Rede Nacional de Ensino e Pesquisa – RNP

Comitê Técnico em Gestão de Identidades – CT-GId

Visão de futuro sobre pesquisas em gestão de identidades digitais

Marco Aurélio Amaral Henriques
Coordenador

Novembro – 2015

(Versão 1.2)

1. Resumo

Este documento 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 com o Comitê Técnico de Gestão de Identidades (CT-GId). Os resultados apontam para a existência de um grande número de desafios e oportunidades para se dar continuidade às pesquisas e desenvolvimentos nesta área, a qual está ganhando uma importância cada vez maior nos cenários nacional e internacional. Constata-se uma constante necessidade de esforços em melhorias na infraestrutura de identidades federadas, com atenção especial à questão de liberação de atributos. Além disso percebe-se a necessidade de mais atenção e agilidade da RNP para liberação de serviços longamente trabalhados até aqui e longamente esperados pela comunidade, como a emissão de certificados pessoais ICPEdu baseados na federação CAFe (Serviço Automático de Emissão de Certificados – SAEC). A grande demora em disponibilizar serviços como SAEC, por exemplo, tem prejudicado a imagem do projeto ICPEdu e deixado os potenciais usuários céticos quanto a novos anúncios deste serviço ou similares. A solução deste problema irá colocar mais um importante serviço com alto valor agregado à disposição das instituições de ensino, auxiliando-as significativamente na implantação de novos processos de trabalho baseados em tecnologias de assinaturas digitais. E, a atenção da RNP para os novos desafios que se assomam no horizonte, conforme descrito neste documento, permitirá que ela se mantenha na vanguarda tecnológica e operacional, destacando-se no cenário nacional e internacional como uma instituição de referência também nos quesitos relacionados a gestão de identidades digitais.

2. Introdução

Já não é novidade que a área de gestão de identidades (GId) tem recebido grande atenção por parte de empresas, provedores de serviço e pelas redes que dão suporte ao ensino e à pesquisa (National Research and Education Networks - NREN) em vários países.

No mundo extremamente conectado e globalizado provido pela Internet, faz-se necessário dispor de meios cada vez mais sofisticados para autenticação e autorização dos inúmeros usuários que buscam resolver seus problemas no trabalho, estudo, pesquisa e lazer por meio de sistemas conectados à rede.

À medida que aumentam os sistemas provedores de serviços na rede, aumentam os usuários e, consequentemente, aumenta a necessidade de se classificar e separar adequadamente aqueles que podem e que não podem ter acesso a determinados serviços e/ou informações. E estes aumentos acabam atraindo também aqueles que têm interesse em fraudar os sistemas de autenticação e autorização para obter algum tipo de vantagem ou benefício.

Pode-se ver, em meio às diversas iniciativas para prover, verificar e aprimorar os controles sobre identidades digitais, uma grande preocupação em aumentar as garantias de se saber quem está efetivamente requerendo um serviço ou fornecendo uma informação, sem contudo aumentar a sobrecarga nos usuários com procedimentos complexos e/ou pouco claros.

Exemplos disso são os serviços ligados a GId que foram lançados e continuam sendo aprimorados

pela RNP, tais como a Infraestrutura de Chaves Públicas de Ensino e Pesquisa (ICPEdu), o sistema de acesso mundial a redes sem fio (WiFi) acadêmicas usando credenciais da instituição de origem do usuário (Eduroam) e a Federação CAFe (Comunidades Acadêmicas Federadas), que permite a usuários de uma instituição participante ter acesso a diversos serviços de outras instituições (nacionais ou estrangeiras), também usando apenas credenciais obtidas localmente na instituição de origem.

Com o aumento de usuários e suas demandas, e com a maior sensação de fragilização da segurança na rede de um modo geral, surgem novas necessidades e novas ideias para gerir as identidades e os processos (serviços) que dependem delas.

Nas seções a seguir, descrevemos algumas das iniciativas que mais têm merecido a atenção de pesquisadores no Brasil e no exterior. São expostos, de maneira resumida, alguns problemas relevantes da área, bem como ideias de possíveis caminhos a seguir para resolver tais problemas e/ou trilhar novos caminhos em GId.

3. Metodologia

O levantamento das iniciativas de pesquisa discutidas neste relatório foi feito de diversas maneiras e em diversas etapas, como listado a seguir.

- Reuniões do Comitê Técnico de Gestão de Identidades

  Em algumas das reuniões promovidas com os membros do CT-GId foi possível identificar alguns temas de pesquisa em andamento ou por serem iniciados por seus membros e que se mostram suficientemente relevantes para serem considerados em desenvolvimentos futuros.

- Encontros com pesquisadores em eventos científicos e tecnológicos

  Foi possível discutir e levantar questões relevantes com pesquisadores da área durante encontros ocorridos em eventos como Workshop da RNP (WRNP), Fórum da RNP, Simpósio Brasileiro de Telecomunicações (SBrT 2015) e Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2015), por exemplo.

- Projetos propostos para o Programa de Gestão de identidade – PGId 2015

  Dentre os vários projetos que foram propostos em resposta ao edital do Programa de Gestão de Identidades 2015 do CT-GId, alguns mostram claramente a visão que um ou mais pesquisadores têm do futuro da área e merecem ser melhor explorados.

- Pesquisa na literatura e em grupos de discussão técnicas

  Em vários grupos de discussão é possível encontrar debates sobre o passado, presente e futuro de tecnologias de autenticação e autorização, de onde é possível extrair uma série de indícios de pontos promissores em termos de pesquisas futuras.

