# Mecanismo de controle e gerência de segurança para ambientes colaborativos

Maykon Chagas de Souza [1]
Jucélio Jair Silva [1]
Michelle Silva Wangham [1]

**Resumo:** As Organizações Virtuais (OVs) permitem a formação de ambientes colaborativos com regras e políticas específicas para conceder acesso de pesquisadores aos recursos disponibilizados pelas OVs. Nestes ambientes, o modelo de identidades federadas oferece ao usuário autenticação única e federada. Como as organizações virtuais podem ser formadas por domínios (instituições) heterogêneos que ultrapassam o escopo de uma única Federação, o estabelecimento de relações de confiança entre os domínios das diferentes Federações se faz necessário. O objetivo deste trabalho é descrever um mecanismo de controle e gerência de segurança para ambientes colaborativos (GSOV) responsável por prover o estabelecimento das relações de confiança e contribuir com autenticação e autorização dos usuários da OV. Como prova de conceito, um protótipo do mecanismo proposto foi desenvolvido e avaliado por especialistas, por meio de uma pesquisa de satisfação. Os resultados obtidos comprovaram a aplicabilidade do mecanismo e validaram suas funcionalidades.

***Palavras-chave*:** Gestão de Identidade. Organização Virtual. Rede Colaborativa.

**Abstract:** *Virtual Organizations (VOs) allow the establishment of collaborative environments with specific rules and policies to provide access for researchers to resources available by VOs. In this environment, the use of federated identity model offers single sign-on (SSO) and federated authentication for the users. VOs can be formed by heterogeneous domains (organizations) that go beyond the barriers of a Federation; this requires the establishment of trust relationship among the federations domains. This work aims to describe a security management mechanism for VOs (GSOV), which is responsible for providing the trust relationship establishment among domains that are in different federations, and for supporting the authentication and authorization of VO users. As proof of concept, a prototype was developed and evaluated by specialists though survey. The result obtained demonstrated the applicability of the mechanisms and validated its functionalities.*

***Keywords*:** *Collaborative Network. Identity Management. Virtual Organization.*

## 1 Introdução

A Internet tem uma grande importância para a sociedade nos dias atuais, provendo a troca de informação e estabelecendo a comunicação em ambientes sociais e comerciais. As pessoas ao redor do mundo utilizam a Internet para manter o contato com famílias, amigos, acessar e trocar informações, além da utilização para comércio e governo eletrônico, estudo e pesquisa.

De acordo com o relatório da CISCO [1], observa-se um crescimento no número de participantes e do uso de serviços providos na Internet, serviços estes que possibilitam a colaboração, a discussão e a cooperação entre os envolvidos. Estes novos serviços podem ser utilizados principalmente para melhorar a comunicação em ambientes de pesquisa nas diversas áreas do conhecimento humano e resolver problemas complexos, obtendo resultados de forma mais rápida e eficiente [2].

[1]Laboratório de Sistemas Embarcados e Distribuídos (LEDS), Universidade do Vale do Itajaí (Univali) campus Kobrasol, BR 101, Km 207 - MundoCar Shopping - Kobrasol - São José - SC
{mchagas,jucelio}@edu.univali.br, wangham@univali.br

**http://dx.doi.org/10.5335/rbca.v9i3.6773**

Universidades, institutos de pesquisas e empresas estão gerando uma grande quantidade de dados que precisam ser acessados através de ambientes colaborativos de pesquisa que ultrapassam os domínios de uma única organização [3]. Instituições, em geral geograficamente distribuídas, se conectam através da Internet e estabelecem relações de confiança entre si para desenvolverem pesquisas colaborativas, pesquisas estas chamadas de *e-science* [4]. De acordo com [4, 5], o termo *e-science* pode ser definido como um ambiente de pesquisa colaborativo que, por meio de uma infraestrutura de serviços conectados através da Internet, compartilha recursos computacionais e processamento de alto desempenho através de computação distribuída.

Nestes ambientes colaborativos, nos quais pesquisadores fazem uso de recursos computacionais distribuídos, as relações de confiança estabelecidas devem permitir a interação entre pesquisadores que não participam de uma mesma instituição (mesmo domínio administrativo), mas que têm interesse em compartilhar recursos e informações sobre um determinado projeto [6]. Como resultado deste cenário, tem-se um grupo sem fronteiras que atua como uma rede de pessoas e instituições conectadas que trabalham juntas com o objetivo de resolver problemas complexos e fazer ciência. Na literatura, este grupo é chamado de Organização Virtual – OV (do inglês, *Virtual Organization - VO*) [7, 8].

Um aspecto relevante em ambientes colaborativos das OVs é prover a gestão de identidade (GId) por meio da criação de um sistema de identificação, de autenticação e de autorização de usuários. Estes ambientes precisam ser protegidos contra acessos não autorizados. É preciso definir quem tem acesso a quais recursos e em quais circunstâncias e também definir quem terá permissões para gerenciar as regras de acesso de outros usuários [8].

A Gestão de Identidade (GId) pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade, garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) e para prover procedimentos de autenticação, autorização e auditoria [9]. Para prover a GId, é necessária a construção de um sistema integrado de políticas e processos para validação e troca de credenciais entre os envolvidos, além das definições, certificação e gerenciamento do ciclo de vida das identidades digitais que permitam o tratamento e manipulação de identidades (atributos de identidades) [10, 11].

Dentre os modelos de GId, utilizados em ambientes colaborativos, destaca-se o de identidades federadas, no qual uma federação é uma forma de associação entre instituições parceiras (domínios administrativos) de uma rede colaborativa que usa um conjunto comum de atributos, práticas e políticas para trocar informações e compartilhar serviços, possibilitando a cooperação entre os membros e usuários da federação [11]. A adoção de um modelo de GId federada tem por objetivo remover a complexidade para o usuário, no que se refere a administrar um nome de usuário e senha para cada serviço que deseja acessar, permitindo que uma mesma identidade possa ser utilizada no acesso a diferentes serviços em domínios administrativos distintos [10, 12].

Um dos principais desafios das OVs, está relacionado ao mecanismo de gestão de políticas de acesso dos usuários dentro das OVs, uma vez que as políticas de acesso em cada provedor de serviço pode solicitar um conjunto diferente de atributos [13].

Quando o provimento de serviços é realizado por intermédio de organizações virtuais, a autorização depende de atributos definidos pela OV e não somente pela instituição de origem do usuário, sendo o mais básico entre esses atributos a própria participação do usuário na organização virtual em questão. O IdP de origem do usuário, que tipicamente atua como sua autoridade de atributos, não detém essa informação. Portanto, um mecanismo de gerenciamento da VO e um mecanismo de agregação de atributos são necessários para fornecer esta funcionalidade de forma transparente [14].

Em pesquisas colaborativas (*e-science*), a utilização de GId federadas se mostra vantajosa, pois permite que os pesquisadores envolvidos não necessitem de um novo usuário para acesso aos recursos compartilhados, possibilitando que os responsáveis pela OV adicionem somente as regras de acesso aos recursos, deixando a autenticação a cargo da instituição de origem de cada pesquisador.

No entanto, de acordo com [15], as soluções tecnológicas atuais de identidades federadas não foram preparadas para atuar em ambientes abertos e dinâmicos, como por exemplo, os encontrados nas organizações virtuais. O estabelecimento de relações de confiança entre as entidades participantes é geralmente difícil de gerenciar, porque a confiança deve ser pré-configurada antes de qualquer interação entre as partes [15]. Além disso, para que as

OVs possam ser formadas por membros pertencentes a federações distintas e heterogêneas[2], a interoperabilidade entre os sistemas de gestão de identidade precisa ser garantida [3].

