programa FAPESP de pesquisa em eScience*. 2015. Disponível em: <https://fapesp.br/publicacoes/2015/folder_escience.pdf>. Acesso em: 9 dez. 2024.

FERNANDEZ, Eduardo B.; BRAZHUK, Andrei. A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, v. 89, p. 103832, 2024. ISSN 0920-5489. DOI: https://doi.org/10.1016/j.csi.2024.103832. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0920548924000011>.

FLAMINI, Andrea et al. On Delegation of Verifiable Presentations. In: 3RD International Workshop on Trends in Digital Identity. Jan. 2025.

FLANAGAN, Heather. *Is There a Future for REFEDS and R&E Federations?* 3 set. 2024. Disponível em: <https://refeds.org/a/2984>.

GARTNER. *Gartner Identifies the Top Cybersecurity Trends for 2024*. 2024.

GÉANT. *AARC Blueprint Architecture*. 2024. Disponível em: <https://aarc-community.org/architecture/>. Acesso em: 10 dez. 2024.

_____. *AARC Technical Revision to Enhance Effectiveness (AARC TREE)*. 2024. Disponível em: <https://aarc-community.org/aarc-tree-project/>. Acesso em: 10 dez. 2024.

_____. *eduTEAMS*. 2024. Disponível em: <https://eduteams.org>. Acesso em: 10 dez. 2024.

_____. *MyAccessID Identity and Access Management Service*. 2022. Disponível em: <https://wiki.geant.org/display/MyAccessID/>. Acesso em: 10 dez. 2024.

GROEP, David. Of AARC TREEs and colourful pictures Enhanced effectiveness for AARC in FIM for Research. In: 19TH FIM4R Workshop (joint with AARC TREE). 2024. Disponível em: <https://indico.cern.ch/event/1438628/>. Acesso em: 16 dez. 2024.

GUDU, Diana; HARDT, Marcus; ZACHAMANN, Gabriel. *SSH access with OIDC tokens*. 2022. Disponível em: <https://github.com/EOSC-synergy/ssh-oidc>. Acesso em: 10 dez. 2024.

HARDT, D. *The OAuth 2.0 Authorization Framework*. Out. 2012. Disponível em: <http://www.rfc-editor.org/rfc/rfc6749.txt>.

HARRIS, Nathan; ALLAN, Ant. *Hype Cycle for Digital Identity, 2024*. Gartner, jul. 2024.

HE, Yuanhang et al. A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communication and Mobile Computing – Securing AI-powered Internet of Things Ecosystems*, John Wiley e Sons Ltd., GBR, v. 2022, jan. 2022. ISSN 1530-8669. DOI: 10.1155/2022/6476274. Disponível em: <https://doi.org/10.1155/2022/6476274>.

HEDBERG, R. et al. *OpenID Federation 1.0 - draft 41*. 24 out. 2024. Disponível em: <https://openid.net/specs/openid-federation-1_0.html>. Acesso em: 7 fev. 2025.

HOFFMANN, E. F.; WESTPHALL, C. M.; MACHADO, C. S. RadChain Connect: Integration Between Blockchain and FreeRADIUS for Secure Authentication in Wi-Fi Networks/Web Environment. In: IEEE 2025 International Conference on Information Networking (ICOIN). ChiangMai, Thailand: IEEE, 2025.

HUANG, Jing et al. *Guidelines for Zero Trust-Based Access Control Platform in Telecommunication Networks*. Mar. 2024. Agreed on 2024-03-01. Disponível em: <https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18032>.

HUGHES, Riley. *Why Verifiable Credentials Aren't Widely Adopted & Why Trinsic Pivoted*. 15 out. 2024. Disponível em: <https://rileyparkerhughes.medium.com/why-verifiable-credentials-arent-widely-adopted-why-trinsic-pivoted-aee946379e3b>.

INCOMMON. *COmanage: Collaborative organization management provided in a secure framework*. 2024. Disponível em: <https://incommon.org/software/comanage>. Acesso em: 10 dez. 2024.

ISO/IEC. *ISO/IEC 18013-5:2021 Information technology — ISO-compliant driving licence. Part 5: Mobile driving licence (mDL) application*. Set. 2021. Disponível em: <https://www.iso.org/standard/69084.html>. Acesso em: 7 fev. 2025.