Após este levantamento inicial, os temas foram discutidos com pesquisadores que atuam em áreas afins à Gestão de Identidades e estes foram solicitados a desenvolver e/ou explorar um pouco mais detalhadamente os temas que fossem de sua expertise ou que lhes fossem mais familiares. O resultado desta contribuição pode ser visto na próxima seção, estando nela incluídos possíveis trabalhos futuros relativos aos quatro projetos PGId financiados em 2015 pela RNP.

4. Visão de Futuro em GId

4.1 Transposição de credenciais por meio de centralização de smart card Ids (Prof. Jean Matina – UFSC)

Por meio de uma exploração mais profunda de novos recursos existentes em smartcards e smartphones de última geração, esta visão se preocupa a investigação de técnicas de autenticação que façam uso de novas tecnologias como geolocalização interna (indoor), NFC (Near Field Communication) e Bluetooth 3 para comunicação entre cartão, telefone celular e rede local (ou internet). Uma combinação dos recursos pode criar um modelo de autenticação mais forte e voltado para a usabilidade, retirando a obrigação do usuário de fazer sua autenticação. Uma possível aplicação seria o controle de frequência de alunos em sala de aula via smartcards dos alunos e o smartphone do professor, o qual poderia já estar integrado a um sistema de apoio ao ensino (Moodle, por exemplo) para fazer o registro das informações coletadas. Outras aplicações podem ser consideradas em vários outros ambientes, como hospitais, creches etc, os quais têm situações e processos de trabalho que exigem uma autenticação confiável e efetiva. Este tipo de modelo de autenticação por localização indoor pode ser usado para ajudar no uso inteligente dos espaços e também para o gerenciamento de risco em ambientes no caso de incidentes graves.

4.2 Proteção de certificados de atributos privados em smartcards (Prof. Jean Matina – UFSC)

A ideia nesta linha é buscar suporte na consagrada teoria de Prova de Conhecimento Nulo (Zero-Knowledge Proof ou ZKP) para a construção de protocolos multi-agentes 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 aos agentes que podem ou não saber o seu conteúdo. E no caso de verificação do conteúdo não guardam provas que possam inviabilizar a privacidade do atributo. As aplicabilidades são inúmeras 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 determinação de quem emitiu o atributo sem que os indivíduos sejam obrigados a renunciar à privacidade, isto é, eles não precisam revelar o porquê de terem uma prioridade que garanta um certo acesso ou serviço privilegiado. 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.

4.3 Materializações de credenciais eletrônicas de identidade

(Prof. Jean Matina – UFSC)

Observam-se alguns problemas práticos no modelo de federação de identidades. O principal deles é que Federações requerem que provedores de serviços e identidades estejam disponíveis *on-line*, ou seja, o provedor de identidade e o provedor de serviço precisam de alguma forma se comunicar para que os usuários possam acessar um dado serviço. Ademais, as identidades providas pela federação requerem o uso de sistemas computacionais para sua verificação, restringindo o seu uso ao contexto de tais sistemas, tornando a verificação por agentes humanos indireta. Porém, o uso de credenciais verificáveis por agentes humanos pode ajudar em vários cenários onde a identificação é corriqueira e necessária. Um exemplo é o requisito de identificação para acesso a certos espaços nas instituições. Uma outra importante questão é que alguns dados são considerados privados, confidenciais e/ou de uso restrito. Neste sentido, a instituição de origem não pode compartilhá-los através de seu provedor de identidade, pois, caso ocorra o um vazamento, a instituição pode sofrer sanções legais pela quebra de privacidade ou do sigilo de tais dados. Um exemplo importante de tal problema é a informação biométrica de um processo de autenticação. Esse tipo de dado pode ser útil como um segundo fator de autenticação, mas sua coleta, armazenamento e transmissão são muito sensíveis a problemas de privacidade em atividades de ambientes federados. Isso faz com que poucas instituições efetivamente façam uso de sistemas fortes de autenticação. Entende-se que para resolver os problemas elencados pela literatura e endereçar as necessidades expostas acima é necessário pensar na concepção de um novo modo de autenticação para as federações. Este modo deve cruzar as barreiras do mundo virtual e permitir a solução de grande parte destes problemas. De fato precisamos de uma materialização da identidade da federação que trabalhe *off-line* e minimize a necessidade de comunicação *on-line* entre as instituições. Também é indispensável que agentes humanos possam verificar identidades sem a utilização de computadores. Por fim, é essencial que o usuário controle seus dados privados (e.g. informações biométricas) e a forma como estes dados são salvos, transmitidos e usados. Desta forma, além de endereçarmos grande parte dos problemas discutidos acima, poderemos abrir um novo leque de opções e oportunidades no âmbitos das federações e dos sistemas de gestão de identidade.

4.4 Autorização em Ambientes de Identidades Federadas (Prof. Carlos Eduardo da Silva – UFRN)

Em um cenário básico de controle de acesso federado, todos os IdPs têm acesso ao SP. Mas existem cenários mais específicos, nos quais (i) somente um IdP tem acesso ao SP (por exemplo, só uma instituição pode pagar e ter acesso ao serviço, mas todos os seus usuários passam a ter acesso ao mesmo), (ii) somente alguns usuários do IdP devem ter acesso ao SP (por exemplo, uma instituição contrata um serviço que é bem caro por usuário e/ou trata de dados sensíveis e, por isso, 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, isto é, somente alguns usuários de alguns IdPs poderão acessar o serviço e seu SP (por exempo, um determinado serviço tem um modelo de negócios que exige que cada usuário faça sua contratação (ou credenciamento) de maneira independente. O administrador de SPs pode precisar lidar com todas essas situações e aí surgem questões tais como: de que forma gerenciar os privilégios específicos do SP? Somente o SP deve saber quais ações podem ser feitas e por quem? Como definir o gerenciamento dos recursos? A

política de uso desses recursos poderia ser definida pela instituição? Uma possível solução a ser pesquisada seria a criação de um sistema de controle de acesso federado que fosse hierárquico e permitisse um controle mais fino e flexível de autenticação e autorização, mediante a adoção de técnicas como Controle de Acesso Baseado em Atributos (ABAC), Controle de Acesso Baseado em Papéis (RBAC) e/ou Controle de Acesso Discricionário (DAC).