Apesar da grande maioria dos domínios administrativos de uma federação acadêmica serem institutos de pesquisa ou universidades, é necessário salientar que algumas empresas também podem colaborar com as pesquisas de *e-science*, seja participando com seus pesquisadores ou provendo serviços utilizados por pesquisadores de outras instituições. Estas empresas podem ou não pertencer a uma federação. Caso estas não pertençam a uma federação, o problema se torna mais complexo já que novas relações de confiança necessitam ser estabelecidas [16, 6].

Mesmo com as facilidades proporcionadas pelos ambientes federados para os usuários, como a autenticação federada e única, existem problemas a serem tratados quando um usuário precisa colaborar em um ambiente de *e-science* que envolve mais de uma federação [3]. Uma das principais questões apresentadas por [17] é, de como lidar com a autenticação e autorização em ambientes federados. Se cada comunidade utilizar uma abordagem diferente para acesso aos dados, o resultado é um ambiente cada vez mais isolado, fazendo com que só aquela comunidade tenha acesso.

Este artigo tem por objetivo descrever um mecanismo de controle e gerência de segurança para ambientes colaborativos (GSOV), responsável por prover o estabelecimento das relações de confiança entre os domínios administrativos que estão em diferentes federações e por contribuir com a autenticação e autorização dos usuários da OV. O presente artigo estende o mecanismo proposto pelos autores em [18] ao permitir o uso de diferentes tecnologias, garantindo assim a interoperabilidade entre os domínios administrativos, para além da especificação SAML. Assim o trabalho tem como principal contribuição prover um ambiente complemente heterogêneo, contemplando além de diferentes domínios administrativos também tecnologias de autenticação e autorização distintas. De forma a avaliar a usabilidade e aplicabilidade do mecanismo GSOV, uma avaliação experimental foi conduzida por especialistas em GId e os resultados desta avaliação estão descritos no presente artigo.

Este artigo está organizado em seis seções. Na Seção 2, são apresentados os conceitos referentes a OVs, *e-science* e gestão de identidade federada. O Mecanismo de Controle e Gerência de Segurança para ambientes colaborativos (GSOV) é descrito na Seção 3 e a avaliação, na Seção 4. Na Seção 5, os trabalhos relacionados são analisados e comparados com o mecanismo proposto. Por fim, a conclusão e os trabalhos futuros são apresentados na Seção 6.

## 2 Fundamentação teórica

Diversos termos são utilizados na literatura para representação das várias manifestações de colaborações entre instituições de pesquisas, profissionais, empresas privadas e públicas. O termo rede colaborativa pode ser definido como: "uma rede que consiste de várias pessoas, entidades, ambientes e ferramentas heterogêneas e geograficamente distribuídas, que colaboram para encontrar a resolução de um problema específico e cujas interações são suportadas pelas redes de computadores" [19].

Dentro destas redes colaborativas, um desafio apontado por [8] é o compartilhamento de recursos para resolução de problemas de pesquisa de forma dinâmica e multi-institucional. Para permitir este compartilhamento, é necessário prover um ambiente controlado, definindo claramente quem é o provedor do serviço e quem é cliente, o que é compartilhado, quem tem acesso a estes recursos e quem pode compartilhá-los. Um grupo de empresas, indivíduos e instituições, que compartilham recursos e conhecimentos para alcançar um objetivo e que atuam por acordos estabelecidos, é denominado de Organização Virtual (OV) [8].

O responsável pelo programa de *e-science* do governo Inglês, John Taylor, define *e-science* como: "*uma forma de colaboração global em determinadas áreas da ciência e a infraestrutura que irá suportá-la*" [20]. Além disto, *e-science* utiliza ferramentas computacionais para a troca de informações, permitindo que pesquisadores possam compartilhar recursos com outros pesquisadores ou, em outros projetos, instituições e até entre diferentes áreas de pesquisa [4].

A colaboração entre as diferentes disciplinas, áreas de conhecimento, não se aplica somente às tecnologias mas também às instituições, nas quais as políticas de coordenação dos projetos de *e-science* ultrapassam as

[2]O termo federações heterogêneas será usado neste trabalho para indicar federações que usam diferentes soluções tecnológicas de gestão de identidade.

fronteiras de países e apresentam obstáculos para o processo, não só técnicos, mas organizacionais [4]. Estas barreiras incluem políticas restritivas de acesso aos recursos computacionais das *grids* acadêmicas providas por um país, suas diferentes leis de direitos autorais e de propriedade intelectual, além de barreiras comerciais como a interconexão de redes seguras.

Nos ambientes colaborativos, um desafio apontado em [8] é o compartilhamento de recursos para resolução de problemas de pesquisa de forma dinâmica e multi-institucional. Para permitir este compartilhamento, é necessário prover um ambiente controlado, definindo claramente quem é o provedor do serviço, o que é compartilhado, quem tem acesso a estes recursos e quem pode compartilhá-los.

Um dos desafios apresentados em uma OV é criar e gerenciar um ambiente seguro e federado entre domínios administrativos autônomos, de forma a garantir a separação entre o provimento, o gerenciamento da aplicação fornecida, o gerenciamento operacional da infraestrutura da OV, o descobrimento dos recursos disponíveis e o estabelecimento das relações de confiança [13].

O ciclo de vida de uma OV é um processo composto dos seguintes estágios: (1) **criação**, que identifica as competências necessárias para desenvolver um projeto de pesquisa, modela o projeto com base nestas competências e identifica os parceiros que melhor se enquadram neste projeto; (2) **operação**, que visa a execução do projeto cooperativo de forma eficiente, sendo que os mecanismos de cooperação e as medidas de desempenho têm papel importante neste estágio; (3) **evolução**, que permite uma pequena alteração ou redistribuição de competências entre os membros[3]; e (4) **dissolução**, que trata da dissolução das relações de cooperação estabelecidas para operação da OV.

Nos ambientes de *e-science* e OVs, o conceito de identidades federadas tem se popularizado justamente pelo fato de permitir maior flexibilidade no uso das identidades dos usuários e no gerenciamento destas pelos administradores de serviços que participam da Federação. Para prover estes ambientes de federação, o SAML tem se mostrado o protocolo mais utilizado, uma vez que possui uma especificação robusta e que foi projetada com o intuito de atender as necessidades para a formação e gerenciamento de Federações. Outros protocolos também podem ser usados em Federações, como o WS-Federation[4] e o OpenID Connect[5].

## 3 Mecanismo de Gerência de Segurança para Organizações Virtuais

Para gerenciar o ciclo de vida de uma OV e fazer uso dos benefícios das identidades federadas e da transposição de autenticação e de atributos para outros domínios fora da federação de origem, foi preciso neste trabalho enfrentar as seguintes questões de pesquisa: como estabelecer as relações de confiança quando os membros da OV (instituições e pesquisadores) não fazem parte da mesma federação? E ainda, quando se trata de relações entre federações que utilizam diferentes sistemas de GId (baseados em SAML ou OpenID Connect), como realizar a transposição de autenticação e de atributos?

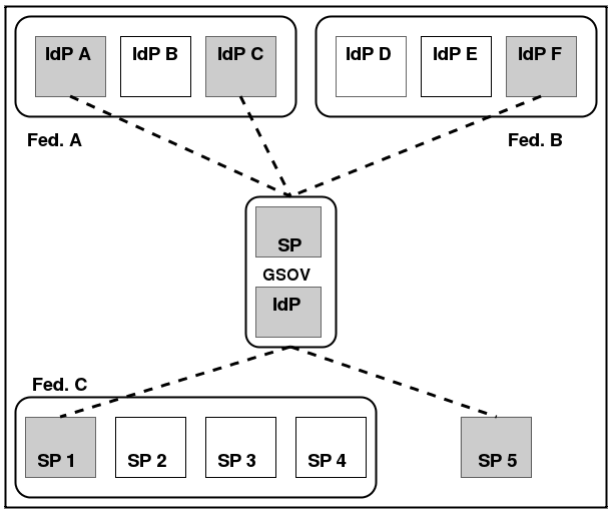
O serviço proposto de gerência de segurança atua como um *proxy*, uma terceira parte confiável, que intermedia os acessos de usuários entre os domínios administrativos das instituições que participam do ambiente de pesquisa colaborativa (*e-Science*). Este serviço está baseado na especificação SAML e estende o conceito de autenticação federada ao possibilitar que os membros da OV estejam em federações distintas. A solução proposta contempla ainda a definição de um metadado de atributos comuns para ambientes de *e-Science*, para que o mapeamento dos atributos dos usuários entre os diferentes domínios administrativos possa acontecer.

