Gestão de Identidade em Testbeds de Internet do Futuro baseada em Federações A&A Acadêmicas

Edelberto F. Silva[1], **Natalia C. Fernandes**[1]
Noemi Rodriguez[2] **e Débora Muchaluat-Saade**[1]

[1]Universidade Federal Fluminense (UFF) – Laboratório MídiaCom
Niterói, RJ – Brasil

[2]Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio)
Rio de Janeiro, RJ – Brasil

{edelberto,debora,natalia}@midiacom.uff.br, noemi@inf.puc-rio.br

Abstract. *With current advances in the construction of experimentation environments (testbeds) for Future Internet (FI) a new challenge arises, the identity management on a globally distributed environment. In this context it is necessary to understand the local and federated models of identity management to integrate testbeds. This paper presents the design and implementation of a module for credential translation with objective to enable a user of Academic Community Federated (CAFe) or a federated LDAP tree to access the testbed federation and delegate its credentials too, aiming to increase the security. The proposal generates X.509 certificates and other standard credentials used in the testbeds federation, defined in SFA, based on user attributes obtained from CAFe. The proposed model suports the integration of testbed federations and academic federations. The developed module also allows an attribute-based access control, denying or allowing user access according to his/her attributes obtained from CAFe or a federated LDAP. The study was conducted using a real experimental laboratory (LabGId), in which provides mirrors of the CAFe federation and of the MySlice platforms.*

Resumo. *Com os atuais avanços na criação de ambientes de experimentação para a Internet do Futuro, surge um novo desafio, a gestão de identidade neste ambiente globalmente distribuído. É necessário entender a gestão de identidade tanto local quanto no modelo federado de integração dos testbeds. Este trabalho apresenta a transposição da identidade do usuário da federação de Internet do Futuro a partir de identidades da Comunidade Acadêmica Federada (CAFe) ou de uma árvore de diretórios LDAP federada e também a delegação de credenciais a fim de aumentar a segurança para o usuário no ambiente. Neste trabalho são gerados certificados X.509 e as demais credenciais utilizadas na federação de testbeds, definidas no padrão SFA, baseando-se nos atributos do usuário obtidos tanto pela CAFe quanto pelo LDAP federado, permitindo que as federações de testbed sejam integradas às federações de identidades acadêmicas. A solução de transposição de credenciais permite, ainda, um controle de acesso baseado em atributos, de tal forma que é possível bloquear ou permitir o acesso de acordo com algumas características do usuário obtidos com a CAFe. O trabalho foi desenvolvido usando um laboratório de experimentação real (LabGId) com um espelho da federação CAFe e a plataforma de gerência de alocação de recursos federada MySlice.*

1. Introdução

A gestão de identidade (GId), do inglês *Identity Management* (IdM), é descrita como o conjunto de processos e tecnologias usados para garantir a identidade de uma

entidade, assegurar a qualidade das informações de identidade (*i.e.* identificadores, credenciais e atributos) e utilizar tais garantias como entrada para processos relacionados à autenticação, autorização e auditoria [ITU-T 2009, Buell and Sandhu 2003]. Descreve-se um procedimento de autenticação como aquele relacionado à confirmação da identidade de uma entidade, isto é, à verificação de que uma entidade é quem ela afirma ser. Já mecanismos de autorização definem os direitos de acesso a recursos associados a uma identidade já determinada. Procedimentos de autorização são utilizados tanto para descrever esses direitos de acesso como para garantir que eles sejam cumpridos. Finalmente, auditoria se refere aos processos que permitem verificar o funcionamento correto dos procedimentos anteriores. GId é fundamental para gestão de sistemas com muitos usuários, tais como sistemas acadêmicos, sistemas de governança, sistemas de segurança, sistemas de comunicação, entre outros.

A comunidade acadêmica vem utilizando identidades federadas como uma forma de regular o acesso a recursos disponíveis com diversas finalidades. Um exemplo importante é o controle de acesso a repositórios de periódicos[1], que evita a necessidade de duplicação de informações e de bases de dados em instituições diferentes. No entanto, pode haver recursos aos quais se deseja que o acesso seja autorizado apenas a um grupo limitado de membros, que por sua vez podem pertencer a instituições distintas. Esses grupos são conhecidos como organizações virtuais (OV) [Foster et al. 2001, Silva et al. 2013c] e apresentam características particulares como a necessidade de políticas de autorização específicas para regular o acesso.

Dentre os serviços que podem ser acessados por meio de uma federação acadêmica, destaca-se um novo serviço promissor para a comunidade acadêmica, as redes experimentais para a Internet do Futuro (IF) [Silva et al. 2013a]. Uma vez conhecidas as limitações da arquitetura atual da Internet, um grande movimento com relação à pesquisa e à proposta de novas arquiteturas surgiu em todo o mundo. Essa nova área de pesquisa visa a criação de uma nova Internet, a Internet do Futuro [Moreira et al. 2009], e deverá ser avaliada em ambientes experimentais antes de efetivamente poder ser utilizada em produção. Para tanto, vários *testbeds* têm sido criados nos últimos anos[2][Jeong and Bavier 2010][Falk 2011]. A necessidade de interconexão dos ambientes de experimentação para avaliação dessas novas arquiteturas permite que pesquisadores de diferentes instituições possam utilizar, em seus experimentos, recursos de rede que são administrados por organizações distintas. A compatibilização dos mecanismos de controle de acesso dos diferentes ambientes e a adaptação de técnicas de identidade federada para os requisitos desse ambiente constituem um caso interessante de organização virtual.