4.5 Autenticação única e uso de um segundo fator de autenticação em SPs privados (Prof. Emerson Ribeiro de Mello – IFSC)

O modelo de gerenciamento de identidades federadas está fundamentado em acordos políticos e adequações técnicas, sendo o framework Shibboleth o software padrão adotado para federações acadêmicas. Do ponto de vista dos usuários, a gestão federada de identidades tem como principais benefícios: a autenticação única (Single Sign-On - SSO) e uma única conta de usuário. Com isso o usuário só precisa passar pelo processo de autenticação uma única vez, independente do número de provedores de serviços que visitar, enquanto mantiver o navegador web aberto. Para alguns sistemas críticos, ou mesmo para algumas partes críticas destes sistemas, fazer uso somente de nome de usuário e senha, aliado ao fato de manter a sessão do usuário enquanto o navegador estiver aberto, é algo que poderia trazer riscos de segurança. O uso de um segundo fator para autenticação ou mesmo a autenticação contínua poderiam ser soluções para obter um nível maior de segurança (Level of Assurance - LOA) para estes sistemas críticos. Recentemente foi lançada a versão 3 do Provedor de Identidade (IdP) Shibboleth e entre as novas funcionalidades tem-se a autenticação com um segundo fator. Desta forma, o fato de uma instituição de ensino já estar na federação CAFe facilita a adoção de um segundo fator quando o IdP desta instituição for atualizado. Este é um trabalho que foi desenvolvido no CT-GId, mas algumas questões ainda permanecem abertas para pesquisas futuras, tais como: (1) permitir diferentes fluxos de autenticação no IdPv3, deixando a Provedor de Serviço (SP) escolher o fluxo mais adequado para atender sua LOA. Atualmente o IdPv3 não está maduro suficiente para permitir diferentes fluxos de autenticação, ou seja, se o administrador optar com configurar um fluxo com múltiplos fatores, então todos os usuários desse IdP deverão passar por esse fluxo para todo SP que tentarem acessar; (2) quais tecnologias seriam as mais adequadas, ou menos intrusivas para os usuários, para atuarem como outros fatores de autenticação? (3) O tradicional par nome de usuário e senha ainda precisaria ser usado como uma forma de autenticação? Estas, entre outras questões, precisam ser investigadas a fim de se ter condições de adotar a autenticação com segundo fator em federações que está em contínua evolução.

4.6 Integração de um sistema de votação eletrônica em uma federação de identidades (Prof. Emerson Ribeiro de Mello – IFSC)

O processo de escolha de representantes em instituições de ensino e pesquisa é muito frequente e cada instituição acaba (re)criando seu próprio sistema de votação e apuração de resultados ou adotando algum dos vários sistemas de votação eletrônica disponíveis. Excetuando-se algumas

diferenças em regras eleitorais de uma instituição para outra, os vários processos de eleição têm muitas similaridades. Portanto, seria de grande interesse das instituições se houvesse uma abordagem única, segura, confiável e configurável disponível para todas usarem quando necessário e que aproveitasse ao máximo os investimentos já feitos em cadastramento e autenticação de usuários em cada instituição. Uma possível linha de pesquisa e desenvolvimento em GId seria então aquela relacionada a um sistema de votação eletrônica que pudesse ser integrado a uma federação (como a CAFe, por exemplo) preservando as vantagens da votação eletrônica e aproveitando as vantagens oferecidas por uma autenticação via federação. Todavia, a oferta de um sistema de votação online federado como um serviço de TIC, exigiria uma dependência mínima do departamento de TI da instituição mantenedora do serviço e isso vai além de simplesmente permitir o acesso aos usuários autenticados em provedores de identidades, cabendo citar as seguintes questões: (1) como determinar quais pessoas na federação poderão criar eleições? (2) Como criar uma eleição para um grupo específico de eleitores? (3) Como listar todas as eleições que estão abertas ou finalizadas de maneira a permitir uma consulta fácil na página pública do Helios? (4) Como adaptar sistemas de informação para fazerem uso de mecanismos de controle de acesso baseado em atributos (ABAC)? (5) Como manter a base única de usuários e fazer a associação de direitos com papéis (modelo RBAC)? Apesar de serem questões muito relacionadas com sistemas de votação eletrônica, elas também têm forte relação com gestão de identidades e trazem novos desafios a esta área que precisam ser abordados e melhor compreendidos.

4.7 Interoperabilidade entre federações e Arquitetura de Federação Fatiada (Profa. Natália Fernandes – UFF)

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 ou a federação de recursos para nuvens. Tais federações trazem grandes vantagens e benefícios, mas também trazem desafios importantes, tais como: como nomear/classificar os recursos? Como lidar com uma base de usuários muito grande e distribuída? Como lidar com uma base de recursos distintos, numerosos e distribuídos? Como cuidar das políticas? É possível fazer uso de federações acadêmicas de identidade? É possível fazer uso de federações públicas de identidade (Facebook, Google etc.)? 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. 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 Arquitetura de Federação Fatiada (*Slice Federation Architecture* – SFA), que pode ser descrita como uma API para 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.

