RNP

ORGANIZAÇÃO SOCIAL DO MCTI

Relatório de Visão de Futuro

Comitê Técnico de Gestão de Identidade - (CT-GId)

Julho de 2021

Coordenador do CT-GId

Emerson Ribeiro de Mello, Dr. (IFSC)

Assistente Técnica do CT-GId

Shirlei Aparecida de Chaves, Ma. (IFSC)

Secretários do CT-GId

André Luiz Almeida Marins, Me. (RNP)
Clayton Reis da Silva, Me. (RNP)

Diretor Adjunto de e-Ciência e Ciberinfraestrutura Avançada

Leandro Neumann Ciuffo, Me. (RNP)

Autores

Andrey Elísio Monteiro Brito, Dr. (UFCG)
Carlos Eduardo da Silva, Dr. (Sheffield Hallam University)
Edelberto Franco Silva, Dr. (UFJF)
Emerson Ribeiro de Mello, Dr. (IFSC)
Jean Everson Martina, Dr. (UFSC)
Marco Aurélio Amaral Henriques, Dr. (Unicamp)
Michelle Silva Wangham, Dra. (RNP/UNIVALI)

Este documento está licenciado sob a Licença Creative Commons “Atribuição-CompartilhaIgual 4.0 Internacional”.

Sumário

Lista de abreviaturas e siglas

AAA Autenticação, Autorização e Accounting

AC Autoridade Certificadora

ACME *Automatic Certificate Management Environment*

AES *Advanced Encryption Standard*

API *Application Programming Interface*

ARX Adição-Rotação-Soma

AWS *Amazon Web Services*

BLE *Bluetooth Low Energy*

BPA *Blueprint Architecture*

CA-GId Comitê Assessor de Gestão de Identidade

CT-GId Comitê Técnico de Gestão de Identidade

CAFe Comunidade Acadêmica Federada

CAR *Consent-informed Attribute Release*

CLPKC *Certificateless Public Key Cryptography*

CNCF *Cloud Native Computing Foundation*

CTAP *Client to Authenticator Protocol*

DAGSer Diretoria Adjunta de Gestão de Serviços

DID *Decentralized Identifier*

DS *Discovery Service*

ECG *Eletrocardiograma*

eduroam *Education Roaming*

FACS *Federated Access Control System*

FIDO *Fast IDentity Online*

GId Gestão de Identidades

GIdLab Laboratório para Experimentação em Gestão de Identidade

HSM *Hardware Security Module*

HTTP *Hypertext Transfer Protocol*

IAA Infraestrutura de Autenticação e de Autorização

IAM *Identity and Access Management*

IBC *Identity-based cryptograhy*

ICP-Brasil Infraestrutura de Chave Pública Brasileira

ICPEdu Infraestrutura de Chaves Públicas para Ensino e Pesquisa

IDD Identidade Digital Descentralizada

IDS *Intrusion detection system*

IdM *Identity Management*

IdP *Identity Provider*

IdPaaS *Identity Provider as a Service*

IIoT *Industrial Internet of Things*

IoT *Internet of Things*

IoHT *Internet of Healthcare Things*

IoMT *Internet of Medical Things*

JSON *JavaScript Object Notation*

JWT *JSON Web Token*

LGPD Lei Geral de Proteção de Dados Pessoais

MEC Ministério da Educação

M2M *Machine-to-Machine*

MFA *Multi-Factor Authentication*

NISO *National Information Standards Organization*

NIST *National Institute of Standards and Technology*

NFC *Near Field Communication*

OTP *One Time Password*

OV Organização Virtual

PGId Programa de Gestão de Identidade

PUF *Physical Unclonable Function*

REFEDS *Research and Education FEDerations group*

RNP Rede Nacional de Ensino e Pesquisa

SAML *Security Assertion Markup Language*

SAN *Subject Alternative Name*

SBSeg Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais

SIRTFI *Security Incident Response Trust Framework for Federated Identity*

SMS *Short Message Service*

SP *Service Provider*

SPIFFE *Secure Production Identity Framework For Everyone*

SPIRE *SPIFFE Runtime Environment*

SSL *Secure Sockets Layer*

SSO *Single Sign-On*

SSI *Self-Sovereign Identity*

STM *International Association of STM Publishers*

TSE Tribunal Superior Eleitoral

U2F *Universal 2nd Factor*

UAF *Universal Authentication Framework*

VC *Verifiable Credentials*

VPN *Virtual Private Network*

WAYF *Where Are You From*

WBA *Wireless Broadband Alliance*

WBAN *Wireless Body Area Network*

WGID Workshop de Gestão de Identidades Digitais

1 Introdução

A Gestão de Identidades (GId) [*Identity Management* (IdM)], como apresentado em ITU (2009), ou a gestão de identidades e de acesso [*Identity and Access Management* (IAM)], como apresentado 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 acelerada, decorrente da 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], composto por membros da RNP e da comunidade acadêmica, foi constituído pela RNP em 2010 e tem como missão a prospecção soluções de gestão de identidade inovadoras e embasadas em pesquisas de médio e longo prazo para o sistema RNP, promovendo a cultura, conscientizando e incentivando o uso de identidades digitais no Brasil. Essa prospecção visa se tornar uma fonte de referência e apoiar as atividades do Comitê Assessor de Gestão de Identidade (CA-GId) da RNP, o que pode gerar impacto direto para RNP e suas instituições usuárias.

Entre as ações e projetos gerados pelo CT-GId, pode-se destacar: a 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 Infraestrutura de Autenticação e de Autorizaçãos (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; a produção de documentos técnicos como recomendações, estudos, relatórios, bem como o documento de visão de futuro; e a participação de seus membros no Workshop de Gestão de Identidades Digitais (WGID) que é realizado anualmente em conjunto com o Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg).

1.1 Escopo e limitações

Este documento tem por objetivo apresentar um visão de futuro sobre temas relacionados à gestão de identidade e de acesso, que possam ser explorados em pesquisas de médio e longo prazo pela RNP. Este documento não tem por objetivo ser uma análise completa de todos os assuntos dentro da grande área de gestão de identidade. Para a escrita desse documento foram considerados os serviços oferecidos atualmente pela RNP e iniciativas acadêmicas e da indústria que apresentam tecnologias e aplicações emergentes na área de gestão de identidade.

2 Metodologia

Para a escrita desse relatório foi feito uso de método de visão qualitativo, do inglês *foresight*, que segundo Teixeira (2013) "*consiste na antecipação de possibilidades futuras com base em percepções de especialistas, cada um deles apoiados exclusivamente em seus conhecimentos e subjetividades*". A organização do documento baseou-se também na estratégia de gestão chamada *Três Horizontes de Inovação*, elaborada pela consultoria McKinsey (BAGHAI; COLEY; WHITE, 2000). Nessa estratégia

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

são apresentados três objetivos, chamados de horizontes, os quais irão indicar como a priorização das ações deverão ser divididas, considerando serviços atuais, negócios emergentes e inovações em produtos disruptivos.

Todos os membros do CT-GId foram consultados sobre o interesse em participar da escrita desse documento. Com o grupo de interessados, foram realizadas reuniões e troca de informações via lista de email para delimitar o contexto e a profundidade esperada para esse relatório. A primeira versão finalizada do documento foi encaminhada para apreciação pelos demais membros do CT-GId e pela Diretoria Adjunta de Gestão de Serviços (DAGSer) da RNP. Por fim, a versão revisada foi encaminhada ao CA-GId da RNP.

3 Panorama

3.1 Problemas e desafios identificados

- Possibilitar a integração do uso do serviço eduroam às redes 5G;
- Garantir a conformidade dos provedores de identidade e de serviços da CAFe com políticas e tecnologias adotadas por outras federações acadêmicas e com interfederação eduGAIN[3] e assim, garantir aos usuários da CAFe o acesso aos serviços dessas federações;
- Tornar o processo de autenticação na CAFe mais robusto e, ainda assim, com uma melhor usabilidade, adotando técnicas de autenticação implícita e contínua, por exemplo;
- Manter a relevância e aumentar o protagonismo da federação CAFe diante de iniciativas como o serviço de autenticação única e federada do portal https://acesso.gov.br;
- Garantir o funcionamento da autenticação federada diante das mudanças nos navegadores. *web* adicionadas para proteger a privacidade de seus usuários contra abusos de serviços de rastreamento.
- Permitir a interoperabilidade da federação CAFe com tecnologias como o OpenID Connect (SAKIMURA et al., 2014), OAuth2 (HARDT, 2012), entre outras para que possa ser ampliado o acesso a serviços nacionais ou internacionais disponibilizados por meio de tais protocolos;
- Prover uma solução integrada de autenticação de dispositivos e de usuários em IdPs federados, como por exemplo os da CAFe e do eduroam, alinhada aos requisitos da IoT;
- Buscar novas e mais amigáveis formas de atender as demandas dos usuários e da Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) por maior privacidade e maior controle da disseminação das informações de identidade, como a Identidade Digital Descentralizada (IDD), por exemplo;
- Facilitar a integração entre autenticação federada CAFe e novas formas de identificação digital;
- Prover soluções de autorização flexíveis e de granularidade fina que reflitam as necessidades de aplicações em saúde eletrônica, pesquisas colaborativas (organizações virtuais), *testbeds* federados e nuvens federadas;
- Permitir a verificação e auditoria das políticas de controle de acesso.

[3] O serviço de interfederação *eduGAIN* conecta federações acadêmicas em todo o mundo, simplificando o acesso a conteúdo, serviços e recursos para a comunidade global de pesquisa e educação.

3.2 Tendências tecnológicas e aplicações emergentes

3.2.1 Cenário de evolução da gestão de identidades

Os modelos de identidade digital evoluíram desde o surgimento da Internet e segundo Allen (2016), tal evolução pode ser dividida em quatro estágios: identidade centralizada, identidade federada, identidade centrada no usuário e Identidade Digital Descentralizada.

O modelo de identidade centralizada (primeiro estágio) ainda é comum hoje, mesmo sendo o menos conveniente, seja pela carga imposta ao usuário, que tem que gerenciar uma identidade digital para cada novo serviço que deseja acessar, seja pelo compartilhamento dos dados do usuário com cada serviço acessado. Além disso, os dados do usuário são centralizados no provedor do serviço e o usuário não tem controle sobre eles.

O modelo de identidade federada (segundo estágio), apesar de diminuir a carga sobre o usuário, ainda apresenta alguns dos problemas do modelo de identidade centralizada, que são a concentração de dados do usuário nos provedores de identidade da federação e a falta de controle do usuário sobre seus dados.

O modelo de identidade centrada no usuário (terceiro estágio) apresenta esforços para que a experiência do usuário seja melhor e para que haja uma maior descentralização das informações e da confiança. Com este modelo começaram a surgir as ideias de que uma identidade digital deveria ficar totalmente sob o controle de seu dono. Entretanto, o foco maior está em duas frentes: consentimento do usuário, dando a este a visibilidade dos atributos que são compartilhados pelo IdP ao SP, e interoperabilidade, para facilitar a autenticação entre múltiplos provedores de serviços.

Neste estágio é possível dar ao usuário o controle total de sua identidade, mas ao custo de ele ter que criar seu próprio serviço de autenticação centrada no usuário, como a instalação de um serviço OpenID, por exemplo. Obviamente, a maior parte dos usuários não têm condições de criar tal serviço e o caminho natural, demonstrado na prática, é o uso de serviços deste tipo disponibilizados por grandes provedores de serviços já consolidados como Facebook, Google e Apple, por exemplo.

