Adoção de modelo controle acesso baseado em atributos em sistema de votação online para ofertá-lo como um serviço de TIC federado

Shirlei Aparecida de Chaves , Emerson Ribeiro de Mello

Instituto Federal de Santa Catarina – SC –Brasil

{shirlei.chaves, mello}@ifsc.edu.br

Resumo. *Na Comunidade Acadêmica Federada (CAFe) a ampla maioria das instituições clientes atua somente como provedor de identidade e consome serviços providos pela Rede Nacional de Ensino e Pesquisa ou de outras federações que a CAFe possui acordo de colaboração. Este trabalho apresenta os pontos que precisaram ser considerados para ofertar o sistema de votação online Helios como um serviço federado. Nesse texto é apresentado como o serviço foi modelado para ter uma dependência mínima do departamento de TI, fator essencial para operar em ambientes de larga escala, como é o caso da CAFe. Espera-se que esse trabalho possa estimular outras instituições a ofertarem serviços na federação.*

Abstract. *Most client institutions of the Federated Academic Community (CAFe) participate just as Identity Providers, consuming services provided by the National Network of Research and Education or by another federation in collaboration agreement with CAFe. This paper presents the main considerations to offer the on-line voting system Helios as a federated service. It also presents how the offering was designed in order to have a minimum dependency on the IT Department. That minimum dependency is crucial to operate in large scale environments like CAFe. It is hoped that this paper stimulates other institutions to offer federated services in CAFe.*

1. Introdução

Nas instituições de ensino superior são realizados diversos processos eleitorais, como para escolha de membros do conselho universitário (ou conselho superior) e colegiados, centro acadêmico, coordenadores de áreas administrativas, diretores de campus (ou centro) e para reitor. Segundo [Chaves and de Mello 2014], no período de 2013 a 2014, a maioria das instituições federais de ensino fez uso de cédulas de papel no processo de escolha dos membros de seus conselhos universitários.

O fato de algumas instituições serem multi campi ou ainda possuírem polos de ensino à distância em cidades que não possuem campus, faz com que a condução de alguns desses pleitos com cédulas de papel possa ser uma atividade complexa ou mesmo custosa, do ponto de vista financeiro. Em alguns casos, os próprios discentes são os responsáveis por organizar os processos de escolha de seus representantes, o que torna a atividade ainda mais desafiadora.

Sistemas de votação online permitem aos eleitores votarem a partir de dispositivos conectados à Internet, sendo este o principal atrativo para instituições de ensino na condução da maioria de seus processos de escolha. Segundo [Chaves and de Mello 2014], o sistema Helios [Adida 2008] se mostrou como o mais adequado e seguro, e vem sendo usado em algumas eleições no Instituto Federal de Santa Catarina desde 2014 e em outras instituições de ensino [Adida et al. 2009].

No sistema de votação online Helios [Adida 2008] não é permitido o voto anônimo, ou seja, todo eleitor só poderá depositar uma cédula na urna após passar por um processo de autenticação. A versão original do Helios, e que também é oferecida como serviço[1] na nuvem (*Software as a Service* – SaaS), permite criar **eleições fechadas** ou **eleições abertas**. Na eleição fechada a lista de eleitores é carregada previamente através de um arquivo CSV com os seguintes campos: login, nome completo, e-mail. Neste caso, os eleitores receberão suas credenciais de acesso (login e senha) por e-mail. Nas eleições abertas, qualquer um que possua conta de usuário nos serviços Google, Facebook ou Yahoo estará apto a votar, ou seja, a lista de eleitores não é carregada previamente.

O formato de eleições fechadas, com eleitores carregados a partir de um arquivo CSV, tem como vantagem o fato de garantir que somente aquelas pessoas poderão depositar um voto na referida eleição. Porém, o fato da senha ser enviada em claro por e-mail pode gerar as seguintes preocupações: (1) a pessoalidade do voto, pois se alguém interceptar o e-mail ou tiver acesso a caixa postal do eleitor, poderia se passar por ele; (2) a garantia de entrega dos e-mails com as credenciais de acesso. A qualidade da lista de eleitores pode não ser boa ao ponto de conter endereços de e-mail que não são mais usados pelos eleitores; ou o e-mail enviado pelo Helios poderia ser barrado por sistemas anti-SPAM.