A habilidade de atuar como um *proxy* possibilita que o serviço se comunique com diferentes entidades (IdPs ou SPs) que podem estar em federações SAML distintas. Para isto, o serviço estabelece as relações de confiança com as entidades de forma independente (não com toda a federação que esta entidade pertence). Ou seja, um IdP ou um SP que pertence a uma Federação pode possuir uma relação de confiança direta com o serviço. Para exemplificar esta funcionalidade, a Figura 1 ilustra uma OV formada pelos domínios A, C e F de diferentes federações. O IdP A e o IdP C da Federação A, o IdP F da Federação B e o SP 1 e o SP 2 possuem relações de confiança com os IdPs, o que possibilita que os usuários da OV que estão nestes IdPs possam acessar serviços do

[3]Mudanças em objetivos ou mudanças de muitos parceiros levam a uma nova formação.
[4]http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html
[5]http://openid.net/developers/specs/

SP 1 e do SP 5. O primeiro SP faz parte da Federação C e o segundo é um serviço independente, que não faz parte de nenhuma Federação, mas que participa da OV.

Figura 1: Visão geral do serviço proposto como Proxy




O serviço proposto não tem a necessidade de estar inserido em um ambiente de uma federação, e esta característica torna a formação de OVs mais flexível, pois permite que os envolvidos na pesquisa colaborativa estabeleçam a relação de confiança para a formação da OV somente entre si. Na solução proposta, é possível ainda ter diferentes serviços gerentes de OV, para diferentes OVs, o que garante a escalabilidade e distribuição da solução. O mecanismo de gerência de segurança é capaz de estabelecer as relações de confiança entre as entidades de diferentes domínios administrativos que participarão de uma OV, permitindo que os atributos dos usuários sejam trocados entre as entidades da OV, tendo como base as relações de confiança e políticas de uso previamente estabelecidas entre os provedores participantes.

Com estas relações de confiança estabelecidas, a transposição de autenticação e de atributos ocorrerá dentro da OV e os provedores de serviços da OV poderão ser acessados de forma segura e transparente. Desta forma, o usuário não terá de se preocupar com detalhes específicos de como acessar os provedores de serviços ou com o gerenciamento de múltiplas identidades para cada SP que desejar acessar na OV.

O processo para estabelecimento de relações de confiança entre os participantes da OV não se difere muito do processo realizado para a entrada de um participante em uma Federação SAML. No entanto, diferentemente de outros trabalhos, como [21] ou [7], em que as relações de confiança precisam ser estabelecidas com toda a federação, na solução proposta, um SP deve ser uma entidade confiável apenas para os domínios envolvidos na OV, sem a necessidade de participar da federação de cada um dos domínios envolvidos. Logo, é necessário estabelecer relações de confiança apenas com os IdPs e os SPs participantes da OV.

Após a criação da OV, o serviço está apto a processar as requisições de acesso aos SPs registrados na OV dos usuários de diferentes domínios administrativos, sejam de domínios de uma mesma federação ou de federações distintas, mesmo quando estes domínios utilizam diferentes sistemas de GId, porém, baseados no padrão SAML. A solução proposta pode ser utilizada em dois cenários de OVs, a saber:

- OV intrafederada, nos quais todos os membros de uma OV participam de uma mesma federação baseada no padrão SAML. Esta é a forma mais simples para criação, operação e dissolução da OV, uma vez que boa parte das relações de confiança já estão estabelecidas e não há necessidade de transposição de autenticação e de atributos entre federações.
- OV interfederada, nos quais os membros da OV são de federações distintas.

A Figura 2 apresenta os dois cenários, sendo que a OV A apresenta a OV intrafederada e a OV B apresenta a OV interfederada. Além da formação de OVs baseadas em federações SAML, este trabalho se propõe a apre-

sentar um terceiro cenário, que consiste na participação de domínios externos a federações e ao uso de tecnologia diferente do SAML, neste caso utilizando OpenID Connect (OIDC). Este cenário permite a formação de OV com domínios que possuem OIDC. Isto expande a gama de possibilidades, permitindo a participação de empresas e outras organizações que não estão associadas a uma federação. A Figura 3 ilustra o cenário com a interação entre domínios de duas federações (A e B), representados pelos domínios B, C e A, respectivamente, e um domínio externo (representado pelo Domínio F), através do uso do OIDC.

Figura 2: OV Intrafederada e OV interfederada

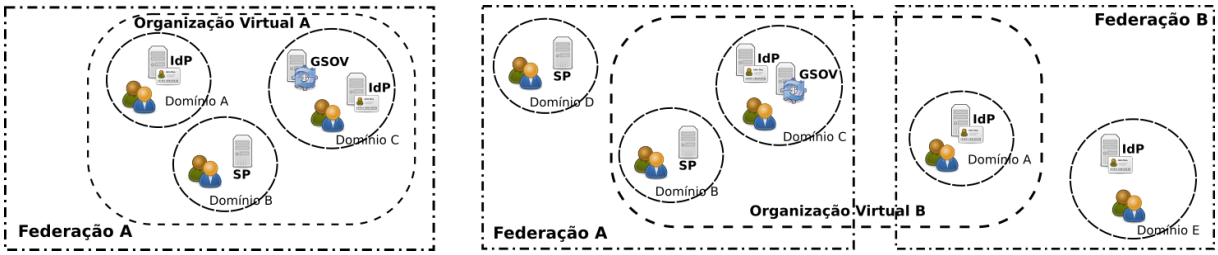
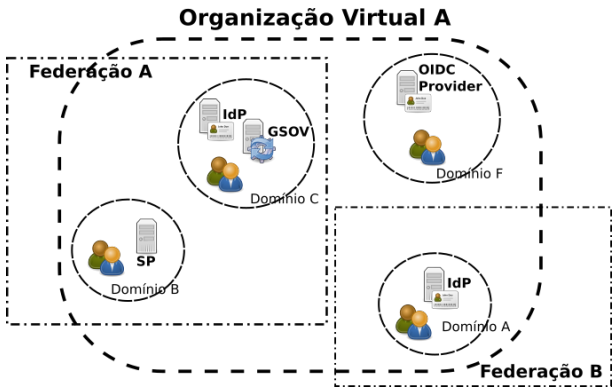