4.8 Autenticação/autorização em organizações virtuais (Profa. Débora Saade - UFF)

Ao longo dos últimos anos, acompanha-se um crescente interesse, principalmente no âmbito acadêmico, das soluções para criação de ambientes federados. Tais federações visam desde facilitar o ingresso de usuários até o compartilhamento de recursos entre as diversas entidades parceiras. Quando um conjunto compartilhado de recursos, oferecidos por diferentes instituições, devem ser compartilhados apenas por determinados membros dessas ou outras instituições, como por exemplo em um projeto interinstitucional, define-se uma organização virtual. Tais ambientes possuem requisitos particulares a cada instituição e também genéricos à organização virtual. Desta forma, é interessante permitir que funcionalidades comuns às organizações virtuais, e também às federações, envolvendo questões sobre autenticação e autorização (A&A), possam ser integradas facilmente a uma nova organização virtual por meio de uso de um framework de A&A. A criação e manutenção de organizações virtuais tem despertado o interesse de vários grupos de pesquisa e tem sido objeto de vários trabalhos. Entretanto, várias questões ainda permanecem em aberto e precisam de uma abordagem mais profunda, tais como o problema da agregação de atributos específicos da organização virtual e o problema da forma de combinar os atributos de um usuário a fim de se tomar a melhor decisão sobre conceder ou não uma determinada autorização. Outro desafio se refere à especificação de políticas para controle de acesso. Como uma organização virtual envolve diferentes instituições, é importante padronizar tipos de políticas que permitam o controle de acesso a recursos distribuídos e gerenciados por vários parceiros e, ao mesmo tempo, oferecer flexibilidade para que cada instituição tenha autonomia na definição de suas políticas de acesso. Outro desafio é a integração de sistemas legados de gestão de identidade e controle de acesso a novas organizações virtuais. Nesse cenário, as instituições já utilizam alguma mecanismo próprio de autenticação e autorização, que precisa ser modificado ou estendido para permitir sua integração a outras soluções utilizadas em outras instituições que participam da mesma organização virtual. É desejável que propostas de soluções para essas questões sejam genéricas e possam ser aplicadas a diferentes organizações virtuais, o que torna esses problemas mais desafiadores.

4.9 Infraestrutura de Autenticação e de Autorização para Web das Coisas (Profa. Michelle Wangham - Univali)

Apesar do termo “Internet das coisas” (ou Internet of things – IoT) estar se tornando cada vez mais comum, é possível considerar também uma teia das coisas (web of things – WoT), uma vez que também é muito comum encontrar protocolos e outras tecnologias web embarcadas em dispositivos diversos conectados à rede. Talvez o exemplo mais dominante hoje sejam os roteadores domésticos, mas a lista de exemplos está crescendo rapidamente. Os roteadores e outros equipamentos de rede profissionais também fazem uso maciço de tecnologia web a fim de facilitarem sua administração e configuração e isso os tem colocado no mesmo patamar de insegurança e vulnerabilidade de outros dispositivos. Dentre as maiores vulnerabilidades em WoT destaca-se a implementação insuficiente e/ou inadequada de processos de autenticação e autorização, o que traz a questão sobre se seria ou não adequado adotar técnicas de GId em WoT. Algumas soluções foram propostas na literatura, sendo umas baseadas em um modelo federado e outras em um modelo centrado no usuário. Para se

compreender melhor os pontos fortes e fracos de cada modelo neste contexto, é preciso aprofundar mais no assunto e fazer avaliações e comparações mais completas de cada um.

4.10 Estudos de impacto relativos a atualizações de versões de Shibboleth (Profa. Michelle Wangham – Univali)

Nos últimos dois anos a atualização da versão do Provedor de Identidade Shibboleth de v2 para v3 tem causado muitas discussões e forçado muitas organizações que adotam esta tecnologia em larga escala a se planejar cuidadosamente para viabilizar esta atualização com seus sistemas em pleno funcionamento e sem causar impactos nos seus usuários. Criar, testar e validar em laboratório formas mais simples e seguras de se fazer as atualizações (tando de IdPs como de SPs) quando surgirem é um trabalho de investigação que precisa de maior atenção visto o grande volume de trabalho, as incertezas e a ansiedade que a presente atualização trouxe para as organizações.

4.11 Perspectivas para A&A em Infraestruturas de Informação em Saúde (Prof. Gustavo Motta – UFPB)

A área da saúde é uma das que mais precisa e mais tem a ganhar com mecanismos eficientes de autenticação e autorização (A&A). Frequentemente se vê propostas de aplicação de técnicas de GId em saúde e há vários grupos de pesquisa atuando nesta área. Um campo que se destaca é o da telerradiologia, capacidade de obter imagem em um local e transmiti-la à distância, a fim de visualizá-la com propósito de diagnóstico ou consulta. Neste contexto há grandes demandas em autenticação e autorização, por exemplo, para aplicá-las no contexto do desenvolvimento e formação de redes sociais profissionais para a prática radiológica. Assim, é preciso investigar em mais profundidade a aplicabilidade de técnicas de A&A, tais como: gestão de identidades múltiplas por usuário; escalabilidade em tecnologias de gestão de identidade; autenticação e controle de acesso federado em aplicações não web e computação móvel; gestão de A&A em projetos interinstitucionais e organizações virtuais; desenvolvimento de aplicações usando infraestrutura de A&A provida pela RNP (ICPEdu , CAFe e RUTE); autenticação e controle de acesso baseado em atributos; novas abordagens de autenticação e autorização (p. ex. baseados em contexto, reputação etc.).