As eleições abertas têm como principal vantagem o fato das credenciais não serem enviadas por e-mail, evitando assim as preocupações apontadas para as eleições fechadas. Porém, a versão original do Helios não permite restringir a lista de eleitores, ou seja, poderá votar qualquer pessoa que tenha acesso ao endereço da eleição e que possua uma conta no Google, Yahoo ou Facebook, algo nada desejado para as eleições dentro das instituições de ensino.

Em [Chaves and de Mello 2014] foi desenvolvido um módulo de autenticação LDAP [Wahl et al. 1997] para o Helios, permitindo assim criar eleições abertas de forma que somente usuários presentes na base LDAP da instituição estariam aptos a votar. Ou seja, tem-se aqui os benefícios da eleição fechada, pois somente um determinado grupo de pessoas poderia votar, e também os benefícios da eleição aberta, pois as credenciais de acesso não são enviadas em claro por e-mail. Porém, tem-se como requisito garantir que a base LDAP usada pelo Helios só contenha pessoas que realmente deveriam ter direito a voto.

Por exemplo, o conselho superior nos Institutos Federais (ou conselho universitário nas Universidades) é composto por representantes dos segmentos discente, docente e técnico administrativo, os quais são escolhidos por seus pares através de uma eleição. Considerando que a instituição possui uma única base central de usuários (base LDAP), então para fazer uso do Helios com eleições abertas e autenticação no LDAP, seria ne-

[1] https://vote.heliosvoting.org

cessário montar o seguinte ambiente:

- Criar três réplicas da base LDAP da instituição, uma para cada segmento (discente, docente e técnico-administrativo);
- Para cada réplica, manter os usuários que forem considerados como eleitores aptos para aquele segmento e excluir todos os demais usuários;
- Criar três instâncias distintas do serviço Helios, sendo que cada uma faria uso de uma das réplicas da base LDAP;
- Criar uma eleição aberta em cada uma das instâncias e divulgar o endereço da eleição para os eleitores.

Montar o ambiente descrito acima não é uma tarefa trivial e precisaria ser feito para cada processo eleitoral, uma vez que a lista de eleitores pode sofrer alteração. Esta é uma atividade exclusiva do Departamento de Tecnologia da Informação (TI) e se considerar o fato que poderiam acontecer vários processos de escolha ao longo de um ano, sendo que alguns de forma concomitante, então isto poderia resultar em uma sobrecarga do departamento de TI.

Este trabalho apresenta as modificações que foram realizadas no sistema de votação online Helios para que o mesmo pudesse ser ofertado como um serviço na Comunidade Acadêmica Federada (CAFe) da Rede Nacional de Ensino e Pesquisa (RNP), ou seja, um serviço de Tecnologia da Informação e Comunicação (TIC) que permita a condução dos processos eleitorais para qualquer uma das instituições usuárias da CAFe e com um mínimo de dependência do departamento de TI, requisito este fundamental para operar em ambientes de larga escala.

O artigo está organizado da seguinte forma. Na Seção 2 é apresentada a abordagem adotada para ofertar o Helios como um serviço federado. A Seção 3 apresenta o ambiente de desenvolvimento que foi usado neste trabalho. Na Seção 4 são apresentados os trabalhos relacionados. Por fim, a Seção 5 apresenta as conclusões e trabalhos futuros.

2. Oferta do sistema Helios como serviço federado

Assim como as principais federações acadêmicas no mundo, como a Internet2 (EUA), Janet (Reino Unido), Switch (Suiça) e Renater (França), a Comunidade Acadêmica Federada (CAFe) também está fundamentada sobre o *framework* Shibboleth [Shibboleth 2005].

Para que uma aplicação possa ser ofertada em uma federação Shibboleth, o principal requisito é a capacidade de consumir asserções SAML [OASIS 2008], as quais são entregues para a aplicação de forma transparente (como atributos de sessão HTTP), através do módulo Shibboleth, para o servidor web Apache HTTP, ou pela aplicação SimpleSAMLPHP[2], por exemplo. O Helios foi desenvolvido na linguagem Python com o *framework* Django e assim a forma mais simples de consumir asserções SAML seria hospedá-lo em servidor Apache HTTP com módulo Shibboleth, opção que foi escolhida para este trabalho.