Dessa forma, os dados do usuário ainda continuam nas mãos dos provedores, que detêm o controle sobre os mesmos, e estes podem desabilitar um usuário a qualquer momento, mesmo sem apresentar justificativas para tal. Além disso, observa-se uma centralização ainda maior do processo de autenticação em alguns poucos e grandes provedores de serviços, o que nos remete a um dos problemas básicos dos primeiros estágios, que é a centralização dos dados no provedor de serviço, sem o controle do usuário.

Com a crescente necessidade do usuário ter mais autonomia sobre seus dados surgiu o conceito de Identidade Digital Descentralizada (IDD), também chamada de Identidade Autossoberana [do inglês *Self-Sovereign Identity* (SSI)], sendo esse o quarto estágio, segundo Allen (2016). Várias iniciativas estão sendo postas em prática com esse objetivo, desde aquelas que se apoiam em técnicas de criptografia até as que se baseiam em regras contratuais entre usuários e provedores. Novas técnicas têm surgido para viabilizar a IDD, destacando-se aquelas baseadas em tecnologia *blockchain*.

3.2.2 Cenário internacional de federações acadêmicas

Os pesquisadores devem ser capazes de acessar e compartilhar recursos facilmente para colaborar. O crescimento das federações acadêmicas em nível nacional e internacional provou ser um modelo de sucesso para aumentar de forma eficiente a colaboração científica. O serviço *eduGAIN* possibilita que pesquisadores possam usar suas credenciais institucionais para acessar inúmeros provedores de serviços disponíveis na interfederação. No entanto, o serviço não foi projetado para ambientes

abertos e dinâmicos que os membros de uma Organização Virtual (OV)[4] necessitam. Os membros das OVs precisam gerenciar, acessar e compartilhar recursos com base em suas funções nessas colaborações. Portanto, as colaborações de pesquisa precisam de uma IAA adequada que permita aos pesquisadores acessar os recursos online de que precisam e que estão em federações heterogêneas.

O projeto *Authentication and Authorisation for Research and Collaboration* (AARC), financiado pelo programa de incentivo à pesquisa e inovação Horizon 2020 da União Europeia, foi lançado em 2015 e finalizado em dezembro de 2019. O projeto teve como objetivo: (i) identificar os requisitos necessários em pesquisa colaborativa internacional, indo além das capacidades de acesso federado atuais; (ii) entregar um modelo de arquitetura [AARC *Blueprint Architecture* (BPA)], (iii) um grupo de diretrizes e políticas para permitir interoperabilidade no contexto de autenticação e autorização, passíveis de serem integrados aos ambientes de produção das instituições, bem como (iv) mostrar os benefícios de uma IAA abrangente para comunidades de pesquisa (e-infraestruturas) e testar novas soluções e abordagens AAI emergentes, por meio de casos de uso da comunidade e pilotos de integração da infraestrutura.

A Figura 1 mostra a visão geral da versão final das camadas da *AARC BPA*, composta por identidade do usuário (topo), serviço de atributo da comunidade (esquerda), transposição do protocolo de acesso (centro), autorização (direita) e serviços final - *Service Provider*s (SPs) (base). As setas em vermelho representam o fluxo de informação de usuário não autenticado, em azul usuário autenticado, em roxo o fluxo de informação sobre autorização e em verde sobre fluxo de informação de atributos.

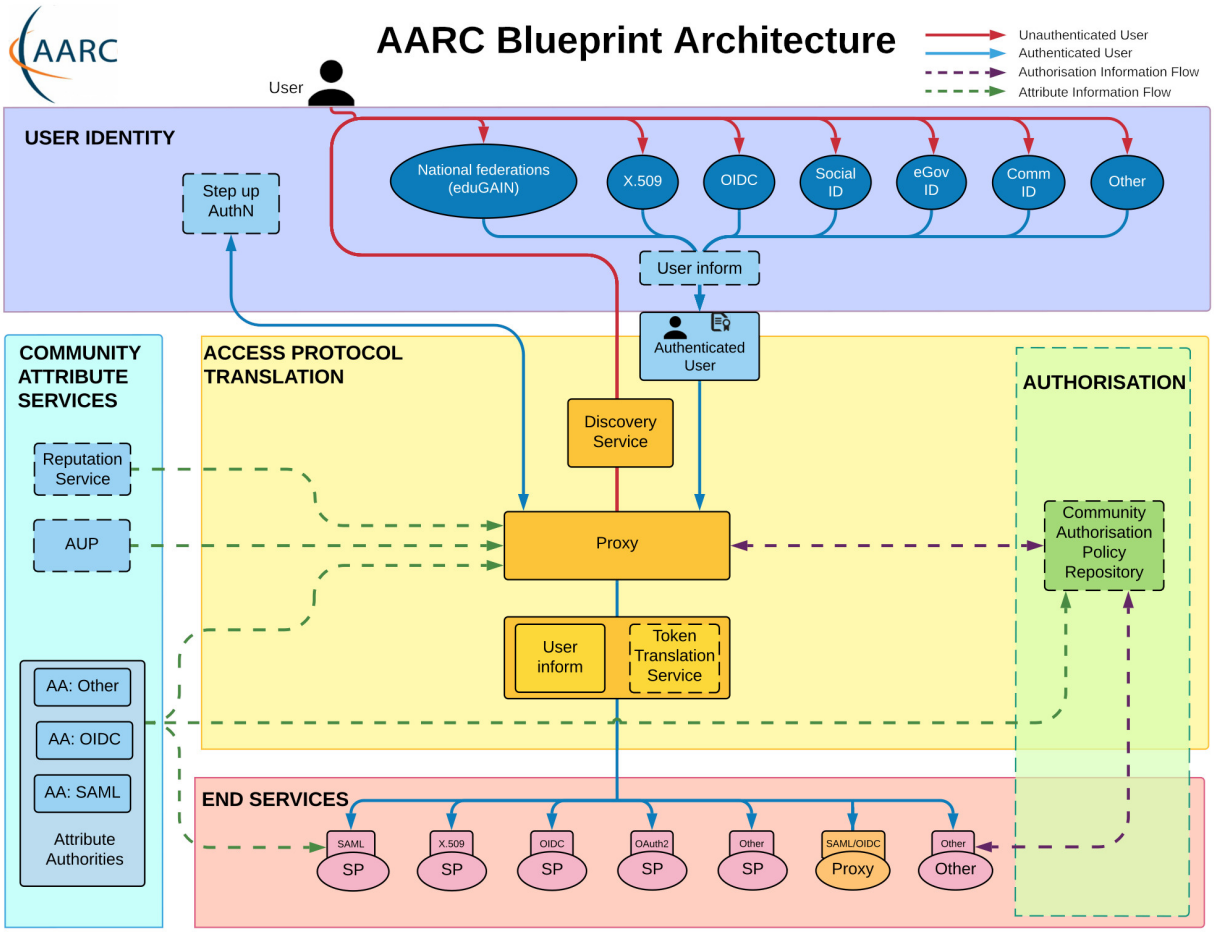

Figura 1: Versão Final do Modelo de Arquitetura AARC (LIAMPOTIS; CONSORTIUM; MEMBERS, 2019)

[4]Uma OV é constituída por um grupo aberto composto por pessoas e instituições, que vão além das federações acadêmicas, que trabalham com pesquisas colaborativas e infraestruturas de *e-science* e que têm como objetivo resolver problemas complexos.

Desde que foi lançado, o modelo de arquitetura do projeto AARC é fortemente recomendado pela *Research and Education FEDerations group* (REFEDS)[5]. No documento de visão de futuro de 2018 (WANGHAM et al., 2018), o modelo também foi recomendado como um modelo de referência para o desenvolvimento de soluções de pesquisas colaborativas (OVs).

A GÉANT foi uma das principais colaboradoras do projeto AARC e, com base na AARC BPA, desenvolveu o serviço eduTEAMS[6], o qual expande a eduGAIN. O eduTEAMS permite que pesquisadores e outros membros da comunidade de pesquisa possam criar e gerenciar times virtuais[7], 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 Serviços *Web* e nativos. 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.

Periodicamente a REFEDS apoia atividades de grupos de trabalho com o intuito de promover o diálogo abordando problemas e objetivos específicos sobre federação. O grupo de trabalho *REFEDS Assurance* projetou o *REFEDS Assurance Suite* para atender às necessidades das federações acadêmicas de um conjunto comum e leve de especificações sobre garantias para o fortalecimento da confiança nas federações. O *Assurance Suite* é composto pelo *REFEDS Assurance Framework* (REFEDS RAF)[8], que define os requisitos para garantia da confiança em identidades (identificador e atributos) e duas especificações: o *REFEDS Single Factor Authentication Profile* (REFEDS SFA) e o *REFEDS Multi Factor Authentication Profile* (REFEDS MFA) para garantia de autenticação.

Outro grupo de trabalho da REFEDS é o *Security Incident Response Trust Framework for Federated Identity* (SIRTFI), que investiga processos para expressar requisitos de tratamento de incidentes de segurança como um perfil de garantia para federações e outros requisitos necessários para implantar e aprimorar efetivamente os processos de resposta a incidentes em federações acadêmicas. Atualmente, o grupo está trabalho em uma nova versão da especificação (versão 2.0).

Há também o grupo REFEDS de Desenvolvimento de Categorias de Entidade, cujo objetivo é explorar o potencial desenvolvimento de categorias de entidades (*Research & Scholarship*) e outras categorias adicionais que possam surgir. O foco atual do grupo é trabalhar em uma versão 2 do REFEDS R&S. Já o grupo *Baseline Expectation* definiu um conjunto comum de comportamentos operacionais necessários das organizações participantes para estabelecer uma base de referência de confiança para as federações. Em abril de 2021, com base no documento elaborado pelo grupo de trabalho, a REFEDS publicou a especificação *Identiy Federation Baseline Expectations*(AXELSSON; BUXEY, 2021) com as orientações para os responsáveis pela operação de Provedores de Identidade, Provedores de Serviço, Federações e Interfederações.

Com o objetivo de identificar o valor da federação e definir recomendações para melhorias no futuro, a REFEDS criou o grupo de trabalho Federação 2.0. Este grupo segue um processo estruturado para reunir contribuições de uma ampla gama de fontes de informação e perspectivas individuais, a fim de revisar os estados passados e atuais e formular possíveis cenários futuros para a evolução das federações de pesquisa e educação. Esses dados estão sendo analisados e sintetizados para articular o valor da federação acadêmica, identificar mudanças potenciais que podem aumentar esse valor e recomendar ações que as federações podem tomar para aumentar seu valor ao longo do tempo.

[5] A missão do grupo da REFEDS é articular as necessidades mútuas das federações de identidade de pesquisa e educação em todo o mundo.

[6] https://www.eduteams.org

[7] Também conhecidos como organizações virtuais ou organizações colaborativas.