4.12 Uso de criptografia visual para autenticação (Prof. Ricardo Dahab - Unicamp)

Este tema trata de uma solução de autenticação mais robusta de usuários por servidores online baseado na técnica de Criptografia Visual (VC) que usa, além do dispositivo primário do usuário (PC, tablet, smartphone etc), um dispositivo-cliente (chamado aqui de DDA) munido de algum tipo de display gráfico de pequeno porte. A propriedade de interesse aqui é que a informação secreta associada à autenticação (algum tipo de senha) não é obtida por um processo computacional, mas pela leitura pelo olho humano da informação exibida na tela do DDA. Tal diferença permite que o sistema seja mais robusto que os baseados em métodos tradicionais, mesmo quando o dispositivo

primário do usuário se encontra comprometido por algum tipo de software malicioso, tornando-o um sistema adequado a autenticação em aplicações mais sensíveis. Alguns avanços já foram feitos nesta abordagem de autenticação por VC, mas vários pontos permanecem ainda em aberto e requerem pesquisas mais aprofundadas, tais como: a forma mais efetiva de se apresentar o segredo para o usuário; os custos envolvidos na solução; a necessidade de se usar equipamentos extras; a possibilidade de se aproveitar dispositivos já comuns no dia a dia dos usuários (como celulares ou smartcards, por exemplo); o volume de modificações necessárias em uma infraestrutura de autenticação existente para adotar a nova forma de autenticação e a relação custo/benefício da solução adotada.

4.13 Monitoramento e Otimização da Federação CAFe (Profa. Michele Nogueira – UFPR)

Diversos avanços têm sido feitos no contexto de gestão de identidades federadas, onde se destaca a federação CAFe como um exemplo de sucesso. Os sistemas de gestão de identidades federadas vêm ganhando cada vez mais a atenção e a importância no monitoramento e no controle de identidades digitais diante das transformações decorrentes de avanços tecnológicos, os quais possibilitam uma maior portabilidade e mobilidade dos dispositivos; uma miniaturização em direção à nanoescala; e uma maior escalabilidade dos sistemas. Apesar da importância crescente dos sistemas de gestão de identidades, pouca atenção vem sendo dada à necessidade de garantir a disponibilidade do serviço de provimento de identidades diante de falhas ocasionadas por eventos maliciosos ou não. Frente a eventos intensivos em carga de trabalho, como requisições legítimas ou maliciosas, os provedores de identidades de uma federação apresentam uma degradação no desempenho, provocando atrasos ou indisponibilidades de operações cruciais, como a autenticação e o controle de acesso. No entanto, frente a eventos que geram uma grande demanda de requisições legítimas ou maliciosas, os provedores de identidades de uma federação podem apresentar uma degradação no desempenho, provocando atrasos ou indisponibilidades de operações cruciais, como a autenticação e o controle de acesso. Na perspectiva de tornar esses provedores resilientes à presença de tais eventos, é necessário pesquisar e desenvolver mecanismos de monitoramento e otimização dos mesmos. Uma possível otimização seria empregar utilizar de forma oportunista provedores de identidades mais ociosos dentro de uma mesma federação para ajudar a equilibrar a carga da mesma da federação, agregando maior resiliência e diminuindo o tempo de resposta das operações prestadas. O monitoramento se faz necessário para identificar provedores sobrecarregados e ociosos e deve ser suportado por alguma das várias técnicas já existentes na literatura. Um bom mecanismo de monitoramento e otimização deve ser capaz de executar procedimentos em resposta a determinados comportamentos considerados críticos para o sistema de gestão de identidades. À medida em que mais instituições se filiam às federações de ensino e pesquisa (como a CAFe) e mais numerosos são os ataques a serviços e infraestruturas de TI, torna-se mais urgente o desenvolvimento destes mecanismos de resiliência e proteção aos componentes que formam a Federação CAFe. Algumas soluções têm sido propostas e implementadas, mas é preciso se aprofundar mais no assunto dado o aumento de complexidade e escalabilidade que se vê nas novas tecnologias e plataformas para federações. Além de aspectos relacionados à disponibilidade de operações cruciais, como autenticação e controle de acesso, em um contexto diante de eventos intensivos em carga de

trabalho, outros aspectos também são igualmente importantes e precisam ser tratados tais como a privacidade das identidades e confidencialidade dos dados dos usuários diante do compartilhamento desses dados pelos provedores de identidades de uma federação. Por este motivo este assunto deve fazer parte da pauta de iniciativas futuras em termos de prospecção, pesquisa e desenvolvimento.

4.14 Atributos: garantias de qualidade e privacidade (Profa. Noemi Rodriguez – UFF)

Nos últimos anos temos progredido bastante no uso de federações de identidade para autenticação de usuários. Muitos usuários já fazem acesso a 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. Uma forma relativamente simples de construir esquemas de autorização em uma federação é com a utilização de um modelo ABAC (attribute based access control). A organização de origem de um usuário normalmente tem condições de fornecer afirmações fidedignas a seu respeito, como por exemplo o tipo de vínculo do usuário com a organização (professor, estudante, funcionário) ou o curso no qual um estudante está matriculado. Um serviço qualquer pode utilizar tais informações para determinar direitos do usuário. Por exemplo, um serviço de vendas de ingresso pode utilizar a informação de vínculo para determinar a oferta de descontos que fará ao usuário, ou um serviço de computação distribuída pode utilizar o curso ao qual o estudante está vinculado para determinar cotas de uso. (Este esquema de autorização funciona para serviços onde o nível de autorização do usuário depende apenas de seu perfil em sua organização de origem; um outro caso bem diferente ocorre no escopo de organizações virtuais, que são discutidas em outro ponto desse texto). Para que este esquema ABAC de autorização funcione em uma federação, precisamos resolver algumas questões. A primeira diz respeito à qualidade da informação provida. Um serviço só poderá contar com esse mecanismo de autorização se tiver garantias sobre os dados fornecidos pelos provedores de identidade da federação. Isso nos remete à questão de níveis de garantia, sobre a qual ainda não nos debruçamos. Uma outra questão diz respeito à privacidade do usuário. Tipicamente não nos preocupamos com o acesso alheio a nossos dados, mas antes de propor que dados de boa qualidade sejam divulgados para serviços arbitrários sem maior controle, precisamos 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, num futuro próximo é preciso enfrentar a questão da garantia da qualidade dos dados fornecidos, problema que aumenta com o aumento do número de instituições participantes, sem contudo abrir mão de proteger tanto quanto possível a privacidade do usuário.