Na versão original do Helios é possível autenticar usuários (administradores ou eleitores) em uma base local ou, através do protocolo OAUTH [Hardt 2012], nos serviços

[2]https://simplesamlphp.org

Google, Facebook ou Yahoo. No trabalho de [Chaves and de Mello 2014] o módulo de autenticação do Helios foi estendido para permitir autenticar usuários a partir de uma base LDAP. Esta mesma abordagem, de extensão do módulo de autenticação do Helios, foi utilizada no presente trabalho, para permitir a autenticação de usuários através do consumo de asserções SAML. Com o módulo de autenticação Shibboleth é possível autenticar administradores, pessoas com privilégios para criar eleições, bem como eleitores para qualquer eleição aberta (Ver Seção 1).

Para usufruir do serviço Helios federado, seja para votar ou para criar eleições, é necessário que o provedor de identidade (IdP) forneça os seguintes atributos de seus usuários: inetOrgPerson-cn, inetOrgPerson-mail e Identity-Provider. Os inetOrgPerson-cn e inetOrgPerson-mail são utilizados no primeiro acesso para a criação de um usuário padrão do Helios, o qual inicialmente não possui privilégios para criar eleições. O atributo Identity-Provider é usado para correlacionar os usuários de uma mesma instituição. Por exemplo, só poderão votar em uma eleição criada por um usuário da instituição X as pessoas que também forem oriundas dessa mesma instituição (Ver Subseção 2.2).

Todavia, a oferta de um sistema de votação online federado como um serviço de TIC, com uma dependência mínima do departamento de TI, 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? As respostas para essas perguntas são apresentadas nas subseções a seguir.

2.1. Perfis de usuários

Na página oficial do Helios, na qual ele é ofertado na modalidade SaaS, qualquer pessoa com conta de usuário Google, Facebook ou Yahoo pode criar eleições abertas ou fechadas. O objetivo deste trabalho está em ofertar um sistema de votação online para instituições de uma federação acadêmica, sendo assim poderia não ser adequado que qualquer pessoa da instituição pudesse criar eleições.

Por exemplo, imagine-se que uma pessoa, nomeada pela instituição como presidente de uma comissão eleitoral, crie uma eleição no sistema Helios e faça uso do e-mail para enviar a URL desta eleição para os eleitores aptos. Uma outra pessoa, mal intencionada, poderia criar uma eleição semelhante e, fazendo uso de técnicas de *phishing* por e-mail, poderia enganar alguns eleitores de forma que estes acessariam a URL da eleição falsa, depositando incorretamente seus votos. Isso poderia ser suficiente para gerar descrédito sobre a solução online e invalidar a eleição.

Na versão original do Helios, o administrador do serviço pode cadastrar manualmente quais usuários locais terão permissão para criar eleições. Essa funcionalidade seria suficiente para sanar as preocupações apontadas acima, contudo não seria adequada para ambientes de larga escala, como uma federação acadêmica. Atualmente a federação CAFe possui aproximadamente 100 instituições usuárias atuando como provedores de identidade. Se um usuário de qualquer uma dessas instituições quisesse usar o Helios para criar eleições, este precisaria entrar em contato com o administrador do serviço e solicitar o direito para tal. Aqui dois problemas se apresentariam para o administrador

do serviço: (1) este poderia receber um número grande e constante de pedidos para delegar ou revogar o direito de criar eleições; (2) este não teria o discernimento necessário para determinar quais pessoas estariam autorizadas a criar eleições para uma determinada instituição.

Com o intuito de garantir a escalabilidade do serviço, foi proposto um conjunto de papéis e direitos, os quais podem ser observados no diagrama de caso de uso UML da Figura 1. Por padrão, todos os usuários da federação possuem o papel **eleitor**, o qual permite ao usuário participar das eleições que este for considerado apto (Veja Subseção 2.2). O papel **gestor de eleição** dá ao usuário o direito de administrar eleições (criar, fechar, etc.). O papel **gestor da instituição**, além dos direitos do gestor da eleição, dá ao usuário o direito de delegar ou revogar os papéis de gestor de eleição ou de gestor da instituição para os demais usuários de sua instituição de origem. O papel **superadmin** é atribuído somente para um usuário local do serviço, o que lhe permite delegar ou revogar o papel de gestor da instituição para outros usuários da federação, bem como cadastrar informações de contatos das instituições.

