O Futuro da Gestão de Identidades Digitais

Michelle Silva Wangham[1], André Marins[2], Carlos A. G. Ferraz[3], Carlos E. da Silva[4], Debora C. M. Saade[5], Edelberto F. Silva[6], Emerson Ribeiro de Mello[7], Fábio B. de Oliveira[8], Flávio Luiz Seixas[5], Leonardo B. Oliveira[9], Marcelo D. Lopes[1], e Marco A. A. Henriques[10]

[1]Universidade do Vale do Itajaí (UNIVALI)
[2]Rede Nacional de Ensino e Pesquisa (RNP)
[3]Universidade Federal de Pernambuco (UFPE)
[4]Universidade Federal do Rio Grande do Norte (UFRN)
[5]Universidade Federal Fluminense (UFF)
[6]Universidade Federal de Juiz de Fora (UFJF)
[7]Instituto Federal de Santa Catarina (IFSC)
[8]Laboratório Nacional de Computação Científica (LNCC)
[9]Universidade Federal de Minas Gerais (UFMG)
[10]Universidade Estadual de Campinas (UNICAMP)

Abstract. *This paper presents a vision of the future on potential topics for research and development in Identity Management according to researchers who have been working in this area and collaborating in the Technical Committee of Identity Management (CT-GId). The results show many challenges and opportunities in this area, which is gaining increasing importance in the national and international scenarios. The RNP's vision for these new challenges that lie ahead, as described in this document, will allow the institution and its services to remain in the technological and operational forefront.*

Resumo. *Este artigo apresenta uma visão de futuro sobre temas com potencial para pesquisas e desenvolvimento em Gestão de Identidades de acordo com pesquisadores que têm atuado na área e colaborado no Comitê Técnico de Gestão de Identidades (CT-GId), vinculado à Rede Nacional de Ensino e Pesquisa (RNP). Os resultados apontam para a existência de muitos desafios e oportunidades nesta área, a qual está ganhando uma importância cada vez maior nos cenários nacional e internacional. A atenção da RNP para os novos desafios que se assomam no horizonte, conforme descrito neste documento, permitirá que a instituição e os serviços providos por esta se mantenham na vanguarda tecnológica e operacional.*

1. Introdução

A gestão de identidades ou GId (*IdM - Identity Management*) pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade ou de um objeto, garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) e para prover procedimentos de autenticação, autorização, responsabilização e auditoria [ITU 2009].

Este é um tema de pesquisa ativo e, diante da sua complexidade e relevância, deverá continuar assim por muito tempo. Esta constatação decorre das inúmeras questões técnicas que os sistemas de gestão de identidades devem considerar, tais como: facilidade de uso, privacidade e anonimato do usuário, autenticação única e federada, autenticação multi-fator, controle de acesso de granularidade fina (baseado em atributos), confiabilidade, escalabilidade, interoperabilidade e custo dos sistemas (*total cost of ownership*).

A Rede Nacional de Ensino e Pesquisa (RNP) oferece à comunidade acadêmica brasileira alguns serviços ligados a GId, a saber: a Infraestrutura de Chaves Públicas de Ensino e Pesquisa (ICPEdu), o sistema de acesso sem fio à Internet usando credenciais da instituição de origem do usuário (Eduroam) e a Federação CAFe (Comunidade Acadêmica Federada), que permite que usuários de uma instituição participante tenham acesso a diversos serviços de outras instituições (nacionais ou estrangeiras), também usando apenas credenciais obtidas localmente na instituição de origem. Diante da necessidade de aprimoramentos destes serviços e de outros serviços que demandem de gestão de identidades, o Comitê Técnico de Gestão de Identidades (CT-GID) da RNP tem por objetivo realizar recomendações técnicas e prospecção tecnológica para apoiar as atividades do Comitê Assessor de Gestão de Identidade (CA-GID).

O objetivo deste artigo, elaborado de forma colaborativa pelos membros do CT-GID, é apresentar uma visão de futuro acerca dos temas relacionados à gestão de identidades que mais têm merecido a atenção de pesquisadores no Brasil e no exterior. De maneira resumida, alguns problemas e oportunidades de pesquisa relevantes, bem como ideias de possíveis caminhos a seguir para resolver tais problemas e/ou trilhar novos caminhos em GId, são descritos.

2. Motivação e Cenários

A fim de ilustrar e motivar as discussões e indicações de ações futuras deste documento são apresentados alguns cenários no qual a Gestão de Identidade se faz necessária ou vem sendo debatida. Os cenários descritos foram estudados e levados em consideração durante os encontros do CT-GId nos anos de 2017 e 2018.

2.1. Cenários Analisados

2.1.1. Aplicações na Área de Saúde

Na área de saúde, sistemas de saúde eletrônica (*eHealth*) estão cada vez mais presentes [Blobel 2010]. Prontuários eletrônicos, exames de imagens e sinais digitais, sistemas de apoio ao diagnóstico de doenças, sistemas de apoio à decisão médica, sistemas para monitoramento em tempo real de sinais vitais, sistemas para prescrição de medicamentos, sistemas para acompanhamento médico e diversos outros precisam utilizar e gerar informações sobre pacientes e seus dados, que precisam ser compartilhados por diversas instituições, membros da equipe de saúde, pacientes e seus familiares [Martínez-Pérez et al. 2014]. No dia a dia, um paciente frequenta diferentes consultórios médicos, clínicas, postos de saúde e hospitais, que utilizam diferentes sistemas de informação médica, o que dificulta o acesso integrado e controlado às suas informações [McGuire et al. 2013].

Em um ambiente ideal, cada paciente deveria ter um único prontuário eletrônico, que integra informações obtidas dos diferentes sistemas e poderia ser acessado, respeitando as devidas autorizações de acesso, por diferentes perfis de usuários [Koopman et al.

2015]. Para a construção desse ambiente ideal, há enormes desafios na área de gestão de identidades. Um ponto crucial é definir como estabelecer uma identidade digital que possa ser utilizada em diferentes sistemas, permitindo a identificação única do paciente [Sujansky and Kunz 2015]. Outro desafio está em especificar um mecanismo de autenticação seguro para permitir acesso integrado aos diversos sistemas de saúde [Fernández-Alemán et al. 2013]. O uso de federações pode ser um caminho promissor para a busca de uma solução para esses problemas [Nelson and Staggers 2016].

Uma outra questão se refere à autorização para acesso aos dados de cada paciente. Em um ambiente de *eHealth*, diferentes atores estão presentes, tais como funcionários das instituições de saúde que atendem um determinado paciente, os diferentes médicos e especialistas em cada área de saúde, o próprio paciente e seus familiares [Lake et al. 2014]. Essa diversidade de perfis de usuários e instituições gera uma infinidade de combinação de direitos possíveis de acesso a essas informações [Martino et al. 2008]. Portanto, um outro problema interessante se refere aos mecanismos de controle de acesso aos dados de saúde, que devem garantir privilégios específicos, dependendo dos usuários, instituições e dos próprios dados. Em certos casos, o médico não deve divulgar diretamente informações ao próprio paciente, caso essa revelação possa causar algum mal-estar ao paciente. Mecanismos de controle de acesso baseados em políticas e atributos podem apontar soluções interessantes para esses desafios da área de saúde [Sanchez-Guerrero et al. 2017].

Privacidade, ou seja, o direito de limitar quem acessa os dados pessoais sobre a saúde de um paciente é um ponto fundamental em qualquer sistema da saúde. Jamais os dados de um paciente podem ser utilizados ou divulgados sem sua prévia autorização [Nelson and Staggers 2016]. A obrigação de outros respeitarem a privacidade dos dados divulgados é outra questão crucial em sistemas de informação de saúde. Qualquer pesquisa científica que envolva uso de dados dos pacientes deve ser previamente autorizada pelos comitês de ética em pesquisa médica, que prezam sempre a privacidade dos dados, o anonimato e o bem-estar dos pacientes [Oladimeji et al. 2011].

Sistemas de auditoria na área médica também têm um papel fundamental [Musen et al. 2014]. Em casos de perícia sobre algum procedimento médico, deve-se identificar todas as partes responsáveis pelo atendimento a um determinado paciente, incluindo todos os membros da equipe médica e hospitalar que realizaram atendimento ao paciente.