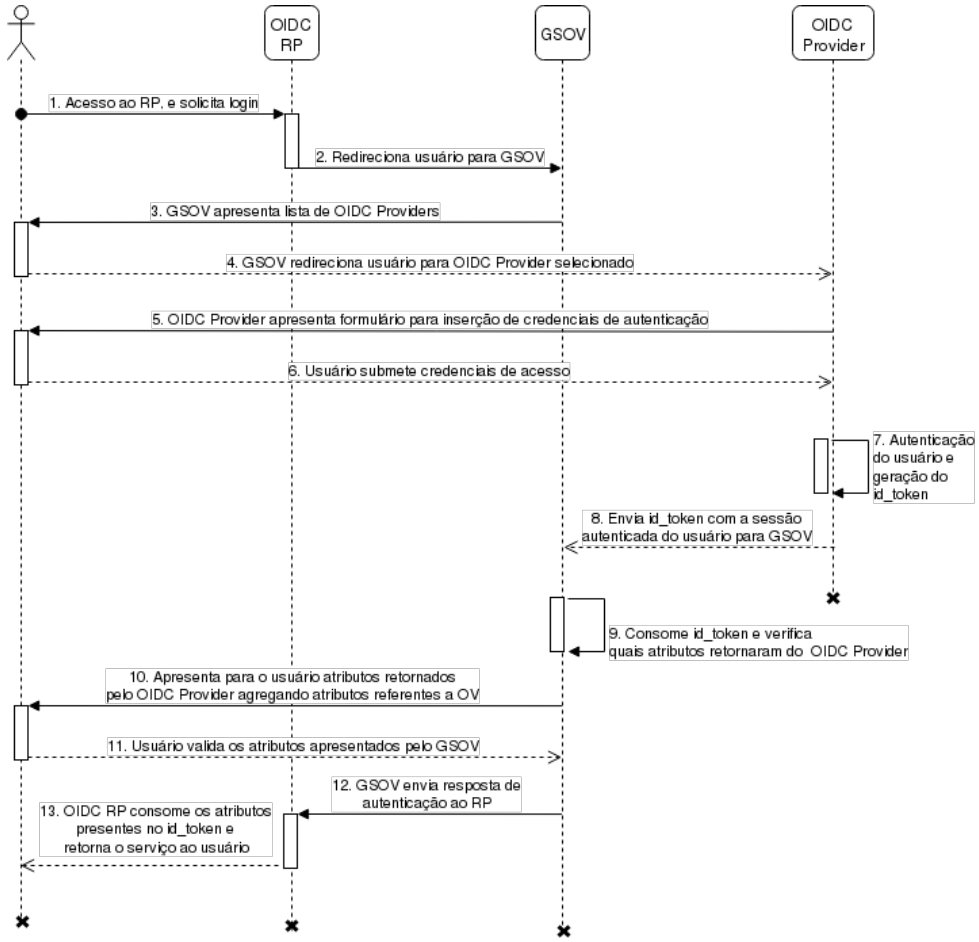

Figura 3: OV com participação de um domínio externo a federações




A Figura 4 apresenta um diagrama de fluxo das mensagens trocadas quando um usuário do domínio com OpenId Connect (OIDC) tenta acessar um SP, também chamado de *Relaying Party* (RP), com a intermediação do GSOV. Neste cenário, é esperado que o RP da OV tenha a opção de autenticação via OpenID Connect para que o usuário realize a autenticação em seu OpenID Connect Provider (OP). Para o GSOV, quando a autenticação via OIDC for requisitada o GSOV tratará a requisição internamente através do mesmo protocolo, possibilitando a tratativa da mensagem de requisição. E a partir deste momento, o GSOV apresentará a lista de OPs disponíveis para autenticação.

Desta forma, o usuário, ao acessar o RP, deve indicar que quer se autenticar via OIDC (passo 1). O RP então envia esta requisição para o GSOV (passo 2), que terá um DS OIDC, previsto na especificação OIDC. O GSOV então apresentará uma lista de OPs (passo 3) registrados na OV. Ao selecionar o seu OP de origem, o GSOV redireciona o usuário (passo 4) para que este se autentique (passos 5 e 6). Após autenticação bem sucedida, no passo 7, o OP gera o `id_token` que contém as informações (atributos) e a sessão de autenticação do usuário e os envia para o GSOV (passo 8). Da mesma forma como nos cenários anteriores, o GSOV se comporta como um *proxy*, possibilitando a interação entre um RP e um OP. O GSOV obtém os atributos do usuário do `id_token` (passo 9) e agrega com os atributos deste usuário registrados na OV. Em seguida, a tela de solicitação de liberação de acesso aos atributos é apresentada ao usuário (passo 10). Após a liberação dos atributos (passo 11), o GSOV retorna o `id_token` para o RP (passo 12) e, com base nos atributos do usuário, decide se permite ou não o seu acesso ao serviço (passo 13).

Figura 4: Diagrama de mensagens de comunicação entre as entidades




### 3.1 Componentes e funcionalidades

Para realizar o estabelecimento das relações de confiança entre os domínios e contribuir com a interoperabilidade entre os sistemas de GId, o serviço proposto possui os seguintes componentes:

Figura 5: Componentes do serviço proposto (GSOV)


- Aplicação de administração: aplicação Web que possibilita ao administrador da OV criar, editar e excluir os membros da OV. Ou seja, uma aplicação com as funcionalidades para gerenciar o ciclo de vida das OVs. Além disto, este componente é responsável por auxiliar o estabelecimento das relações de confiança entre os IdPs que farão parte da OV e os SPs que hospedarão serviços colaborativos para a OV;
- *Embedded Discovery Service* (EDS): responsável por apresentar uma lista de IdPs para o usuário para que este indique qual seu IdP de origem. Com base na escolha do usuário, o EDS redirecionará o mesmo para o IdP escolhido para a autenticação;

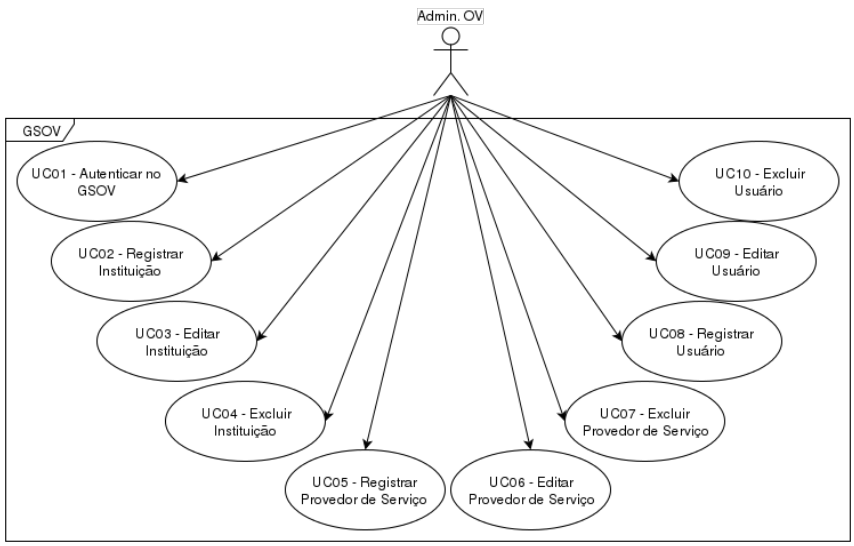
- Agregador de Atributos: responsável por realizar a agregação de atributos do usuário. O agregador recebe os atributos liberados pelo IdP do usuário e agrega (concatena) novos atributos que foram definidos pelo administrador da OV no momento do registro deste usuário no serviço. Os atributos agregados podem ser, por exemplo, o nome da OV que o usuário participa e o papel deste na OV;
- IdP Proxy: responsável pela mediação entre os IdPs e os SPs da OV e que está baseado na especificação IdP Proxy SAML [22]. Este componente permite que entidades de Federações diferentes ou que não participam de uma Federação possam interagir de forma a permitir que um usuário autenticado em um IdP, cadastrado na OV, possa acessar os serviços colaborativos que estão em outro domínio administrativo.

Os atributos provenientes do IdP do pesquisador podem não ser suficientes para garantir que este pesquisador, que está tentando acessar o recurso, tenha permissão de acesso. Desta maneira, o serviço gerente de segurança possibilita que atributos específicos da OV sejam criados e concedidos aos membros da OV. Para isto, um mecanismo agregador de atributos, que é um mecanismo que coleta e une atributos de um usuário provenientes de diferentes provedores de identidades [23], foi concebido e integrado ao serviço proposto. Diante disto, o serviço proposto possibilita o registro de usuários para que os atributos específicos da OV sejam criados e atribuídos aos membros da OV. Vale destacar que o serviço proposto atua como um provedor e agregador de atributos.