4.15 Os serviços de GId da RNP

A RNP colocou no dia a dia dos pesquisadores uma série de serviços inovadores e de grande valor agregado na área de GId, tais como a Infraestrutura de Chaves Públicas de Ensino e Pesquisa (ICPEdu), a federação CAFe (Comunidades Acadêmicas Federadas) e o sistema de autenticação global em redes WiFi Eduroam. Há vários anos estes serviços têm sido amplamente divulgados e oferecidos às instituições de ensino e pesquisa brasileiras e a adesão cresce dia a dia, à medida que

os usuários vão descobrindo as vantagens proporcionadas pelos mesmos.

Em relação ao serviço de certificação digital ICPEdu, vimos uma radical transformação no mesmo que objetivou facilitar a adesão mais rápida e transparente por parte das instituições. Dentre as mudanças se destacou a separação da forma de emissão de certificados digitais para serviços (servidores web, SSH etc) e para pessoas.

No primeiro caso constatamos uma melhoria significativa não só na emissão dos certificados de serviços, como também uma melhoria no conteúdo destes certificados, já que eles passaram a ser assinados pela Autoridade Certificadora Internacional Globalsign e a ser reconhecidos pelos principais navegadores (browsers) do mercado sem alertas de segurança como ocorria anteriormente.

Já no segundo caso, constatamos uma certa frustração dos que se envolveram com a questão de certificados digitais pessoais para toda a comunidade de ensino e pesquisa, uma vez que os novos serviços deste tipo anunciados por diversas vezes pela RNP não se concretizaram até hoje, mesmo tendo se passado mais de dois anos desde que a reforma do ICPEdu foi anunciada. Como resultado desta demora, vimos algumas instituições abandonando algumas ideias de implantar certificação digital em larga escala e adotando, mesmo onde não era necessário um valor oficial e jurídico, o certificado pessoal da ICP-Brasil. Em várias oportunidades, ajudamos na divulgação deste novo modelo de certificação pessoal maciça e de baixo custo, mas percebemos hoje que as pessoas já não estão mais acreditando que um dia este serviço chegará até elas.

Portanto, com o objetivo de não perdermos o enorme esforço que já foi feito até hoje no sentido de se colocar uma infraestrutura de chaves públicas de boa qualidade e de baixo custo à disposição das instituições de ensino e pesquisa, entendemos ser de grande importância que a RNP priorize o início do serviço de emissão de certificados pessoais, sob pena de se perder uma janela de oportunidades e de se perder a confiança das pessoas de que algum dia este serviço será disponibilizado. Se todo o esforço feito até aqui no ICPEdu, não só pela RNP, mas também por uma boa parcela da comunidade acadêmica, for perdido ou se o serviço continuar na atual indefinição, acreditamos que nesta área a RNP poderá ter dificuldades no futuro para conseguir arregimentar um grupo motivado e comprometido de colaboradores fora de seus quadros técnicos como conseguiu durante todo este projeto. O potencial dos certificados pessoais é muito grande e certamente a RNP irá colher muitos frutos dos investimentos feitos até aqui com a ampla disseminação desta tecnologia de GId pelas instituições de ensino e pesquisa nacionais.

4.16 Algumas visões no exterior

Por meio do acompanhamento de listas de discussão e de documentos publicados na web na área de gestão de identidades, é possível obter uma ideia sobre os principais desafios que estão na pauta de discussões de pesquisadores e instituições em várias partes do mundo. Citaremos a seguir alguns destes desafios na área de organizações virtuais.

Desafios relacionados a Organizações Virtuais

As Organizações Virtuais (VOs) são um forte exemplo de uso de federação de identidade. A associação entre várias pessoas (identidades) sob uma VO é orientada mais pelo objetivo comum

entre elas do que por fronteiras de instituições ou países. É cada vez mais forte o incentivo da academia e de agências de fomento em relação à colaboração entre pesquisadores e as redes nacionais de apoio à pesquisa e ensino (NRENs como a RNP, por exemplo) têm se esforçado para prover recursos básicos que facilitem esta colaboração e não exijam a replicação de recursos computacionais e de credenciais, provendo assim uma federação de identidades.

Federated Identity Management for Researchers (FIM4R) é um dos grupos que têm atuado fortemente na elaboração de documentos sobre requisitos e formas de uso de identidades digitais e federações. Um desses documentos é um *white paper* publicado em 2012 (https://cdsweb.cern.ch/record/1442597) e intitulado "Federated Identity Management for Research Collaborations". O artigo descreve as necessidades da comunidade de pesquisa no tocante a autenticação federada, o estado atual das atividades em gerenciamento de identidades federadas (FIM) e destaca alguns casos de uso específicos. É ainda apresentada uma visão de FIM através desta comunidade, os estágios principais de um *roadmap* e um conjunto de recomendações para garantir a implementação do mesmo.

