# Serviço de Gerenciamento de Organizações Virtuais entre Federações SAML

**Maykon Chagas de Souza, Jucélio Jair Silva, Michelle Silva Wangham**

[1]Universidade do Vale do Itajaí – (UNIVALI)

{mchagas,jucelio}@edu.univali.br, wangham@univali.br

***Abstract.*** *Collaborative environments are based on the establishment of virtual organizations (VOs) and have specific rules and policies to allow access to researchers. The use of federated identity model simplifies management identity to the user and provides single sign-on authentication. However, to create VOs that go beyond the barriers of a Federation, it is necessary to establish trust relationship among the domains of different Federations.This work aims to describe a service responsible for (1) providing a trust relationship establishment between the VO providers that are in different SAML federations and (2) supporting the authentication and authorization of VO users.*

***Resumo.*** *Ambientes colaborativos são baseados na formação de organizações virtuais (OVs) e possuem regras e políticas específicas para permitir o acesso dos pesquisadores. O uso do modelo de identidades federadas simplifica para o usuário a gestão de identidades, proporcionando a funcionalidade de autenticação federada e única (SSO). No entanto, para a formação de OVs, que ultrapassam o domínio de uma única Federação, é necessário o estabelecimento de relações de confiança entre os domínios de diferentes Federações. O objetivo deste trabalho é descrever um serviço responsável por (1) prover o estabelecimento das relações de confiança entre os provedores usados em uma OV formada por domínios administrativos que estão em diferentes federações SAML, e (2), contribuir com a autenticação e autorização dos usuários da OV.*

## 1. Introdução

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 [Broeder et al. 2012]. Instituições, normalmente geograficamente distribuídas, se conectam através da Internet e estabelecem relações de confiança entre si para desenvolverem pesquisas colaborativas, pesquisas estas chamadas de *e-science* [Schroeder 2008].

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 uma determinada linha de pesquisa ou projeto [Zhang et al. 2012]. 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) [Gemmill et al. 2009, Foster et al. 2001].

 

Um ponto chave para os ambientes colaborativos das OVs é prover a gestão de identidades (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 [Foster et al. 2001].

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 [ITU-T 2009]. 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) [Jøsang et al. 2005, Chadwick 2009].

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 [Carmody et al. 2005]. A adoção de um modelo de GId federadas, tem por objetivo remover a complexidade do 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 que podem estar em domínios administrativos diferentes [Jøsang et al. 2005, Bhargav-Spantzel et al. 2007].

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 que serão 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. Motivados por essas necessidades, representantes de diferentes instituições têm se organizado para discutir como resolver os desafios relacionados a definição de uma política comum para gestão de identidades nas estruturas, federações e tecnologias existentes com o objetivo de desenvolverem pesquisas colaborativas [Broeder et al. 2012].

Este trabalho tem por objetivo descrever um serviço de gerência de segurança de OVs, que visa auxiliar as etapas do ciclo de vida de uma OV, em especial, que possibilite o estabelecimento das relações de confiança entre provedores que estão em federações SAML distintas e contribua com a autenticação e autorização em ambiente colaborativos. De forma a avaliar a aplicabilidade do serviço proposto, um protótipo foi desenvolvido e um cenário de uma OV foi concebido para os experimentos de avaliação.

Este artigo está organizado em cinco seções. Na Seção 2, são apresentados os conceitos referentes a OVs, *e-science* e gestão de identidades federadas. A solução proposta (serviço de gerência de segurança para OVs) é descrita na Seção 3. Na Seção 4, os trabalhos relacionados são analisados e comparados com o serviço proposto. Por fim, a conclusão e os trabalhos futuros são apresentados na Seção 5.

 

## 2. Organizações Virtuais - OV

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*" [Taylor 2001]. 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 [Schroeder 2008].

A colaboração entre as diferentes disciplinas, áreas de conhecimento, não se aplicam somente às tecnologias mas também às instituições, nas quais as políticas de coordenação dos projetos de *e-science* ultrapassam as fronteiras de países e apresentam obstáculos para o processo, não só técnicos, mas organizacionais [Schroeder 2008]. Estas barreiras incluem políticas restritivas de acesso aos recursos computacionais das *grids* acadêmicas providas por um país, 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 por [Foster et al. 2001] 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. Uma Organização Virtual (OV) é um grupo formado por universidades, empresas e indivíduos que compartilham recursos e conhecimentos para alcançar um objetivo e que atuam por acordos estabelecidos [Foster et al. 2001].