### 3.2 Desenvolvimento do Protótipo

De forma a avaliar a aplicabilidade do serviço proposto, como prova de conceito, um protótipo do GSOV foi desenvolvido utilizando o ambiente de experimentação do GIdLab[6] [24], com o objetivo de analisar os cenários de OVs intrafederada e interfederada. O mecanismo GSOV, que gerencia o ciclo de vida da OV, foi desenvolvido em PHP e utiliza o *framework* SimpleSAMLphp[7] que implementa o protocolo SAML. As funcionalidades implementadas no GSOV estão indicadas no diagrama de casos de uso da Figura 6. Para armazenar as informações referentes às instituições (provedores de identidades, provedores de serviços e os atributos dos usuários que fazem parte da OV), uma base de dados utilizando MySQL foi integrada ao mecanismo proposto.

Figura 6: Casos de uso

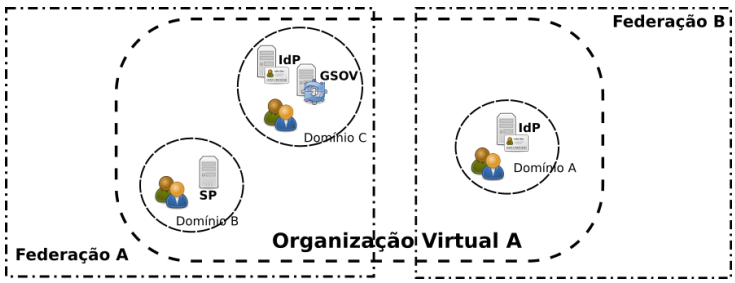



O cenário desenvolvido, ilustrado na Figura 7, é composto por duas Federações. A aplicação colaborativa implantada no SP foi um ambiente de apoio para documentação de projetos (*Wiki*). Utilizou-se o software MediaWiki que provê a criação destes ambientes. Para realizar autenticação via SAML, foi utilizada a extensão SimpleSAMLAuth disponível neste software[8].

[6]https://gidlab.rnp.br
[7]https://simplesamlphp.org/
[8]https://www.mediawiki.org/wiki/Extension:SimpleSamlAuth

Para exemplificar a relação de confiança com IdPs de diferentes domínios administrativos (em diferentes federações), foram implantados três IdPs, utilizando dois *frameworks* distintos. Nos IdP1 e IdP2, utilizou-se o SimpleSAMLphp e, no IdP3, o Shibboleth[9]. Em todos os IdPs, foram definidos um conjunto de usuários para realização dos testes. Estes usuários foram armazenados em uma estrutura de diretórios OpenLDAP[10].

Figura 7: Cenário da Prova de Conceito




Para avaliar o protótipo desenvolvido, foram definidos e executados quatro casos de testes, tendo como base os principais casos de uso do GSOV, ilustrados na Figura 6. O primeiro caso de testes teve como objetivo verificar a função de autenticação para acesso às funcionalidades de administração de uma OV provida pelo GSOV. Neste caso de teste, o administrador da OV realizou a autenticação através da página de *login* da aplicação gerente de OV. No segundo caso de teste, o objetivo era validar o processo de criação da OV, através do cadastro dos membros da OV (instituições e pesquisadores participantes da OV) e dos SPs. Neste referido caso de teste, foram validados os casos de usos referentes a registro, edição e exclusão da OV e de seus participantes. No terceiro caso de testes, o objetivo foi validar o acesso de um pesquisador participante da OV ao serviço colaborativo da OV. Além do acesso, foi validado ainda o processo de agregação de atributos (atributos vindos do IdP mais os atributos específicos da OV). O objetivo do último caso de teste foi verificar se usuários não registrados na aplicação gerente de OV, mas cadastrados em um IdP, seriam impedidos de acessar o serviço colaborativo.

Os casos de teste foram executados por dois usuários, um com registro prévio, que necessitou da agregação de atributos e outro sem registro, que tem como resultado uma tela de acesso negado. Todos os casos de testes executados obtiveram resultados positivos, logo é possível afirmar que as funcionalidades desenvolvidas estão de acordo com seus casos de uso.

## 4 Avaliação dos Resultados Obtidos

Esta seção apresenta a análise e os resultados de uma pesquisa de satisfação (teste de usabilidade) realizada em um período de seis (6) dias que visou avaliar o protótipo desenvolvido e suas funcionalidades, assim como a sua aplicabilidade em ambientes de projetos de pesquisas colaborativas. Nesta fase de avaliação qualitativa o mecanismo foi analisado considerando um ambiente de uma organização virtual homogênea, ou seja, composta apenas por federações SAML.

Após a execução de um experimento guiado, um questionário com a pesquisa de satisfação foi aplicado e respondido por treze (13) especialistas na área de Gestão de Identidade. A primeira parte do questionário teve por objetivo identificar o conhecimento do avaliador nos conceitos e tecnologias envolvidos no experimento. Em seguida, a aplicação do questionário serviu para detectar o nível de satisfação dos avaliadores no que tange a utilização do mecanismo GSOV. A seguir, alguns dos resultados obtidos são analisados.

A primeira questão teve como objetivo identificar se os avaliadores conhecem os conceitos e tecnologias de Gestão de Identidade. As respostas indicaram que 84.6% (11) dos avaliadores conhecem o conceito de Organizações Virtuais e somente 15.4% (2) não têm conhecimento deste tipo de ambiente. Era esperado que todos os avaliadores tivessem conhecimento de Organizações Virtuais e Autenticação Federada, sendo que referente a Autenticação Federada, 100% (13) dos avaliadores indicaram ter conhecimento sobre este conceito. 100% (13) dos

[9]https://shibboleth.net
[10]http://www.openldap.org/

avaliadores conhecem a especificação SAML, e 61.5% (8) dos avaliadores tem conhecimento sobre a especificação OpenID Connect, como pode ser visto na Figura 8

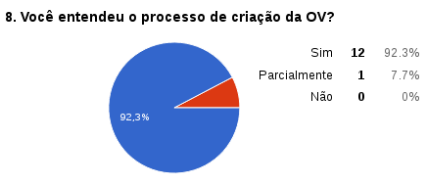
Figura 8: Avaliação de conhecimento de tecnologias de GId


Referente ao conceito de Autenticação Única (*Single Sign-On – SSO*), 92.3% (12) dos avaliadores têm conhecimento sobre este conceito e somente 7.7% (1) dos avaliadores não sabem do que se trata. Por fim, os especialistas foram questionados sobre seus conhecimentos referentes aos componentes que formam uma federação (IdP e SP). Assim, 100% (13) dos avaliadores responderam que têm conhecimento sobre estes componentes. Pode-se concluir que, apesar dos poucos que não conhecem a tecnologia OpenId Connect, todos os avaliadores possuíam conhecimentos suficientes para execução dos experimentos.

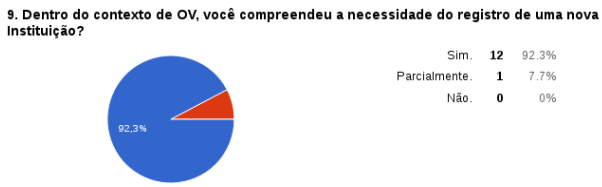
Após o preenchimento das questões referentes ao perfil do usuário, a execução do experimento foi iniciada considerando o ciclo de vida de uma Organização Virtual. Sendo assim, foram realizados a criação da OV e o registro das Instituições participantes e seus usuários, bem como o registro do serviço colaborativo e, por fim, a associação destes membros em uma Organização Virtual. Posterior à criação inicial da OV, foi considerado o processo de evolução desta, no qual eram executados passos para associação de um nome membro (uma instituição) e seus usuários (pesquisadores).

A segunda parte do experimento teve como finalidade identificar se os avaliadores compreenderam o procedimento de criação de uma OV e se enfrentaram dificuldades no experimento. De acordo com as respostas, 92.3% (12) dos avaliadores compreenderam o processo de criação da OV. E, somente 7.7% (1) dos avaliadores compreenderam parcialmente o processo de criação da OV. Já 76.9% (10) dos avaliadores não encontraram nenhuma dificuldade em registrar os membros da OV e a criação da OV e associação desses membros à OV recém criada. Dos 23.1% (3) dos avaliadores que encontraram dificuldades, foi possível identificar, através de um campo para preenchimento, quais foram as dificuldades encontradas.