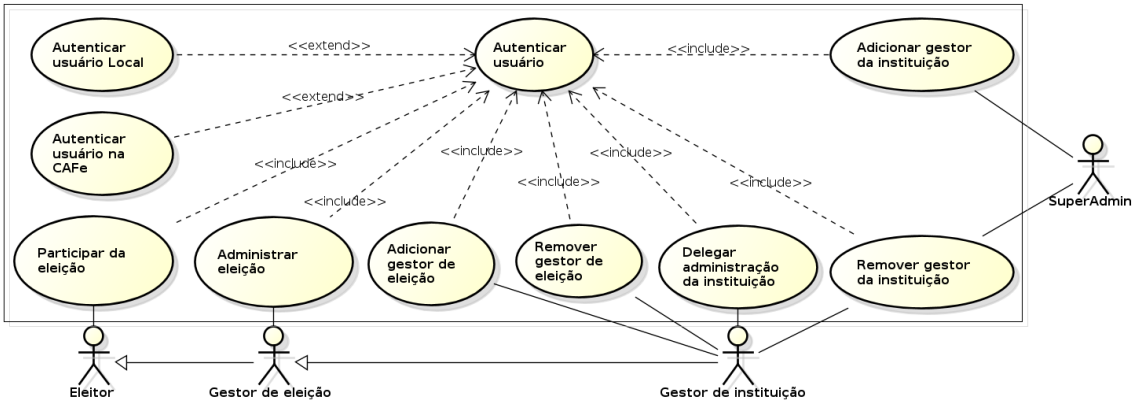


Figura 1. Diagrama de Casos de Uso com os papéis de usuários propostos

Para a oferta deste serviço na federação, a abordagem considerada é a de que a instituição de origem deve fazer um pedido de adesão, como é o caso de muitos serviços da eduGain[3]. A instituição interessada, por meio de sua autoridade máxima, deve encaminhar ao administrador do serviço o formulário de adesão onde indica a pessoa responsável para atuar como o gestor da instituição. Este procedimento garante que o administrador do serviço terá que tratar um único pedido por instituição e este terá garantias de que a pessoa foi autorizada oficialmente pela instituição, evitando assim as preocupações apontadas no início desta seção.

Uma vez autenticado no serviço, qualquer usuário terá acesso às informações de contato (nome, telefone e e-mail) dos gestores de sua instituição. Isso permite que aqueles que desejarem criar eleições saibam com quais pessoas precisarão interagir dentro de sua instituição para solicitar tal direito. O gestor da instituição poderá a qualquer momento delegar ou revogar os papéis de gestor de instituição ou gestor de eleição (Veja Figura 2). Sendo assim, não há mais a necessidade de interação com o administrador do serviço, atendendo o requisito inicial da oferta de um serviço de TIC que exija o mínimo

[3]http://services.geant.net/edugain

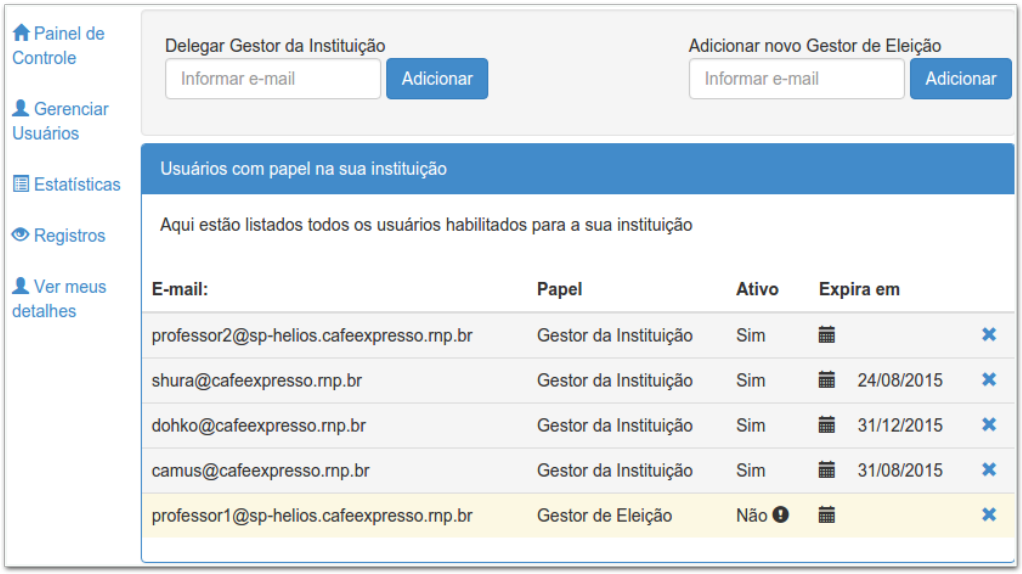


Figura 2. Interface de administração de usuários de uma instituição

de administração por parte do departamento de TI, responsável pelo serviço Helios federado.