No mesmo ano de 2012, GÉANT (rede pan-européia de pesquisa e educação que interconecta as NRENs da Europa, anteriormente conhecida por TERENA) publicou um outro artigo (Advancing Technologies and Federated Communities – https://www.terena.org/publications/files/2012-AAA-Study-report-final.pdf) com um outro conjunto de recomendações similares às do FIM4R. Neste artigo, a rede GÉANT tratou de questões legais, tecnologia, políticas e financiamento e deu destaque especial para os seguintes pontos: tecnologias de federação são peças-chave a serem melhor aproveitadas pelas redes nacionais com o aprimoramento de suas infraestruturas; os atuais modelos de autenticação e autorização não podem ser escalados mais do que já foram; federação de identidades não é algo trivial e é preciso um esforço conjunto de NRENs, órgãos de financiamento, universidades e órgãos jurídicos para se buscar uma federação de identidades mais eficiente, fácil de implementar e de usar.

Em um recente artigo (22 de outubro de 2015 – Ongoing Challenges in the VO Space – https://wiki.refeds.org/display/GROUP/Ongoing+Challenges+in+the+VO+Space) a pesquisadora do grupo REFEDS (Research and Education FEDerations group), Heather Flanagan, destaca que não houve muito progresso nestes últimos três anos e que muitas das recomendações ainda esperam para serem implementadas. Ela considera que a liberação de atributos é um ponto fundamental para a ampla adoção de federação de identidades, mas nota que uma série de dúvidas sobre como proteger a segurança e a integridade dos dados por parte dos responsáveis pelos dados dos usuários em universidades e outras instituições de pesquisa tem dificultado o avanço desta liberação. Neste mesmo artigo, a autora aponta os progressos alcançados desde 2012:

- criação de categorias de entidades como a categoria Research & Scholarship (R&S) pelo REFEDS: trata-se de uma iniciativa de peso, mas que ainda tem um longo caminho até ser amplamente adotada pela comunidade já que neste primeiro ano só obteve a adesão de 43 dentre os 1440 IdPs (Provedores de Identidade) que fazem parte do serviço interfederações eduGAIN;
- Código de Conduta para Proteção de Dados: este documento (disponível em https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home) busca

dar mais suporte à questão de confiança nos dados, bem como definir melhor os limites de responsabilidade de cada participante da federação. É um documento mais voltado para a realidade europeia, já que é baseado na Diretiva Europeia de Proteção de Dados (EU Data Protection Directive), mas pode ser usado como base por provedores de serviço (SPs) em outras regiões para aumentar a confiança sobre como as informações devem ser tratadas por estes provedores. Também é uma iniciativa com um longo caminho a percorrer, dado que até agora, apenas 69 dos 991 SPs do eduGAIN aderiram a este Código de Conduta;

- Autenticação e Autorização para Pesquisa e Colaboração (AARC- https://aarc-project.eu): trata-se de um projeto plurianual iniciado em 2015 e financiado pela Comunidade Europeia com o objetivo de desenvolver e amadurecer a infraestrutura de TIC requerida pela comunidade acadêmica e de pesquisa na Europa no tocante a federação de identidades e evitar o surgimento de diferentes e incompatíveis infraestruturas para colaboração entre os pesquisadores que venham a operar de forma independente. O projeto ainda se encontra em seus estágios iniciais, nos quais está levantando todas as ferramentas já existentes e que possam ser aprimoradas e integradas em uma infraestrutura única e comum a todos, sem desenvolver novas ferramentas onde não for necessário;

- CILogon 2.0 - An Integrated Identity and Access Management Platform for Science (http://www.nsf.gov/awardsearch/showAward?AWD_ID=1547268): projeto de três anos financiado pela National Science Foundation (USA) com início previsto para janeiro/2016, tem como objetivo agregar os projetos CILogon e COmanage para prover um serviço integrado de gestão de identidades e controle de acesso. Este projeto deverá atender as demandas de pesquisadores relativas a formação dinâmica de grupos de colaboração através de instituições e até de países, compartilhando acesso a dados, instrumentos, clusters computacionais e demais recursos necessários para suporte às pesquisas. Não está claro o quão compatível o mesmo será com as federações que participam atualmente do eduGAIN, mas certamente deverão haver resultados neste projeto que merecem uma atenção por parte das NRENs.

Além destes avanços, a autora também destaca alguns obstáculos que tornam a criação de VOs um desafio maior. Um destes obstáculos é a questão legal, uma vez que VOs não são entidades formais e portanto não podem assinar contratos, convênios e acordos. Outra dificuldade é a carência que VOs têm de pessoal técnico suficientemente qualificado para configurar e disponibilizar as (ainda) sofisticadas ferramentas necessárias para criação e administração de tal tipo de organização. Enquanto não forem criadas e disponibilizadas ferramentas simples para a comunidade de pesquisa, esta não irá conseguir se organizar em VOs e as vantagens deste tipo de tecnologia permanecerão não aproveitadas.

Como sugestões para promover projetos de VOs são apontados os seguintes itens:

- tornar as tecnologias mais simples de implementar e de usar: iniciativas como o AARC mencionado acima ou o projeto TIER – Trust and Identity in Education and Research (http://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/) na Internet2 (USA) têm este objetivo de facilitar a adoção das tecnologias necessárias para implementação de federações e de VOs, devendo, portanto, ser acompanhadas mais de

perto;

- aprimorar a segurança em federações: segurança tem sido uma das preocupações em federações, já que uma instituição precisa confiar nas informações providas por outras e saber de imediato quando houve algum comprometimento das informações. Mesmo que algumas instituições tenham times de resposta a incidentes de segurança, é preciso trabalhar mais no sentido de compartilhar de forma mais eficiente estas informações sobre incidentes. Uma iniciativa neste sentido é a SIRTFI – Security Incidents Response Trust Framework for Federated Identity (https://wiki.refeds.org/display/GROUPS/SIRTFI), que está buscando propor formas de acordo entre instituições que facilitem a troca de informações relacionadas a segurança.