2.1.2. Federação de *testbeds* - *Clearinghouse*

Uma federação de recursos é aquela que faz a união de recursos de diferentes instituições como, por exemplo, a federação de recursos de *testbeds* para Internet do Futuro (FIBRE[1]) ou a federação de recursos para nuvens. Tais federações trazem grandes vantagens e benefícios, mas também trazem desafios importantes, tais como: nomear/classificar os recursos, lidar com uma base de usuários muito grande e distribuída, lidar com uma base de recursos distintos, numerosos e distribuídos e cuidar das políticas a nível local e global [Alfieri et al. 2003]. Estudos relacionados à gestão de identidade em federações de recursos lidam também com o uso de federações acadêmicas, tais como a CAFe, e o uso de outros provedores de identidade de mídias sociais, tais como os providos pelo Facebook e Google.

[1]https://fibre.org.br/

No contexto específico dos *testbeds* para experimentação para Internet do Futuro, o conceito de *clearinghouse* aparece como ponto chave, oferecendo a infraestrutura para certificação e confiança dentro da federação [Foster et al. 2001], [Internet2 2016], [Hu et al. 2013]. Contudo, a arquitetura ideal para a *clearinghouse* ainda é um ponto em discussão. Nesse sentido, é importante definir como a gestão de identidades pode ser integrada à federação de recursos. Por exemplo, a *Slice Federation Architecture – SFA* [Mortimore et al. 2015], que pode ser descrita como uma API para federar e dar acesso aos recursos de uma federação de recursos para os usuários autorizados, é fortemente baseada no uso de certificados. Contudo, como integrar a gestão de identidades da organização virtual que compõe a federação de recursos e como gerenciar a autorização e a certificação nesse ambiente é um desafio, em especial quando se considera que diferentes instituições podem usar formas distintas de autenticar e descrever recursos e usuários.

2.1.3. Federação de Nuvens

O CICN (Centro de Inovação em Computação em Nuvem) é um projeto apoiado financeiramente pela FINEP e com a colaboração de TELEBRAS, LNCC, SERPRO e DATAPREV. Este projeto tem o objetivo de desenvolver atividades de pesquisa, desenvolvimento, absorção e transferência de tecnologias em computação em nuvem, estimulando sua adoção pelo setor público. O CICN propõe a definição de uma arquitetura de referência para computação em nuvem para governo eletrônico (e-Gov) e, a partir dela, soluções que permitam a criação de serviços de e-Gov em nuvem.

Este projeto é apoiado em um *middleware* chamado *Fogbow*[2] que federa nuvens privadas. Dizer que essa solução federa soluções em nuvens é afirmar que realiza a comunicação e a união entre sistemas diferentes de gestão em nuvem para a sua gestão interna. Por exemplo, é possível que uma das nuvens participante esteja apoiada sobre a solução *OpenStack*, e outro a participante utilize o *OpenNebula*.

O acesso à federação de recursos em nuvem é possível porque o *Fogbow* oferta uma interface de programação – API – comum aos participantes, padronizando a forma de comunicação entre as gerências das soluções em nuvem e a visão global da federação de nuvens ofertada pelo FogBow. Sendo assim, sua principal ideia é fornecer as funcionalidades de uma federação de recursos distribuídos em nuvem em um nível superior, através da implementação de um *middleware* cujo único propósito é suportar operações na federação. O Fogbow é implantado no topo do orquestrador de nuvens da infraestrutura como serviço – *IaaS* – em cada membro da federação, e para deixar mais clara essa visão, este projeto define como a autenticação e autorização acontecem no ambiente.

Está em desenvolvimento um modelo de gestão de identidade para a autenticação e deverá ser avaliada também uma proposta de autorização neste ambiente. Atualmente, os controles de acesso são realizados apenas pelos orquestradores locais da nuvem. É necessário relatar que a integração com federações baseadas no Shibboleth e VOMS para autenticação já são suportadas. A integração com OpenID Connect e LDAP (uma realidade das instituições públicas) é intenção do projeto e está em andamento.

[2]http://www.fogbowcloud.org/

2.1.4. Iniciativas de Pesquisa e Colaboração em A&A

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 desde então vem trabalhando com mais de vinte parceiros para proporem o design e testes (pilotos) de técnicas e políticas para: (i) identificar os requisitos necessários em pesquisa colaborativa internacional, indo além das capacidades de acesso federado atuais; e (ii) entregar um modelo de arquitetura bem como um grupo de diretrizes para permitir interoperabilidade no contexto de Autenticação e Autorização (AA), passíveis de serem integrados aos ambientes de produção das instituições.

A primeira fase do AARC foi encerrada em abril de 2017. Uma segunda fase do projeto (AARC2) começou em maio de 2017 para continuar a desenvolver e avaliar um *framework* para interoperabilidade em questões de AA, construído em infraestruturas já existentes. O *framework* contempla três aspectos: (i) um modelo de arquitetura em camadas, para proporcionar interoperabilidade em contextos federados; (ii) um grupo de políticas e de boas práticas; e (iii) testes das técnicas e políticas propostas com base nos requisitos identificados junto à comunidade (pilotos).

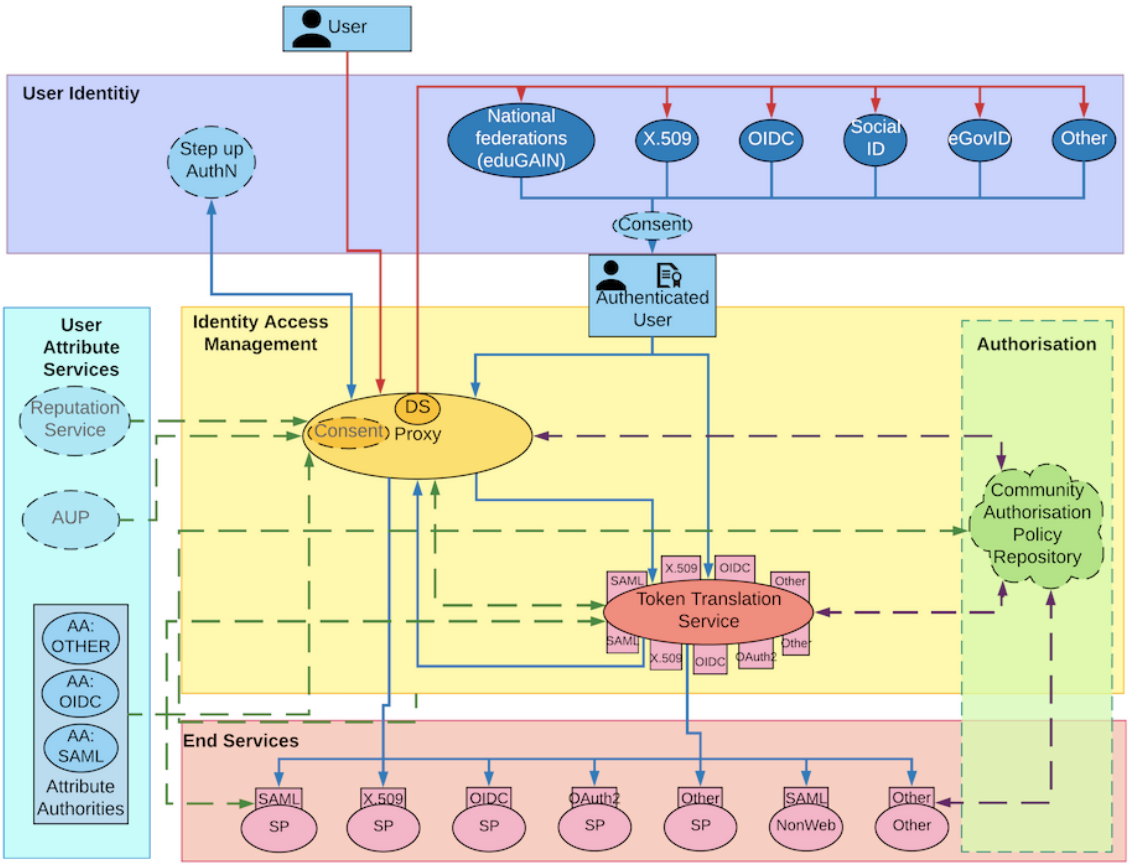

Figura 1. Modelo de Arquitetura AARC

.