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 [Capuano et al. 2010].

O ciclo de vida de uma OV é um processo composto dos seguintes estágios: (1) **criação**, 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**, 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**, permite uma pequena alteração ou redistribuição de competências entre os membros[1]; e (4) **dissolução**, 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* e o OpenID Connect.

[1]Mudanças em objetivos ou mudanças de muitos parceiros levam a uma nova formação.

 

## 3. Serviço 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), 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. Os IdPs A e C da Federação A, o IdP F da Federação B e os SPs 1 e 2 possuem relações de confiança com o serviço, o que possibilita que os usuários da OV que estão nestes IdPs possam acessar serviços do SP1 e do SP5. 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.

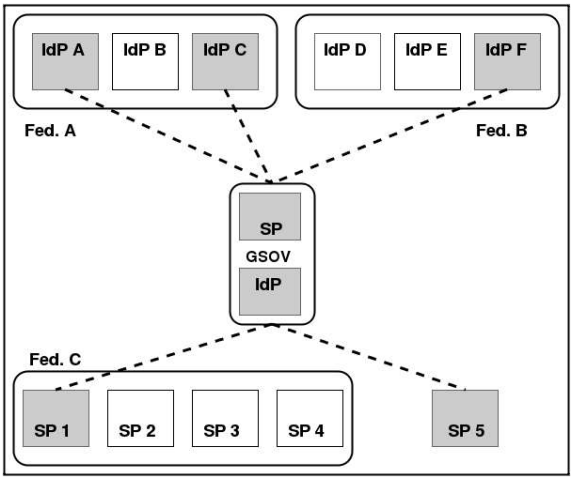


**Figura 1. Visão geral do serviço proposto como Proxy**

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 serviço 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 confianças 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 [Vullings et al. 2007] ou [Gemmill et al. 2009], em que as relações de confiança precisam ser estabelecidas com toda a federação, na solução proposta, o serviço 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 Org. Virtual B apresenta a OV intrafederada e a Org. Virtual A apresenta a OV interfederada. A Figura 3 apresenta o fluxo de mensagens entre os domínios que participam de uma OV (seja intra ou interfederação). A seguir, o fluxo de mensagens entre as entidades é descrito.

No **passo 1** da Figura 3, o usuário, usando um navegador Web, tenta acessar o serviço no SP. O SP redireciona o navegador do usuário para o serviço gerente de segurança (**passo 2**). No **passo 3**, o usuário deve indicar o seu IdP de origem, que deve estar na lista apresentada pelo serviço gerente. No **passo 4**, o navegador do usuário é redirecionado pelo serviço gerente para a página de autenticação do IdP escolhido, que é apresentada para o usuário no **passo 5**. No **passo 6**, após o usuário inserir suas credenciais (usuário e senha), o IdP autentica o usuário e, caso autenticação seja bem sucedida, este gera asserção SAML de atributos (**passo 7**. O IdP envia a resposta de autenticação para o serviço gerente, conforme indicado no **passo 8**. No **passo 9**, o gerente agrega os

 

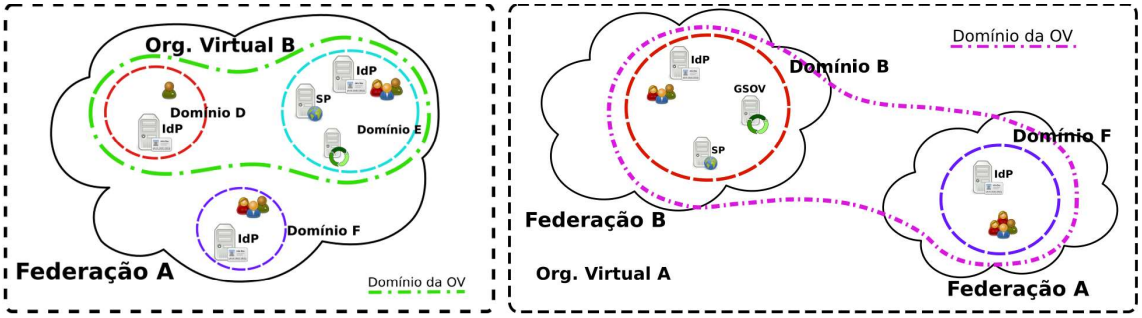


**Figura 2. OV Intrafederada e interfederada**

atributos vindos do IdP com os atributos já registrados no serviço referente ao usuário e apresenta para o usuário estas informações (**passo 10**). No **passo 11**, o usuário confirma a liberação de atributos para SP. No **passo 12**, o serviço envia os atributos resultantes do usuário para o SP e, com base nos atributos do usuário, decide se permite ou não o seu acesso ao serviço **passo 13**.

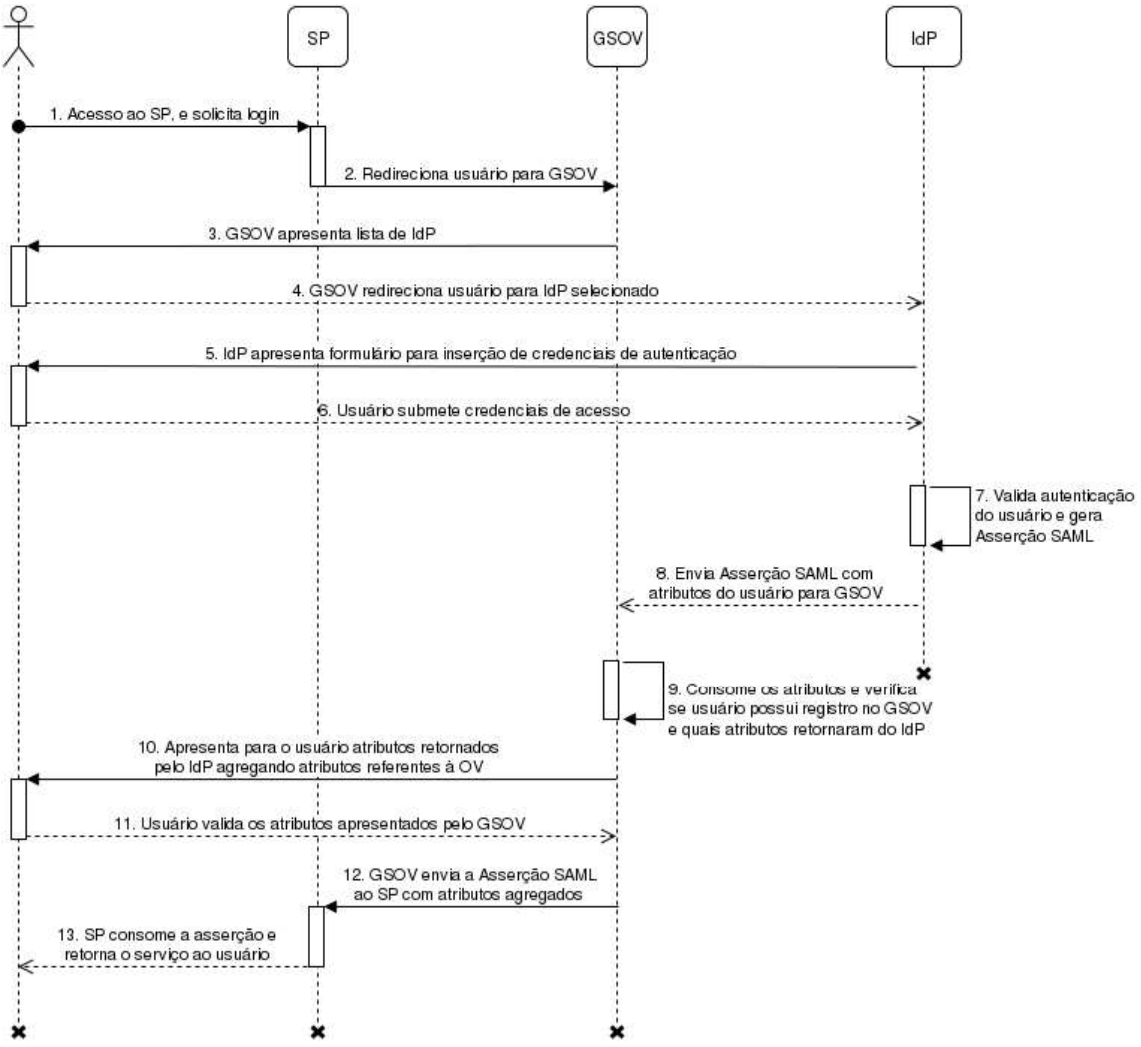


**Figura 3. Diagrama de mensagens de comunicação entre as entidades**

### 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:

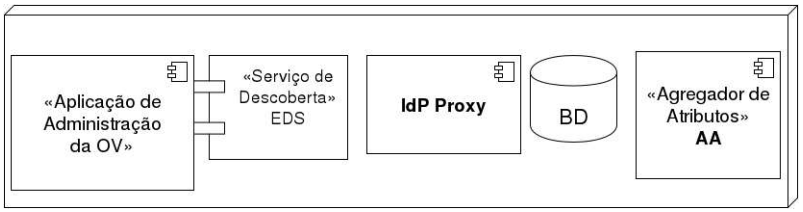


**Figura 4. Componentes do serviço proposto**

- 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 são: 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 [OASIS 2008]. 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.

### 3.2. Agregação de atributos

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 mecanismos agregador de atributos, que é um mecanismo que coleta e une atributos de um usuário provenientes de diferentes provedores de identidades [Chadwick et al. 2011], 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.

 

### 3.3. Implementação e Resultados

De forma a avaliar a aplicabilidade do serviço proposto, uma prova de conceito foi desenvolvida utilizando o o ambiente de experimentação do GIdLab [Souza et al. 2014], com o objetivo de analisar os cenários de OVs intrafederada e interfederada. O serviço gerente de segurança para OVs, que gerencia o ciclo de vida da OV, foi desenvolvido em PHP e utiliza o *framework* SimpleSAMLphp[2] que implementa o protocolo SAML. As funcionalidades implementadas no serviço gerente estão indicadas no diagrama de casos de uso da Figura 5. Para armazenar as informações referentes as instituições, provedores de serviços e atributos agregados dos usuários que formam a OV, foi modelado um banco de dados MySQL para armazenamento.

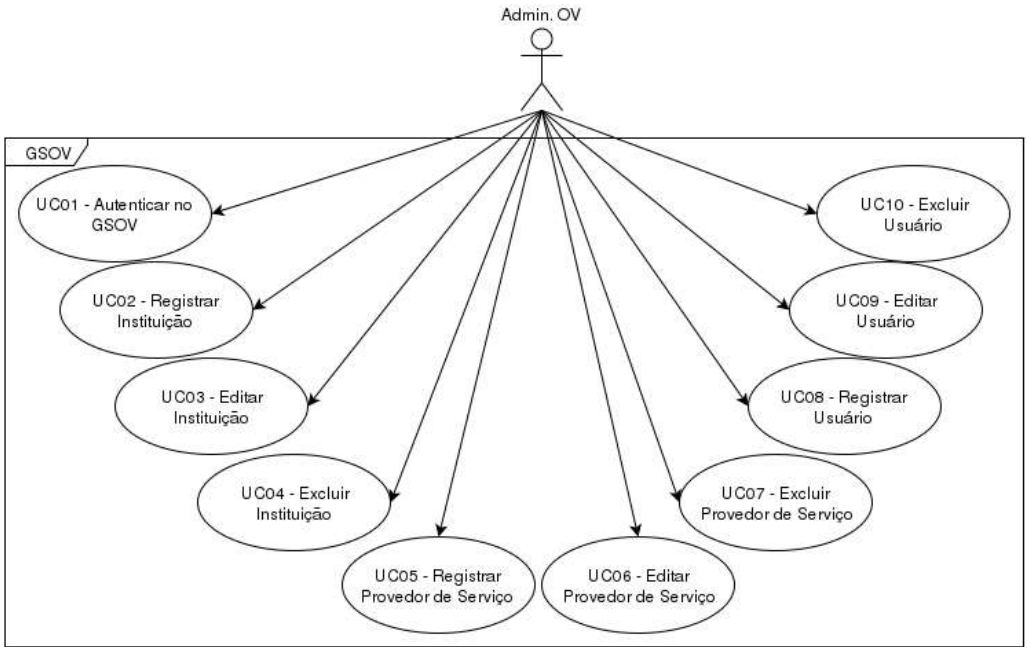


**Figura 5. Casos de uso**

O cenário desenvolvido, ilustrado na Figura 6, é composto por duas Federações. A aplicação colaborativa implantada no SP foi um ambiente de apoio para documentação de projetos (*Wiki*). Utilizou-se a o software MediaWiki que provê a criação destes ambientes. Para realizar autenticação via SAML, foi utilizada a extensão SimpleSAMLphp disponível neste software [3].

Para exemplificar a relação de confiança com IdPs de diferentes domínios administrativos (em diferentes federações), foram implantados três IdPs, utilizando dois *frameworks* distintos. IdPs1 e IdP2 utilizou-se o SimpleSAMLphp e no IdP3 o Shibboleth[4]. Em todos os IdPs foram definidos um conjunto de usuários para realização dos testes. Estes usuários foram armazenados em uma estrutura de diretórios OpenLDAP[5].

Para avaliar a solução do serviço gerente de segurança para organizações virtuais,

[2]https://simplesamlphp.org/
[3]https://www.mediawiki.org/wiki/Extension:SimpleSamlAuth
[4]https://shibboleth.net
[5]http://www.openldap.org/

 

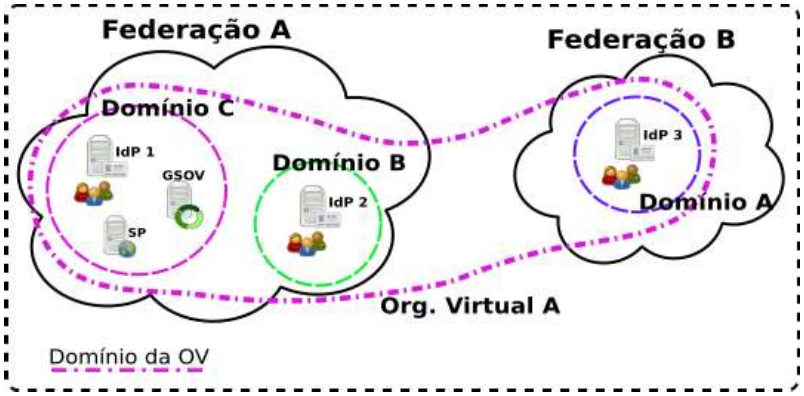


**Figura 6. Cenário da Prova de Conceito**

foram definidos e executados quatro casos de testes, tendo como base os principais casos de uso do serviço ilustrados na Figura 5.

O primeiro caso de testes teve como objetivo verificar a função de autenticação para acesso as funcionalidades de administração de uma OV providas pelo serviço. 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 participante da OV) e dos serviços. Neste 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 participantes 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. 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. Trabalhos relacionados

[Vullings et al. 2007] apresentam uma solução de Infraestrutura de Autenticação e Autorização (IAA) chamada *Identity Access Management Suite*[6], 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.e.: 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.

[Gemmill et al. 2009] apresentam um ambiente chamado myVOCS, que permite a criação e gerenciamento de OVs para ambientes de Grid de forma autônoma e flexível,

[6]Compatível com o portal do ambiente GridSphere `http://www.gridsphere.org/`

 

utilizando autenticação federada através do Shibboleth (SAML). myVOCS é uma alternativa ao uso de soluções como VOMS[7] e PERMIS[8], utilizados para gerenciamento de autorização das OVs. 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 permitindo 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 requisições dos SPs, e como um SP, enviando requisições de autenticação para os IdPs dos usuários. Os autores não descrevem como são estabelecidas as relações de confiança entre os serviços colaborativos e os IdPs (que realizam autenticação dos usuários participantes das OVs).

[Lopez Garcia et al. 2013] utilizam 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[9]. 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. Neste 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 qual OV o usuário participa. Este trabalho não possui um mecanismo para criação e gerenciamento de de OVs.

[SILVA et al. 2015] propuseram o ACROSS (**A**ttribute-based access **C**ont**RO**l and di**S**tributed policie**S**), 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.

[Chard et al. 2016] apresentam a solução *Globus Nexus*, uma *Plaform as a Service* (PaaS) desenvolvida como parte do projeto Globus[10], 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 [Vullings et al. 2007], [Gemmill et al. 2009] [SILVA et al. 2015], 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. Além disso, ao

[7]http://toolkit.globus.org/grid_software/security/voms.php
[8]http://sec.cs.kent.ac.uk/permis/index.shtml
[9]http://openstack.org/
[10]https://www.globus.org/

 

contrários das soluções apresentadas em [Lopez Garcia et al. 2013] e [Chard et al. 2016], focadas em nuvem ou em grids computacionais, respectivamente, a presente solução pode ser empregada em diferentes cenários de OVs para realiza *e-science*.

## 5. Conclusão

Este trabalho teve como objetivo apresentar uma solução para a criação de ambientes de OVs quando há a necessidade de colaboração em projetos e os participantes (instituições e usuários) que estão em diferentes federações SAML. O serviço 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 granularidade e flexibilidade das políticas de controle de acesso baseadas em atributos dos serviços colaborativos das OVs.

Federações de serviços que adotam o modelo federado, baseadas o 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 um cenário que utiliza *testbeds* de experimentação para Internet do Futuro.

## Referências

Bhargav-Spantzel, A., Camenisch, J., Gross, T., e Sommer, D. (2007). User Centric: A Taxonomy and Open Issues . *Journal of Computer Security*, page 493–527.

Broeder, D., Jones, B., Kelsey, D., Kershaw, P., Lüders, S., Lyall, A., Nyrönen, T., Wartel, R., e Weyer, H. J. (2012). Federated Identity Management for Research Collaborations, CERN-OPEN-2012-006. Technical Report CERN-OPEN-2012-006, CERN, Geneva.

Capuano, N., Gaeta, A., Gaeta, M., Orciuoli, F., Brossard, D., e Gusmini, A. (2010). Management of virtual organizations. In Dimitrakos, T., Martrat, J., e Wesner, S., editors, *Service Oriented Infrastructures and Cloud Service Platforms for the Enterprise*, pages 49–73. Springer Berlin Heidelberg.

Carmody, S., Erdos, M., Hazelton, K., Hoehm, W., Morgan, B., Scavo, T., e Wasley, D. (2005). Incommon Technical Requirements and Information. Technical report, Incommon.

Chadwick, D. (2009). Federated identity management. In Aldini, A., Barthe, G., e Gorrieri, R., editors, *Foundations of Security Analysis and Design V*, volume 5705 of *Lecture Notes in Computer Science*, pages 96–120. Springer Berlin Heidelberg.

Chadwick, D. W., Inman, G. L., Siu, K. W., e Ferdous, M. S. (2011). Leveraging social networks to gain access to organisational resources. In *Proceedings of the 7th ACM Workshop on Digital Identity Management*, DIM '11, pages 43–52, New York, NY, USA. ACM.

 

Chard, K., Lidman, M., McCollam, B., Bryan, J., Ananthakrishnan, R., Tuecke, S., e Foster, I. (2016). Globus nexus: A platform-as-a-service provider of research identity, profile, and group management. *Future Gener. Comput. Syst.*, 56(C):571–583.

Foster, I., Kesselman, C., e Tuecke, S. (2001). The anatomy of the grid - enabling scalable virtual organizations. *International Journal of Supercomputer Applications*, 15:2001.

Gemmill, J., Robinson, J.-P., Scavo, T., e Bangalore, P. (2009). Cross-domain authorization for federated virtual organizations using the myvocs collaboration environment. *Concurr. Comput. : Pract. Exper.*, 21(4):509–532.

ITU-T (2009). NGN Identity Management Framework - Recommendation Y.2720. Technical report, ITU-T.

Jøsang, A., Fabre, J., Hay, B., Dalziel, J., e Pope, S. (2005). Trust Requirements in Identity Management. In *ACSW Frontiers*, volume 44 of *CRPIT*, page 99–108. Australian Computer Society.

Lopez Garcia, A., Fernandez-del Castillo, E., e Puel, M. (2013). Identity federation with voms in cloud infrastructures. In *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, volume 1, pages 42–48.

OASIS (2008). Security Assertion Markup Language (SAML). Technical Report Technical Overview, OASIS.

Schroeder, R. (2008). e-Sciences as research technologies: reconfiguring disciplines, globalizing knowledge. *Social Science Information*, 47(2):131–157.

SILVA, E. F., FERNANDES, N. C., e Muchaluat-Saade, D. (2015). 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)*, pages 1–12. Sociedade Brasileira de Computação.

Souza, M. C., Mello, E. R., e Wangham, M. S. (2014). 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)*, page 467–468. Sociedade Brasileira de Computação.

Taylor, J. (2001). News from the e-Science Programme, first phase. *Social Science Information*, 47(2):131–157.

Vullings, E., Dalziel, J., e Buchhorn, M. (2007). Secure federated authentication and authorisation to grid portal applications using saml and xacml. *Journal of Research and Practice in Information Technology*, 39(2):101–113. cited By 5.

Zhang, H., Wu, W., e Li, Z. (2012). Open social based group access control framework for e-science data infrastructure. In *E-Science (e-Science), 2012 IEEE 8th International Conference on*, pages 1–8.

 