Outras visões sobre VOs , atributos e provedores de identidade

Não há um consenso entre os pesquisadores sobre como, onde e quando liberar os atributos necessários para a criação de uma organização virtual (VO). Acompanhando discussões recentes em uma lista de emails encontramos argumentos que apontam fortemente contra a liberação de atributos por provedores de identidades (IdP). Tais argumentos vão na linha de que os IdPs não sabem, a princípio, que atributos devem ser liberados para cada VO. Além disso, os administradores dos IdPs não irão concordar em dar poderes aos controladores dos VOs para que eles configurem os IdPs na parte de liberação de atributos. Nesta linha de raciocínio, acredita-se então que será necessário criar um serviço de VOs que permita aos gerentes destas VOs atribuir os atributos necessários aos seus usuários e que serão necessárias ferramentas de fácil uso que permitam integrar de forma simples e transparente estes recém-atribuídos atributos à infraestrutura de federação de identidades existente. Desta forma, liberação de atributos pelos IdPs, um dos grandes problemas de VOs, deixa de ser necessária, sendo substituída pela atribuição pelas próprias Vos.

A Terena Networking Conference (TNC) oferece ótimas oportunidades para conhecermos mais de perto estes e outros desafios na área de gestão de identidades. Infelizmente não foi viável participarmos da TNC em 2015, mas identificamos um vídeo de treinamento sobre liberação de atributos que é muito interessante e pode ser de grande utilidade para a RNP e para o CT-GId. Mais detalhes estão disponíveis em https://wiki.edugain.org/AttributeReleaseTraining2015 .

Um ponto fundamental para a implantação de VOs é a disponibilidade de ferramentas adequadas. Nesta linha, uma proposta interessante é conhecida por VOOT, ou Virtual Organization Orthogonal Technology, que consiste em um protocolo para troca de informações entre grupos externos a uma ou mais instituições. Trata-se de um trabalho conjunto da SURFNet, Uninett, SUnet e Renater que estão trabalhando na especificação e implementação da versão VOOT 1. O foco de VOOT é em contextos inter-federações, com colaboradores provenientes de diferentes federações. Entretanto, VOOT não se sobrepõe ou tem conflitos com federações de identidades. Ela não requer autenticação federada, apesar de poder usufruir da mesma. Alguns testes já foram feitos com uma prova de conceito e mais detalhes podem ser conhecidos nos slides de Maarten Kremers, disponíveis em https://events.nordu.net/plugins/servlet/conference-attachment/talks/47/162. Há pelo menos dois projetos de aplicação concreta desta tecnologia disponíveis no Github:

- Conector VOOT para Grouper: parte da distiribuição oficial de Grouper e disponível em

https://github.com/Internet2/grouper/tree/master/grouper-misc/grouper-voot ;

- Plugin de inscrição Moodle para VOOT: este é um projeto-piloto bem simples para fins de demonstração e não tem usuários ou suporte por trás dele. Está disponível em https://github.com/ConsortiumGARR/moodle-enrol_voot .

Resoluções de ano novo do REFEDS

O grupo de federações de ensino e pesquisa (REFEDS – Research and Education Federations Group) objetiva articular e satisfazer os requisitos mútuos entre federações do mundo todo. É composto por vários grupos de trabalho e está muito ativo na área de gestão de identidades. O grupo faz uma sugestão para as federações de lista de "Resoluções de Ano Novo para 2016" e achamos interessante compartilhá-la aqui com todos, uma vez que ela mostra que pontos são prioritários em uma visão de larga escala.

1. Implementar a categoria de entidades Research & Scholarship (R&S)
2. Atualizar todo o software de federação
3. Deixar de usar o SAML 1
4. Entrar para o eduGAIN
5. Aprimorar o processo de Discovery
6. Usar um Código de Conduta

Autenticação com segundo fator universal (U2F)

U2F é um padrão de autenticação aberto que permite aos usuários acessar serviços online com um dispositivo USB e sem requerer nenhum software adicional além de um navegador compatível (Chrome atualmente). Trata-se de um padrão criado pelas empresas Google, Yubico e NXP e que se encontra hoje encampado pelo consórcio de indústrias para autenticação aberta chamado FIDO Alliance. Foi lançado em 2014 com suporte para contas Google, mas já evoluiu desde então e desde junho de 2015 oferece suporte também para dispositivos móveis e para novos protocolos de comunicação (NFC, por exemplo). Hoje é suportado também por Dropbox, Facebook e Laboratório CERN. Explicando de forma resumida, U2F se baseia no uso de um dispositivo USB que possui um token criptográfico baseado em criptografia de chaves públicas, o qual precisa estar conectado ao dispositivo do cliente para que seja usado como um segundo fator de autenticação. Além de servir para autenticação, as novas versões deste token estão suportando também assinatura digital e criptografia de arquivos, e-mails e discos. Os dispositivos estão sendo vendidos por empresas como Yubico (Yubikey custando a partir de USD40) e Nitrokey (a partir de 19 euros), que está propondo uma especificação de hardware aberto.

Acreditamos que esta iniciativa deve ser acompanhada de perto pelo CT-GId para ver como evolui e quais seriam as possibilidades de vir a ser adotada nas instituições participantes da federação CAFe. Uma forma de experimentar com facilidade estas tecnologias envolvidas com U2F é usar um Gluu Server, um pacote de componentes de software livre (free open source) para gerenciamento de identidades e controle de acesso (www.gluu.org).

5. Conclusões

Como pode ser depreendido deste documento, existem muito 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 feitos aqui, sabe que pode contar com