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.

JR., Joseph R. Biden. *Improving the Nation's Cybersecurity*. Maio 2021. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity. Executive Order 14028, Federal Register Vol. 86, No. 93, pp. 26633-26647.

_____. *Strengthening and Promoting Innovation in the Nation's Cybersecurity*. Jan. 2025. https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity. Executive Order 14144, Federal Register Vol. 90, No. 12, pp. 6755-6771.

KANELLOPOULOS, Christos et al. *GÉANT - Trust and identity strategy 2025 - 2027*. Nov. 2023.

KASSELMAN, Pieter; RICHER, Justin. *WIMSE Working Group: Serious Business for Cloud Computing*. Out. 2024. https://www.ietf.org/blog/wimse-working-group/. Acessado em: 16 de fevereiro de 2025.

LERNER, Andrew; WATTS, John; BHOGAL, Charanpal. *Hype Cycle for Zero-Trust Networking, 2024*. Gartner, jul. 2024.

MARCO, G. de et al. *OpenID Federation Wallet Architectures 1.0 - draft 03*. 16 out. 2024. Disponível em: <https://openid.net/specs/openid-federation-wallet-1_0.html>.

MELLO, Emerson Ribeiro de; BRITO, Andrey Elísio et al. *Relatório de visão de futuro em Gestão de Identidade*. Maio 2023. Publicações técnicas do Comitê Técnico de Gestão de Identidade (CT-GId) da RNP.

MELLO, Emerson Ribeiro de; CHAVES, Shirlei Aparecida de et al. Autenticação e Autorização: antigas demandas, novos desafios e tecnologias emergentes. In: MINICURSOS do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg). Porto Alegre, RS: Sociedade Brasileira de Computação, set. 2022. P. 1–50. ISBN 978-85-7669-510-3. DOI: 10.5753/sbc.10710.3.

METABLOX LABS. *Roam: Decentralized OpenRoaming WiFi Networks*. 2024. https://weroam.xyz/whitepaper. Acessado em: 24 de fevereiro de 2025.

OLIVEIRA, Leonardo Azalim de; SILVA, Edelberto Franco. Eduroam e 5G: Autenticaçao Integrada via Redes Móveis e Wi-Fi no Core 5G. In: SBC. SIMPÓSIO Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg). 2024. P. 189–192.

_____. *Evaluation of EAP Usage for Authenticating Eduroam Users in 5G Networks*. 2024. arXiv: 2402.10889 [cs.CR]. Disponível em: <https://arxiv.org/abs/2402.10889>.

OPENROAMING. *Wireless Broadband Alliance*. 2025. Disponível em: <https://wballiance.com/openroaming/>. Acesso em: 9 jan. 2025.

OWASP. *Open Web Application Security Project (OWASP) - Non-Human Identities Top 10*. 2025. https://owasp.org/www-project-non-human-identities-top-10. Acessado em: 16 de fevereiro de 2025.

PETRLIC, Ronald. Specifying SSI over EAP: Towards an Even Better Eduroam in the Future. In: BAROLLI, Leonard (Ed.). *Advanced Information Networking and Applications*. Cham: Springer Nature Switzerland, 2024. P. 61–73. ISBN 978-3-031-57916-5.

REFEDS. *Research and Scholarship Entity Category*. Set. 2016. DOI: https://doi.org/10.5281/zenodo.6832218.

_____. *VC Subcommittee*. 2025. Disponível em: <https://wiki.refeds.org/display/STAN/VC+Subcommittee>. Acesso em: 7 fev. 2025.

RNP. *Comitê Técnico de Cibersegurança (CT-Ciber)*. 2025. Disponível em: <https://plataforma.rnp.br/ct-ciberseguranca>. Acesso em: 15 fev. 2025.

_____. *Comitê Técnico de Gestão de Identidade (CT-GId)*. 2024. Disponível em: <https://www.rnp.br/ct-gid>. Acesso em: 17 out. 2024.

_____. *Comunidade Acadêmica Federada (CAFe)*. 2024. Disponível em: <https://www.rnp.br/servicos/cafe>. Acesso em: 17 out. 2024.