O modelo de arquitetura proposto pelo projeto AARC, denominado *Blueprint Ar-*

chitecture (BPA)[3], tem por objetivo fornecer um modelo de arquitetura interoperável para arquitetos de software e gestores, que projetam e implementam soluções de gerenciamento de identidade para pesquisa internacional colaborativa. A Figura 1 mostra a visão geral da BPA, composta por camada de identidade do usuário (topo), camada de atributo de usuário (esquerda), camada de gestão de identidade e de acesso (centro), camada de serviço final - SPs (base) e camada de autorização (direita). 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 informação sobre atributos.

- **Camada de identidade do usuário** fornece identidades eletrônicas aos usuários participantes de colaborações internacionais de pesquisa. Normalmente, os serviços nesta camada estão fora dos limites administrativos destas iniciativas, cabendo a estas fornecer autenticação segura.
- **Camada de gestão de identidade e de acesso** define fronteiras administrativas, políticas e tecnológicas entre serviços internos das instituições. Proporciona a redução de custo na implementação de novos serviços, bem como a flexibilidade para escolha de protocolos e mecanismos de segurança adequados a contextos específicos. Um componente importante desta camada é o serviço de tradução de *tokens*, responsável por transpor credenciais em diferentes tecnologias tais como, SAML, X.509, OIDC, OAuth2 e outras.
- **Camada de atributos**, fornece atributos de usuários, tais como grupos e papéis, além de atributos provenientes diretamente da identidade. Esta camada tem dois componentes: a AUP (*Acceptable Use Policy*), e um serviço de reputação (delimitados na Figura 1 por linhas tracejadas). O primeiro denota um serviço que registra as políticas de acesso aceitas pelos usuários (requerido pelo SIRTFI). O segundo registra a reputação do usuário (*Design for Deploying Solutions for "Guest Identities" - AARC-MJRA1.2*).
- **Camada de autorização**, uma abordagem centralizada permite aos gestores e desenvolvedores delegar questões complexas de autorização a um componente central, o que garante a redução de esforço em aspectos relacionados ao gerenciamento de políticas de autorização, bem como sua avaliação em cada serviço de forma individual.
- **Camada de serviços finais** onde se encontram os serviços que os usuários finais utilizam. Estes vão desde serviços Web simples como *wikis* ou portais que oferecem acesso a dados e serviços, até SPs não baseados em browser, tais como *shell* de comando, serviços de FTP e sistemas de gerenciamento de carga.

O CT-GId avalia que é necessário acompanhar de perto os trabalhos e pesquisas realizados no projeto AARC, bem como utilizar o modelo de arquitetura do projeto AARC como um modelo de referência de GId.

3. Autenticação

3.1. Autenticação Multi-fator

Atualmente, credenciais de acesso baseadas no par `nome de usuário/senha` são as mais comuns usadas pelos mecanismos de autenticação. Sabe-se que essa solução possui

[3] `https://aarc-project.eu/architecture/`

diversas fragilidades, como por exemplo usuário escolher senhas fáceis e suscetíveis a diversos ataques, como por exemplo *phishing*[4].

Credenciais de acesso são geralmente classificadas nas seguintes categorias: **aquilo que você sabe** – como as senhas; **aquilo que você possui** – como um cartão inteligente; **aquilo que você é** – como a biometria do usuário.

Para cada uma dessas categorias, tem-se vantagens e desvantagens que podem impedir o usuário correto de ter acesso ao recurso. Por exemplo, as senhas podem ser esquecidas assim como um cartão inteligente. A biometria não pode ser esquecida, mas pode ficar indisponível temporariamente, como a falta de voz, impressão digital apagada devido a um trabalho manual, etc. Além disso, apesar da biometria apresentar maior disponibilidade, seu uso como único fator de autenticação não é considerado seguro, tendo em vista que as características de uma pessoa, apesar de serem únicas, são públicas, o que torna fácil a sua captura sem que a pessoa percebesse [Brainard et al. 2006].

A autenticação multi-fator, às vezes chamada de autenticação com dois fatores (*two factor authentication*), surge como uma solução para aumentar a robustez dos processos de autenticação e, geralmente, combina fatores das diferentes categorias apresentadas anteriormente, ou poderiam ainda combinar dois ou mais fatores de uma mesma categoria, como é o caso das senhas descartáveis (*One Time Password* – OTP) [Haller et al. 1998]. Nesse caso, parte-se do pressuposto que um atacante conseguiria comprometer um desses fatores, porém o grau de dificuldade aumentaria muito se fosse necessário comprometer dois ou mais fatores.

Atualmente, diversos provedores de serviços públicos como Google, Github, Dropbox, Facebook, etc. oferecem formas de autenticação com mais de um fator. Há ainda algumas iniciativas específicas para o *framework* Shibboleth, usado pela Federação CAFe, propostas pela academia [da Silva and de Mello 2015, Langenberg 2015, Cantor 2015, de Mello et al. 2018] e pela indústria[5].

Em [Weiser 1991], foi apresentada a visão de um mundo no qual a computação do século 21 seria móvel e onipresente. Pode-se concluir que isso tornou-se realidade principalmente por causa dos telefones inteligentes (*smartphones*), que levaram a computação para o ambiente do usuário, ou seja, para o seu dia-a-dia. Deste modo, os *smartphones* se tornaram um dos candidatos a dispositivo de suporte a autenticação multi-fator, como de fato já é usado por soluções comerciais, seja para recebimento de mensagens curtas de texto (SMS) ou para executar algum aplicativo que permita o uso de senhas descartáveis. Em [NIST 2017], o uso de SMS como segundo fator de autenticação foi considerado como inseguro e não deveria mais ser usado. Dessa forma, aplicativos para dispositivos móveis são candidatos nato para substituí-los.

Aumentar a robustez do processo de autenticação, fazendo uso de mais de um fator, pode diminuir a facilidade de uso da solução. Por exemplo, o uso de senhas descartáveis obtidas por meio de um aplicativo para telefone móvel implica na necessidade de um usuário sempre ter em mãos o telefone no momento que desejar acessar o sistema remoto. Não ter o telefone faz com que o usuário não tenha acessa ao recurso que, em tese, ele deveria ter.

[4]Atacante poderia induzir o usuário correto fornecer suas credenciais de acesso em uma página *web* maliciosa.

[5]`https://duo.com/docs/shibboleth`

Uma outra dificuldade com a autenticação multi-fator está na gestão do ciclo de vida (emissão, renovação, expiração e revogação) das credenciais das diferentes categorias. Por exemplo, se um usuário esquecer sua senha, este consegue recuperá-la sem que necessite interagir com uma pessoa responsável pelo serviço. O provedor de serviço poderia gerar e enviar uma nova senha para o e-mail previamente cadastrado pelo usuário, fazer uso de perguntas de segurança, também cadastradas previamente, etc.

Para credenciais das categorias **aquilo que o usuário possui** ou **aquilo que o usuário é**, a renovação pode não ser algo tão simples caso o usuário perca o segundo fator (p. ex. perdeu o telefone móvel onde estava o aplicativo OTP). O Google, e alguns outros provedores de serviço, tratam dessa questão com um conjunto de senhas descartáveis que o usuário pode imprimir e manter em um local seguro. Essas senhas poderiam, então, ser usadas caso o usuário esteja impossibilitado de usar o segundo fator padrão (p. ex. aplicativo OTP). O Github[6] provê uma alternativa baseada na delegação do processo de recuperação de acesso à conta por meio de um outro provedor de serviço que o usuário também possua conta, no caso, o Facebook.

O modelo de gestão de identidade federada trouxe alguns benefícios que melhoraram a usabilidade para os usuários, como o fato de o usuário ter uma única credencial e acessar diversos provedores de serviço, e só passar pelo processo de autenticação uma única vez (SSO) durante a sessão. Contudo, a principal forma de autenticação de usuário (*username/password*) é a maior fragilidade da solução. A autenticação multi-fator é algo que a indústria já vem trabalhando e ainda não existe um consenso sobre como gerenciar todo o ciclo de vida das credenciais desses fatores adicionais, sendo aqui um ponto que caberia uma investigação. Cabe ainda citar que em [NIST 2017] foi proposto um guia com orientações específicas para o gerenciamento do ciclo de vida das credenciais.

3.2. Autenticação Contínua

Com o processo de autenticação é possível assegurar que um sujeito é realmente quem dizer, tendo como bases as credenciais fornecidas por esse. Geralmente os usuários só precisam passar pelo processo de autenticação antes de terem acesso ao recurso desejado. Uma vez autenticados, esses poderão usufruir dos recursos até o fim de sua sessão.