Figura 9: Avaliação do procedimento de criação de uma OV




(a) Entendimento de criação de uma OV




(b) Entendimento de um novo registro na OV

Dentre os comentários, os avaliadores informaram que tiveram problemas na sessão do *login*, informando que a aplicação não salva o estado. Por questão de segurança, no protótipo, a sessão expira depois de um determinado tempo. Outro comentário foi relacionado a duplicação de informação, registros de instituições e usuários. Devido às funcionalidades do protótipo e do tipo de avaliação realizada, não se encontrou uma forma de realizar a avaliação, garantindo a privacidade do avaliador, ocasionando a duplicidade, pois o roteiro de avaliação considerava o cadastro de um conjunto de informações fixas. Com isso também foi possível verificar que o mecanismo não trata o registros duplicados, melhoria que precisará ser implementada em versões futuras.

Além disso, buscou-se identificar se os avaliadores compreenderam a necessidade do registro de um novo membro da OV (Instituição e seus Usuários), que caracterizava a evolução da OV. Referente ao processo de evolução da OV, foi realizada a avaliação sob o registro de um novo membro (Instituição) e seus pesquisadores no GSOV. Neste passo, foi solicitado ao avaliador realizar o registro e a associação deste novo membro a OV já criada. Posteriormente, questionou-se se o mesmo entendeu o objetivo da adição de novos membros. De acordo com

os índices, 92.3% (12) dos avaliadores compreenderam o processo de evolução da OV. E somente 7.7% (1) dos avaliadores compreenderam parcialmente o processo de evolução da OV.

Em seguida, os avaliadores precisaram também simular dois testes de acesso a recursos da OV. No primeiro teste, o objetivo era exemplificar um acesso autorizado, no qual o usuário tenta acessar um serviço de uma OV com um usuário que está registrado como participante de uma OV. Neste teste, é apresentada também a tela que indica a agregação de atributos originários do IdP do usuário com os atributos necessários para acesso ao serviço e que são solicitados pelo mesmo para a OV. Posteriormente ao teste de acesso com usuário registrado, os avaliadores realizaram um teste com um usuário não registrado na OV, mas que possuia cadastro em um IdP membro da OV. Neste segundo teste, o objetivo era comprovar que somente aqueles usuários que fossem elencados para a participação na OV podem acessar serviços desta OV.

Outra questão tinha como finalidade identificar se os avaliadores compreenderam o processo de agregação de atributos, realizado no acesso do usuário registrado na OV. Os resultados indicam que 46.2% (6) dos avaliadores compreenderam o processo de agregação de atributos e que outros 53.8% (7) dos avaliadores compreenderam parcialmente o processo de agregação de atributos. Constata-se que este resultado pode ser devido ao fato que a agregação não é um processo comumente utilizado dentro da federação e que, quando usado, é transparente para os usuários. No protótipo desenvolvido, a necessidade de mais informações (atributos) que aquelas liberadas pelo seu IdP era informada aos usuários para que estes consentissem com a agregação de novos atributos.

Após a execução do roteiro, uma série de questionamentos foi apresentada aos avaliadores para validar as funcionalidades do protótipo, assim como o grau de satisfação e experiência e o sucesso na execução das ações do roteiro. Dentre as questões sobre o uso, buscou-se identificar se o pesquisador obteve sucesso em todos os passos na execução do roteiro. Assim, 69.2% (9) dos avaliadores obtiveram sucesso na execução do experimento, e 30.8% (4) dos avaliadores tiveram algum problema na execução. Para estes, foi questionado em qual momento o protótipo apresentou algum problema. Dentre algumas das respostas, foram relatados problemas de acesso aos servidores, falta de clareza no roteiro e, problemas na agregação de atributos, não sendo apresentada a tela de agregação, solicitando o consentimento do avaliador, permitindo acesso direto ao serviço da OV. Este comportamento se deu devido à execução do roteiro por mais de um avaliador simultâneo, pois ao realizar a agregação de um usuário, em um novo acesso esta tela não é apresentada novamente. Sendo assim, quando o segundo avaliador realizava o acesso com um usuário que havia agregado os atributos do usuário de acesso, a tela de agregação não era apresentada.

Foi questionado se durante a execução do roteiro o avaliador precisou cancelar a execução e iniciar novamente, e se as mensagens de erros, caso ocorreram, foram suficientes para sanar os problemas. Os índices indicam que 84.6% (11) dos avaliadores não precisaram cancelar a execução e iniciar novamente, e somente 15.4% (2) tiveram que reiniciar algum serviço. Além disto, referente a mensagens de erros, 15.4% (2) dos avaliadores informaram que as mensagens de erros foram parcialmente suficientes para apontar e contornar os problemas. Já 30.8% (4) dos avaliadores informaram que as mensagens foram suficientes e 53.8% (7) dos avaliadores informaram que esta questão não se aplica.

Figura 10: Questões sobre o cancelamento da execução


(a) Avaliação se foi necessário cancelar a execução

(b) Avaliação das mensagens de erro

Ainda sobre o uso do mecanismo, tentou-se identificar se os avaliadores foram sempre solicitados a realizar alguma ação e se em algum momento não souberam o que fazer. Os índices indicam que 84.6% (11) dos avaliadores indicaram que o mecanismo sempre exigiu alguma ação do avaliador e 15.4% (2) indicaram que o mecanismo solicitou parcialmente a ação do avaliador na utilização do protótipo. Já 53.8% (7) dos avaliadores informaram que sempre souberam o que fazer no experimento para realização das ações e 15.4% (2) dos avaliadores informaram que não souberam parcialmente o que fazer, enquanto 30.8% (4) dos avaliadores informaram que não souberam o

que fazer ao acessar o protótipo. Conclui-se que há necessidade de aprimorar a usabilidade do protótipo para tratar destas questões.

Além disso, buscou-se identificar a satisfação de uso do protótipo, a apresentação das informações e a compreensão das funções, assim como a recomendação da aplicação para uso em ambiente de *e-science*.

Para 76.9% (10) dos avaliadores, as informações foram claras e apresentadas de forma adequadas, e 23.1% (3) dos avaliadores informaram que as informações foram apresentadas com certa clareza e de forma compreensiva. Todos os avaliadores, compreenderam as funções do mecanismo rapidamente. E 100% (13) recomendariam a aplicação para o uso em ambientes de *e-science*. Dentre os avaliadores, 92.3% (12) indicaram a experiência como satisfatória, e somente 7.7% (1) não considerou a experiência satisfatória.

Figura 11: Questões sobre satisfação de uso


(a) Avaliação de satisfação de uso


(b) Avaliação de uso e dúvida do que fazer

Através da aplicação da pesquisa qualitativa, foi possível identificar que o mecanismo se mostrou adequado para o propósito ao qual foi desenvolvido, demonstrando que as funcionalidades básicas do protótipo se mostraram satisfatórias para o funcionamento do mesmo dentro do ambiente de organizações virtuais. Foi possível avaliar que o protótipo satisfaz os requisitos no que diz respeito a criação, gerenciamento e dissolução de uma organização virtual assim como a criação de ambientes, utilizando-se de duas federações distintas que fazem uso da mesma tecnologia. Como forma de aprimorar o trabalho, falta ainda a formação de ambientes totalmente heterogêneos, incluindo diferentes tecnologias como OpenID. Ainda como parte da avaliação, a compreensão do uso da agregação de atributos mostra a necessidade dessa funcionalidade, quando se trata de ambientes formados por diferentes domínios administrativos que utilizam conjuntos de atributos distintos.