Optou-se pelo modelo de controle de acesso baseado em papéis (*Role Based Access Control* – RBAC) para o cadastro de gestores de eleição e instituição, tendo em vista que o modelo baseado em atributos (*Attribute Based Access Control* – ABAC), apesar de atender melhor as questões de dinamicidade e escalabilidade, aumentaria a complexidade para os administradores de provedores de identidade. Com o modelo ABAC, os provedores de identidade teriam que manter em sua base de usuários atributos que indicassem os gestores de eleição ou da instituição, os quais são exigidos pelo provedor de serviço do Helios.

2.2. Consumo de atributos fornecidos pelo IdP

Como visto na Seção 1, ao criar uma eleição é necessário indicar a lista de eleitores aptos. Se for uma eleição fechada, a lista deve ser carregada por meio de arquivo CSV, porém o ponto fraco neste caso é que as credenciais são enviadas em claro por e-mail para os eleitores. Se for uma eleição aberta com autenticação LDAP (ou OAUTH), a vantagem está no fato de que as credenciais não precisam ser enviadas aos eleitores, porém qualquer usuário da base LDAP (ou com contas Google, Facebook ou Yahoo), estará apto a votar.

Neste trabalho foi criada a opção de montar a lista de eleitores através do consumo dos atributos que são fornecidos pelo IdP. Dessa forma, tem-se os benefícios de uma eleição fechada, mas sem a necessidade de se enviar as credenciais de acesso por e-mail para os eleitores. A tela de configuração da lista de eleitores é apresentada na Figura 3.

No exemplo da Figura 3, está sendo criada uma eleição para escolha dos membros discentes do conselho superior e assim, só poderão votar nessa eleição as pessoas que possuírem o atributo “brEduAffilationType” com o valor igual a “student”, e que pertencerem a mesma instituição da pessoa que está criando a referida eleição.

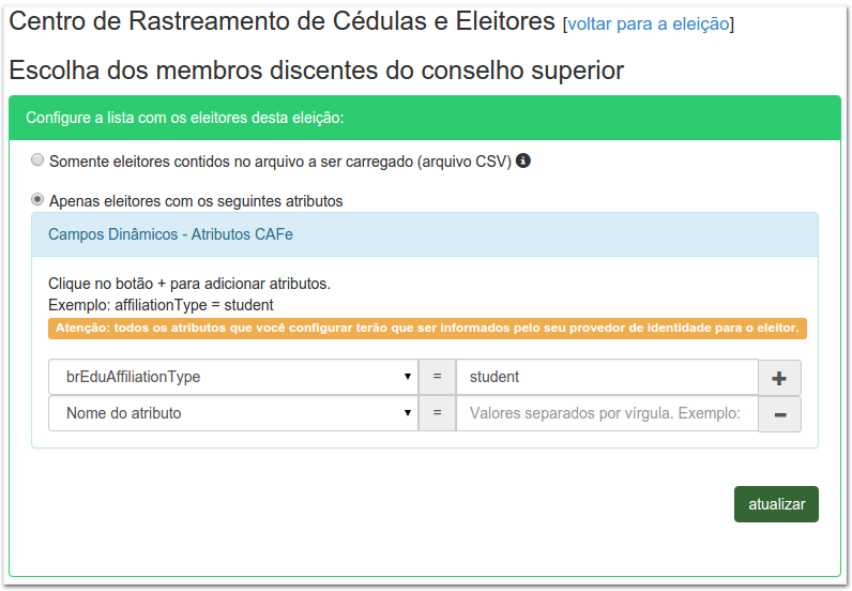


Figura 3. Consumo de atributos Shibboleth para montar lista de eleitores

A federação CAFe apresenta uma lista de atributos[4] obrigatórios e opcionais, bem como seus possíveis valores, porém ainda é possível que o IdP libere um conjunto maior de atributos ao provedor de serviço do Helios. Por exemplo, o IdP poderia fornecer o nome do curso e o campus onde o aluno está matriculado, o departamento onde o professor está lotado, etc. Cabe frisar que compete somente ao administrador do IdP indicar quais atributos irá liberar para o Helios e este o fará de acordo com as necessidades e interesses de sua instituição no uso do Helios para atender seus pleitos.