A autenticação contínua surge como uma solução para assegurar a identidade do usuário durante toda sua sessão e não somente no início. Isso poderia ser obtido, por exemplo, solicitando para o usuário fornecer suas credenciais (*password*), periodicamente, ou quando acessar funcionalidades mais críticas, como a transferência de dinheiro em uma aplicação bancária ou o lançamento de notas dos alunos em um sistema acadêmico.

A autenticação contínua também pode ser feita de forma implícita, ou seja, sem que o usuário fique ciente que está passando pelo processo de autenticação. Em [Shepherd 1995] é feito uso do padrão de digitação do usuário como uma forma de autenticá-lo continuamente de forma implícita. Com o advento da popularização dos telefones inteligentes e pela riqueza de sensores que esses possuem, a autenticação contínua implícita poderia ser obtida com base na geolocalização do usuário, como esse segura seu telefone enquanto toca na tela, por reconhecimento facial, etc. Atualmente tem-se diversos trabalhos na literatura que fazem uso do aprendizado de máquina, aliado aos telefones inteligentes. O

[6] `https://goo.gl/sw1cd2`

FaceID[7], lançado com o iPhone X, é uma ferramenta rica que poderia ser explorada para a autenticação contínua de usuários.

No contexto da Internet das Coisas, a autenticação contínua também poderia ser interessante. Uma pessoa poderia se locomover em seu ambiente de trabalho e as coisas que essa carrega (p. ex. celular, relógio, pulseira, etc.), ou mesmo as coisas ao seu redor (p. ex. câmeras, *beacons* BLE, etc.), poderiam garantir que aquela pessoa poderia estar ali, ou abrir portas sem que a pessoa precise passar explicitamente pelo processo de autenticação, como por exemplo, fornecendo a senha numérica ou encostando seu cartão de acesso no leitor que fica ao lado das portas.

Ter constante certeza de que a pessoa que está acessando um recurso realmente tem permissão para tal é algo interessante do ponto de vista da segurança. Contudo, essa contínua autenticação poderia ferir a privacidade dos usuários. Em [Mehrnezhad et al. 2016], mostrou-se que por meio de códigos *JavaScript*, seria possível um *website* remoto identificar seus visitantes e até mesmo descobrir a senha (PIN *number*) que digitam em seus telefones, simplesmente explorando os dados dos sensores de movimento e orientação, que de acordo com as especificações da W3C, estão disponíveis aos navegadores *web*. Tal tipo de preocupação pode ser replicado para o FaceID da Apple, uma vez que a empresa planeja compartilhar os dados biométricos colhidos com FaceID com desenvolvedores de aplicativos para iOS.

Soluções de autenticação contínua para sistemas ou no contexto da Internet da Coisas é algo desejado e um tema relativamente ativo. Garantir a autenticação contínua sem que isso possa vir a ferir a privacidade dos usuários é algo que ainda precisa ser melhor investigado.

3.3. Autenticação de Dispositivos - IoT

Apesar de vários grupos de pesquisa estarem atuando nesta área, a autenticação e a autorização ainda são problemas em aberto em IoT [Oliveira et al. 2017]. Neste contexto, ambas podem se dar de duas formas: (1) de dispositivo para dispositivos (*device-to-device* – D2D) ou [Aranha et al. 2009, Oliveira et al. 2011, Souza et al. 2013](2) de usuário para dispositivo (*user-to-device* – U2D) [Souza et al. 2018]. As propostas tradicionais que abordam D2D são, muitas vezes, baseadas no modelo tradicional de ICP/certificados digitais. Entretanto, o custo computacional deste modelo é alto demais para as classes de dispositivos em IoT que têm poucos recursos computacionais a oferecer. Assim sendo, é imprescindível a concepção de soluções de autenticação e autorização mais adequadas para dispositivos em IoT.

Algumas soluções baseadas em *gateways* e *proxies* foram propostas, nas quais um equipamento de maior capacidade computacional age na rede em nome de um ou vários dispositivos, implementando tecnologias de autenticação e/ou autorização mais demandantes. Esta solução baseada em *gateways* torna o sistema mais complexo, custoso e menos flexível em termos de mobilidade de dispositivos. Seria mais interessante, portanto, se os próprios dispositivos pudessem se encarregar de questões relativas a autenticação e autorização, desde que as tecnologias utilizadas não fossem tão exigentes em termos de recursos computacionais.

[7] `https://support.apple.com/pt-br/HT208108`

Uma abordagem para tal problema é empregar criptossistemas não baseados em certificados. Dentre eles, destacam-se os Certificados Implícitos [Brown et al. 2002], a Criptografia Baseada em Identidade [Boneh and Franklin 2001] e os sistemas híbridos [Al-Riyami and Paterson 2003]. Cada um destes criptossistemas pode ser implementado de múltiplas formas, o que, por sua vez, impacta (negativa ou positivamente) nas métricas de desempenho temporal (velocidade de operação) e espacial (consumo de memória) e consumo energético.

Dentre os sistemas não baseados em certificados, destacam-se também as Assinaturas Baseadas em Atributos. A criptografia baseada em atributos é uma extensão da criptografia baseada em identidade que se concentra em grupos de usuários em vez de apenas em identidades. Nesse criptossistema, usuários recebem chaves privadas baseadas nos atributos que possuem e utilizam assinaturas para comprovar a posse desses atributos. Com isso, assinaturas baseadas em atributos são ideais para implementar políticas de controle de acesso baseado em atributos, nas quais os atributos de um usuário têm um papel central na concessão de acesso a um determinado recurso [Neto et al. 2016].

Uma segunda abordagem é a integração de atributos do meio físico no processo de autenticação [Wu et al. 2017]. Essa abordagem pode se valer de dados intrínsecos ou extrínsecos para estabelecer a autenticação. Assinaturas intrínsecas se valem de características inerentes aos dispositivos, canais de comunicação ou ao ambiente no processo de autenticação. Assinaturas intrínsecas já foram exploradas no passado para identificar características de dispositivos em gravações de imagens, vídeo e som [Garg et al. 2013]. Assinaturas extrínsecas, por sua vez, se referem a dados artificialmente injetados e monitorados no ambiente físico para detectar comportamento malicioso [Mao and Wu 2007]. Exemplos dessas assinaturas incluem o uso de marcas d'água no ambiente físico ou sequências piloto no ambiente digital [Mao and Wu 2007].

Outra interessante abordagem é o emprego de tecnologias baseadas em *blockchain*, uma cadeia de blocos distribuída, inicialmente, proposta e criada para funcionar como livro-caixa da criptomoeda Bitcoin [Nakamoto 2008]. Como os registros cadastrados no *blockchain* são permanentes, confiáveis e praticamente imutáveis, após serem confirmados um certo número de vezes (6 vezes no *Bitcoin*), e como a verificação da autenticidade destes registros tem um custo baixo, há um grande potencial para que a plataforma *blockchain* seja uma interessante alternativa para facilitar a verificação de uma determinada identidade online [Zyskind et al. 2015].

A associação entre o identificador de um dispositivo e sua chave pública poderia, por exemplo, ser registrada em um *blockchain* (com um certo custo computacional e financeiro para fazê-la, mas com baixo custo para consultá-la). Tal associação poderia ser verificada com facilidade por qualquer dispositivo online, consultando apenas um dos milhares de nós que mantêm o *blockchain* no ar. Acreditamos que esta tecnologia tem o potencial de contribuir significativamente para processos mais eficientes e enxutos de autenticação e autorização de dispositivos em IoT e, por isso, consideramos importante que o CT-GId avance mais nesta área.

Analogamente ao que ocorre em D2D, propostas tradicionais para U2D não são plenamente satisfatórias. Isso porque tais propostas, no momento em que foram concebidas, não levaram em consideração as peculiaridades de dispositivos IoT (e.g., mobilidade,

funcionalidades e sensores). Uma abordagem para criar soluções sob medida para U2D é tirar proveito do padrão de funcionamento dos dispositivos (novamente, mobilidade [Jakobsson et al. 2009], sensores [Liu et al. 2009], funcionalidades [De Luca et al. 2012] etc.) para aumentar o nível de segurança sem, no entanto, impactar negativamente a experiência de usuários.