## 5 Trabalhos relacionados

O trabalho apresentado em [21] oferece uma solução de Infraestrutura de Autenticação e Autorização (IAA) chamada *Identity Access Management Suite*[11], baseada nas especificações SAML e XACML para acesso a um ambiente de pesquisas virtuais (VRE). A IAA pode realizar a agregação de atributos provida por um IdP interno da OV (elemento VO AA), combinando atributos recebidos pelo IdP do usuário com os atributos específicos da VRE. A IAA também permite o acesso a serviços que estão em diferentes federações, baseado nas relações de confiança entre federações (p.ex.: Federação InCommon e a Federação Australiana). A solução permite acessar os ambientes através de um portal *web* ou uma aplicação *desktop*, realizando autenticação via SAML ou através de certificados digitais X.509. A solução visa atender uma plataforma utilizada em ambientes de *Grid*, responsável pela criação e gerenciamento das OVs.

O myVOCS é um ambiente proposto em [7] que permite a criação e gerenciamento de OVs para ambientes de *Grid* de forma autônoma e flexível, utilizando autenticação federada através do *framework* Shibboleth (SAML). O myVOCS é uma alternativa ao uso de soluções como VOMS[12] e PERMIS[13], utilizados para gerenciamento de autorização das OVs. Foi desenvolvido como um serviço de gerenciamento dos atributos de afiliação de OV com a inserção dos atributos providos pelos IdPs dos usuários. A solução provê o acesso a contextos de segurança em domínios distribuídos, independentemente administrados, que permite ao usuário acessar diretamente e de forma transparente um recurso. A solução é implementada como um *proxy*, que se comporta como um IdP, recebendo as

[11] Compatível com o portal do ambiente GridSphere <http://www.gridsphere.org/>
[12] http://toolkit.globus.org/grid_software/security/voms.php
[13] http://sec.cs.kent.ac.uk/permis/index.shtml

requisições dos SPs, e como um SP, enviando requisições de autenticação para os IdPs dos usuários. Os autores deste trabalho não descrevem como são estabelecidas as relações de confiança entre os serviços colaborativos e os IdPs (que realizam autenticação dos usuários participantes das OVs).

O trabalho descrito em [25] utiliza o VOMS para prover a autenticação e autorização em um ambiente multi-institucional para experimentos com nuvens, com diferentes provedores de recursos. No trabalho em questão, foi utilizado o OpenStack[14]. O suporte ao VOMS foi implementado através de um módulo adicionado ao servidor web que utiliza a funcionalidade de autenticação externa, permitida na arquitetura do OpenStack, que delega a autenticação a um terceiro. No referido trabalho, os autores apresentam a alteração realizada no mecanismo de autenticação e autorização do OpenStack, o Keystone, para permitir autorização, usando certificados X.509, emitidos pelo VOMS, sendo que neste certificado um dos atributos identifica em que OV o usuário participa. Este trabalho não possui um mecanismo para criação e gerenciamento de OVs.

O ACROSS (**A**ttribute-based access **C**ont**RO**l and di**S**tributed policie**S**), trabalho proposto em [26], é um arcabouço para autenticação e autorização em ambientes federados para criação de OVs. O ACROSS trata tanto da autenticação federada dentro da OV quanto do controle de acesso ao recursos através de políticas locais e globais. A arquitetura do ACROSS está organizada em módulos, sendo que os principais módulos são: Federação de Identidade, Provedor de atributos e de Controle de Acesso (ABAC). Neste trabalho, os membros da OV estão todos em uma única Federação baseada no SAML.

A solução *Globus Nexus*, descrita em [27], é uma *Plaform as a Service* (PaaS) desenvolvida como parte do projeto Globus[15], que tem como foco disponibilizar uma plataforma para o ambiente colaborativo de *e-science* e uma série de serviços, como armazenamento de dados, provedores de recursos computacionais e outros serviços para *e-science*. O Globus Nexus funciona como um Provedor de Identidade (que agrega diferentes atributos de diferentes IdPs associados a uma identidade), além disso provê gerenciamento de grupos e suporta a criação de domínios customizados.

Em relação aos trabalhos [21, 7, 26], o presente trabalho tem como diferencial a possibilidade da formação de OVs de forma descentralizada, de acordo com a demanda dos participantes dos projetos envolvidos na OV. Outro diferencial da presente solução é criação de OVs com a participação de membros que estejam em diferentes federações SAML, sem a necessidade de que estas federações estejam em uma confederação (uma federação de federações, como exemplo, a EduGAIN[16]). Além disso, ao contrário das soluções apresentadas em [25] e [27], focadas em nuvem ou em *grids* computacionais, respectivamente, a presente solução pode ser empregada em diferentes cenários de OVs para realização de *e-science*.

## 6 Conclusão

Este trabalho teve como principal objetivo apresentar uma solução para a criação de ambientes de OVs quando há a necessidade de colaboração em projetos e pesquisas, possibilitando a criação desses ambientes mesmo quando os participantes (instituições e usuários) estão em diferentes federações. O mecanismo de gerência de segurança para OVs provê ainda um mecanismo agregador de atributos capaz de complementar os atributos vindos dos IdPs das federações, de forma a contribuir com a flexibilidade, visto que cada federação pode fazer uso de atributos distintos, a padronização de um conjunto de atributos com base nos atributos advindos dos SPs promove uma maior granularidade das políticas de controle de acesso baseadas em atributos dos serviços colaborativos das OVs. Federações de serviços que adotam o modelo federado, baseadas no padrão SAML, emergiram com grande aceitação nas redes nacionais de ensino e pesquisa (NRENs) e outras redes colaborativas. Porém, outras tecnologias como *OpenID Connect*, *OAuth* e *WS-Federation* também podem ser utilizadas nestes ambientes. Como trabalho futuro, pretende-se estender a solução proposta de forma a contribuir com a interoperabilidade entre os sistemas de gestão de identidades federadas que podem ser utilizados nos administrativos dos membros que compõem uma OV. Ainda como trabalho futuro, pretende-se empregar a solução proposta em um cenário de *e-Science* mais complexo, como por exemplo, uma federação de *testbeds* de experimentação para Internet do Futuro, conhecida como FIBRE (*Future Internet Brazilian Environment for Experimentation* [17]).

[14] http://openstack.org/
[15] https://www.globus.org/
[16] https://technical.edugain.org/
[17] http://fibre.org.br

## Agradecimentos

Os autores agradecem à Rede Nacional de Ensino e Pesquisa (RNP) por disponibilizar o ambiente de experimentação GIdLab que foi essencial para condução dos experimentos e desenvolvimento do protótipo. Este trabalho foi parcialmente financiado pela CAPES[18] através do Programa de Suporte à Pós-Graduação de Instituições de Ensino Particulares (PROSUP).

## Referências

[1] CISCO. *Cisco Visual Networking Index: Forecast and Methodology, 2013–2018*. [S.l.], 2014. Disponível em: <https://www.terena.org/mail-archives/storage/pdfVVqL9tLHLH.pdf>.

[2] HENDRIKX, F.; BUBENDORFER, K. Malleable access rights to establish and enable scientific collaboration. In: *eScience (eScience), 2013 IEEE 9th International Conference on*. [s.n.], 2013. p. 334–341. Disponível em: <https://doi.org/10.1109/eScience.2013.26>.

[3] BROEDER, D. et al. *Federated Identity Management for Research Collaborations*. Geneva, 2012. CERN-OPEN-2012-006. Disponível em: <https://cds.cern.ch/record/1442597>.

[4] SCHROEDER, R. e-sciences as research technologies: reconfiguring disciplines, globalizing knowledge. *Social Science Information*, v. 47, n. 2, p. 131–157, 2008. Disponível em: <http://dx.doi.org/10.1177/0539018408089075>.