Uma recente iniciativa para a criação de *testbeds* no Brasil é o Projeto FIBRE (*Future Internet testbeds experimentation between BRazil and Europe*)[3] [Sallent et al. 2012]. O FIBRE tem como proposta a construção de uma rede para experimentação de larga escala, a qual inclui ambientes cabeados e sem fio, através da interligação de ilhas em diversos pontos do Brasil e da Europa. Assim, além de construir novos *testbeds*, ou ilhas, o FIBRE também é fortemente embasado na construção de um ambiente federado [Fernandes et al. 2013].

Este trabalho é motivado pela heterogeneidade encontrada dentro do ambiente de experimentação para a IF. São tratados os problemas de comunicação entre diversos softwares de gerência da federação de experimentação e suas bases de dados, assim como a integração da federação acadêmica com este ambiente a partir da transposição de credenciais.

[1] Periódicos CAPES: http://www.periodicos.capes.gov.br/ [2] http://cordis.europa.eu/fp7/ict/fire/ , http://www.geni.net [3] http://www.fibre-ict.eu/

Abordando o problema da integração de uma federação acadêmica de identidade a uma federação de recursos para experimentação de redes, onde podemos tratar o conjunto de usuários/experimentadores, membros da comunidade acadêmica, como integrantes de uma OV, focando no contexto de A&A (Autenticação e Autorização). Esta organização virtual engloba um grupo de pesquisadores que desejam realizar experimentos compartilhados entre instituições geograficamente dispersas para a construção de uma nova solução em tecnologia de escala global, devendo assim estabelecer acordos entre as instituições parceiras para alcançar este objetivo. Neste cenário, a GId aparece como um forte requisito para o estabelecimento de confiança entre os participantes desse grupo. Existe, neste ambiente, a intenção do compartilhamento de ferramentas e recursos de redes experimentais com base na confiança mútua onde os participantes motivam-se a partir de objetivos comuns, conceitos que fortalecem a intenção de criação de uma federação.

Este trabalho propõe a transposição da identidade do usuário de uma federação de Internet do Futuro a partir de sua identidade da Comunidade Acadêmica Federada (CAFe) ou, no caso de usuários de instituições que não participam da CAFe, de uma base de diretórios LDAP (*Lightweight Directory Access Protocol*) [Group 2006] federada. O artigo também propõe a delegação de credenciais a fim de aumentar a segurança para o usuário no ambiente. São gerados certificados X.509 e as demais credenciais utilizadas na federação de testbeds, definidas seguindo o padrão SFA (*Slice-based Federation Architecture*) [Peterson et al. 2010], baseando-se nos atributos do usuário obtidos tanto pela CAFe quanto pelo LDAP federado, permitindo que as federações de testbed sejam integradas às federações de identidades acadêmicas. A solução de transposição de credenciais permite, ainda, um controle de acesso baseado em atributos, de tal forma que seja possível bloquear ou permitir o acesso de acordo com alguns atributos do usuário obtidos com a CAFe. O trabalho foi desenvolvido usando um laboratório de experimentação real (LabGId) com um espelho da federação CAFe e a plataforma de gerência de alocação de recursos federada MySlice [4].

O restante do artigo encontra-se organizado da seguinte forma. A Seção 2 comenta alguns trabalhos relacionados. A Seção 3 apresenta o embasamento teórico para a compreensão das tecnologias utilizadas neste trabalho. A Seção 4 descreve a proposta deste trabalho e a Seção 5 expõe os resultados. Na Seção 6, são apresentas as considerações finais.

2. Trabalhos Relacionados

Quando se observam as pesquisas que abordam os esforços para a transposição de credenciais, destacam-se os ambientes de federação em Grid. Geralmente nesse ambiente é necessário acessar os recursos utilizando credenciais no formato de certificados X.509, o que exige que credenciais advindas de outros formatos sejam traduzidas (ou transpostas) para tal.

Pode-se destacar diversos trabalhos dentro do cenário de grids, como projetos apoiados pelo JISC (*Joint Information Systems Committee*)[5], como o ShibGrid, SHEBANGS (*Shibboleth Enabled Bridge to Access the National Grid Service*) e SARoNGS (*Shibboleth Access to Resources on the NGS*), além de projetos apoiados pela NSF (*National Science Foundation*)[6], como o ShibGrid, CILogon e o go.teragrid [Spence et al. 2006, Barton et al. 2006]. Assim como a proposta apresentada por este trabalho, os projetos citados realizam a transposição de credenciais advindas de um provedor de identidade pertencente a uma federação e o traduzem para um formato específico para acesso ao ambiente de Grid.

[4] http://www.myslice.info [5] http://www.jisc.ac.uk/ [6] http://www.nsf.gov/

Os trabalhos citados utilizam Shibboleth como comunicação entre a instituição e o serviço, e a partir das credenciais do usuário recebidas realizam a sua transposição para o ambiente de Grid, o que geralmente é representado por certificados X.509. No presente trabalho, além da utilização do Shibboleth foi inserida outra fonte de credenciais de usuários, como será visto mais à frente, na intenção de generalizar nossa proposta quanto à origem dos atributos do usuário.