4. Autorização

4.1. Soluções de Controle de Acesso Federado

Em um cenário de federação, usuários de todos os IdPs têm acesso aos SPs. Entretanto, existem cenários mais específicos, como por exemplo, quando (i) somente um IdP específico tem acesso ao SP (por exemplo, uma instituição paga para que todos os seus usuários tenham acesso ao serviço); (ii) somente alguns usuários do IdP devem ter acesso ao SP (por exemplo, uma instituição contrata um serviço, no qual somente alguns de seus usuários poderão ter acesso ao mesmo, seja por questões de custo ou de sigilo; ou (iii) somente alguns usuários da federação têm acesso ao SP (por exemplo, um serviço exige que cada usuário faça sua contratação ou credenciamento de maneira independente). Atualmente, o administrador de um SP pode precisar lidar com todas essas situações, como foi o caso no projeto CNC (Computação em Nuvem para Ciência)[8], um serviço de armazenamento em nuvem implantado na infraestrutura de redes da RNP.

Para lidar com esses problemas, foi desenvolvido o *Federated Access Control System* (FACS)[Diniz et al. 2015]. FACS apresenta uma solução hierárquica para a definição de políticas de controle de acesso em um ambiente federado, sendo capaz de lidar com os cenários apresentados anteriormente. A abordagem considera que o FACS seja mantido pela instituição que mantém a federação e que seja utilizado por administradores de SPs e IdPs para gerenciar o acesso a diversos serviços. O FACS permite o gerenciamento de políticas de controle de acesso em dois níveis. O primeiro nível, denominado independente de SP, considera o gerenciamento de qual IdP terá acesso ao SP. Sua independência é relacionada ao fato de que políticas de controle de acesso neste nível não dependem das ações específicas que um usuário pode realizar no serviço. Por outro lado, o nível que dependente de SP lida com políticas de controle de acesso específicas para as ações do SP.

O FACS se encontra atualmente em produção, sendo aplicado para o gerenciamento de controle de acesso do serviço *edudrive*. Assim como o *edudrive*, o FACS é mantido hoje pela empresa Anolis TI em conjunto com a Diretoria de Serviços da RNP.

Existem outros sistemas/serviços providos pela RNP com requisitos de gerenciamento de controle de acesso similar ao *edudrive*, como por exemplo o serviço Conferência Web. Entretanto, em sua versão atual, o FACS foi desenvolvido focado no gerenciamento de controle de acesso do serviço *edudrive*, e portanto, se faz necessária uma etapa de Pesquisa e Desenvolvimento para que o mesmo possa ser aplicado a outros serviços. Neste contexto, identificamos algumas questões, a saber:

- Como suportar o uso do FACS em diversos SPs, uma vez que sua implementação envolve componentes específicos do SP? É necessário definir um processo de customização da solução de forma a permitir sua aplicação em vários SPs.

[8]O projeto resultou no serviço edudrive: https://edudrive.rnp.br/

- Como permitir a definição de políticas de acesso (quais ações podem ser feitas e por quem) para diferentes SPs uma vez que somente o SP tem conhecimento de quais ações podem ser desempenhadas por seus usuários?
- Como lidar com a gestão do ciclo de vida de uma identidade digital em SPs?
- Como permitir o gerenciamento de recursos do SP? A política de uso desses recursos poderia ser definida pela instituição dona do IdP?
- Como realizar o mapeamento entre diferentes modelos de controle de acesso, políticas, e atributos entre várias instituições (IdPs/SPs)?

4.2. ACROSS

Comparado a outros trabalhos, o ACROSS (*Attribute-based access ContROl and diStributed policieS*) [Silva et al. 2018] apresenta uma solução genérica de gestão de identidade focada em autenticação e autorização para organizações virtuais ou IAA (Infraestrutura de Autenticação e Autorização). O ACROSS foi proposto para ser utilizado em ambientes com quaisquer tipos de recursos distribuídos. A solução apresenta um *framework* que permite toda a integração de um ambiente qualquer de organização virtual desde a comunicação com uma federação de identidade Shibboleth/SAML até o controle de acesso a recursos através de atributos, baseado no ABAC (*Attribute-Based Access Control*). uma facilidade do *framework* é a integração aos diversos tipos de ambientes de recursos compartilhados, a partir da troca de mensagens para chamadas entre os módulos do *framework* de forma padronizada. O ACROSS oferece também uma ferramenta complementar ao *framework* chamada de ACROSS *Wizards*. Basicamente, o que essa ferramenta faz é guiar o administrador da OV na instalação e configuração de todos os módulos.

Na arquitetura do ACROSS destacam-se os componentes *Identity Federation Module*, *Attribute Module* e *Access Control Module*. O *Identity Federation Module* tem como principal função se comunicar com uma federação SAML/Shibboleth, como é o caso da CAFe. Esse módulo realiza a transposição de credenciais advindas da federação para o ambiente da OV, por exemplo, um certificado X.509. Caso seja necessário, para complementar a credencial do usuário, é possível utilizar o *Attribute Module*, que tem como função a agregação de atributos adicionais específicos do ambiente da OV. O *Access Control Module* se baseia nos atributos do usuário, utilizados para a criação de sua credencial, para realizar um controle de acesso fino, baseado em atributos, ABAC. Esse controle de acesso é implementado em XACML e permite políticas distribuídas, chamadas de globais e locais. As globais ficam no nível do administrador da OV e as locais são criadas pelos administradores de cada instituição, ou ilha de recursos.

O ACROSS foi validado em um ambiente hipotético e no FIBRE [9], porém não foi avaliado no ambiente de nuvens computacionais, sendo uma intenção expressa pelos autores em trabalhos futuros. Soluções de IAA a serem desenvolvidas ou já existentes, seja para quaisquer tipos de recursos distribuídos, devem levar em consideração a experiência e possibilidade de integração do ACROSS e FACS para facilitar a GId.

4.3. Políticas de Controle de Acesso em Ambientes Multi-Nuvens Heterogêneos

Múltiplos provedores de computação em nuvem ofertam seus serviços de forma competitiva. Para evitar dependência (o chamado *vendor lock-in*), usuários utilizam muitos

[9] `http://www.fibre.org.br`

serviços em ambiente multi-nuvens terceirizado e heterogêneo. Desta forma, a segurança de dados e sistemas depende normalmente de mecanismos existentes de forma isolada em cada um dos provedores. Mecanismos de controle de acesso são responsáveis pela identificação, autenticação e autorização dos usuários aos recursos. No caso de um ambiente multi-nuvens, usuários geralmente precisam se autenticar diversas vezes e definir políticas de segurança para cada um dos serviços, que, possivelmente, podem apresentar inconsistências.

Proporcionar aos usuários de sistemas heterogêneos multi-nuvens uma experiência de acesso homogênea a estes serviços é um grande desafio. Federações de identidade proporcionam o *Single Sign-On (SSO)*, em que os usuários são identificados e autenticados por provedores de identidade (IdPs) uma única vez e, através de protocolos como OpenID Connect, SAML ou ABFAB [Howlett et al. 2016], recebem acesso a serviços federados com os quais possuem relação de confiança. No entanto, as políticas de controle de acesso não são comuns. Cada serviço de nuvem costuma ter seu próprio mecanismo de controle de acesso, com linguagens próprias para definição de políticas.

O trabalho de Sette [Sette 2016] define uma solução que provê autenticação e autorização homogêneas a usuários de múltiplos serviços de computação em nuvem heterogêneos no modelo de Infraestrutura como Serviço (*Infrastrucuture as a Service* - IaaS). Isso é possível através de federações de identidade e de políticas de autorização. Nesta solução, políticas de segurança são armazenadas de forma centralizada em uma Forma Normal Disjuntiva (*Disjunctive Normal Form* - DNF) com semântica definida em uma Ontologia. Portanto, clientes de múltiplas nuvens podem criar "Federações de Políticas de Autorização"(*Authorization Policy Federation* - APF) e associar suas contas em cada provedor a estas federações. Desta forma, regras de autorização globais, definidas e gerenciadas pela APF, passam a valer em todas as contas que fazem parte da federação, garantindo uma experiência homogênea de acesso.

Um protótipo do sistema, composto de um Ponto de Administração de Políticas (PAP) centralizado e mecanismos de tradução e sincronismo de políticas, foi implementado para nuvens OpenStack e Amazon Web Services (AWS) [Sette et al. 2017]. Uma ontologia também foi definida, baseada no controle de acesso destas tecnologias.