_____. *Eduroam*. 2024. Disponível em: <https://www.rnp.br/servicos/eduroam>. Acesso em: 17 out. 2024.

_____. *Infraestrutura de Chaves Públicas para Educação (ICPEdu)*. 2024. Disponível em: <https://www.rnp.br/servicos/icpedu>. Acesso em: 17 out. 2024.

_____. *Laboratório para experimentação em Gestão de Identidade (GIdLab)*. 2024. Disponível em: <https://www.rnp.br/servicos/testbeds/gidlab>. Acesso em: 17 out. 2024.

_____. *Programa de Gestão de Identidade*. 2023. Disponível em: <https://www.rnp.br/chamadas-publicas/programa-de-gestao-de-identidade-2023/>. Acesso em: 9 dez. 2023.

ROSE, Scott et al. *Zero Trust Architecture*. National Institute of Standards e Technology, ago. 2020. DOI: 10.6028/NIST.SP.800-207. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-207/final>.

RUSSINOVICH, Mark. Confidential Computing: Elevating Cloud Security and Privacy: Working toward a more secure and innovative future. *Queue*, Association for Computing Machinery, New York, NY, USA, v. 21, n. 4, p. 44–48, set. 2023. ISSN 1542-7730. DOI: 10.1145/3623461. Disponível em: <https://doi.org/10.1145/3623461>.

SAKIMURA, Nat et al. *OpenID Connect Core 1.0*. Dez. 2023. Disponível em: <https://openid.net/specs/openid-connect-core-1_0.html>. Acesso em: 20 dez. 2024.

SCHARDONG, Frederico; CUSTÓDIO, Ricardo. From Self-Sovereign Identity to Fiduciary Identity: A Journey Towards Greater User Privacy and Usability. In: ACM/sigapp symposium on applied computing. *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*. 2024. ACM, p. 687–694. DOI: 10.1145/3605098.3636061.

SPIFFE PROJECT. *SPIFFE: Secure Production Identity Framework for Everyone*. 2025. https://spiffe.io/. Acessado em: 17 de fevereiro de 2025.

SUNET. *EUDIW pilot setup*. 2024. Disponível em: <https://wiki.sunet.se/display/Projekt/EUDIW+pilot+setup>. Acesso em: 7 fev. 2025.

SYED, Naeem Firdous et al. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, v. 10, p. 57143–57179, 2022. DOI: 10.1109/ACCESS.2022.3174679.

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

TEMOSHOK, David et al. *Digital Identity Guidelines*. National Institute of Standards e Technology, ago. 2024. DOI: 10.6028/NIST.SP.800-63-4.2pd. Disponível em: <https://csrc.nist.gov/pubs/sp/800/63/4/2pd>.

W3C. *Federated Credential Management API - W3C First Public Working Draft*. 2025. Disponível em: <https://www.w3.org/TR/fedcm/>. Acesso em: 7 fev. 2025.

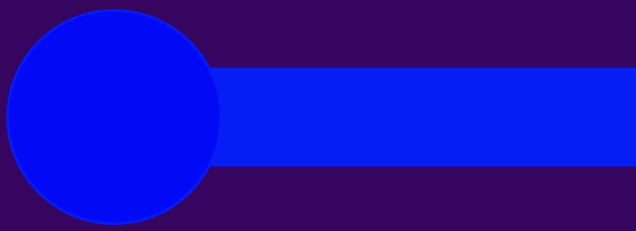
_____. *Verifiable Credentials Data Model 1.1*. Mar. 2022. Disponível em: <https://www.w3.org/TR/vc-data-model/>. Acesso em: 7 fev. 2025.

_____. *Verifiable Credentials Data Model v2.0*. Jan. 2025. Disponível em: <https://www.w3.org/TR/vc-data-model-2.0>. Acesso em: 7 fev. 2025.

WILKINSON, M. et al. *The FAIR Guiding Principles for scientific data management and stewardship*. Mar. 2016. DOI: https://doi.org/10.1038/sdata.2016.18. Disponível em: <https://www.nature.com/articles/sdata201618>.

YEOH, William et al. Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security*, v. 133, p. 103412, 2023. ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2023.103412. Disponível em: <https://www.sciencedirect.com/science/article/pii/S016740482300322X>.

YOUNG, Shalanda D. *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. Jan. 2022. Memorando para os Chefes dos Departamentos e Agências Executivas. Disponível em: <https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf>.



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