Como ilustração, vamos destacar os trabalhos de ShibGrid [Spence et al. 2006] e SHEBANGS [Wang et al. 2009]. Desenvolvidos especialmente para o NGS (*UK National Grid Service*), sua infraestrutura é baseada em certificados X.509 e uma base para armazenamento dos certificados. Essa base funciona como um proxy na comunicação entre o usuário e o serviço e é chamado de MyProxy [Basney et al. 2005]. No caso do SHEBANGS, o usuário, após se autenticar via Shibboleth, tem seus atributos recebidos pelo serviço de transposição de credenciais que gera e armazena o certificado X.509 no MyProxy. Já o ShibGrid, utiliza o MyProxy para associar uma identidade advinda do Shibboleth com um certificado X.509 já existente, a partir do DN (*Distinguished Name*) do certificado do usuário, realizando assim uma associação da credencial do usuário Shibboleth com um certificado X.509 a cada autenticação. Na solução proposta por este trabalho, não há a utilização de proxies e sim uma ferramenta de administração de recursos federada (MySlice) que realiza tanto a gerência dos recursos como a transposição das credenciais. Acreditamos assim que todo o processo ganhe mais liberdade com relação ao controle de acesso e apresente uma maior agilidade na transposição.

A delegação de credenciais é muitas vezes necessária quando um gerenciador de recursos precisa agir como intermediário em alguma ação do usuário (do inglês *behalf*). Por exemplo, para a alocação de recursos em uma rede de experimentação utilizando o gerenciador MySlice, ele necessitará agir como intermediário entre o usuário e o recurso. Sendo assim, em nossa solução veremos que é necessário ter as credenciais do usuário armazenadas (chave pública e privada) no próprio serviço ou receber a delegação de cada uma de suas credenciais.

Para a delegação de credenciais há vários trabalhos também em Grid, como caGrid[7] e no âmbito do projeto Globus[8]. Vamos destacar o projeto Globus, onde a delegação de credenciais é realizada pelo intermédio de um proxy que, a partir de uma conexão SSL entre o usuário e o serviço, gera um par de chaves temporário e um certificado de proxy para este usuário, que é assinado pelo próprio proxy e devolvido ao usuário. Assim que o usuário o recebe, ele assina o mesmo certificado com sua chave privada e devolve ao proxy, funcionando como uma delegação de sua credencial. Já no trabalho apresentado neste artigo seguem-se as recomendações do SFA (*Slice-based Federation Architecture*) – que veremos com um pouco mais de detalhes nas próximas seções – para a delegação de credenciais, onde o usuário localmente assina suas credenciais delegando-as a uma outra entidade na rede, em nosso caso a ferramenta MySlice. A identificação dos pares envolvidos nessa ação é feita a partir do identificador único na federação de recursos, chamado de GID (*Global Identifier*).

Apesar deste trabalho abordar um ambiente similar ao de transposição de credenciais para Grid, ele apresenta suas particularidades que serão observadas ao longo deste texto, como as diferenças no modelo de credenciais gerado e nos atributos no contexto acadêmico de experimentação para a IF. Apesar de esforços em grupos de desenvolvimento para a Internet do Futuro, como o GENI (*Global Environment for Network Innovations*), para a transposição de credenciais de usuários advindos de comunidades acadêmicas [Mitchell 2011, Mitchell 2010], a trabalho aqui apresentado é o único na lite-

[7] http://www.cagrid.org/display/cds/Home [8] http://toolkit.globus.org/

ratura que apresenta uma arquitetura de forma clara tanto para a transposição de credenciais quanto para a delegação de credenciais para este ambiente.

3. Embasamento Teórico

3.1. FIBRE

O FIBRE (*Future Internet experimentation between BRazil and Europe*) [Sallent et al. 2012] é uma parceria entre instituições brasileiras e europeias com o fim de criar um *testbed* de larga escala. Topologicamente, o FIBRE pode ser visto como a união de uma grande ilha europeia e uma grande ilha brasileira. A ilha brasileira, chamada de FIBRE-BR, consiste da federação de diversas pequenas ilhas, situadas em diferentes universidades e centros de pesquisa. A interligação dessas ilhas é feita através do uso do *backbone* da RNP e de outras redes de pesquisa, como a GIGA e a Kyatera.

No FIBRE existem diversos arcabouços de controle de experimentação como, por exemplos, para ilhas OpenFlow [McKeown et al. 2008] o experimentador usa o arcabouço *OFELIA Control Framework* (OCF) [Köpsel and Woesner 2011] e para equipamentos sem fio o *cOntrol and Management Framework* (OMF) [Rakotoarivelo et al. 2010]. Esses arcabouços são responsáveis pela gerência de recursos entre o experimentador e as ilhas. A heterogeneidade das ilhas cria a necessidade de uma solução de interligação entre as ilhas, sendo assim foi adotado um portal único para a autenticação e reserva de recursos e monitoramento, o portal MySlice. Além disso, utiliza-se uma interface para o compartilhamento de recursos, o SFA [Peterson et al. 2010], que será apresentada mais a frente.

3.2. SFA

Com o intuito de padronizar a comunicação entre arcabouços e a federação de experimentação em IF surgiu o SFA (*Slice-based Federation Architecture*) [Peterson et al. 2010]. Uma vez que os projetos de IF representam a união de diversos *testbeds*, cada um com seu arcabouço de controle específico se faz necessária a padronização da comunicação entre esses arcabouços. É neste momento que surge a proposta do SFA.