A métrica “nível de equivalência semântica” (*Level of Semantic Equivalence* - LSE) foi definida para calcular o percentual de regras de uma política que pode ser traduzido para termos de uma ontologia. Na validação da solução, políticas de autorização baseadas em exemplos fornecidos por OpenStack e AWS foram convertidas para regras globais, baseadas na ontologia, e vice-versa, com LSE superior a 80%. Mais detalhes do trabalho podem ser encontrados em [Sette 2016].

Alguns trabalhos futuros estão listados, a seguir:

- A ontologia para Controle de Acesso em IaaS pode ter novos serviços acrescentados, como *storage*, *orchestration*, *network* etc., bem como novos elementos podem ser adicionados aos serviços existentes;
- A solução APF pode ser modificada para reconhecer usuários que se autenticam em múltiplos IdPs como uma entidade única. Por exemplo, um usuário pode se autenticar, usando sua conta no IdP Google ou no IdP Facebook e ser reconhecido como um usuário único;
- Estudar outras tecnologias de nuvem para que estas tenham suporte na ontologia

(ex. Google Cloud, Microsoft Azure);
- Permitir que computação em nuvem suporte o paradigma *Verifiable Credentials* como meio de acesso.

Verifiable Credentials são um novo paradigma em gerenciamento de identidade e tem o potencial de ser uma tecnologia muito disruptiva. Elas são o equivalente eletrônico de passaportes, cartões de crédito etc. e permitirão que os usuários acessem com segurança recursos baseados na web. No entanto, as credenciais verificáveis são muito mais seguras e protegem mais a privacidade do que as credenciais físicas, pois usam meios criptográficos para permitir que o usuário divulgue minimamente seus atributos de identidade aos serviços da web. Um simples atributo, como a idade, pode ser liberado para o serviço da Web, sem revelar outras informações, como nome ou endereço. Ser criptograficamente protegidas significa que elas podem ser totalmente confiáveis pelo serviço que as recebe. *Verifiable Credentials* estão em um estágio inicial de seu desenvolvimento e seu formato está sendo padronizado pelo W3C[10], o que é essencial para que estas se tornem amplamente utilizadas na Internet.

5. Privacidade

Mesmo não havendo no Brasil uma cultura mais forte voltada para proteção da privacidade dos usuários das redes e sistemas e para a responsabilização dos administradores de rede e de sistemas que não preservarem a privacidade, recomendamos que se envide esforços no sentido de priorizar a proteção da privacidade dos usuários. Tais esforços passam por treinamentos dos técnicos sobre procedimentos e técnicas pró-privacidade, bem como por uma maior conscientização da comunidade de usuários sobre os riscos à privacidade ocasionadas pelos procedimentos executados. Seguindo o exemplo da União Europeia[11], o Brasil estabeleceu[12] a lei Nº 13.709, de 14 de agosto de 2018 que dispõe sobre a proteção de dados pessoais.

Nos últimos anos, tivemos um considerável progresso no uso de federações de identidade. Muitos usuários já acessam serviços de terceiros usando o serviço de autenticação de sua instituição de origem. Por outro lado, na construção de esquemas de autorização, o uso dos mecanismos proporcionados por federações não avançou tanto. Um serviço só poderá contar com um mecanismo de autorização se tiver garantias sobre os dados fornecidos pelos provedores de identidade da federação. Isso remete à questão de níveis de garantia (*Level of Assurance - LoA*), sobre a qual mais esforços ainda são necessários.

Uma outra questão diz respeito à privacidade do usuário. Tipicamente, não nos preocupamos com o acesso alheio aos nossos dados, mas antes de propor que dados de boa qualidade sejam divulgados para serviços arbitrários sem maior controle, é preciso refletir um pouco sobre o valor dessa informação. Propagandas direcionadas são apenas um exemplo relativamente ingênuo do inconveniente que a circulação irrestrita de dados pode gerar. Portanto, é preciso enfrentar a questão da garantia da qualidade dos dados fornecidos, problema que aumenta com o aumento do número de instituições participantes. Entretanto, é preciso fazer isso sem abrir mão de proteger tanto quanto possível a privacidade do usuário.

[10] https://www.w3.org/community/credentials/

[11] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

[12] http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Alguns problemas de privacidade são extremamente complexos e dependem de diversos fatores, a começar pela própria definição do que é privado e do que não é. No entanto, outros problemas podem ser resolvidos com implementações nos ambientes federados. Técnicas criptográficas como comprometimento (*commitments*) e ADC-Nets (*asymmetric dining cryptographers network*) podem ser usadas para fornecer garantias e proteger a privacidade. Assim, o repúdio de informações seria evitado, e consequentemente, quem provê a identidade poderia ser responsabilizado. ADC-Nets poderiam ser usadas para gerar estatísticas anônimas de registros dos sistemas (logs), que por sinal deveriam ser cifrados com técnicas de segredo compartilhado (*secret sharing*) para evitar que um dos administradores tenha acesso irrestrito às informações privadas dos usuários.

Tais técnicas vão de encontro com a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que regulamente a criação de um Comitê de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta. Em vez de um técnico administrador de sistemas, apenas um número predeterminado de membros do comitê poderia acessar informações privadas. Além de terem acesso restrito, os logs deveriam expirar após um prazo predeterminado. Inspirado na lei 8.078, de 11 de setembro de 1990 [GovBR 1990] e no decreto 2.181, de 20 de março de 1997[13], os logs poderiam ser armazenados por apenas cinco anos. Mais grave que armazenamento e tratamento dos logs é o armazenamento e tratamento das senhas. Parece não haver dúvidas no tratamento de chaves criptográficas. Segundo o Art. 6o da medida provisória no 2.200-2, de 24 de agosto de 2001, "O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento" [GovBR 2001].

Para alguns administradores, parece haver dúvidas que a senha do usuário é um tipo de chave privada. O vazamento de senha compromete a segurança e a privacidade. Em vez de armazenar o resumo criptográfico (hash) de cada senha, os sistemas deveriam armazenar o resumo criptográfico da concatenação do endereço de e-mail com a senha. Tal prática evitaria a identificação de senhas iguais devido a resumos criptográficos iguais. Mas, isto não evita que usuários entrem com a mesma senha em sistemas que tratam as senhas de forma equivocada. Precisamos de protocolos de autenticação e procedimentos de gerenciamento de senhas que garantam o tratamento adequado das mesmas.

É possível identificar com certa facilidade um sistema com gerenciamento deficiente de senhas. Basta que o usuário informe que esqueceu a senha para ver que tipo de alternativas lhe são apresentadas. Se o sistema apresentar alguma das alternativas abaixo, há um problema no tratamento das senhas que precisa ser corrigido.

1. O sistema informa que a senha é a mesma de outros sistemas, como por exemplo, e-mail.
2. O sistema envia a senha para o usuário, indicando que administradores (ou programas maliciosos) poderiam ter acesso a ela.
3. A senha é enviada por e-mail com ou sem criptografia.
4. O sistema envia um link que permite acesso direto a uma página com a identidade e senha do usuário.
5. O sistema diz que o usuário não deve criar mais de uma conta para usar o mesmo serviço.

[13] http://www.planalto.gov.br/ccivil03/decreto/d2181.htm

Certamente, as implementações necessárias para aumentar a segurança, estabelecer garantias e proteger a privacidade devem ser feitas em vários níveis das aplicações até sistemas operacionais. Elas são os primeiros desafios antes do encaminhamento para questões mais árduas referente a privacidade em sistemas de gestão de identidades.

Outra ideia nesta linha é buscar suporte na consagrada teoria de Prova de Conhecimento Nulo (Zero-Knowledge Proof ou ZKP) para a construção de protocolos multiagentes que garantam a autenticidade e integridade de um repositório de certificados de atributos em smartcards, em particular, protegendo certificados de atributos privados. Nesse sentido pode-se trabalhar com primitivas criptográficas homomórficas que permitem que as provas de conhecimento sejam entregues a agentes que não podem saber o conteúdo de tal conhecimento. E, no caso de verificação do conteúdo, estes não guardam provas que possam comprometer a privacidade do atributo.

A aplicabilidade é ampla no ambiente acadêmico, em especial nas questões de saúde e priorização social. Estas poderiam ser embarcadas como certificados de atributos que fazem com que as prioridades sejam respeitadas por uma ordem superior de quem emitiu o atributo sem que os indivíduos sejam obrigados a renunciar à privacidade. Um cenário comum pode ser o acesso a um restaurante universitário com passe gratuito onde é impossível para o sistema identificar um detentor de auxílio social pelo seu tipo de auxílio, assim evitando quaisquer discriminações. Na área de saúde, isso é ainda mais evidente, dando privilégios para portadores de doenças sem que as partes precisem saber qual é a doença.