[5] CHO, K.; KIM, J.; NAM, S.-h. Collider physics based on e-Science paradigm of experiment–computing–theory. *Computer Physics Communications Special Edition for Conference on Computational Physics Trondheim*, Elsevier, v. 182, p. 1756–1759, September 2011. Disponível em: <https://doi.org/10.1016/j.cpc.2010.12.019>.

[6] ZHANG, H.; WU, W.; LI, Z. Open social based group access control framework for e-science data infrastructure. p. 1–8, Oct 2012. Disponível em: <https://doi.org/10.1109/eScience.2012.6404488>.

[7] GEMMILL, J. et al. Cross-domain authorization for federated virtual organizations using the myvocs collaboration environment. *Concurr. Comput. : Pract. Exper.*, John Wiley and Sons Ltd., Chichester, UK, v. 21, n. 4, p. 509–532, mar. 2009. ISSN 1532-0626. Disponível em: <http://dx.doi.org/10.1002/cpe.v21:4>.

[8] FOSTER, I.; KESSELMAN, C.; TUECKE, S. The anatomy of the grid: Enabling scalable virtual organizations. *The International Journal of High Performance Computing Applications*, v. 15, n. 3, p. 200–222, 2001. Disponível em: <http://dx.doi.org/10.1177/109434200101500302>.

[9] ITU-T. *NGN Identity Management Framework - Recommendation Y.2720*. [S.l.], 2009. Disponível em: <http://www.itu.int/rec/T-REC-Y.2720-200901-I/en>.

[10] JøSANG, A. et al. Trust Requirements in Identity Management. In: *ACSW Frontiers*. Australian Computer Society, 2005. (CRPIT, v. 44), p. 99–108. ISBN 1-920682-26-0. Disponível em: <http://www.bibsonomy.org/bibtex/251946c951612ab5bdad6acb268a9e522/dblp>.

[11] CHADWICK, D. Federated identity management. In: ALDINI, A.; BARTHE, G.; GORRIERI, R. (Ed.). *Foundations of Security Analysis and Design V*. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer Science, v. 5705). p. 96–120. ISBN 978-3-642-03828-0. Disponível em: <http://dx.doi.org/10.1007/978-3-642-03829-7_3>.

[12] BHARGAV-SPANTZEL, A. et al. User centricity: A taxonomy and open issues. *J. Comput. Secur.*, IOS Press, Amsterdam, The Netherlands, The Netherlands, v. 15, n. 5, p. 493–527, out. 2007. ISSN 0926-227X. Disponível em: <http://dl.acm.org/citation.cfm?id=1370624.1370625>.

[18] https://capes.gov.br

[13] CAPUANO, N. et al. Management of virtual organizations. In: DIMITRAKOS, T.; MARTRAT, J.; WESNER, S. (Ed.). *Service Oriented Infrastructures and Cloud Service Platforms for the Enterprise*. Springer Berlin Heidelberg, 2010. p. 49–73. ISBN 978-3-642-04085-6. Disponível em: <http://dx.doi.org/10.1007/978-3-642-04086-3_3>.

[14] SILVA, E. F. et al. Gestão de identidade em redes experimentais para a internet do futuro. In: GIOZZA, J. da Silva Fraga; Jacir Luiz Bordim; RafaTimóteo de S. J. W. F. (Ed.). *Livro de Minicursos do SBRC*. [S.l.]: SBC, 2013. v. 31, p. 165–209.

[15] CABARCOS, P. A. et al. Enabling saml for dynamic identity federation management. In: WOZNIAK, J. et al. (Ed.). *Wireless and Mobile Networking*. Springer Berlin Heidelberg, 2009. (IFIP Advances in Information and Communication Technology, v. 308), p. 173–184. ISBN 978-3-642-03840-2. Disponível em: <http://dx.doi.org/10.1007/978-3-642-03841-9_16>.

[16] PöHN, D.; METZGER, S.; HOMMEL, W. Project GÉANT-TrustBroker – dynamic identity management across federation borders. In: HUIZER, E. (Ed.). *Networking with the World, The 30th Trans European Research and Education Networking Conference, 19-22 May, 2014, Dublin, Ireland, Selected Papers*. TERENA, 2014. ISBN 978-90-77559-24-6. Disponível em: <http://www.terena.org/publications/tnc2014-proceedings/>.

[17] HARDT, M. et al. Combining the x.509 and the saml federated identity management systems. In: PéREZ, G. M. et al. (Ed.). *Recent Trends in Computer Networks and Distributed Systems Security*. Springer Berlin Heidelberg, 2014, (Communications in Computer and Information Science, v. 420). p. 404–415. ISBN 978-3-642-54524-5. Disponível em: <http://dx.doi.org/10.1007/978-3-642-54525-2_36>.

[18] SOUZA, M. C.; SILVA, J. J.; WANGHAM, M. S. Serviço de gerenciamento de organizações virtuais entre federações saml. In: *Workshop de Gestão de Identidade (WGID), Anais do XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg2016)*. [S.l.]: Sociedade Brasileira de Computação, 2016. p. 672–683.

[19] CAMARINHA-MATOS, L. M.; AFSARMANESH, H. The emerging discipline of collaborative networks. In: CAMARINHA-MATOS, L. (Ed.). *Virtual Enterprises and Collaborative Networks*. Springer US, 2004, (IFIP International Federation for Information Processing, v. 149). p. 3–16. ISBN 978-1-4020-8138-5. Disponível em: <http://dx.doi.org/10.1007/1-4020-8139-1_1>.

[20] TAYLOR, J. News from the e-Science Programme, first phase. *Social Science Information*, RCUK website, v. 47, n. 2, p. 131–157, 2001.

[21] VULLINGS, E.; DALZIEL, J.; BUCHHORN, M. Secure federated authentication and authorisation to grid portal applications using saml and xacml. *Journal of Research and Practice in Information Technology*, v. 39, n. 2, p. 101–113, 2007. Cited By 5. Disponível em: <http://www.scopus.com/inward/record.url?eid=2-s2.0-34248391856&partnerID=40&md5=0cc93efd2e49d5e412fc79c6a24769a5>.

[22] OASIS. *Security Assertion Markup Language (SAML)*. v.2. [S.l.], 2008. Disponível em: <https://www.oasis-open.org/standards\#samlv2.0>.

[23] CHADWICK, D. W. et al. Leveraging social networks to gain access to organisational resources. In: *Proceedings of the 7th ACM Workshop on Digital Identity Management*. New York, NY, USA: ACM, 2011. (DIM '11), p. 43–52. ISBN 978-1-4503-1006-2. Disponível em: <http://doi.acm.org/10.1145/2046642.2046653>.

[24] SOUZA, M. C.; MELLO, E. R.; WANGHAM, M. S. Gidlab: Laboratório de experimentação em gestão de identidade. In: *Workshop de Gestão de Identidade (WGID), Anais do XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg2014)*. [S.l.]: Sociedade Brasileira de Computação, 2014. p. 467–468.

[25] GARCIA, A. L.; CASTILLO, E. Fernandez-del; PUEL, M. Identity federation with voms in cloud infrastructures. In: *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*. [s.n.], 2013. v. 1, p. 42–48. Disponível em: <http://dx.doi.org/10.1109/CloudCom.2013.13>.

[26] SILVA, E. F.; FERNANDES, N. C.; MUCHALUAT-SAADE, D. Modelagem do across: Um arcabouço de aa baseado em políticas e atributos para organizações virtuais. In: *Workshop de Gestão de Identidade (WGID), Anais do XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg2015)*. [S.l.]: Sociedade Brasileira de Computação, 2015. p. 1–12.

[27] CHARD, K. et al. Globus nexus: A platform-as-a-service provider of research identity, profile, and group management. *Future Gener. Comput. Syst.*, Elsevier Science Publishers B. V., Amsterdam, The Netherlands, The Netherlands, v. 56, n. C, p. 571–583, mar. 2016. ISSN 0167-739X. Disponível em: <http://dx.doi.org/10.1016/j.future.2015.09.006>.