Inicialmente desenvolvido para ser empregado no PlanetLab, Emulab, VINI [Bavier et al. 2006] e GENI, o SFA também pode ser expandido a outros *testbeds*. No SFA, cada entidade do sistema possui um identificador global (*Global Identifier* - GID), o qual é usado para autenticação e autorização. Especificamente, o GID é um certificado que contém três campos: uma chave pública, um UUID (*Universally Unique Identifier*) e uma validade. O GID é assinado por uma autoridade, de forma a validar as informações, gerando um certificado X.509.

Após a autenticação, o usuário pode requisitar suas credenciais SFA junto ao sistema de autorização. As credenciais SFA descrevem os direitos e privilégios de um determinado usuário e são utilizadas para a obtenção de Tickets, que dão acesso ao uso de recursos específicos dentro do *testbed*. De forma geral, pode-se descrever as credenciais e os tickets como arquivos XML assinados. Assim como na autenticação do ProtoGENI, o SFA utiliza o conceito de uma rede de confiança (*web of trust*). Ou seja, cada ilha tem os certificados raiz de todas as outras ilhas participantes da federação, de forma que os membros da federação confiem uns nos outros.

3.3. Shibboleth e CAFe

O projeto Shibboleth [Scavo 2005], uma iniciativa do consórcio americano Internet2 [9], desenvolveu um software livre que dá suporte à criação de federações de

[9] http://www.internet2.edu/

autenticação e autorização. O software Shibboleth implementa boa parte do SAML (*Security Assertion Markup Language*) [OASIS 2005], além de oferecer suporte às aplicações web para que usufruam das facilidades providas pelo modelo de identidades federadas, como o conceito de autenticação única (SSO - *Single Sign On*), essa solução também segue o princípio da privacidade dos atributos. Este princípio visa a troca segura de atributos dos usuários por todos provedores de serviços que compõem a federação. Neste contexto, os atributos dos usuários são liberados para os provedores de serviços, respeitando a política de privacidade da instituição de origem do usuário e também suas preferências pessoais.

No SAML há duas entidades principais, os provedores de identidade (IdP – *Identity Provider*), responsáveis pela manutenção e fornecimento das informações sobre usuários e por sua autenticação e provedores de serviço (SP – *Service Provider*), responsáveis por um ou mais serviços (ou recursos) oferecidos.

Já a CAFe (Comunidade Acadêmica Federada) é uma federação baseada em Shibboleth que reúne instituições de ensino e pesquisa brasileiras. Através da CAFe, um usuário mantém todas as suas informações na instituição de origem e pode acessar serviços oferecidos pelas instituições que participam da federação, por meio de SSO. O serviço CAFe[10], iniciado como um projeto da RNP em 2007, une várias instituições de ensino e pesquisa brasileiras[11] em uma rede de confiança.

3.4. MySlice

O MySlice tem se destacado como ferramenta de gerência de experimentos dentre as iniciativas propostas nos diversos âmbitos de grupos de trabalho de IF. Essa ferramenta será utilizada no contexto do FIBRE e, por isso, é usada na implementação da proposta deste artigo para integração de federação de identidade e gerência de *testbeds*.

Surgindo no âmbito do projeto OneLab2 de *testbed* de IF[12], o MySlice evoluiu, suportando o SFA como padrão de comunicação federada para a gestão de recursos em *testbeds*. Essa solução foi iniciada pelos projetos europeus FIRE e NOVI, e por suportar a comunicação baseada em SFA é um dos mais fortes candidatos a ser o principal gerenciador visual para os experimentadores de IF. Outro ponto de suma relevância do MySlice é sua plataforma ser baseada na web, diferentemente das ferramentas anteriores para administração do SFA, como o SFACE [Silva et al. 2013a].

No MySlice, há um passo adicional no qual o usuário deve realizar o envio, em uma área específica do portal, de seu par de chaves para a geração dos certificados SFA (certificados do tipo X.509). Um certificado SFA é necessário para cada recurso que o usuário deseja utilizar, e o envio ou manutenção do par de chaves do usuário no MySlice permite com que o portal aja como intermediário (*behalf*) do usuário no processo de busca e alocação de recursos nos *testbeds*. Este mesmo processo, apesar de crítico, uma vez que armazena a chave privada do usuário na base de dados da ferramenta, vem sendo adotado por outras federações de IF, como é o caso do GENI[13] e do ProtoGENI[14]. Para que esta vulnerabilidade possa ser eliminada, é necessário que o usuário obtenha as credenciais de cada recurso por meio de uma ferramenta externa à interface gráfica do MySlice e delegue suas credenciais, também "por fora" da interface do MySlice. Essa delegação de credenciais deve ser realizada a cada vez que um novo recurso é criado e também quando as credenciais dos recursos existentes expiram, geralmente credenciais de recursos têm um tempo curto, necessário apenas para a realização dos experimentos em questão. Neste trabalho chamamos tal delegação de CDM (*Credential Delegation Module*)

[10] http://portal.rnp.br/web/servicos/cafe [11] http://portal.rnp.br/web/servicos/instituicoes-clientes
[12] http://www.onelab.eu/ [13] https://portal.geni.net/ [14] http://www.protogeni.net/wiki/FlackManual

4. Descrição da Proposta

Esta proposta realiza a integração entre a federação de *testbeds* para a alocação de recursos, chamada SFA [Peterson et al. 2010], através da ferramenta de gerência de experimentos MySlice[15], com a federação acadêmica brasileira CAFe, através da implementação do padrão SAML [OASIS 2005] Shibboleth [Scavo 2005]. No âmbito do projeto FIBRE, nem todos os usuários participam da federação CAFe, por isso também são utilizadas bases LDAP federadas tanto no Brasil quanto na União Européia. Este trabalho também permite o uso de ambas as bases LDAP independentes para autenticação de usuários através do MySlice, facilitando assim a adesão de mais usuários experimentadores. A comunicação entre as diversas fontes de credenciais e a transposição de credencias realizada com intermédio do MySlice pode ser vista na Figura 1.

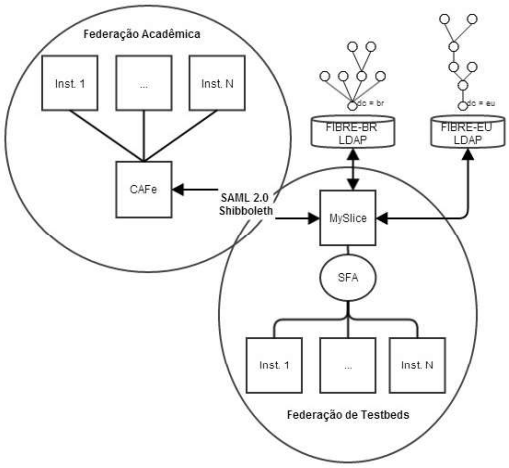

Figura 1. Esquema da proposta de união entre federações.

No contexto deste trabalho, temos os IdPs, associados às universidades e centros de pesquisa participantes da federação, e os SPs, sendo representados pelos gerenciadores de experimentos, onde o usuário deve fornecer suas credenciais e obter autorização de acesso a fim de utilizar algum recurso a ele associado. Como exemplo, pode-se imaginar o envio de uma requisição de alocação de recursos feita por um usuário/experimentador a uma instituição parceira para a disponibilização de um certo número de computadores e uma quantidade mínima de banda. Na implementação da presente proposta, o SP, que é responsável por alocar recursos, autenticar e autorizar usuários, é representado pela ferramenta web de gerência MySlice, utilizada pelo usuário experimentador para acesso aos *testbeds* da federação SFA.

A proposta deste trabalho é que, por meio da interface MySlice de gerenciamento da federação de experimentação, seja possível realizar a vinculação da rede de testes com a federação de identidade CAFe, utilizando a transposição de credenciais. Uma motivação inicial para o desenvolvimento da arquitetura apresentada nesse trabalho foi descrita em [Silva et al. 2013b]. No trabalho inicial, foram apresentados os principais requisitos para a construção de uma arquitetura de integração da gestão de identidades com a federação de testbeds. Contudo, o modelo era em alto nível e não discutia questões práticas. Dentre os principais avanços do presente trabalho, tem-se a apresentação da arquitetura completa da solução de autenticação, além da implementação e testes práticos do modelo proposto dentro do contexto do Projeto FIBRE. Além disso, neste trabalho é proposta a criação de um módulo específico para a comunicação entre as federações,

[15] http://www.myslice.info

o que permite testes de validação da solução; é utilizada a nova versão da ferramenta MySlice, baseada em Django; são integrados outros tipos de bases de usuários ao modelo de identificação e autenticação; e ainda é realizada a aplicação do conceito de ABAC (*Attribute-Based Access Control*) em um ambiente real de experimentação.

Todo o desenvolvimento da proposta foi realizado respeitando o modelo MVC (*Model View Controller*) do Django, o que permitiu uma independência do código com relação às demais funcionalidades da ferramenta MySlice. O processo de autenticação de um usuário do MySlice através da CAFe é realizado por um novo módulo proposto, denominado Módulo de Transposição de Credenciais (*Credential Translations Module* – CTM) e este é totalmente independente dos outros métodos de autenticação já suportados pelo sistema, que continuam funcionando e não sofreram quaisquer alterações. Há também o CDM (*Credential Delegation Module*) que é responsável por realizar a delegação das credenciais de usuário por meio de linha de comando. O CDM surge para tratar o ponto de vulnerabilidade com relação ao armazenamento da chave privada do usuário no MySlice, permitindo que o usuário tenha uma maior confiabilidade nas credenciais utilizadas pelo intermediário MySlice, uma vez que as credenciais utilizadas por este em nome do usuário foram apenas delegadas e geradas localmente pelo usuário.

O ambiente como um todo se divide, basicamente, em 4 (quatro) entidades, como pode ser visto pela Figura 2. São elas: a interface com o usuário (MySlice) com sua base de usuários (SQLite – Django DB), a Federação CAFe (Com o DS – *Discovery Service* – e o IdP com sua base de usuários LDAP), a ferramenta de comunicação com a federação de testbeds de IF (Manifold) com sua base de usuários (SQLite – Manifold DB) e o próprio testbed (representado pelo Dummy PlanetLab) e sua base de usuários chamada de Registry (PostgreSQL).

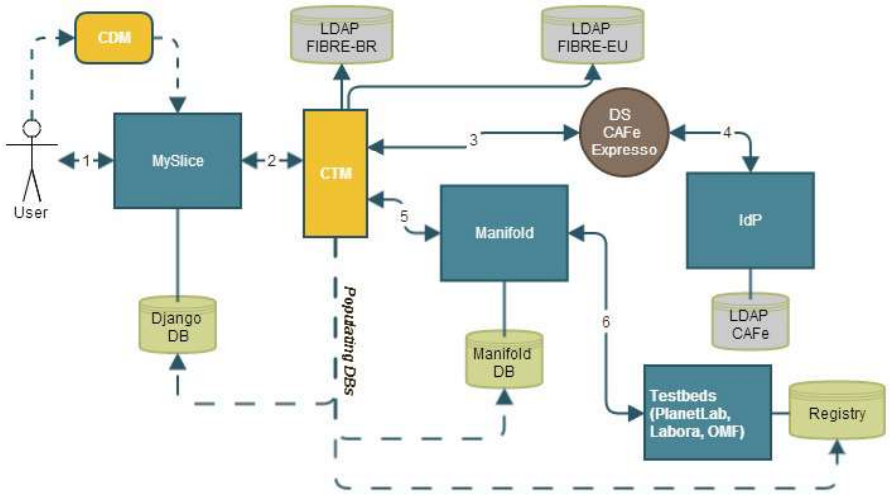

Figura 2. Comunicação entre as entidades envolvidas.

A base de usuários do MySlice é exigida apenas para se manter um vínculo de sessão ativa entre o Manifold e o Django. Isso ocorre porque a implementação inicial da ferramenta tomou como base utilizar o processo de autenticação padrão do Django, estendendo-o apenas, e uma das primitivas desta funcionalidade é manter uma base de usuários para associá-los a uma sessão ativa. Já a base de dados de usuários do Manifold mantém todos os dados referentes ao usuário, como HRN (*Human Readable Name*), par de chaves (caso existam), *testbeds* aos quais ele está vinculado, *slices* etc. A base de usuários do Manifold, portanto, é basicamente uma referência dentro do sistema MyS-

lice/Manifold com os testbeds da federação de IF, já que a federação de IF mantém uma base com dados muito parecidos aos armazenados no Manifold, a chamada Registry. Essa base contém todos os dados do usuário, recursos dos *testbeds* e ainda os vínculos e permissões de cada usuário dentro do contexto daquele *testbed*.

Como se pode perceber, é necessária uma interação entre todas as bases de usuários, desde a CAFe até o Registry. Na proposta, foi necessário, além de tratar os atributos de identidade originários da CAFe, manter todas as bases de dados componentes do ambiente federado de experimentação sincronizadas, cada qual com seu formato particular.

Destaca-se que existem outros esforços no contexto de SFA e GENI para o desenvolvimento de ferramentas para a realização da autenticação e do controle de acesso através do uso do Shibboleth [Mitchell 2011, Mitchell 2010]. Porém, até o momento, não foi encontrada nenhuma ferramenta final disponível à comunidade. Sendo assim, este trabalho, além de ser integrado como mecanismo de identificação e autenticação do projeto FIBRE, pode ser estendido a todas as demais iniciativas de pesquisas em IF que essas utilizem o Shibboleth para autenticação e controle de acesso.

5. Detalhamento e Validação da Implementação da Proposta

Todos os resultados foram obtidos a partir da utilização de um ambiente real criado pela RNP, chamado de Laboratório de Gestão de Identidade (LabGId)[16]. O LabGId permite que sejam utilizadas máquinas virtuais (VM) para a criação das federações, tanto a federação de identidade acadêmica baseada na CAFe quanto a federação de *testbeds* para a experimentação em IF. Neste ambiente, foram criadas VMs para cada um dos serviços exibidos na Figura 2, ou seja, uma VM para o MySlice e Manifold, outra para os arcabouços de controle do PlanetLab, OMF e Labora, além de duas outras responsáveis pelo DS (*Discovery Service*) da federação acadêmica e um IdP. Devemos destacar que o LabGId disponibiliza a CAFe Expresso, que apresenta a mesma estrutura que a federação CAFe oficial, proporcionando assim maior credibilidade à implementação da proposta deste trabalho.

Como dito, o CTM, proposto neste artigo, é o módulo responsável por toda a interação com o usuário/experimentador e, sendo assim, realiza desde o redirecionamento desse usuário para a interface da CAFe e a coleta dos atributos até o tratamento necessário à autenticação e autorização. Conforme cada situação, o usuário sofrerá uma ação do sistema, podendo se autenticar normalmente, ter o acesso negado ou ainda ser automaticamente cadastrado.

Tomando como referência a Figura 2 para a descrição dos passos de autenticação de um usuário, temos que inicialmente (1) o usuário/experimentador irá selecionar a opção de autenticação utilizando a CAFe, a partir do botão exibido na Figura 3(a). Após este passo, ele será redirecionado para o WAYF (*Where Are You From*) da federação acadêmica (3), onde deverá selecionar a sua instituição. Uma vez selecionada sua instituição, ele deverá autenticar-se no seu IdP (4). Considerando que este usuário obteve sucesso em sua autenticação, o seu acesso será permitido ao portal MySlice assim como recursos da federação de *testbeds* serão listados conforme os passos (5) e (6).

Sempre que o usuário inicia o processo de autenticação pela CAFe a partir do CTM, assim que sua credencial é obtida, o CTM consulta, por meio do módulo de autenticação, as bases do MySlice e Manifold. As situações previstas pelo CTM atualmente são: **(I)** Usuário CAFe já existe na base do MySlice e é automaticamente autenticado no sistema; **(II)** Usuário CAFe não tem permissão para acessar o MySlice e **(III)**

[16] Devemos destacar também que a proposta aqui apresentada já se encontra em fase de testes no projeto FIBRE.

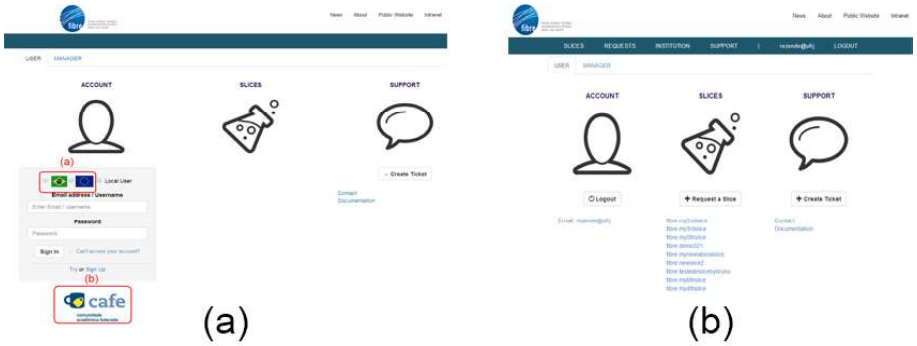

Figura 3. (a) Opção de autenticação utilizando a CAFe. (b) Usuário autenticado no MySlice com listagem de recursos (*slices*).

Usuário CAFe não existe na base do MySlice mas tem permissão. Nesse último caso, sua conta é automaticamente criada na plataforma do MySlice.

Para a situação **(I)**, temos a autenticação de forma transparente para um usuário CAFe previamente cadastrado no MySlice. Já para a situação **(II)**, temos a negação de acesso conforme os atributos do usuário (ABAC). Atualmente levamos em consideração apenas o atributo *affiliation="student"* obtido através da CAFe para a tomada de decisão. Para qualquer valor diferente disto, o acesso ao sistema é negado. Futuramente o mecanismo de controle de acesso baseado em atributos será estendido para levar em consideração outras informações do usuário/experimentador.

Já para **(III)**, o CTM requisita a criação de uma entrada para este usuário em todas as bases (MySlice, Manifold e Registry/SFA), autenticando-o automaticamente no portal e associando a ele um HRN (*Human Readable Name*), gerando automaticamente seu par de chaves através ou importando a chave pública do usuário a partir de seus atributos vindos do IdP.

Como mencionado anteriormente neste trabalho, atualmente temos a geração das credenciais dentro do ambiente da federação de *testbeds* sendo realizada pelo MySlice/Manifold, onde este age como intermediário entre o usuário/experimentador e a federação de recursos (SFA). Para tanto, armazena-se o par de chaves gerado para o usuário no banco de dados do Manifold. Como sabemos que isso é uma vulnerabilidade, temos a geração de credenciais delegadas na máquina do usuário a partir do terminal *bash* utilizando o CDM, porém desejamos ainda criar uma interface mais amigável que a linha de comando para essa delegação.

6. Considerações Finais

Este trabalho teve como motivação a necessidade de interconexão de ambientes de experimentação para a Internet do Futuro. Neste contexto, as chamadas federações de autenticação e autorização podem ser utilizadas para facilitar o uso compartilhado dos recursos por pesquisadores de diferentes instituições. Sendo assim, neste trabalho foram apresentadas a proposta e a implementação de integração destas duas federações, facilitando a integração da academia ao ambiente de experimentação para a Internet do Futuro.

Entre os objetivos alcançados, foram observados os principais requisitos para integrar a federação de testbeds com a federação de identidades, em nosso caso a CAFe. Incorporamos também a possibilidade de autenticação via bases LDAP federadas, demonstrando a liberdade quanto a origem das credenciais do usuário. Foi estudada a arquitetura

de novas ferramentas para a federação de testbeds, como o SFA e o MySlice, observando como a arquitetura do sistema integrado pode ser melhorada em termos de praticidade, eficiência e segurança. O modelo proposto foi implementado e testado, verificando-se suas funcionalidades, em especial ao que tange à autenticação e ao controle de acesso. Outra vantagem do modelo proposto é que, além de integrar o Shibboleth à federação de redes de teste, ele também permite outras formas de autenticação, de forma a manter compatibilidade com as formas já existentes de autenticação.

Cabe observar que a transposição de credenciais, neste cenário de federação de redes de teste, se mostra de suma importância e, por isso, visa-se continuar a pesquisa de novas formas para facilitar a integração das redes de teste com a solução apresentada neste trabalho. A delegação de credenciais também se mostrou um ponto importante nesse ambiente e desejamos evoluir o CDM a fim de que seja mais simples a interação com o usuário.

Outro ponto futuro é a extensão da funcionalidade de agregação de atributos para a evolução do ABAC apresentado neste trabalho. Considera-se a utilização de um agregador de atributos, que funcionará como provedor de atributos e será responsável por armazenar atributos adicionais que não pertençam à federação acadêmica por padrão.

A proposta já está sendo integrada ao ambiente atual de experimentação do Projeto FIBRE, sendo crucial para a federação das redes de forma simples, prática e segura para o usuário.

7. Agradecimentos

Agradecemos à CAPES, RNP (equipe LabGId), ao Laboratório OneLab/LIP6 e ao projeto FIBRE por auxiliarem esta pesquisa.

Referências

Barton, T., Basney, J., Freeman, T., Scavo, T., Siebenlist, F., Welch, V., Ananthakrishnan, R., Baker, B., Goode, M., and Keahey, K. (2006). Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, Gridshib, and MyProxy. In *5th Annual PKI R&D Workshop*.

Basney, J., Humphrey, M., and Welch, V. (2005). The myproxy online credential repository. *Softw., Pract. Exper.*, 35(9):801–816.

Bavier, A., Feamster, N., Huang, M., Peterson, L., and Rexford, J. (2006). In VINI veritas: realistic and controlled network experimentation. *SIGCOMM Comput. Commun. Rev.*, 36(4):3–14.

Buell, D. A. and Sandhu, R. S. (2003). IEEE Internet Computing: Guest Editors' Introduction - Identity Management. *IEEE Distributed Systems Online*, 4(12).

Falk, A. (2011). Federation in geni - draft proposal - comments invited. In *GENI Engineering Conferences - GEC11*.

Fernandes, N. C., Silva, E., Muchaluat-Saade, D., and Magalhaes, L. (2013). Gestão de identidade em testbeds brasileiros para a internet do futuro. In *SBRC 2013 - WPEIF*, Brasília.

Foster, I., Kesselman, C., and Tuecke, S. (2001). The anatomy of the grid: Enabling scalable virtual organizations. *Int. J. High Perform. Comput. Appl.*, 15(3):200–222.

Group, N. W. (2006). Comment on rfc 4516 - lightweight directory access protocol (ldap).

ITU-T (2009). NGN identity management framework. Recommendation Y.2720.

Jeong, S. and Bavier, A. (2010). *GENI Federation Scenarios and Requirements*.

Köpsel, A. and Woesner, H. (2011). Ofelia: pan-european test facility for openflow experimentation. In *Proceedings of the 4th European conference on Towards a service-based internet*, ServiceWave'11, pages 311–312, Berlin, Heidelberg. Springer-Verlag.

McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., and Turner, J. (2008). Openflow: enabling innovation in campus networks. *SIGCOMM Computer Communication Review*, 38(2):69–74.

Mitchell, T. (2010). External Identity and Authorization in GENI. In *8th GENI Engineering Conference - GEC8*.

Mitchell, T. (2011). Identity Management and Attributes in GENI. In *11th GENI Engineering Conference - GEC11*.

Moreira, M. D. D., Fernandes, N. C., Costa, L. H. M. K., and Duarte, O. C. M. B. (2009). Internet do futuro: Um novo horizonte. In *Minicursos do Simpósio Brasileiro de Redes de Computadores*, SBRC'2009, pages 1–59. SBC.

OASIS (2005). Security assertion markup language (saml) v2.0.

Peterson, L., Ricci, R., Falk, A., and Chase, J. (2010). Slice-based federation architecture. Technical report.

Rakotoarivelo, T., Ott, M., Jourjon, G., and Seskar, I. (2010). OMF: a control and management framework for networking testbeds. *SIGOPS Oper. Syst. Rev.*, 43(4):54–59.

Sallent, S., Abelém, A., Machado, I., Bergesio, L., Fdida, S., Rezende, J., Simeonidou, D., Salvador, M., Ciuffo, L., Tassiulas, L., and Bermudo, C. (2012). FIBRE project: Brazil and Europe unite forces and testbeds for the Internet of the future. In *Proceedings of TridentCom 2012*.

Scavo, T. e Cantor, S. (2005). Shibboleth architecture. Technical report.

Silva, E., Fernandes, N. C., Magalhaes, L., Muchaluat-Saade, D., and Rodriguez, N. (2013a). Gestão de identidade em redes experimentais para a internet do futuro. In *SBRC 2013 - Minicursos*.

Silva, E., Muchaluat-Saade, D., and Fernandes, N. C. (2013b). Transposicão de credenciais para uso de testbeds para a internet do futuro. In *SBSeg 2013 - WGID*, Manaus.

Silva, E., Muchaluat-Saade, D., Magalhaes, L., Fernandes, N. C., and Rodriguez, N. (2013c). Gestão de identidade em organizacões virtuais. In *JAI 2013*.

Spence, D., Geddes, N., Jensen, J., Richards, A., Viljoen, M., Martin, A., Dovey, M., Norman, M., Tang, K., Trefethen, A., Wallom, D., Allan, R., and Meredith, D. (2006). ShibGrid: Shibboleth access for the UK National Grid Service. In *eScience 2006, Amsterdam*.

Wang, X. D., Jones, M., Jensen, J., Richards, A., Wallom, D., Ma, T., Frank, R., Spence, D., Young, S., Devereux, C., and Geddes, N. (2009). Shibboleth access for resources on the national grid service (sarongs). In *Information Assurance and Security, 2009. IAS '09. Fifth International Conference on*, volume 2, pages 338–341.