2.3. Página inicial com a lista de eleições em andamento ou encerradas

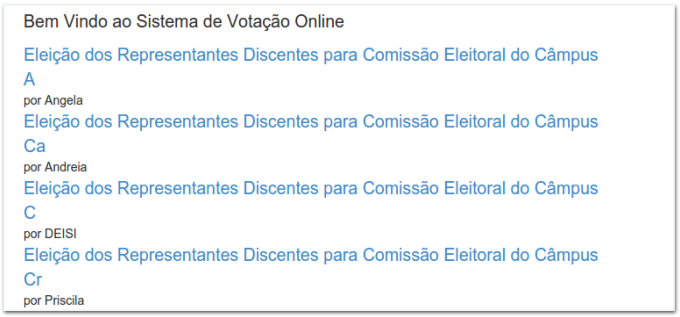
Em um cenário onde o Helios fosse usado somente por uma única instituição, a versão original do projeto pode ser considerada adequada. Ao criar uma eleição é possível indicar se a mesma deve aparecer na página inicial do Helios ou não. A motivação para deixar uma eleição publicada na página inicial está no fato de facilitar o acesso às eleições que estão em andamento ou mesmo eleições que já foram encerradas. Caso a eleição não esteja publicada nesta página, só será possível acessar a página de uma eleição se a URL da mesma for conhecida.

Este comportamento não seria adequado para um serviço em uma federação, pois a médio prazo essa página listaria muitas eleições, de diferentes instituições, e seria difícil para o interessado encontrar a eleição que deseja acessar (Ver Figura 4(a)). Neste trabalho a página pública foi remodelada de forma a apresentar inicialmente a lista de instituições que aderiram ao serviço (Ver Figura 4(b)), bem como o total de eleições que estão em andamento e eleições finalizadas por ano, por instituição. Na Figura 4(c) é apresentada a lista de eleições que foram finalizadas na instituição hipotética, chamada CAFe Expresso.

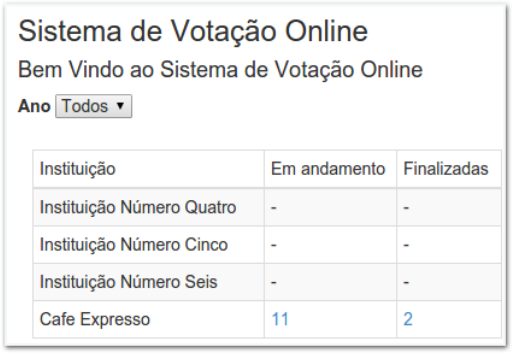
3. Ambiente de desenvolvimento e experimentos

A grande dificuldade para desenvolver um serviço federado está na necessidade de preparar o ambiente de desenvolvimento nos mesmos moldes de uma federação real. Preparar

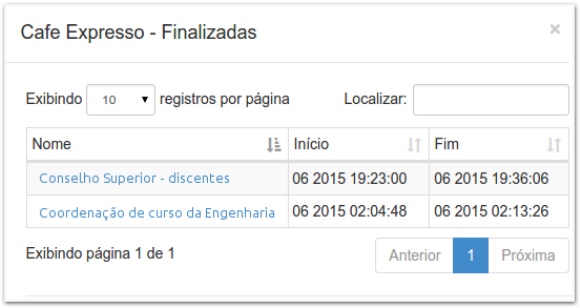
[4]https://goo.gl/ZgVhpG



(a) Página original do Helios



(b) Nova página pública Helios



(c) Lista com as eleições finalizadas em uma instituição

Figura 4. Páginas públicas da versão original do Helios e da versão proposta

tal ambiente consiste de atividades como alocação de computadores (p.e. máquinas virtuais) para atuarem como SP, IdP e serviço de descoberta (também conhecido como WAYF), instalação do *framework* Shibboleth, configuração de servidor *web* e estabelecimento de relações de confiança (troca de metadados) em cada um desses computadores.

Em 2013 a Rede Nacional de Ensino e Pesquisa (RNP) lançou o Laboratório de Gestão de Identidade (GidLab) [Wangham et al. 2013], que atua como uma plataforma de apoio aos pesquisadores que desejam investigar temas na área de gestão de identidade. Um dos serviços oferecidos pelo GidLab é a federação CAFeExpresso[5]. A federação é composta por diversos IdPs e SPs, bem como o serviço de descoberta. O pesquisador pode solicitar para hospedar sua aplicação em um dos provedores de serviço existentes ou mesmo solicitar um provedor de serviço dedicado, porém neste caso toda a administração do SP fica sob responsabilidade do pesquisador.