[8] https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0

3.2.3 Autenticação federada pra aplicações *web*

Na 4ª reunião ordinária do CT-GId no ano de 2013 (CT-GID, 2013) foi dito que a CAFe trouxe vantagens para o usuário, como a possibilidade de usar uma única conta de usuário e senha para interagir com todos os Provedores de Serviço [SP] da federação, além da autenticação única [*Single Sign-On* (SSO)]. Porém, o modelo federado introduziu um componente intermediário, inicialmente chamado como *Where Are You From* (WAYF) e posteriormente como *Discovery Service* (DS), que para o usuário aparece como uma terceira parte a quem também deve confiar. Concluiu-se que a gestão de identidades deveria ser o mais transparente possível para os usuários, evitando passos intermediários e redirecionamentos HTTP, uma vez que esses buscam pelo serviço desejado e não precisam entender o funcionamento da implementação do modelo federado.

O projeto SeamlessAcces (SEAMLESSACCESS, 2021), ainda em fase beta, é uma iniciativa conjunta da GÉANT, Internet2, *National Information Standards Organization* (NISO) e *International Association of STM Publishers* (STM) que tem por objetivo resolver os atuais problemas de usabilidade das federações acadêmicas baseadas em asserções *Security Assertion Markup Language* (SAML). O projeto SeamlessAccess permite uma experiência de SSO verdadeira e transparente nas federações acadêmicas. O DS continua a existir, porém os SPs podem escolher um dos três modos como o DS seria apresentado aos seus usuários: modo limitado, semelhante ao que se tem atualmente na CAFe, ou seja, com o redirecionamento HTTP para o DS bem evidente (SP $\rightarrow$ DS $\rightarrow$ IdP $\rightarrow$ SP); modo padrão, onde o DS aparece embarcado e integrado com a página *web* do próprio SP e o redirecionamento ao IdP só aconteceria no primeiro acesso do usuário durante aquela sessão do navegador *web* (SP $\rightarrow$ IdP $\rightarrow$ SP); modo avançado, com comportamento semelhante ao modo padrão, porém permite ao SP indicar a listar de IdP que confia.

Apesar de não obrigatório, o projeto SeamlessAcess indica como uma boa prática aos Provedores de Identidade [*Identity Provider* (IdP)] a implementação do serviço *Consent-informed Attribute Release* (CAR) (INTERNET2, 2021). Esse serviço apresenta uma evolução se comparado com o atual formulário de consentimento de usuário presente na CAFe, pois dá ao usuário o poder de escolher quais atributos dos solicitados pelo SP, que não são obrigatórios para o funcionamento do serviço, irá compartilhar.

Outro ponto de atenção, de acordo com WebIncubatorCG (2021), é que as tecnologias usadas pelas federações acadêmicas estão fundamentadas sobre primitivas de baixo nível dos navegadores *web* como redirecionamentos, *cookies* e *pop-up*, que frequentemente sofrem abusos por serviços de rastreamento de usuários. De acordo com WebIncubatorCG (2021), os principais fabricantes de navegadores *web*, Apple, Google e Mozilla, atuam em uma frente comum para proteger a privacidade de seus usuários e o primeiro ponto já implementado consiste no bloqueio de *cookies* de terceiros (WILANDER, 2020; VALE, 2021; WOOD, 2019). Em WebIncubatorCG (2021) é proposta uma nova *Application Programming Interface* (API) para os navegadores *web* proverem suporte às aplicações que seguem o modelo federado sem depender das primitivas de baixo nível que são usadas atualmente. Os proponentes reconhecem que uma solução poderá levar anos até ser definitivamente implementada pelos navegadores, mas antes que isso ocorra, é fato que as tecnologias atuais usadas pelas federações acadêmicas precisarão passar por atualização para explorar a nova API que está sendo proposta.

3.2.4 Autenticação multifator

A autenticação multifator [*Multi-Factor Authentication* (MFA)] saiu de um estágio onde poucos provedores de serviços a ofereciam como uma solução para usuários mais preocupados com a segurança de suas contas, para um estágio onde está presente na maioria dos provedores de serviços e, em alguns casos, sendo imposta para todos os usuários desses serviços.

As senhas descartáveis [*One Time Password* (OTP)] é uma das tecnologias mais utilizadas pelos provedores de serviços para oferta da MFA. As primeiras soluções com OTP faziam uso

de *hardware* específico (*token* criptográfico) ou de cartão impresso com um conjunto limitado de códigos. Atualmente, o OTP se dá por meio do envio de mensagens curtas de texto [*Short Message Service* (SMS)], envio de códigos para o email do usuário ou pelo uso de aplicativos específicos instalados em telefones inteligentes (*i.e.* Google Authenticator, Authy, etc). Vale destacar que o *National Institute of Standards and Technology* (NIST) (GRASSI et al., 2017), considerou que o uso de SMS não é seguro, visto que é possível personificar a estação do usuário (telefone móvel), ou mesmo relevar a senha recebida para uma parte maliciosa, por meio de um aplicativo malicioso em execução no telefone do usuário.

Com a popularização dos telefones inteligentes e dos aplicativos móveis, a autenticação biométrica se mostrou como uma alternativa interessante às senhas descartáveis. Contudo, grande parte das aplicações fazem uso de soluções proprietárias, não interoperáveis e geralmente optam pela captura e a transmissão da face do usuário, não usufruindo assim dos sensores biométricos presentes nesses dispositivos, como por exemplo, leitor de impressão digital.

Os protocolos de autenticação *Fast IDentity Online* (FIDO) *Universal Authentication Framework* (UAF) (MACHANI et al., 2017) e *Universal 2nd Factor* (U2F) (SRINIVAS et al., 2017) surgiram em 2014 com o intuito de aumentar a robustez do processo de autenticação em sistemas *web*. Fundamentados sobre criptografia de chave pública, as especificações FIDO permitem a autenticação com dois fatores (U2F) e até mesmo a autenticação sem o uso de senha (UAF), ou seja, o FIDO seria o único fator de autenticação. Com o FIDO2, combinou-se as funcionalidades dos protocolos UAF e U2F e dois novos padrões foram propostos: WebAuthN (W3C, 2019b), uma API para navegadores *web*; e *Client to Authenticator Protocol* (CTAP) (LINDEMANN et al., 2019), um protocolo que permite a comunicação via USB, *Near Field Communication* (NFC) ou *Bluetooth Low Energy* (BLE) entre os navegadores *web* e dispositivos FIDO2, que podem ser desde chaves de segurança USB a telefones inteligentes.

O padrão WebAuthN está em ampla adoção pelos principais provedores de serviço comerciais e por fabricantes de sistemas operacionais para computadores pessoais e dispositivos móveis (GOOGLE, 2018; MICROSOFT, 2019; APPLE, 2021). Cabe citar ainda os resultados do projeto de P&D GT-AMPTo da RNP (MELLO et al., 2020), que adicionaram a funcionalidade de autenticação multifator no IdP Shibboleth versão 3.1, sendo o WebAuthN uma das tecnologias ofertadas. Importante ainda pontuar que o padrão WebAuthN também está sendo amplamente discutido na REFEDS e na federação InCommon como o padrão indicado para implementar uma solução de autenticação sem senha[9].

3.2.5 Autenticação em cenários IoT

Algumas plataformas IoT fornecem *Identity Provider as a Service* (IdPaaS) para autenticação de usuário e de dispositivo, como *Amazon Web Services* (AWS) IoT, Microsoft Azure IoT, plataforma Google Cloud IoT e WSO2. A maioria fornece autenticação de dispositivo baseada em certificado, como AWS IoT, Azure IoT, WSO2 ou ainda autenticação baseada em criptografia de chave pública por dispositivo usando *JSON Web Token* (JWT), como *Google Cloud IoT Platform* e *WSO2 platform*.

O crescente número de dispositivos na *Internet of Things* (IoT) reforça que a gestão da identidade, com foco na autenticação e autorização nesse ambiente, se tornará cada vez mais complexa. Por exemplo, considerando bilhões de dispositivos ligados à IoT, se torna não escalável a utilização de infraestruturas de chaves públicas. De acordo com (OLIVEIRA et al., 2018), os protocolos devem ser leves e fáceis de implementar, exigindo que as infraestruturas de chave pública tradicionais e as caras operações de tratamento de certificados sejam restritas aos nós mais poderosos e melhor conectados. Uma abordagem para tal problema é empregar criptossistemas de certificação implícita, como a criptografia baseada em identidade [*Identity-based cryptograhy* (IBC)] e a criptografia sem certificados [*Certificateless Public Key Cryptography* (CLPKC)]. Além disso, considerando algoritmos assimétricos, tem-se ainda, em geral, a restrição de recursos desses dispositivos, o que pode

[9] https://www.incommon.org/news/october-community-updatepasswordless-authentication-and-saml-identifiers

ser considerado ainda como outro limitador. Isto motivou o desenvolvimento de novas primitivas criptográficas, chamadas de criptografia leve. Construções simétricas importantes são LS-Designs, redes Feistel e Adição-Rotação-Soma (ARX) modernas e a cifra de bloco PRESENT. No caso de funções *hash*, um projeto pode até mesmo compensar propriedades de segurança avançadas (como resistência à colisão) pela simplicidade em alguns cenários, como por exemplo o uso de MACs curtos usando Sip Hash ou assinaturas digitais construídas a partir de *hashs* com entradas curtas (não resistentes à colisão). Outra opção eficiente e forte de *hash*, é o BLAKE3. Destacam-se ainda as formas de autenticação leves que utilizem esquemas simétricos de compartilhamento de chaves, como proposto pelo GT-Cofee da RNP (SANTOS et al., 2020), até a utilização de características intrínsecas dos dispositivos para uma comunicação segura com a rede.

A geração de chaves simétricas, ou identificadores únicos utilizando funções físicas não-clonáveis [*Physical Unclonable Function* (PUF)] existe desde a última década, porém a sua utilização ainda continua de interesse para a pesquisa de segurança e gestão de identidade. Um exemplo de função física não clonável é a consulta a um circuito integrado do dispositivo final, que apesar de ter sido impresso em até um mesmo lote, contém características únicas, como seu atraso de processamento, desgaste do circuito, dentre outros. Além disso, é possível incluir pequenas porções, ou componentes, no circuito para realizar exatamente essa função. Desta forma, a geração de uma identificação a partir de tais circuitos pode ser uma forma de utilização para a autenticação de um dispositivo, e além disso, a identificação gerada pode representar uma sequência binária referente a um número verdadeiramente aleatório, o que motiva, por exemplo, a sua utilização também como semente para chave(s) de um método de criptografia como o *Advanced Encryption Standard* (AES). Assim, a geração de identificação única para dispositivos utilizando essa funcionalidade, apresenta bastante relevância para a área de autenticação, confidencialidade dos dados e não repúdio.

A utilização de características intrínsecas dos dispositivos pode ser utilizada para identificação dos mesmos. Quando pensamos em identificar um dispositivo dentre milhões ou, até mesmo de bilhões, características únicas devem ser levadas em consideração. A utilização de características como o sinal de radiofrequência, ou ciclos internos a um dispositivo, podem identificá-lo de forma única. Um exemplo que podemos citar é a identificação de dispositivos móveis em redes sem fio através do comportamento de seus parâmetros, como localização, frequência utilizada, taxa de envio de datagramas, dentre outras. Tais formas devem ser levadas em consideração para a identificação e merecem a atenção da área de GId.

Por fim, outra interessante abordagem para autenticação de dispositivos é o emprego de tecnologias baseadas em *blockchain*. Este uso será melhor descrito na seção 3.2.7.

3.2.6 Autenticação em cenários da saúde

Relacionado à *Internet of Healthcare Things* (IoHT) [ou *Internet of Medical Things* (IoMT)] e às *Wireless Body Area Network* (WBAN), destaca-se a popularização dos dispositivos vestíveis e a necessidade de incremento do nível de segurança exigido pelos dados pessoais gerados por eles. Os dispositivos vestíveis detectam ou coletam dados gerados pelo próprio corpo do usuário ou de seu ambiente, transmitindo-os por meio de canais de comunicação sujeitos a espionagem e outros tipos de ataques, sendo então fundamental proteger a privacidade do usuário, garantindo a confidencialidade de seus dados pessoais sensíveis. Nesse contexto, o acordo de chaves é uma tarefa importante para soluções de segurança e privacidade de dados. Ele desempenha um papel crucial no suporte à criptografia de chave simétrica pelo acordo de uma chave compartilhada entre um par de dispositivos de comunicação vestíveis. Porém, dispositivos vestíveis apresentam um conjunto de restrições computacionais, obrigando a novos protocolos de acordo-chave que economizam recursos computacionais (por exemplo, memória) e inibindo o uso de soluções sofisticadas e caras existentes. Portanto, há uma necessidade crescente de projetar novos protocolos de acordo de chave para melhorar a segurança da rede vestível. Existem, assim, propostas de protocolos de acordo de

chave simétrica de baixo custo empregando sinais vitais do usuário [*e.g.*, *Eletrocardiograma* (ECG)] como parte da aleatoriedade necessária na geração de chave compartilhada e em sua proteção.

3.2.7 Identidade digital descentralizada

Além de aplicações relacionadas a criptomoedas, as *blockchains* têm se mostrado úteis em outros casos de uso como registro notarial, controle de cadeia de suprimentos, entre outros, devido às suas propriedades características de descentralização, confiabilidade e persistência. Várias propriedades das *blockchains* coincidem com algumas das propriedades desejáveis em uma IDD. Por exemplo, *blockchains* públicas fornecem um domínio descentralizado, fora do controle de um agente único. Os dados armazenados em uma *blockchain* estão sempre disponíveis quando são necessários. O proprietário dos dados armazenados em uma *blockchain* tem controle sobre como e quando tais dados são compartilhados com outros usuários.

Um controle mais fino sobre o nível de dados de identidade que são liberados a terceiros pode ser exercido por pacotes de software chamados de contratos inteligentes em *blockchains* que proveem suporte a este tipo de contratos. Além disso, uma *blockchain* também pode ajudar na implantação de um sistema de IDD devido às suas propriedades de imutabilidade dos dados confirmados, controle distribuído, transparência e outros que não estão presentes em outros sistemas distribuídos.

Por esses motivos, uma *blockchain* pode prover uma interessante base para a implementação prática de sistemas de gestão de identidades com características de IDD. Ferdous, Chowdhury e Alassafi (2019) analisaram quatro sistemas de gestão de identidades descentralizadas baseados em blockchains: uPort/Serto [10], Jolocom [11], Sovrin [12] e Blockcerts [13]. Desses, apenas Jolocom e Sovrin se propõem como sistemas de suporte a IDD. Segundo a análise feita no artigo, Sovrin é a plataforma que mais possui propriedades de uma IDD ideal. No caso de Jolocom, são identificadas só algumas das propriedades, ficando as demais em aberto.

Jolocom (FEI, 2018) foi desenvolvido sobre a *blockchain* da criptomoeda Ethereum e consiste de vários contratos inteligentes. Os usuários fazem uso de um aplicativo móvel para interagir com o sistema a fim de criar, gerenciar e compartilhar suas identidades. A documentação ainda não detalha todos os aspectos da implementação para que se possa compreender o quão próximo esse sistema está de um IDD ideal. Um *whitepaper* mais atual sobre este sistema está disponível em (FEI, 2019).

Sovrin (D. REED; HARDMAN, 2016) é um sistema proposto pela *Sovrin Foundation*, uma entidade que procura facilitar e promover as ideias relacionadas a IDD. O sistema Sovrin é baseado em sua própria *blockchain* chamada *Sovrin Ledger* que usa um novo mecanismos de consenso chamado Plenum. Um usuário pode interagir com o sistema por meio de um aplicativo móvel ou um navegador web para criar, gerenciar e compartilhar sua identidade. O sistema também possui agentes de software que são considerados Terceiros Confiáveis e utilizados na certificação de dados de identidade do usuário. Um usuário pode fazer alegações sobre si mesmo ou sobre outros participantes e tem acesso a um nível de controle de dados que permite que escolha exatamente quais partes de seus dados de identidade poderão ser compartilhados com outras partes. Apesar de Sovrin ser um dos sistemas mais completos e que mais se aproxima da ideia de uma IDD ideal, ele ainda está em fase de desenvolvimento, não deixando claro ainda se consegue atender todas as promessas que faz.

Na Subsubseção 3.2.8 é descrita uma iniciativa da União Europeia no sentido de aproveitar as características de IDD na criação de uma nova identidade digital para o bloco.

[10] https://www.serto.id
[11] https://jolocom.io
[12] https://sovrin.org
[13] https://www.blockcerts.org

3.2.8 Conjunto de instrumentos da comunidade europeia para identidade digital

Como apresentado na Seção 1, a pandemia de Covid-19 acelerou a mudança e a relevância da digitalização da sociedade, demandando assim por meios seguros para identificar e autenticar usuários em serviços digitais *online*. A Comunidade Europeia publicou uma orientação que fixa como 2030 o limite para digitalização dos processos e a implantação de um sistema de identidade confiável e controlado pelo usuário, permitindo a cada usuário o controle sobre sua presença e interações *online* (RECOMENDAÇÃO..., 2021).

O Regulamento eIDAS (REGULAMENTO..., 2014) visa permitir o reconhecimento de identidades eletrônicas governamentais além das fronteiras para acessar serviços públicos com as mesmas garantias legais que os processos equivalentes que usam documentos de identificação com suporte em papel. Em RECOMENDAÇÃO... (2021) é proposta uma alteração no Regulamento eIDAS que visa fornecer aos usuários carteiras digitais pessoais autossoberanas, com controle total e exclusivo por parte do usuário, como forma de garantir um acesso fácil e seguro a serviços públicos ou privados. Aliado a isso, pretende-se criar um novo serviço de confiança qualificado para certificados de atributos relacionados com as identidades, como endereço, idade, gênero, estado civil, nacionalidade, qualificações acadêmicas e profissionais, títulos, licenças, renda, etc.

O documento apresenta ainda preocupações sobre a necessidade de um processo centralizado e coordenado para a escrita de um conjunto de instrumentos (*toolbox*), o qual terá detalhes sobre uma arquitetura de referência que cobrirá quatro dimensões (RECOMENDAÇÃO..., 2021): fornecimento e intercâmbio de atributos de identidade; funcionalidade e segurança das carteiras europeias de identidade digital; uso das carteiras de identidade digital e correspondência das identidades; e governança. Por fim, o documento apresenta um cronograma indicando que os trabalhos para escrita do conjunto de instrumentos deverá iniciar em setembro de 2021 e que a publicação deste conjunto deverá ocorrer até 30 de outubro de 2022.

3.2.9 Credenciais verificáveis e identificadores descentralizados

Credenciais verificáveis [*Verifiable Credentials* (VC)] consistem de um padrão aberto W3C (W3C, 2019a) para credenciais digitais. Assim como as credenciais com suporte em papel (i.e. documento de identidade), as VCs permitem representar informações sobre seu detentor. Porém, por serem assinadas digitalmente, as VCs são mais adequadas para o ambiente digital, pois é possível ter garantia sobre a integridade e autenticidade das mesmas.

VCs podem ser emitidas por qualquer pessoa, dispositivo ou entidade, sobre qualquer informação e podem ser apresentadas e verificadas por qualquer pessoa ou entidade. No padrão são definidas três entidades: emissor, aquele que cria a credencial; detentor, aquele quem recebe e armazena a credencial para um uso posterior; verificador, aquele que recebe a credencial e realiza o procedimento para verificar a integridade e autenticidade da mesma. Dessa forma, o modelo de confiança do padrão consiste no emissor confiar no detentor, o detentor confiar no verificador e o verificador confiar no emissor.

Segue-se aqui o modelo de gestão de identidade centrado no usuário (veja Subsubseção 3.2.1), de forma que o detentor da credencial possui controle total sobre os atributos relacionados com sua identidade. A VC pode ser representada como um documento *JavaScript Object Notation* (JSON) que contém: o contexto, emissor, instante da emissão, validade, tipo, sujeito, atributos do sujeito e prova criptográfica para garantir sua integridade e autenticidade. A prova criptográfica pode ser uma assinatura digital expressa como um JWT ou usando esquemas de confiança zero.

Baseado no paradigma da Identidade Digital Descentralizada (veja Subsubseção 3.2.7), os identificadores descentralizados [*Decentralized Identifier* (DID)] (W3C, 2021) consistem em um tipo de identificador que permite a verificação, de forma descentralizada, de uma identidade digital. Tais identificadores são geralmente usados em uma VC e são associados com um sujeito (detentor da

VC) de forma que uma VC possa facilmente ser portada de um repositório de credenciais para outro sem a necessidade da emissão de uma nova credencial.

3.2.10 Autorização e controle de acesso

Dentro da gestão de identidades, autorização e controle de acesso são dois conceitos, erroneamente utilizados como sinônimos, que envolvem um conjunto de funcionalidades para restringir o acesso a recursos ou serviços. De acordo com Jøsang (2017), autorização corresponde à especificação de políticas de acesso, atribuindo privilégios a usuários ou sistemas. Políticas de acesso normalmente envolvem um conjunto de regras com direitos, propriedades, ações e permissões para realizar essas ações. O controle de acesso consiste então na aplicação das políticas de acesso, efetivamente decidindo se um determinado sujeito (p.ex. um usuário) pode ou não acessar um determinado recurso, fazendo com que o acesso a recursos e/ou serviços só seja concedido àqueles usuários autorizados para tal.

Dentre as tendências observadas neste tópico podemos citar sua aplicação nos diversos cenários que exploram IoT, tais como *Industrial Internet of Things* (IIoT), *Internet of Medical Things* (IoMT) e seu uso em ambientes de casas e prédios inteligentes, e veículos conectados. Ravidas et al. (2019) apresenta uma análise sobre o uso de ferramentas para autorização e controle de acesso para IoT. Dentre as conclusões apresentadas, os autores identificaram que é necessário o desenvolvimento de soluções que levem em considerações características do domínio de aplicação e que os padrões atuais, como o OAuth2 (HARDT, 2012), não são suficientes para as diversas aplicações de IoT. Outro ponto importante identificado pelos autores é a necessidade de administração de políticas multi-domínio, onde dispositivos e recursos são gerenciados por múltiplas autoridades, além de questões ligadas a avaliação de confiabilidade e validação.

Outra tendência observada está relacionado ao conceito de mineração de políticas de acesso. Este é um problema já conhecido pela comunidade (MOLLOY et al., 2009), onde informações históricas de um sistema, por exemplo *logs*, são coletada e analisadas em busca de se identificar os comportamentos dos usuários e assim extrair políticas de acesso. Tal abordagem pode ser utilizada para a identificação de novas políticas, assim como para verificação de conformidade dos sistemas implementados com as políticas existentes. Com os recentes avanços e relevância da área de aprendizagem de máquina este tópico continua recebendo atenção da comunidade científica. Por exemplo, Anderer et al. (2021) apresenta um conjunto de *datasets* para o problema de mineração de papéis em políticas de acesso.

3.2.11 Identidades para serviços de nuvem em modelo de confiança zero

Assim como usuários humanos, sistemas de software precisam de identidades que serão usadas para autorização e controle de acesso. Tradicionalmente, esta identidade é atribuída de forma manual, a partir de uma configuração, e a autorização é definida com base em aspectos como a localização daquela aplicação ou serviço (por exemplo, cria-se uma regra em um *firewall*). No entanto, este modelo não é adequado quando se observam as tendências atuais de desenvolvimento de microsserviços que serão distribuídos em dispositivos na borda da rede ou em múltiplas nuvens.

O desenvolvimento de aplicações baseadas em microsserviços com distribuição mais dinâmica impede, por exemplo, que regras de *firewall* sejam usadas para controle de acesso. Além disso, considerar localização para construção das políticas de autorização é um processo bastante passível de erros e que se torna proibitivo quando as aplicações passam a ser compostas por dezenas ou centenas de serviços.

O modelo de confiança zero defende que mesmo aplicações em uma rede local usem autenticação, autorização e criptografia nas suas comunicações. Assim, se os microsserviços são obrigados a ter

todas as conexões protegidas, não é preciso se preocupar com a configuração de serviços como *firewalls* e *Virtual Private Network*s (VPNs), liberando estes serviços para executar em qualquer lugar. Por causa desta flexibilidade, somada ao ganho de robustez gerado pela adição de controles de segurança, este modelo tem se tornado tendência e também tem sido fortemente associado ao desenvolvimento de microsserviços.

Um dos desafios para o modelo de confiança zero é então o provimento de identidades de forma automática e de forma a não complicar ainda mais os processos de desenvolvimento dos serviços e de geração de políticas de autorização. Duas implementações desse modelo são a BeyondCorp[14], da Google, e a *SPIFFE Runtime Environment* (SPIRE)[15], implementação de código aberto incubada pela *Cloud Native Computing Foundation* (CNCF)[16].

Para implementar o modelo de confiança zero, o BeyondCorp determina a inserção de *proxies* na frente de todos os clientes e serviços. Os *proxies* dos clientes assumirão identidades em nome dos clientes e usarão estas identidades em todas as comunicações. De forma semelhante, os *proxies* dos serviços restringirão o acesso aos serviços às identidades autorizadas, garantido que todas as conexões serão autenticadas, autorizadas e criptografadas. As identidades são geradas através de serviços da própria Google e podem ser identidades de contas de usuários ou contas de serviços.

O SPIRE (FELDMAN et al., 2020) é uma implementação aberta do padrão *Secure Production Identity Framework For Everyone* (SPIFFE). De forma semelhante ao BeyondCorp, ele permite que clientes e servidores legados possam integrar um ambiente de confiança zero através de *proxies* que intermedeiam todas as conexões. No caso do SPIRE (e de outras implementações que usam identidades SPIFFE, como o Istio[17]), as identidades são providas por um processo de atestação que pode ser baseada em propriedades do ambiente ou da própria aplicação. Por exemplo, uma identidade específica pode ser provida automaticamente para uma aplicação caso ela seja executada em uma máquina virtual que pertence a um determinado grupo de segurança na nuvem da AWS.

O processo de gestão de identidades e de geração de políticas de autorização pode ser então simplificado atribuindo a mesma identidade para instâncias da aplicação consideradas equivalentes. Por exemplo, a mesma identidade acima poderia ser atribuída para instâncias executando num certo grupo de segurança da AWS ou em uma certa conta de serviço em um cluster Kubernetes nas premissas da organização. Desta forma, o controle de acesso não precisa distinguir entre um acesso local ou vindo do grupo de segurança correto na AWS, pois ambos usam a mesma identidade (mesmo que a diferenciação ainda seja possível para razões de responsabilização). No caso do SPIFFE, as identidades são tipicamente certificados digitais (X.509v3) com informações adicionais nos campos *Subject Alternative Name* (SAN). O uso de certificados digitais simplifica a implementação de serviços que suportam nativamente este padrão e permite a interoperabilidade com serviços que suportam apenas certificados digitais comuns (sem as identidades SPIFFE).

3.2.12 Integração eduroam ao Hotspot 2.0/Passpoint e redes 5G

O *Education Roaming* (eduroam) (SAADE et al., 2013) é uma federação de acesso à rede sem fio de forma segura e federada, e apesar de estar presente em mais de 100 países com milhares de pontos de acesso espalhados pelo mundo, há áreas que podem não divulgar sua rede sem fio (SSID - nome de rede sem fio divulgado - eduroam). Porém, com base na emenda ao padrão IEEE 802.11, chamada de IEEE 802.11u[18], ficou suportado o tratamento de mensagens e conexões entre federações Autenticação, Autorização e Accounting (AAA) baseadas no IEEE 802.1X e EAP.

[14] https://cloud.google.com/beyondcorp

[15] https://spiffe.io

[16] Fundação criada para impulsionar a adoção de computação nativa da nuvem. Entre seus projetos graduados estão o Kubernetes e o Conteinerd. https://cncf.io

[17] https://istio.io

[18] https://standards.ieee.org/standard/802_11u-2011.html

Em 2020 o consórcio eduroam se associou ao *Wireless Broadband Alliance* (WBA)[19]. A WBA tem a intenção de ser uma grande federação (ou unir federações já existentes) para o acesso sem fio seguro, eliminando os pontos de acesso sem segurança (*public-guest Wi-Fi*), e, mais que isso, expandir a conexão sem fio segura entre parceiros WBA sem a necessidade de efetivamente o SSID de uma certa rede (*e.g.*, eduroam) precise estar sendo divulgada.

Para possibilitar essa ambiciosa proposta, a WBA se apoia no padrão citado IEEE 802.11u, que por sua vez foi implementado em parte e chamado de Hotspot 2.0, ou ainda Passpoint. A Wi-Fi Alliance, que certifica equipamentos que implementam o padrão IEEE 802.11 (Wi-Fi), agora também vem certificando equipamentos com o selo Passpoint, demonstrando que eles estão em conformidade com o padrão. Sistemas operacionais, como Windows 10, Android, Linux e iOS também já estão vindo com a possibilidade de habilitação dessa tecnologia, e normalmente a chamam de Hotspot 2.0 em suas configurações.

Essa é, além de uma oportunidade de facilitação do acesso à rede sem fio de maneira segura, uma oportunidade da integração de forma facilitada às redes móveis de operadoras de telecomunicações. Pensando na possibilidade de escoamento de tráfego de redes móveis 5G em redes sem fio locais e no provimento de segurança na comunicação nesse ambiente, a utilização do Hotspot 2.0/Passpoint pelo serviço eduroam merece atenção como tendência tecnológica e emergente. Vale destacar serviços relacionados já existentes oferecidos por empresas como a CISCO [20], através do OpenRoaming[21].

4 Visão de futuro

Na Subseção 3.2 foram apresentadas tendências tecnológicas e aplicações emergentes que estão sendo discutidas na academia ou mesmo sendo implementadas ou padronizadas pela indústria. Nessa seção é feita uma distribuição das tendências levantadas dentro de três horizontes de tempo, conforme metodologia descrita na Seção 2.

4.1 Primeiro horizonte: serviços atuais da RNP

4.1.1 Federação CAFe

O governo federal está cada vez mais investindo em soluções de Governo Eletrônico (e-GOV) e o serviço **Conta gov.br** - https://acesso.gov.br - aparece como ambiente de autenticação digital único que possibilitará aos cidadãos ter acesso a serviços públicos digitais de diferentes esferas administrativas. A criação de contas de usuário no serviço se beneficia das bases de dados e outros serviços já mantidos pelo governo federal, dando aos provedores de serviço uma maior garantia sobre a fidedignidade dos dados pessoais dos usuários.

Além de mecanismos que já estão presentes nos IdPs da CAFe, como o SSO e o termo que informa ao usuário quais atributos serão compartilhados com o SP, o serviço **Conta gov.br** conta com autenticação com dois fatores, *captcha* no formulário de autenticação, página *web* que permite ao usuário ver quais dados delegou para cada provedor de serviço, bem como para fazer a revogação dessas permissões, além do nível de confiabilidade dos dados do usuário. As contas de usuário são classificadas em três níveis: bronze – para conta básica criada por meio de carrossel de perguntas; prata – para conta verificada por meio de instituições bancárias ou outras instituições públicas; ouro - para conta comprovada por meio de certificado digital Infraestrutura de Chave Pública Brasileira (ICP-Brasil) ou por meio de biometria do Tribunal Superior Eleitoral (TSE).

[19] https://wballiance.com/
[20] https://www.cisco.com/c/pt_br/solutions/enterprise-networks/802-11ax-solution/openroaming.html
[21] https://wballiance.com/openroaming/

Diante do exposto, entende-se que a curto prazo o serviço **Conta gov.br** pode-se tornar o principal provedor de identidade brasileiro para serviços de instituições públicas. Para as instituições acadêmicas a delegação da autenticação ao serviço **Conta gov.br** pode ser benéfica em diversos cenários, como: para novos ingressos (estudantes ou servidores); para interação com pesquisadores de outras instituições em seus sistemas, etc. Ou seja, o serviço **Conta gov.br** pode chegar a sistemas internos dessas instituições que até hoje não aceitam autenticação federada pela CAFe. E se o fizer, existe a possibilidade de que as instituições de ensino e pesquisa se tornem muito vulneráveis e sejam impedidas de funcionar devido a uma eventual falha no sistema federal e enxerguem a relevância do modelo federado atual (CAFe) e de um futuro modelo ainda mais descentralizado representado pela Identidade Digital Descentralizada.

A REFEDS possui diferentes frentes de trabalho para evolução das tecnologias e políticas usadas pelas principais federações acadêmicas no mundo. A RNP desempenhou um importante papel para implantação da CAFe e sua adoção pelas principais instituições de ensino e pesquisa do Brasil. Contudo, observa-se que diversas iniciativas da REFEDS ainda não chegaram a ser implementadas de forma efetiva na CAFe, tais como as especificações SIRTFI, *Identity Federation Baseline Expectations*, *Multi-Factor Authentication (MFA) Profile*, e *Assurance Framework*[22]. O SeamlessAcces (SEAMLESSACCESS, 2021) é uma iniciativa que impacta diretamente os SPs e tem o intuito de resolver questões de usabilidade e garantir um SSO efetivo nas federações baseadas no SAML. A implantação efetiva de tais iniciativas tendem a demandar mais ações na área de gestão e política e menos ações na área técnica. Não acompanhar tais iniciativas podem deixar os IdPs e SPs da CAFe não compatíveis com seus pares na eduGAIN[23].

4.1.2 ICPedu

O ICPEdu é um projeto de RNP desenvolvido desde o incio da década de 2000 que visa a disponibilização de certificados digitais X.509 para as entidades participantes da rede da RNP. Este serviço surgiu inicialmente com uma ideia de entregar Autoridade Certificadora (AC) para as instituições, dando assim autonomia para elas. Este modelo se mostrou obsoleto e se exauriu a partir de 2015. Desde 2015 a RNP dividiu o ICPEdu em duas vertentes distintas: Certificados *Secure Sockets Layer* (SSL) e Certificados pessoais.

Quanto aos certificados SSL a RNP contratou uma autoridade certificadora da empresa *Globalsign*, a qual permite que as instituições cadastradas possam emitir livremente certificados SSL que são amplamente reconhecidos pelos navegadores de mercado. O grande desafio desta vertente do ICPEdu é permanecer relevante quando comparado com serviços como o *Let's Encrypt*. Por isso é primordial que neste serviço seja implementado o protocolo *Automatic Certificate Management Environment* (ACME) (BARNES et al., 2019) a fim de garantir a automatização e facilidade hoje existente em outros modelos. Existe um espaço ainda para inovação na parte administrativa para a emissão de certificado do tipo estrela (*), visto que estes não são cobertos.

Na segunda vertente de certificados pessoais, a RNP re-lançou junto com o Ministério da Educação (MEC) no início de 2021 o projeto ICPEdu visando oferecer certificado digitais pessoas para os usuários das instituições parceiras por meio de dados extraídos dos IdPs da federação CAFe. Este serviço, embora funcional, provê pouca ou nenhuma usabilidade para as instituições e usuários finais. Isso se deve ao fato que faltam aplicações que permitam o consumo destes certificados de forma a agregar valor as atividades do usuários finais. A grande oportunidade deste tipo de certificado digital esta na produção de documentos eletrônicos assinados digitalmente pelas instituições.

A grande oportunidade e o grande desafio para esta vertente do ICPEdu é o advento das assinaturas digitais avançadas conforme preconizado pela lei federal 14.063/2020 (BRASIL, 2020b). Embora, juridicamente aceitável como um certificado avançado, o certificado pessoal do ICPEdu não

[22] Estas especificações estão disponíveis em https://refeds.org/specifications.
[23] https://edugain.org

atende o decreto federal nº 10.543/2020 (BRASIL, 2020a) e suas portarias. O atendimento deste deverá levar a um novo entendimento da forma como dados pessoais são validados em IdPs da federação CAFe e pode ser algo bastante disruptivo para a federação.

4.1.3 Soluções integradas de GId

A RNP atualmente utiliza soluções de monitoramento e análise de dados voltados para serviços de GId da RNP, como por exemplo o BI4eduroam, BI4CAFe e BI4ICPEdu. É relevante citar que essas ferramentas poderiam ser facilmente expandidas para outras soluções existentes no mercado. Voltando às soluções RNP, em cada um dos serviços é possível analisar dados e perfis, tanto dos usuários quanto dos serviços em si. A partir dessa análise é possível identificar falhas e realizar ações antes de que algo saia do considerado normal. Assim, o monitoramento a partir de dados coletados em tempo real para a geração de credenciais, como o BI4ICPEdu, quanto a análise de autenticação e autorização baseados nos serviços *web* CAFe e sem fio eduroam, com, respectivamente, o BI4CAFe e BI4eduroam, geram conhecimento ao administrador do serviço e a nível de todos os participantes da federação. Desta forma, é importante avaliar a possibilidade de análise refinada dos dados utilizando técnicas de inteligência computacional a fim de incrementar os serviços citados.

4.1.4 Integração eduroam ao Hotspot2.0/Passpoint e redes 5G

O suporte ao Hotspot 2.0/Passpoint é uma realidade na comunidade eduroam, e tende a ser adotada em maior escala pelas federações acadêmicas a partir de 2021. Desta forma, é importante procurar alinhamento com outras federações acadêmicas que têm demonstrado *expertise* no assunto, a fim de entender quais os requisitos para a RNP se integrar ao *hub* do consórcio OpenRoaming [24] e ingressar nessa grande rede de federações. Acreditamos que a integração à redes 5G e a expansão da cobertura da rede eduroam tem grandes chances de sucesso se esta janela de oportunidade for aproveitada.

4.1.5 Autorização

O uso de autorização e controle de acesso em sistemas computacionais segue uma arquitetura de referência bem estabelecida, com processos e componentes bem definidos para lidar com as diversas etapas envolvidas (HU et al., 2014). Entretanto, é comum ainda encontrar diversas instituições que não fazem uso efetivo dos mecanismos de autorização e controle de acesso, embora possuam sistemas de informações que possibilitam seu uso. Tal problema merece ser estudado em busca de soluções que permitam a concretização desses mecanismos.

Nesse sentido, uma frente de trabalho deveria se voltar para o diagnóstico e a correta utilização de mecanismos de autorização e controle de acesso por parte dos *stakeholders* da RNP. Esta frente está fortemente alinhada com a implementação do ciclo de vida de gestão de identidade nas instituições, considerando tanto a definição de processos para as atividades do ciclo de vida, por exemplo, a definição de políticas de acesso, e o necessário suporte tecnológico na forma de soluções de produto, serviços e treinamentos. Também é possível identificar oportunidades de pesquisa, tais como:

- Processos e serviços para auxiliar na definição e mineração de políticas de acesso;
- Verificação da conformidade das políticas implementadas com as políticas de segurança da instituição, bem como auditoria e análise dos registros de acesso.

[24] https://wballiance.com/openroaming/

4.2 Segundo horizonte: negócios emergentes

4.2.1 Autenticação usando padrões FIDO2

Principais provedores de serviços comerciais já adotaram os protocolos FIDO2 (LINDEMANN et al., 2019; W3C, 2019b) como uma alternativa às senhas descartáveis. Contudo, muitos provedores, que fazem uso da autenticação de usuários por meio da biometria, ainda não apresentaram soluções baseadas no potencial do FIDO2. Tais soluções estão fundamentadas em protocolos e regras proprietárias e não são interoperáveis. Ou seja, a concepção de um serviço de autenticação multifator, que permita a autenticação biométrica local e que esteja fundamentado sobre padrões criptográficos robustos, pode resultar em benefícios para usuários e administradores desses serviços. Segundo Allan (2020), os protocolos FIDO2 tornaram-se maduros e por estarem presentes nos principais navegadores *web* e sistemas operacionais de dispositivos móveis, apresentam-se como uma solução capaz de ser adotada plenamente dentro de dois a cinco anos.

4.2.2 Autorização e controle de acesso

Uma possibilidade para o segundo horizonte é a incorporação dos mecanismos de controle de acesso nos sistemas existentes e em desenvolvimento ou implantação em diversos domínios de aplicação.

Práticas de gestão de identidade hoje perpassam o ambiente acadêmico, incluindo provedores comerciais como Google, Facebook e Twitter, e serviços governamentais, como o gov.br. Este cenário traz desafios adicionais para autorização e controle de acesso, como por exemplo, a definição de políticas de acesso por parte de provedores de serviço quando se tem um número elevado de provedores de identidades com regras específicas de acesso (DINIZ et al., 2015). A própria RNP oferece um conjunto de serviços que podem ser acessados por usuários da comunidade acadêmica por meio da federação CAFe, como o serviço de conferência *web*[25], por exemplo, e os serviços avançados[26] para suporte à ciência e *testbeds*.

Neste contexto, é necessário o desenvolvimento de produtos ou serviços que auxiliem este e outros processos relacionados a autorização e controle de acesso. Considerando a entrada em vigor da LGPD (BRASIL, 2018), deve-se ter agora um cuidado extra com a proteção de dados, principalmente dados para pesquisa que podem ser compartilhados usando os serviços da RNP. O que faz com que o uso dos mecanismos de autorização e controle de acesso nos serviços oferecidos seja cada vez mais relevante.

O *Federated Access Control System* (FACS) (DINIZ et al., 2015) desenvolvido pela RNP, e que era utilizado para definição de políticas de acesso no serviço Edudrive, é um exemplo de serviço que auxilia este processo e merece ser explorado. Sua utilização em outras aplicações ou serviços, além de pesquisas baseadas em sua utilização atual, são oportunidades para o desenvolvimento de produtos que podem ser ofertados para os *stakeholders* da RNP ou para o mercado em geral.

Além da federação de identidades há também o fenômeno de federação de serviços: de soluções para redes sociais descentralizadas (GUIDI et al., 2018), como o Mastodon (RAMAN et al., 2019) e o protocolo Matrix (JACOB; GRASHÖFER; HARTENSTEIN, 2019), a soluções de nível corporativas, como o suporte a federação de multinuvens (KOGIAS; XEVGENIS; PATRIKAKIS, 2016). Deste modo, pesquisas já desenvolvidas com o apoio da RNP tais como ACROSS (SILVA; MUCHALUAT-SAADE; FERNANDES, 2018), FACS (DINIZ et al., 2015) e o trabalho de Sette, Chadwick e Ferraz (2017) merecem ter seus conceitos revisitados em novos cenários de aplicação, considerando por exemplo os resultados do projeto Fogbow[27] e o serviço Nas Nuvens[28] da RNP.

[25] https://conferenciaweb.rnp.br/
[26] https://www.rnp.br/servicos/experimentos-avancados
[27] http://www.fogbowcloud.org/
[28] https://www.nasnuvens.rnp.br/

Para viabilizar pesquisas colaborativas nacionais e internacionais, o uso de infraestruturas de autenticação e autorização flexíveis são essenciais. A oferta pela RNP de um serviço semelhante ao eduTEAMS, que possibilite a criação e gerenciamento das colaborações virtuais, pode contribuir para criação de times virtuais nas comunidades de pesquisa brasileiras e viabilizar a cooperação internacional.

4.2.3 Identidade digital descentralizada

O tema de identidades digitais descentralizadas e autossoberanas tem chamado muito a atenção da comunidade científica, como já destacado anteriormente. A RNP deve ficar atenta às inovações produzidas nesta área de modo a poder incorporá-las o quanto antes em seu portfólio de serviços e, assim, manter o protagonismo em gestão de identidades perante as instituições de ensino e pesquisa.

Entre possíveis abordagens está um estudo mais aprofundado das possibilidades e alternativas disponíveis para implantação de um sistema de IDD na RNP, avançando mais um passo em relação à Federação CAFe. Considerando a evolução contínua que a área de gestão de identidades tem sofrido, a RNP deve avaliar se uma IDD seria viável como uma evolução da Federação CAFe em operação e a que custo de implementação e operação. Apesar de um sistema baseado em IDD trazer muitas promessas de vantagens, é preciso avaliar também o ponto de vista do usuário: ainda não está totalmente claro se o custo de operação a ser colocado sobre o dono da identidade é algo razoável e admissível. Mais estudos precisam avaliar esta questão e, se possível, identificar formas de reduzir tal custo.

Um foco maior em identidades descentralizadas também seria benéfico do ponto de vista de proposta de alternativa a uma centralização maciça de autenticação no sistema federal. Este sistema federal poderá se tornar um ponto único de falha e impactar fortemente todos os serviços em todas as instituições em caso de falha. Por isso, a RNP deve estar à frente no tocante aos desafios e soluções relativas à identidades descentralizadas, já que este parece ser o mecanismo com um bom potencial de escalabilidade, dado seu caráter distribuído.

Com o objetivo de tornar mais suave e segura a transição de um modelo centralizado (como a ICP-Brasil) para um totalmente distribuído (como o IDD, por exemplo), podem ser buscadas formas de ancoragem de confiança mútua entre os dois modelos, de maneira a usar as garantias hoje oferecidas pela ICP-Brasil na autenticação de alguns elementos iniciais dentro de uma estrutura de identificadores descentralizados [DIDs].

Por fim, as iniciativas da União Europeia no tocante ao uso amplo e geral de identidades autossoberanas (RECOMENDAÇÃO..., 2021) deve ser acompanhado de perto, pois é possível vislumbrar um potencial de cooperação e de interoperabilidade caso haja compatibilidade técnica entre as futuras identidades descentralizadas europeias e brasileiras.

4.2.4 Certificados digitais descartáveis

Certificados descartáveis são interessantes pra alguns cenários de documento eletrônico, onde você não quer arcar com o custo de armazenar a chave privada. Dessa forma, você gera o certificado com alguns minutos de validade, e assina um documento. O certificado vence e o documento continua válido pois foi assinado durante a validade do certificado. Este tipo de solução só faz sentido se tivermos carimbadoras de tempo, pois a validade de longo prazo do documento é dada por essa âncora temporal.

4.2.5 Certificados digitais para IoT

Certificados IoT podem ser usados para identificar dispositivos de forma geral. Trata-se de uma solução razoavelmente simples de implantar, visto que basta usar uma AC pronta (ex. fabric-ca do *Hyperledger*) e o dispositivo tem uma senha pra gerar seu par de chaves e assiná-lo pela AC. Com um certificado digital por exemplo, os dispositivos IoT podem facilmente conectar no eduroam usando EAP-TTLS (FUNK; BLAKE-WILSON, 2008). Na prática isto permite um controle de acesso à infraestrutura existente para conectar IoT, o que é um grande ganho para as instituições.

4.2.6 Certificados digitais autogerados para sistemas de software

Ataques internos têm custos e impactos médios muito maiores que os ataques originados fora das organizações. Estes ataques podem ter origens variadas: um usuário autorizado pode resolver atacar um sistema ao qual tem acesso para obter vantagens financeiras (por exemplo, venda de dados) ou para simplesmente causar prejuízo (por exemplo, em razão de uma insatisfação ou demissão); por outro lado, a falta de cuidado ou o uso de ataques sociais ou direcionados pode levar ao sequestro de credenciais associadas a usuários humanos. Em ambos os casos, mecanismos de controle que não dependem da confiança em humanos podem criar barreiras adicionais contra este tipo de ameaça.

Com o objetivo de deslocar a confiança do usuário humano para código, certificados digitais podem ser gerados de forma automatizada de acordo com as propriedades de um serviço. Por exemplo, um serviço de validação de dados pode precisar de acesso a um banco de dados com informações pessoais. No entanto, ao invés de se criar credenciais que poderiam ser observadas por um operador desses sistemas, as credenciais são geradas diretamente para o código após a validação que este código é seguro e está sendo executado em um ambiente protegido.

Para garantir que este código é seguro, modificações podem ser aceitas somente se assinadas digitalmente por comitês (considerando que o comprometimento de vários usuários é muito menos provável que o comprometimento de um único). Já a garantia de que o código executa em um ambiente seguro pode ser realizada com base na atestação deste ambiente. Esta atestação pode incluir fatores como o *hash* do processo de carregamento do sistema operacional, o nível de atualização do *firmware* do processador, e até o *hash* do carregamento da própria aplicação.

Iniciativas como SPIFFE (FELDMAN et al., 2020) da CNCF definem padrões para a geração de identidades para componentes de software (na forma de certificados digitais X.509v3 ou *tokens* JWT) e implementações como SPIRE definem formas de atestação de código para a emissão destas identidades. Finalmente, uma vez que estas credenciais são geradas de forma automática, elas podem ter validades curtas, de minutos ou horas, minimizando o impacto de vazamentos e forçando a reexecução periódica dos procedimentos de verificação de integridade.

É inevitável que a RNP, que oferece diversos serviços de nuvem, ofereça cada vez mais serviços *Machine-to-Machine* (M2M), e estes serviços precisarão de mecanismos de gestão de identidades e de autorização para entidades de software. Assim, a RNP precisará prover suporte a padrões e mecanismos para geração e validação de identidades de sistemas de software. Além de operar sistemas para gerar e consumir as identidades, a RNP deverá também prover suporte a mecanismos para atestação de integridade dos sistemas que receberão estas identidades (como com base em mecanismos de computação confidencial e tecnologias como Intel SGX, TPM, ARM TrustZone, AMD SEV, e disponibilizadas por provedores como Microsoft Azure, IBM Cloud, Alibaba, e Google Cloud).

4.2.7 Certificados de atributos

Certificados de atributos já são uma realidade na questão de identificação profissionais por conselhos, assim como por entidades estudantis. Os certificados de atributos podem facilmente ser embarcados em documentos eletrônicos a fim de qualificar o assinante. Por exemplo, é muito simples integrar

atributos a um sistema de portarias internas para qualificar assinaturas de funções gratificadas de coordenação de curso. Existem também outras oportunidades com um padrão de QR code seguro baseado em certificados de atributos que também pode ter aplicabilidade na academia.

4.2.8 Autoridades certificadoras em curvas elípticas

Na linha de Autoridade Certificadora (AC) pessoais e de IoT, entende-se que a RNP precise emitir uma nova cadeia de ACs de Curvas Elípticas. Existem uma séries de aplicações para tal, mas talvez a mais importante seja a possibilidade de uso destes certificados para comandar aplicações em *Hyperledger Fabric* (ANDROULAKI et al., 2018), além de melhorar a eficiência das soluções de certificados de atributos, certificados IoT, certificados pessoais e certificados para aplicações inovadoras.

4.3 Terceiro horizonte: semear iniciativas para futuros negócios

4.3.1 Autorização e controle de acesso

Uma outra frente de trabalho cada vez mais relevante é como lidar com ameaças internas. De acordo com Legg et al. (2015) uma ameaça interna pode ser definida como um usuário atuando como funcionário, ex-funcionário, terceirizado, ou parceiro comercial que tem ou teve acesso autorizado à rede, sistemas ou dados, e de forma intencional ou não intencional abusa de suas permissões para afetar a confidencialidade, integridade e/ou disponibilidade de sistemas e informações da uma instituição, causando prejuízos financeiros, danos a reputação, entre outros.

Tradicionalmente, organizações usam mecanismos de controle de acesso para proteger recursos e serviços computacionais e garantir o acesso somente a pessoas autorizadas para tal. Entretanto, tais mecanismos não são capazes de detectar comportamentos anômalos ou desvios comportamentais de um usuário legitimamente autorizado. Por exemplo, um usuário que normalmente acessa cerca de 10 documentos por dia não seria detectado como uma anomalia caso ele passasse a acessar milhares de documentos em um curto espaço de tempo. Diversos casos foram reportados ao redor do globo (BOOTH; BROOKE; MORRIS, 2010; GREENWALD, 2014; YASEEN, 2017).

Diversos trabalhos de pesquisa tem sido publicados na área, como por exemplo, explorando conceitos de sistemas auto-adaptativos como auto-proteção (*self-protection*) (TZIAKOURIS; BAHSOON; BABAR, 2018; YUAN; ESFAHANI; MALEK, 2014) para monitorar e adaptar infraestruturas de autorização e controle de acesso (BAILEY; CHADWICK; DE LEMOS, 2014), e o uso de modelos comportamentais para analisar registros de *logs* de sistemas baseados em processos de negócios (SILVA; SILVA et al., 2017). Neste direção é possível visualizar oportunidades de pesquisa envolvendo tais métodos em combinação com as práticas já empregadas comercialmente para detecção de intrusão em redes [*Intrusion detection system* (IDS)] e com o problema de mineração de políticas. Por exemplo, a aplicação de técnicas de análise baseada em inteligências artificial aplicadas no domínio de autorização e controle de acesso.

Atualmente, elementos de rede vêm ganhando alto poder de armazenamento e processamento, o que abre a perspectiva recuperação de identidade em *cache* para aplicações sensíveis a atraso. A partir do paradigma de névoa computacional, da distribuição e da manutenção de identidades por meio da *cache* através dos elementos intermediários da rede é possível armazenar e distribuir atributos ou identidade. Assim, políticas de *cache* de identidades multinível para névoas computacionais devem ser estudadas e propostas. Como sugestão tem-se a utilização de técnicas de aprendizado de máquina para a predição da mobilidade de usuários em redes sem fio aplicadas no auxílio à criação de políticas de priorização de espaço em *cache*.

4.3.2 ICPEdu com algoritmos híbridos 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 (útil) seja anunciado. Há muitas discussões na comunidade internacional sugerindo que não se gaste tempo e esforço (que não são pequenos) 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 deste problemas para que a solução estejam disponíveis com a tempestividade requerida.

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 mai. 2021.

ALLEN, Christopher (Ed.). *The Path to Self-Sovereign Identity*. Abr. 2016. Disponível em: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html>. Acesso em: 14 mai. 2021.

ANDERER, Simon et al. RMPlib: A Library of Benchmarks for the Role Mining Problem. In: PROCEEDINGS of the 26th ACM Symposium on Access Control Models and Technologies. Virtual Event, Spain: Association for Computing Machinery, 2021. (SACMAT '21), p. 3–13. ISBN 9781450383653. DOI: 10.1145/3450569.3463566. Disponível em: <https://doi.org/10.1145/3450569.3463566>.

ANDROULAKI, Elli et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: PROCEEDINGS of the thirteenth EuroSys conference. 2018. p. 1–15.

APPLE. *Move beyond passwords*. Jun. 2021. Disponível em: <https://developer.apple.com/videos/play/wwdc2021/10106>. Acesso em: 17 jul. 2021.

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.

BAILEY, Christopher; CHADWICK, David W.; DE LEMOS, Rogério. Self-adaptive federated authorization infrastructures. *Journal of Computer and System Sciences*, v. 80, n. 5, p. 935–952, 2014. Special Issue on Dependable and Secure Computing. ISSN 0022-0000. DOI: https://doi.org/10.1016/j.jcss.2014.02.003. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0022000014000154>.

BARNES, R. et al. *Automatic Certificate Management Environment (ACME)*. Mar. 2019. Disponível em: <https://datatracker.ietf.org/doc/html/rfc8555>. Acesso em: 22 jun. 2021.

BOOTH, Robert; BROOKE, Heather; MORRIS, Steven. *WikiLeaks cables: Bradley Manning faces 52 years in jail*. Nov. 2010. Disponível em: <http://www.guardian.co.uk/world/2010/nov/30/wikileaks-cables-bradley-manning>. Acesso em: 10 jan. 2017.

BRASIL. Decreto nº 10.543, de 13 de novembro de 2020. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 13 nov. 2020a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10543.htm>. Acesso em: 22 jun. 2021.

_____. Lei nº 13.709, de 14 de agosto de 2018. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 28 mai. 2021.

_____. Lei nº 14.063, de 23 de setembro de 2020. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 23 jul. 2020b. Disponível em: <https://www.in.gov.br/web/dou/-/lei-n-14.063-de-23-de-setembro-de-2020-279185931>. Acesso em: 22 jun. 2021.

D. REED, J. Law; HARDMAN, D. (Ed.). *The Technical Foundations of Sovrin*. Set. 2016. Disponível em: <https://www.evernym.com/wp-content/uploads/2017/07/The-Technical-Foundations-of-Sovrin.pdf>. Acesso em: 14 mai. 2021.

DINIZ, Thomas F. S. et al. Managing Access to Service Providers in Federated Identity Environments: A Case Study in a Cloud Storage Service. In: 2015 XXXIII Brazilian Symposium on Computer Networks and Distributed Systems. Vitoria, ES, Brazil, 2015. (SBRC 2015), p. 199–207. DOI: 10.1109/SBRC.2015.32.

FEI (Ed.). *A Decentralized, Open Source Solution for Digital Identity and Access Management*. Dez. 2019. Disponível em: <https://jolocom.io/wp-content/uploads/2019/12/Jolocom-Whitepaper-v2.1-A-Decentralized-Open-Source-Solution-for-Digital-Identity-and-Access-Management.pdf>. Acesso em: 14 mai. 2021.

_____. *Self-Sovereign and Decentralised Identity By Design*. Mar. 2018. Disponível em: <https://jolocom.io/wp-content/uploads/2018/07/Jolocom-Technical-WP-_-Self-Sovereign-and-Decentralised-Identity-By-Design-2018-03-09.pdf>. Acesso em: 14 mai. 2021.

FELDMAN, Daniel et al. *Solving the Bottom Turtle - a SPIFFE Way to Establish Trust in Your Infrastructure via Universal Identity*. spiffe.io, 2020. ISBN 978-0-578-77737-5.

FERDOUS, Md Sadek; CHOWDHURY, Farida; ALASSAFI, Madini O. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access*, v. 7, p. 103059–103079, 2019. DOI: 10.1109/ACCESS.2019.2931173.

FUNK, P.; BLAKE-WILSON, S. *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)*. Ago. 2008. Disponível em: <https://datatracker.ietf.org/doc/html/rfc5281>. Acesso em: 22 jun. 2021.

CT-GID. *Grandes desafios de Gestão de Identidade. 4ª reunião ordinária do CT-GId*. Nov. 2013. Disponível em: <https://wiki.rnp.br/pages/viewpage.action?pageId=72515916>. Acesso em: 5 mai. 2021.

GOOGLE. *Enabling Strong Authentication with WebAuthn*. Mai. 2018. Disponível em: <https://developers.google.com/web/updates/2018/05/webauthn>. Acesso em: 17 jul. 2021.

GRASSI, Paul A et al. *NIST Special Publication 800 63B Digital Identity Guidelines*. 2017. https://pages.nist.gov/800-63-3/sp800-63b.html.

GREENWALD, Glenn. *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Edição: Metropolitan Books. Macmillan, 2014. ISBN 1250062586.

GUIDI, Barbara et al. Managing social contents in Decentralized Online Social Networks: A survey. *Online Social Networks and Media*, Elsevier BV, v. 7, p. 12–29, set. 2018. ISSN 2468-6964. DOI: 10.1016/j.osnem.2018.07.001.

HARDT, D. *The OAuth 2.0 Authorization Framework*. Out. 2012. Disponível em: <https://datatracker.ietf.org/doc/html/rfc6749>.

HU, Vincent C. et al. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. Jan. 2014. DOI: 10.6028/nist.sp.800-162.

INTERNET2. *Consent-informed Attribute Release system (CAR)*. Disponível em: <https://spaces.at.internet2.edu/display/CAR/CAR%3A+Consent-informed+Attribute+Release+system>. Acesso em: 5 mai. 2021.

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 mai. 2021.

JACOB, Florian; GRASHÖFER, Jan; HARTENSTEIN, Hannes. A Glimpse of the Matrix: Scalability Issues of a New Message-Oriented Data Synchronization Middleware. In: (Middleware '19), p. 5–6. ISBN 9781450370424. DOI: 10.1145/3366627.3368106. Disponível em: <https://doi.org/10.1145/3366627.3368106>.

JØSANG, Audun. A Consistent Definition of Authorization. In: 13TH International Workshop on Security and Trust Management (STM 2017). Springer International Publishing, 2017. p. 134–144. ISBN 978-3-319-68063-7. DOI: 10.1007/978-3-319-68063-7_9.

KOGIAS, D. G.; XEVGENIS, M. G.; PATRIKAKIS, C. Z. Cloud Federation and the Evolution of Cloud Computing. *Computer*, IEEE Computer Society, Los Alamitos, CA, USA, v. 49, n. 11, p. 96–99, nov. 2016. ISSN 1558-0814. DOI: 10.1109/MC.2016.344.

LEGG, Philip A. et al. Caught in the act of an insider attack: detection and assessment of insider threat. In: 2015 IEEE International Symposium on Technologies for Homeland Security (HST). 2015. DOI: 10.1109/THS.2015.7446229.

LIAMPOTIS, Nicolas; CONSORTIUM, AARC; MEMBERS, AppInt. *Evolution of the AARC Blueprint Architecture*. Mar. 2019. Disponível em: <https://aarc-project.eu/wp-content/uploads/2019/05/AARC2-DJRA1.4_v2-FINAL.pdf>. Acesso em: 30 jun. 2021.

LINDEMANN, R. et al. *Client to Authenticator Protocol "(CTAP)"*. Jan. 2019. Disponível em: <https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.pdf>.

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>.

MELLO, Emerson Ribeiro de et al. Multi-factor authentication for shibboleth identity providers. *Journal of Internet Services and Applications*, v. 11, n. 1, p. 8, 2020. DOI: 10.1186/s13174-020-00128-1. Disponível em: <https://doi.org/10.1186/s13174-020-00128-1>. Acesso em: 22 jun. 2021.

MICROSOFT. *APIs WebAuthn para autenticação sem senha no Windows 10*. Fev. 2019. Disponível em: <https://docs.microsoft.com/pt-br/windows/security/identity-protection/hello-for-business/webauthnapis>. Acesso em: 17 jul. 2021.

MOLLOY, Ian et al. Evaluating Role Mining Algorithms. In: PROCEEDINGS of the 14th ACM Symposium on Access Control Models and Technologies. Stresa, Italy: Association for Computing Machinery, 2009. (SACMAT '09), p. 95–104. ISBN 9781605585376. DOI: 10.1145/1542207.1542224. Disponível em: <https://doi.org/10.1145/1542207.1542224>.

OLIVEIRA, Leonardo B et al. The computer for the 21st century: present security & privacy challenges. *Journal of Internet Services and Applications*, Springer, v. 9, n. 1, p. 1–25, 2018.

RAMAN, Aravindh et al. Challenges in the Decentralised Web: The Mastodon Case. In: PROCEEDINGS of the Internet Measurement Conference. Amsterdam, Netherlands: Association for Computing Machinery, 2019. (IMC '19), p. 217–229. ISBN 9781450369480. DOI: 10.1145/3355369.3355572. Disponível em: <https://doi.org/10.1145/3355369.3355572>.

RAVIDAS, Sowmya et al. Access control in Internet-of-Things: A survey. *Journal of Network and Computer Applications*, v. 144, p. 79–101, 2019. ISSN 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2019.06.017. Disponível em: <https://www.sciencedirect.com/science/article/pii/S108480451930222X>.

RECOMENDAÇÃO (UE) 2021/946 da comissão relativa a um conjunto de instrumentos comuns a nível da União para uma abordagem coordenada do quadro europeu para a identidade digital. *Jornal Oficial da União Europeia*, v. L 210/51, jun. 2021. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32021H0946&from=EN>. Acesso em: 30 jun. 2021.

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.

SAADE, Débora C Muchaluat et al. Eduroam: Acesso sem fio seguro para a Comunidade Acadêmica Federada. *Rede Nacional de Ensino e Pesquisa*, 2013.

SAKIMURA, Natsuhiko et al. Openid connect core 1.0. *The OpenID Foundation*, s3, 2014.

SANTOS, Maria L.B.A. et al. FLAT: Federated lightweight authentication for the Internet of Things. *Ad Hoc Networks*, v. 107, p. 102253, 2020. ISSN 1570-8705. DOI: https://doi.org/10.1016/j.adhoc.2020.102253. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1570870520302468>.

SEAMLESSACCESS. *SeamlessAccess enables true Single Sign-On*. Disponível em: <https://seamlessaccess.org>. Acesso em: 5 mai. 2021.

SETTE, I. S.; CHADWICK, D. W.; FERRAZ, C. A. G. Authorization Policy Federation in Heterogeneous Multicloud Environments. *IEEE Cloud Computing*, v. 4, n. 4, p. 38–47, 2017. DOI: 10.1109/MCC.2017.3791018.

SILVA, Carlos Eduardo da; SILVA, José Diego Saraiva da et al. Self-Adaptive Role-Based Access Control for Business Processes. In: (SEAMS '17), p. 193–203. ISBN 9781538615508. DOI: 10.1109/SEAMS.2017.13. Disponível em: <https://doi.org/10.1109/SEAMS.2017.13>.

SILVA, Edelberto Franco; MUCHALUAT-SAADE, Débora Christina; FERNANDES, Natalia Castro. ACROSS: A generic framework for attribute-based access control with distributed policies for virtual organizations. *Future Generation Computer Systems*, v. 78, p. 1–17, 2018. ISSN 0167-739X. DOI: https://doi.org/10.1016/j.future.2017.07.049. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X17316060>.

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.

TZIAKOURIS, Giannis; BAHSOON, Rami; BABAR, Muhammad Ali. A Survey on Self-Adaptive Security for Large-Scale Open Environments. *ACM Comput. Surv.*, Association for Computing Machinery, New York, NY, USA, v. 51, n. 5, out. 2018. ISSN 0360-0300. DOI: 10.1145/3234148. Disponível em: <https://doi.org/10.1145/3234148>.

VALE, Marshall. *Privacy, sustainability and the importance of "and"*. Mar. 2021. Disponível em: <https://blog.google/products/chrome/privacy-sustainability-and-the-importance-of-and/>. Acesso em: 5 mai. 2021.

W3C. *Decentralized Identifiers (DIDs) v1.0*. Jun. 2021. Disponível em: <https://www.w3.org/TR/did-core/>. Acesso em: 5 mai. 2021.

_____. *Verifiable Credentials Data Model 1.0*. Nov. 2019a. Disponível em: <https://www.w3.org/TR/vc-data-model/>. Acesso em: 5 mai. 2021.

_____. *Web Authentication: An API for accessing Public Key Credentials Level 1*. Mar. 2019b. Disponível em: <https://www.w3.org/TR/webauthn>. Acesso em: 5 mai. 2021.

WANGHAM, Michelle Silva et al. O Futuro da Gestão de Identidades Digitais. In: ANAIS do Workshop de Gestão de Identidade (WGID) do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg). SBC, 2018.

WEBINCUBATORCG. *WebID*. Fev. 2021. Disponível em: <https://wicg.github.io/WebID/README.html>. Acesso em: 5 mai. 2021.

WILANDER, John. *Full Third-Party Cookie Blocking and More*. Mar. 2020. Disponível em: <https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/>. Acesso em: 5 mai. 2021.

WOOD, Marissa. *Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default*. Set. 2019. Disponível em: <https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/>. Acesso em: 5 mai. 2021.

YASEEN, Qussai. Insider Threat in Banking Systems. *Online Banking Security Measures and Data Protection*, IGI Global, p. 222, 2017. DOI: 10.4018/978-1-5225-0864-9.ch013.

YUAN, Eric; ESFAHANI, Naeem; MALEK, Sam. A Systematic Survey of Self-Protecting Software Systems. *TAAS*, v. 8, n. 4, 17:1–17:41, 2014. DOI: 10.1145/2555611.

RNP
ORGANIZAÇÃO SOCIAL DO MCTI
MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES
PÁTRIA AMADA BRASIL
GOVERNO FEDERAL