6. Interoperabilidade entre Sistemas de Gestão de Identidade

A diversidade de sistemas e de especificações para prover a gestão de identidades dentro dos ambientes corporativos ou acadêmicos aumenta a preocupação no que diz respeito a interoperabilidade entre estes diferentes sistemas de GID. Diversos aspectos precisam ser considerados quando uma organização deseja disponibilizar acesso aos seus recursos por meio de diferentes sistemas de GID. Por exemplo, para promover a colaboração entre pesquisadores de diferentes federações e que utilizam diferentes sistemas de GID (federações heterogêneas), é preciso estabelecer relações de confiança entre as federações ou entre as entidades envolvidas (IdPs, SPs ou proxies) para disponibilizar ou consumir informações dos diferentes sistemas adotados pelas organizações. Dentre as tecnologias de gestão de identidades federadas, atualmente, destacam-se as especificações SAML, OpenID Connect, OAUTH e WS-Federation. A transposição de informações dos usuários (tokens de autenticação, de atributos e de autorização) entre federações heterogêneas é um problema que precisa ser melhor investigado.

A Iniciativa Kantara[14], através do Grupo de Trabalho de Interoperabilidade entre Federações (FIWG[15]), discute e analisa soluções de interoperabilidade com foco voltado para interoperabilidade entre federações. De acordo com o FIGW, os sistemas de GId devem permitir que usuários possam acessar recursos mesmo que estes façam parte de um domínio de outra federação e que utiliza outra tecnologia. Um dos objetivos do FIWG é definir a especificação de um perfil SAML que possibilita a interoperabilidade entre o SAML e outros protocolos de autenticação e de autorização. As pesquisas realizadas pelo

[14]https://kantarainitiative.org/

[15]https://kantarainitiative.org/groups/federation-interoperability-work-group/

FIWG resultaram na definição de alguns requisitos[16] que tentam caracterizar as formas e níveis de interoperabilidade e as entidades que interagem nestes níveis.

Para concepção de um ambiente interoperável, outro aspecto citado pelo FIWG que necessita de atenção é a sintaxe e a semântica dos atributos (como mapear os modelos de dados das federações e como manipulá-los). A especificação System for Cross-domain Identity Management (SCIM)[17], definida pela IETF para ambientes de nuvem de recursos interdomínios, pode contribuir com este aspecto. Esta especificação apresenta um conjunto de atributos bem definidos que são atribuídos a uma organização, contemplando usuários, grupos, recursos, e a própria organização em si. A especificação SCIM define uma API para manipulação dos dados que possibilita a interação entre diferentes organizações.

De acordo com o grupo de trabalho FIWG, a interoperabilidade pode ser caracterizada por: (1) interoperabilidade promovida por entidades que representam instituições, como os IdPs, SPs, *proxies*, provedores de atributos, serviços de descoberta (DS) ou operadores de federações (confederações); (2) interoperabilidade tratada por camada, sendo representada pela camada técnica (protocolos), camada legal e a camada de privacidade.

Na camada de protocolos, têm-se iniciativas do próprio projeto Shibboleth[18][19], sendo discutidas dentro do contexto do consórcio e nas listas de discussões, de integração de uma camada OpenID Connect dentro do Shibboleth IdP. Outra iniciativa vem através de esforços da GÈANT, no projeto SATOSA [20], que implementa um proxy SAML que é capaz de se comunicar com mídias sociais e provedores de identidades como Facebook e Google. Estas iniciativas demonstram o interesse em aproximar diferentes protocolos, SAML e OpenID Connect, que atuam em diferentes contextos, voltados para ambientes acadêmicos e corporativos, respectivamente.

Prover a interoperabilidade entre sistemas de GId é um desafio e pode contribuir com diferentes cenários, tais como: colaboração entre empresas e universidades, entre governos [21], sistemas de *e-saúde* e *e-science* (organizações virtuais).

Sugerimos que estes aspectos de interoperabilidade sejam amplamente investigados, experimentados e avaliados para que estes cenários colaborativos possam ser mais flexíveis e abertos.

7. Conclusão

Como pode ser depreendido deste documento, existem muitos desafios interessantes e motivadores na área técnica de gestão de identidades. A RNP certamente deverá enfrentar alguns destes desafios no contínuo aprimoramento dos seus serviços e, pelos relatos e direções presentes no documento, esta poderá contar com um bom número de pesquisadores brasileiros para contribuir em diferentes aspectos relacionados à gestão de identidades.

[16]https://kantarainitiative.org/confluence/display/fiwg/Federation+Interoperability+Patterns
[17] http://www.simplecloud.info/
[18]https://identityblog.switch.ch/2016/03/08/openid-connect-meets-saml-and-shibboleth/
[19]https://wiki.shibboleth.net/confluence/display/IDP30/Contributions+and+Extensions
[20]https://github.com/its-dirg/SATOSA
[21]https://eid-stork.eu

Agradecimentos

Agradecemos à Rede Nacional de Ensino e Pesquisa (RNP) por suportar o Comitê Técnico de Gestão de Identidades (CT-GId), bem como aos demais membros do CT-GId que contribuíram nas discussões que levaram a produção deste artigo.

Referências

[Al-Riyami and Paterson 2003] Al-Riyami, S. S. and Paterson, K. G. (2003). Certificateless public key cryptography. In *Advances in Cryptology-ASIACRYPT 2003*. Springer Berlin Heidelberg.

[Alfieri et al. 2003] Alfieri, R., Cecchini, R., Ciaschini, V., dell'Agnello, L., Gianoli, A., Spataro, F., Bonnassieux, F., Broadfoot, P. J., Lowe, G., Cornwall, L., Jensen, J., Kelsey, D. P., Frohner, Á., Groep, D. L., de Cerff, W. S., Steenbakkers, M., Venekamp, G., Kouril, D., McNab, A., Mulmo, O., Silander, M., Hahkala, J., and Lörentey, K. (2003). Managing dynamic user communities in a grid of autonomous resources. *CoRR*, cs.DC/0306004.

[Aranha et al. 2009] Aranha, D. F., Oliveira, L. B., López, J., and Dahab, R. (2009). NanoPBC: implementing cryptographic pairings on an 8-bit platform. In *Conference on Hyperelliptic curves, discrete Logarithms, Encryption, etc (CHiLE 2009)*.

[Blobel 2010] Blobel, B. (2010). Architectural Approach to eHealth for Enabling Paradigm Changes in Health. *Methods of Information in Medicine*, 49(2):123–134.

[Boneh and Franklin 2001] Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *Advances in Cryptology—CRYPTO 2001*.

[Brainard et al. 2006] Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., and Yung, M. (2006). Fourth-factor authentication: somebody you know. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 168–178. ACM.

[Brown et al. 2002] Brown, D. R. L., Gallant, R. P., and Vanstone, S. A. (2002). Provably secure implicit certificate schemes. In *Proceedings of the 5th International Conference on Financial Cryptography*.

[Cantor 2015] Cantor (2015). Authentication flow selection. `https://wiki.shibboleth.net/confluence/display/IDP30/AuthenticationFlowSelection#AuthenticationFlowSelection-FlowSelection`.

[da Silva and de Mello 2015] da Silva, S. N. and de Mello, E. R. (2015). O uso de um segundo fator e autenticação contínua em provedores de serviços críticos. Programa de gestão de identidade (PGID) da Rede Nacional de Ensino e Pesquisa (RNP).

[De Luca et al. 2012] De Luca, A., Hang, A., Brudy, F., Lindner, C., and Hussmann, H. (2012). Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns. In *CHI*.

[de Mello et al. 2018] de Mello, E. R., Wangham, M. S., Loli, S. B., da Silva, C. E., and da Silva, G. C. (2018). Autenticação multi-fator em provedores de identidade shibboleth. In *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*.

[Diniz et al. 2015] Diniz, T., d. Felippe, A. C., Medeiros, T., d. Silva, C. E., and Araujo, R. (2015). 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*, pages 199–207.

[Fernández-Alemán et al. 2013] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., and Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3):541–562.

[Foster et al. 2001] Foster, I., Kesselman, C., and Tuecke, S. (2001). The anatomy of the grid: Enabling scalable virtual organizations. *International Journal of High Performance Computing Applications*, 15(3):200–222.