Para o desenvolvimento deste trabalho foi solicitado um SP exclusivo, além de um conjunto de contas de usuários em dois diferentes IdPs. Essas contas foram criadas com diferentes atributos de forma que fosse possível verificar se o controle de acesso dos eleitores funcionaria de forma efetiva. Ao todo foram solicitadas 14 contas de usuário, 7 em cada IdP, sendo que cada uma possuía características que a tornava distinta das demais. Por exemplo, uma pessoa com vínculo de aluno ativo; outra com dois vínculos ativos (servidor e aluno); outra com um vínculo ativo e outro vínculo inativo, etc.

[5]https://wiki.rnp.br/display/gidlab/CAFe+Expresso

Para os experimentos buscou-se fazer um teste de cobertura sobre todas as novas funcionalidades adicionadas ao Helios, bem como verificar se essas melhoriais não provocaram algum erro em outras partes do sistema. Foram realizadas atividades como cadastro de gestores de instituições, delegação e revogação de direitos para gestores de eleições, bem como a criação de diversas eleições fazendo uso de diferentes atributos.

Uma vez que o serviço foi validado no ambiente de desenvolvimento da CAFe-expresso, foi solicitado aos administradores da federação de homologação Chimarrão[6], mantida pela RNP, o ingresso desse SP. Neste caso, pôde-se observar que não foi necessário fazer qualquer adaptação na aplicação Helios para que a mesma operasse corretamente neste ambiente. Todos os IdPs da federação CAFe também estão presentes na federação Chimarrão e assim foi possível verificar que a integração do SP Helios com o IdP de produção do IFSC funcionou como o esperado.

4. Trabalhos relacionados

Para ofertar um serviço de forma federada, a instituição ofertante deve considerar inicialmente que o processo de autenticação de usuários não será mais atribuição do serviço, pois essa função será delegada para os IdPs com os quais esse serviço possuir relação de confiança. Deve também analisar se existe a necessidade de adotar o modelo de controle de acesso baseado em atributos, uma vez que os IdPs fornecem um conjunto de atributos de seus usuários para os provedores de serviço. Por fim, deve considerar se irá dispor de uma equipe de suporte para atender pedidos oriundos de todos os usuários da federação ou se optará por uma abordagem de auto-serviço, de forma que os próprios usuários, na maioria dos casos, consigam usar o serviço sem necessidade de envolver a equipe de suporte técnico. Nesta seção serão apresentados alguns dos serviços que são ofertados para os usuários membros da federação CAFe[7].

Os serviços video@RNP e videoaula@RNP foram remodelados recentemente para que fossem ofertados de forma federada. Em ambos os serviços, todos os vídeos estão disponíveis de forma pública, porém qualquer usuário autenticado na CAFe possui direito para fazer comentários no portal. Para a publicação de vídeos é necessário que o interessado faça a solicitação ao suporte de TI da RNP, cuja análise levará em consideração a política de uso do serviço[8].

A principal diferença dos serviços de vídeo da RNP do sistema de votação apresentado neste trabalho, está na forma de tratar as solicitações por direitos adicionais. Qualquer usuário da federação CAFe pode atuar como eleitor sem que necessite solicitar previamente o direito. Contudo, para que o usuário possa criar eleições, este deverá solicitar direitos ao gestor de sua instituição, cadastrado previamente, e não ao suporte de TI que mantém o serviço.

A delegação da responsabilidade de gerenciar gestores de eleição, para o gestor da instituição, garante escalabilidade ao serviço e evita uma sobrecarga da equipe de suporte de TI da instituição mantenedora do serviço. Outro diferencial deste trabalho está na forma como os direitos são revogados. O gestor da instituição pode a qualquer momento

[6]De acordo com a política de uso da federação CAFe, todo IdP ou SP antes de ingressar na CAFe precisa primeiramente ser homologado na federação Chimarrão.

[7]http://www.rnp.br/servicos/servicos-avancados/cafe

[8]http://www.rnp.br/file/725/download?token=j2wdDrQr

indicar quando o direito concedido irá expirar (Veja Figura 2). Ciente que nas instituições de ensino as comissões eleitorais são temporárias e esporádicas, esta funcionalidade é essencial para manter a base de gestores atualizada e íntegra. No caso dos serviços de vídeo da RNP, o procedimento adotado não garante que usuários não mais autorizados pela instituição tenham seus direitos revogados.

5. Conclusões

Neste trabalho foram apresentadas as modificações realizadas no sistema de votação online Helios para que o mesmo pudesse ser ofertado como um serviço de TIC federado. O principal objetivo do trabalho era oferecer uma solução simples para que qualquer pessoa autorizada, e sem acesso privilegiado aos sistemas de TI da instituição, pudesse criar uma eleição fechada (Veja Seção 1), cuja lista de eleitores fosse montada de forma dinâmica através do consumo de atributos fornecidos pelo seu provedor de identidade. Foi adotado um modelo de administração de usuários baseado em papéis com o intuito de minimizar pedidos de suporte para a equipe de TI mantenedora do serviço. Por fim, a página pública do serviço foi remodelada para que pudesse facilitar a apresentação das eleições em andamento ou encerradas em cada uma das instituições usuárias do serviço.

Apesar da solução estar adequada para ser ofertada como um serviço na federação CAFe, a mesma poderia ser implantada como um serviço privado de uma instituição. Neste caso, o serviço poderia ser configurado para somente aceitar usuários autenticados no IdP da instituição. Este IdP poderia ofertar uma gama maior de atributos para o serviço, dando aos gestores de eleição uma maior flexibilidade para montar a lista de eleitores.

Para o desenvolvimento deste trabalho foi criada uma ramificação (*fork*) do projeto original e foi codificado de forma a permitir o realinhamento de código com novas versões que forem lançadas do projeto original. O código fonte da solução (sob licença de software livre), bem como documentação para instalação podem ser obtidos no endereço https://github.com/shirlei/helios-server.

Como trabalhos futuros pretende-se melhorar a tela de configuração da lista de eleitores (Veja Figura 3) de forma que seja possível escolher diferentes operadores relacionais ($=, \neq, <, \leq, >, \geq$) na comparação entre atributos e valores. Atualmente só é possível usar o operador de igualdade e assim informar quais são os valores válidos (separados por vírgula) para cada atributo. Esses outros operadores relacionais permitiriam, por exemplo, criar uma eleição de forma que somente estudantes maiores de 16 anos pudessem votar.

Ainda na configuração da lista de eleitores será feita uma melhoria para que seja possível indicar mais de um IdP, além daquele de quem está criando a eleição, ou mesmo, não restringir o IdP. Com isso seria possível criar uma eleição para uma "organização virtual", com eleitores oriundos de algumas instituições na CAFe ou ainda, criar uma eleição que considere como eleitor apto qualquer pessoa que possua uma conta de usuário em algum IdP na CAFe ou de outras federações com quem a CAFe possua acordos, como por exemplo a eduGAIN.

Por fim, para ofertá-lo como serviço na federação CAFe será necessário elaborar a política de privacidade, para indicar se os dados coletados serão usados de alguma forma pelo mantenedor do serviço; política de uso, para indicar os deveres e as implicações do

não cumprimento dos mesmos por parte dos usuários do serviço, bem como o termo de adesão, o qual deverá ser assinado pela autoridade máxima da instituição.

Referências

[Adida 2008] Adida, B. (2008). Helios: Web based open audit voting. In *17th USENIX Security Symposium*.

[Adida et al. 2009] Adida, B., de Marneffe, O., Pereira, O., e Quisquater, J.-J. (2009). Electing a university president using open-audit voting: Analysis of real-world use of helios. *EVT/WOTE*.

[Chaves and de Mello 2014] Chaves, S. A. e de Mello, E. R. (2014). O uso de um sistema de votação on-line para escolha do conselho universitário. In *I Workshop de Tecnologia Eleitoral – XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg*.

[Hardt 2012] Hardt, D. (2012). Rfc 679: The oauth 2.0 authorization framework. Technical report, IETF.

[OASIS 2008] OASIS (2008). Security Assertion Markup Language (SAML). Technical report, OASIS.

[Shibboleth 2005] Shibboleth (2005). Shibboleth architecture. Technical report, Internet2.

[Wahl et al. 1997] Wahl, M., Howes, T., e Kille, S. (1997). Lightweight directory access protocol (v3).

[Wangham et al. 2013] Wangham, M. S., de Mello, E. R., de Souza, M. C., e Coelho, H. (2013). Gidlab: Laboratório de experimentação em gestão de identidades. In *III Workshop Gestão de Identidades (WGID) – XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg*.