[Garg et al. 2013] Garg, R., Hajj-Ahmad, A., and Wu, M. (2013). Geo-location estimation from electrical network frequency signals. In *International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*.

[GovBR 1990] GovBR (1990). L8078compilado. `https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm`. Accessed: 2016-11-28.

[GovBR 2001] GovBR (2001). 2200-2. `http://www.planalto.gov.br/Ccivil_03/MPV/Antigas_2001/2200-2.htm`. Accessed: 2016-11-28.

[Haller et al. 1998] Haller, N., Metz, C., Nesser, P., and Straw, M. (1998). Rfc 2289: A one-time password system. Technical report, Technical report, IETF.

[Howlett et al. 2016] Howlett, J., Hartman, S., Tschofenig, H., and Schaad, J. (2016). Rfc 7831: Application bridging for federated access beyond web (abfab) architecture. Technical report, IETF.

[Hu et al. 2013] Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K., et al. (2013). Guide to attribute based access control (abac) definition and considerations (draft). *NIST Special Publication*, 800(162).

[Internet2 2016] Internet2 (2016). Grouper internet2. `http://www.internet2.edu/products-services/trust-identity/grouper/`. Accessed: 2016-07-15.

[ITU 2009] ITU (2009). Ngn identity management framework. Recommendation Y.2720.

[Jakobsson et al. 2009] Jakobsson, M., Shi, E., Golle, P., and Chow, R. (2009). Implicit Authentication for Mobile Devices. In *HotSec*.

[Koopman et al. 2015] Koopman, R. J., Steege, L. M. B., Moore, J. L., Clarke, M. A., Canfield, S. M., Kim, M. S., and Belden, J. L. (2015). Physician Information Needs and Electronic Health Records (EHRs): Time to Reengineer the Clinic Note. *Journal of the American Board of Family Medicine : JABFM*, 28(3):316–23.

[Lake et al. 2014] Lake, D., Milito, R., Morrow, M., and Vargheese, R. (2014). Internet of Things: Architectural Framework for eHealth Security. *Journal of ICT Standardization*, 1(3):301–328.

[Langenberg 2015] Langenberg, D. (2015). Multi context broker. `https://spaces.internet2.edu/display/InCAssurance/Multi-Context+Broker`.

[Liu et al. 2009] Liu, J., Wang, Z., Zhong, L., Wickramasuriya, J., and Vasudevan, V. (2009). uWave: Accelerometer-based Personalized Gesture Recognition and Its Applications. In *PerCom*.

[Mao and Wu 2007] Mao, Y. and Wu, M. (2007). Tracing malicious relays in cooperative wireless communications. *IEEE Transactions on Information Forensics and Security*, 2(2):198–212.

[Martínez-Pérez et al. 2014] Martínez-Pérez, B., de la Torre-Díez, I., López-Coronado, M., Sainz-de Abajo, B., Robles, M., and García-Gómez, J. M. (2014). Mobile Clinical Decision Support Systems and Applications: A Literature and Commercial Review. *Journal of Medical Systems*, 38(1):4.

[Martino et al. 2008] Martino, L. D., Qun Ni, Lin, D., and Bertino, E. (2008). Multi-domain and privacy-aware role based access control in eHealth. In *2008 Second International Conference on Pervasive Computing Technologies for Healthcare*, pages 131–134. IEEE.

[McGuire et al. 2013] McGuire, M. J., Noronha, G., Samal, L., Yeh, H.-C., Crocetti, S., and Kravet, S. (2013). Patient Safety Perceptions of Primary Care Providers after Implementation of an Electronic Medical Record System. *Journal of General Internal Medicine*, 28(2):184–192.

[Mehrnezhad et al. 2016] Mehrnezhad, M., Toreini, E., Shahandashti, S. F., and Hao, F. (2016). Touchsignatures: identification of user touch actions and pins based on mobile sensor data via javascript. *Journal of Information Security and Applications*, 26:23–38.

[Mortimore et al. 2015] Mortimore, C., Ansari, M., Grizzle, K., Hunt, P., and Wahlstroem, E. (2015). System for Cross-domain Identity Management: Protocol. RFC 7644.

[Musen et al. 2014] Musen, M. A., Middleton, B., and Greenes, R. A. (2014). Clinical Decision-Support Systems. In *Biomedical Informatics*, pages 643–674. Springer London, London.

[Nakamoto 2008] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[Nelson and Staggers 2016] Nelson, R. and Staggers, N. (2016). *Health informatics : an interprofessional approach*. Elsevier.

[Neto et al. 2016] Neto, A. L. M., Souza, A. L., Cunha, I., Nogueira, M., Nunes, I. O., Cotta, L., Gentille, N., Loureiro, A. A., Aranha, D. F., Patil, H. K., and Oliveira, L. B. (2016). AoT: Authentication and Access Control for the Entire IoT Device Life-Cycle. In *SenSys*.

[NIST 2017] NIST (2017). Digital Authentication Guideline. *DRAFT NIST Special Publication 800-63*. `https://pages.nist.gov/800-63-3/`.

[Oladimeji et al. 2011] Oladimeji, E. A., Chung, L., Jung, H. T., and Kim, J. (2011). Managing security and privacy in ubiquitous eHealth information interchange. In *Proceedings of the 5th International Confernece on Ubiquitous Information Management and Communication - ICUIMC '11*, page 1, New York, New York, USA. ACM Press.

[Oliveira et al. 2011] Oliveira, L. B., Aranha, D. F., Gouvêa, C. P., Scott, M., Câmara, D. F., López, J., and Dahab, R. (2011). Tinypbc: Pairings for authenticated identity-

based non-interactive key distribution in sensor networks. *Computer Communications*, 34(3):485–493.

[Oliveira et al. 2017] Oliveira, L. B., Pereira, F. M. Q., Misoczki, R., Aranha, D. F., Borges, F., and Liu, J. (2017). The computer for the 21st century: Security & privacy challenges after 25 years. In *ICCCN*, pages 1–10. IEEE.

[Sanchez-Guerrero et al. 2017] Sanchez-Guerrero, R., Mendoza, F. A., Diaz-Sanchez, D., Cabarcos, P. A., and Lopez, A. M. (2017). Collaborative eHealth Meets Security: Privacy-Enhancing Patient Profile Management. *IEEE Journal of Biomedical and Health Informatics*, 21(6):1741–1749.

[Sette 2016] Sette, I. S. (2016). *Access Control in IaaS Multi-cloud Heterogeneous Environments*. PhD thesis, Universidade Federal de Pernambuco.

[Sette et al. 2017] Sette, I. S., Chadwick, D. W., and Ferraz, C. A. G. (2017). Authorization policy federation in heterogeneous multicloud environments. *IEEE Cloud Computing*, 4(4):38–47.

[Shepherd 1995] Shepherd, S. (1995). Continuous authentication by analysis of keyboard typing characteristics. In *European Convention on Security and Detection*. IET.

[Silva et al. 2018] Silva, E. F., Muchaluat-Saade, D. C., and Fernandes, N. C. (2018). Across: A generic framework for attribute-based access control with distributed policies for virtual organizations. *Future Generation Computer Systems*, 78(Part 1):1 – 17.

[Souza et al. 2018] Souza, A., Cunha, Í., and B Oliveira, L. (2018). Nomadikey: User authentication for smart devices based on nomadic keys. *International Journal of Network Management*, 28(1):e1998.

[Souza et al. 2013] Souza, E., Wong, H. C., Cunha, I., Cunha, I., Vieira, L. F. M., and Oliveira, L. B. (2013). End-to-end authentication in under-water sensor networks. In *2013 IEEE Symposium on Computers and Communications (ISCC)*, pages 000299–000304.

[Sujansky and Kunz 2015] Sujansky, W. and Kunz, D. (2015). A standard-based model for the sharing of patient-generated health information with electronic health records. *Personal and Ubiquitous Computing*, 19(1):9–25.

[Weiser 1991] Weiser, M. (1991). The computer for the 21st century. *Scientific american*, 265(3):94–104.

[Wu et al. 2017] Wu, M., Quintão Pereira, F., Liu, J., Ramos, H., Alvim, M., and Oliveira, L. (2017). New directions: Proof-carrying sensing — towards real-world authentication in cyber-physical systems. In *Conference on Embedded Networked Sensor Systems (SenSys)*.

[Zyskind et al. 2015] Zyskind, G., Nathan, O., et al. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE.