Maykon Chagas de Souza

Implantação de uma Comunidade Acadêmica Federada para Experimentação usando Framework Shibboleth

São José – SC

Julho / 2014

Maykon Chagas de Souza

Implantação de uma Comunidade Acadêmica Federada para Experimentação usando Framework Shibboleth

Monografia apresentada à Coordenação do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal de Santa Catarina para a obtenção do diploma de Tecnólogo em Sistemas de Telecomunicações.

Orientadora:
Prof. Michelle S. Wangham, Dra.

Co-orientador:
Prof. Emerson Ribeiro de Mello, Dr.

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES
INSTITUTO FEDERAL DE SANTA CATARINA

São José – SC

Julho / 2014

Monografia sob o título *"Implantação de uma Comunidade Acadêmica Federada para Experimentação usando Framework Shibboleth"*, defendida por Maykon Chagas de Souza e aprovada em 9 de Julho de 2014, em São José, Santa Catarina, pela banca examinadora assim constituída:

Profª. Michelle S. Wangham, Dra.
Orientadora
UNIVALI

Prof. Emerson Ribeiro de Mello, Dr.
Co-orientador
IFSC

Prof. Eraldo Silveira e Silva, Dr.
IFSC

Prof. Arliones Stevert Hoeller Junior, Msc.
IFSC

Sempre que te perguntarem se podes fazer um trabalho,
respondas que sim e te ponhas em seguida a aprender como se faz.
F. Roosevelt

Agradecimentos

Dedico meus sinceros agradecimentos à minha orientadora, prof. Michelle S. Wangham, pela paciência e dedicação com que me conduziu para conclusão deste trabalho. Ao prof. Emerson Ribeiro de Mello, por ter acreditado em mim e ter me indicado para a Bolsa de Iniciação Científica, que proporcionou a elaboração deste trabalho, e a RNP pelo financiamento e crença na pesquisa no âmbito de Gestão de Identidade.

Gostaria também de agradecer especialmente à minha família e a Eliza Sodré de Souza.

Resumo

A disponibilidade de serviços e aplicações acessíveis remotamente na Internet tornou a gestão de identidades uma estrutura complexa de manter, tanto para usuários quanto para administradores de sistemas. Para contornar isto, o modelo de gestão identidades federadas tem como objetivo facilitar o acesso aos serviços. No entanto, a implantação de uma federação não é trivial e, para muitos pesquisadores que estão desenvolvendo trabalhos nesta área, implantar uma federação para realizar experimentos práticos é uma tarefa custosa e demorada. Este trabalho tem como objetivo implantar e disponibilizar uma infraestrutura para que pesquisadores possam conduzir experimentos em uma federação acadêmica baseada no framework Shibboleth. Este trabalho envolveu (1) um estudo bibliográfico sobre gestão de identidades federadas, em especial do *Framework* Shibboleth e do padrão SAML; (2) a instalação e configuração das entidades que compõem uma federação; (3) a preparação de máquinas virtuais pré configuradas com uma federação completa e com as entidades da federação; (4) a disponibilização da federação para experimentação e o apoio técnico aos pesquisadores; e, por fim (5) a avaliação dos serviços oferecidos na federação e o serviço de apoio prestado.

Palavras-chave: Gestão de identidades federadas, Especificação SAML, Framework Shibboleth, Ambiente virtual, Experimentação

Abstract

The availability of accessible services and applications on the Internet has complicated the management of identities, for both users and system administrators. To go around this, the federated identity model aims to improve the access to services. However the implementation of a federation is not trivial and, for many researchers who are developing studies on this field, deploying a federation to conduct practical experiments is a long and costly task. This paper aims to implement and provide a virtual environment for researchers to conduct experiments in a fedaration based on the Shibboleth framework. This paper involved (1) a bibliographic study of federated identity management, in particular the Framework Shibboleth and SAML standard; (2) the installation and configuration of entities within a federation; (3) the preparation of pre-configured virtual machines with a full federation and the federation entities; (4) the availability of the federation for experimentation and technical support to researchers; and finally (5) the evaluation of the services offered in the federation and service support.

Keywords: Federated Identity Manager, SAML, Framework Shibboleth, testbed

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

CA *Certificate Authority*

CAFe Comunidade Acadêmica Federada

CAPES Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CEFET-MG Centro Federal de Educação Tecnológica de Minas Gerais

CENAPAD Centros Nacionais de Processamento de Alto Desempenho

CPF Cadastro de Pessoa Física

CSS *Cascading Style Sheets*

CT-GId Comitê Técnico de Gestão de Identidade

DS *Discovery Service*

e-AA Infraestrutura de Autenticação e Autorização Eletrônica

ECP *Enhanced Client or Proxy*

EDS *Embedded Discovery Service*

GEANT *pan-European Research and Education Network*

GENI *Global Environment for Network Innovations*

GId Lab Laboratório de Experimentação em Gestão de Identidades

GISELA *Grid Initiatives for e-Science virtual Communities in Europe and Latin America*

GT Grupo de Trabalho

GT-STCFed Grupo de Trabalho Serviços para Transposição de Credenciais de Autenticação Federadas

HTTP *Hypertext Transfer Protocol*

HTML *Hypertext Markup Language*

IAA Infraestrutura de Autenticação e Autorização

ICP Infraestrutura de Chave Pública

ICPEdu Infraestrutura de Chaves Públicas para Ensino e Pesquisa

IdP *Identity Provider*

INPE Instituto Nacional de Pesquisas Espaciais

INPA Instituto Nacional de Pesquisas da Amazônia

JEMS *Journal and Event Management System*

LDAP *Lightweight Directory Access Protocol*

LNCC Laboratório Nacional de Computação Científica

MACE *Middleware Architecture Committee for Education*

MCTI Ministério da Ciência, Tecnologia e Inovação

NREN *National Research and Education Network*

NSF *National Science Foundation*

OASIS *Organization for the Advancement of Structured Information Standard*

PoP Ponto de Presença

PADBR Infra-estrutura Nacional de Processamento Computacional Avançado

PGID Programa de Gestão de Identidade

RedCLARA Cooperação Latino Americana de Redes Avançadas

REFEDS *Research and Education Federations*

RG Registro Geral

RNP Rede Nacional de Ensino e Pesquisa

SAML *Security Assertion Markup Language*

SBC Sociedade Brasileira de Computação

SCHAC *SCHema for ACademia*

SGC Serviço Gerador de Certificados

SGCI Sistema de Gerenciamento de Certificados Digitais ICPEdu

SLO *Single Logout*

SOAP *Simple Object Access Protocol*

SP *Service Provider*

SSO *Single Sign-On*

SSTC *Security Services Technical Committee*

TERENA *Trans-European Research and Education Networking*

UFC Universidade Federal do Ceará

UFF Universidade Federal Fluminense

UFMG Universidade Federal de Minas Gerais

UFPE Universidade Federal de Pernambuco

UFRGS Universidade Federal do Rio Grande do Sul

UFRJ Universidade Federal do Rio de Janeiro

UNICAMP Universidade de Campinas

URL *Uniform Resource Locator*

URI *Uniform Resource Identifier*

VoIP *Voice over IP*

VM *Virtual Machine*

WAYF *Where Are You From*

XML *Extensible Markup Language*

1 Introdução

A disponibilidade de serviços e aplicações acessíveis remotamente na Internet se tornou um processo relativamente simples de implementação. O avanço das tecnologias de redes de computadores foi responsável pela construção dessas aplicações e a facilidade para acesso às mesmas. No entanto, além de manter a própria aplicação, administradores de sistemas necessitam ainda manter uma base de usuários própria com informações e níveis de privilégio para permitir acesso às aplicações, tornando o trabalho custoso (MOREIRA et al., 2011).

Do lado do usuário, com tantos serviços disponíveis, é permitida a criação de múltiplas identidades para acesso a esses serviços. Cada novo serviço que o usuário deseja acessar, este deve repassar algumas informações pessoais e um nome de usuário e senha para acessar o serviço. Criar um nome de usuário e senha para cada serviço seria uma boa prática de segurança, porém, administrar essas informações é uma tarefa difícil para os usuários, diante da grande gama de serviços que são oferecidos na Internet (WANGHAM et al., 2010a).

Segundo Kallela (2008) e Wangham et al. (2010b), o problema de gestão de identidades afeta tanto o usuário, que repete informações sem dar a devida importância ou usa senhas fracas, quanto as empresas que além de prover o serviço ainda precisam se preocupar com a gestão de identidades dos usuários, gerando custos administrativos e de infraestrutura. O modelo de gestão de identidades federadas surgiu como uma opção de solução para estes problemas.

No modelo de gestão de identidades federadas (JøSANG et al., 2005; JøSANG; POPE, 2005; BHARGAV-SPANTZEL et al., 2007), objetiva-se remover a complexidade do usuário em ter que administrar um nome de usuário e senha para cada serviço que deseja acessar, permitindo que uma mesma identidade possa ser utilizada para o acesso a diferentes serviços. O conceito de federação visa minimizar as demandas dos provedores de serviços e de usuários de um domínio. Uma federação é composta por dois componentes principais: (1) provedores de identidades, (*Identity Providers – IdPs*), responsáveis pela autenticação e gerenciamento das informações dos usuários de um domínio; e (2) provedores de serviços, (*Service Providers – SPs*), que disponibilizam serviços para acesso dos usuários (MOREIRA et al., 2011).

Neste modelo, informações dos usuários são compartilhadas entre provedores de identidade e provedores de serviços, que possuem relações de confiança entre si e pertencem ao círculo de confiança da federação. Este modelo provê a facilidade de autenticação única, *Single Sign-On* (SSO), que garante ao usuário passar uma única vez pelo processo de autenticação e acessar qualquer provedor de serviços da federação, cabendo a estes provedores realizarem somente o controle de acesso dos usuários (WANGHAM et al., 2010a). O modelo de gestão de identidades federadas se mostra vantajoso para o usuário, que necessitará de uma única identidade para acessar os diversos serviços da federação, e para o administrador do sistema, que ao prover um serviço para a federação não precisará se preocupar com a autenticação e com o cadastro de usuários.

Existem diferentes soluções para realizar o gerenciamento de identidades federadas, dentre estas o *framework* Shibboleth, um *middleware* desenvolvido pela Internet2, gratuito e de código aberto que provê uma solução de SSO para autenticação e autorização *web*, baseada nas especificações SAML. O Shibboleth é um sistema para criação de federações que oferece funcionalidades para a troca segura de dados para acessar recursos entre diferentes domínios. O *framework* Shibboleth surgiu inicialmente com o foco voltado para federações acadêmicas, no entanto, hoje é usado por uma variedade de instituições em todo o mundo (FELICIANO et al., 2011).

No Brasil, a Rede Nacional de Ensino e Pesquisa (RNP), em conjunto com as instituições de ensino UFC, UFMG, UFF, UFRGS e CEFET-MG, iniciaram o projeto da Comunidade Acadêmica Federada (CAFe)[1] com o intuito de reunir os serviços das universidades e instituições de pesquisa do País (MOREIRA et al., 2011). Desde o ano de 2009, a RNP disponibiliza o serviço da CAFe às suas organizações usuárias. Através da CAFe, um usuário mantém todas as suas informações na sua instituição de origem e pode acessar serviços oferecidos pelas instituições que participam da federação acadêmica.

1.1 Problema de pesquisa

Desenvolver pesquisa aplicada na área de gestão de identidades federadas exige que os experimentos sejam conduzidos em um ambiente que implemente uma federacão em sua totalidade, sendo que a complexidade de montar tal ambiente depende do *framework* escolhido (WANGHAM et al., 2013).

A federação CAFe é um ambiente de produção, ou seja, nesta federação não deve ser per-

[1] http://portal.rnp.br/web/servicos/cafe

mitida a realização de experimentos e assim pesquisadores que fazem prospecções tecnológicas e pesquisas científicas em gestão de identidades necessitam montar sua própria federação de testes para que possam conduzir seus projetos e experimentos.

Conceber uma federação acadêmica baseada no *framework* Shibboleth para realizar experimentos práticos pode ser uma tarefa, muitas vezes, mais trabalhosa do que a implementação da pesquisa propriamente dita. Ter que implantar este ambiente complexo para o desenvolvimento da pesquisa, que demanda um tempo considerável dos pesquisadores envolvidos, para que então os experimentos possam ser executados pode inibir pesquisas na área. Outro complicador é o fato de que manter esse ambiente é custoso, em termos de recursos computacionais, atualizações de segurança e de *software* entre outras atividades (WANGHAM et al., 2013).

1.2 Solução proposta

Ciente desta necessidade e com o intuito de motivar pesquisas em Gestão de Identidade, a RNP criou em 2013 o projeto Laboratório de Experimentação em Gestão de Identidades (GId Lab)[2] que tem por objetivo geral disponibilizar para a comunidade acadêmica um ambiente virtual no qual os pesquisadores poderão realizar testes com Infraestruturas de Autenticação e Autorização (IAA) e também Infraestruturas de Chave Pública (ICP) (WANGHAM et al., 2013).

Este trabalho de conclusão de curso terá como objetivo implantar uma parcela do GId Lab foi implantada, a CAFe Expresso, uma federação acadêmica para experimentação. A CAFe Expresso é constituída de provedores de identidade (IdPs), provedores de serviço (SPs) e dois diferentes serviço de descoberta, *Discovery Service* (DS), um chamado *Where Are You From* (WAYF)[3] e outro chamado *Embedded Discovery Service* (EDS)[4], que realizam o redirecionamento do usuário para o seu IdP de origem para que este se autentique. Foi implementado também um serviço chamado *uApprove*, que permite ao usuário saber quais atributos (informações) estão sendo liberados para o SP que deseja acessar, permitindo que o usuário aceite ou não a liberação destes atributos. Ainda no contexto deste trabalho, foram configurados e disponibilizados para *download*, por meio de máquinas virtuais pré-configuradas, dois ambientes, de forma a facilitar a implantação destes provedores nas instituições que estão realizando seus experimentos no GId Lab. Um ambiente contém todos os elementos necessários para uma federação Shibboleth, que é composto por um IdP, um SP e um WAYF, para ser execu-

[2] http://wiki.rnp.br/display/gidlab/
[3] https://wayf.switch.ch/
[4] http://shibboleth.net/products/embedded-discovery-service.html

tado localmente na máquina do pesquisador. Outra possibilidade é o pesquisador obter um dos componentes de uma federação baseada em Shibboleth, um IdP ou um SP (ou ainda ambos), possibilitando que este possa configurar o provedor com as informações da sua instituição e realizar testes através da CAFe Expresso, juntamente com outros pesquisadores.

O presente trabalho foi desenvolvido dentro do escopo do projeto GId Lab, sendo que o aluno é Bolsista de Iniciação Científica, financiado pela RNP.

1.3 Objetivos

Esta seção formaliza os objetivos do trabalho, conforme descrito a seguir.

1.3.1 Objetivo geral

O objetivo geral deste trabalho é disponibilizar para a comunidade científica um ambiente virtual para realização de pesquisas e testes em Gestão de Identidade em uma federação acadêmica para experimentação (CAFe Expresso), baseada no *framework* Shibboleth.

1.3.2 Objetivos específicos

1. Instalar e configurar as entidades necessárias para o funcionamento de uma federação Shibboleth alinhada aos padrões adotados na federação CAFe;
2. Disponilizar serviços do Framework Shibboleth que ainda não são oferecidos na CAFe e que podem ser do interesse dos pesquisadores;
3. Disponibilizar máquinas virtuais para fácil implantação de elementos de uma federação, como IdP ou SP;
4. Disponibilizar aos pesquisadores os serviços de uma federação e documentação de apoio para a condução de experimentos;
5. Avaliar os serviços oferecidos na Federação CAFe Expresso e o apoio dado aos pesquisadores.

1.4 Metodologia

Segundo Gil (2008), a metodologia é caracterizada como um conjunto de procedimentos técnicos e intelectuais utilizados para atingir um objetivo, onde os métodos fornecem as bases lógicas para investigação do problema de pesquisa. A partir deste contexto a metodologia deve se relacionar diretamente com os objetivos específicos como ferramenta de auxílio para o alcance do objetivo geral da pesquisa.

1.4.1 Metodologia da pesquisa

A pesquisa buscou gerar conhecimento para implantação de uma solução para promover pesquisas e prospecções tecnológicas dentro do âmbito de Gestão de Identidade. O resultado, é um ambiente para experimentação destas pesquisas, retirando a complexidade de implantação da infraestrutura de uma federação da responsabilidade dos pesquisadores, entregando um ambiente pré-configurado e pronto para o uso. Desta forma, este trabalho pode ser caracterizado como uma pesquisa de natureza aplicada.

Quanto aos objetivos de pesquisa, este trabalho se caracteriza como uma pesquisa exploratória uma vez que realizou um levantamento dos serviços de uma federação e concebeu uma solução que visa facilitar o desenvolvimento de pesquisas na área. Foi utilizada uma abordagem em parte quantitativa e em parte qualitativa no processo de avaliação da CAFe Expresso, conforme está registrado no Capítulo 4.

1.4.2 Procedimentos metodológicos

- Pesquisa bibliográfica: A pesquisa bibliográfica consistiu em obter conhecimento sobre as tecnologias utilizadas para implantação do ambiente de gestão de identidades federada. Dentre os assuntos estudados estão: os modelos de Gestão de Identidades, as especificações SAML, o *framework* Shibboleth e seus componentes;
- Identificação dos Requisitos de *hardware*: Definição dos requisitos básicos de *hardware* para implantação de cada elemento (IdP, SP e WAYF) da federação;
- Identificação dos Requisitos de *software*: Definição do conjunto de *software* para cada elemento da federação;
- Implantação do ambiente: Implantação de cada elemento do ambiente proposto, resultando em uma federação acadêmica para experimentação;

- Documentação: Registro da documentação para auxiliar na implantação das máquinas virtuais disponibilizadas para os pesquisadores e interessados em implantar um ambiente completo localmente ou um dos componentes do *framework* Shibboleth (IdP e/ou SP);

- Criação das máquinas virtuais: Configuração de dois ambientes de máquinas virtuais diferentes, um para execução local, composto por um IdP, um SP e um WAYF, e outro para execução remota e adesão na CAFe Expresso, composto pelos componentes do *framework* Shibboleth, um IdP ou um SP;

- Customização das páginas *web*: Customização das páginas *web* de cada elemento, com o intuito de caracterizar o ambiente, criando um logotipo, e assim definindo uma identidade visual para a CAFe Expresso;

- Avaliação do ambiente proposto: Avaliação do ambiente através de pesquisa de satisfação, proposto em conjunto com uma pesquisa de uso onde um conjunto de usuários realizará testes no ambiente e avaliará suas funcionalidades e usabilidade.

1.5 Estrutura do trabalho

Este trabalho está dividido em cinco Capítulos. O Capítulo 1 contemplou uma introdução ao problema de pesquisa, a descrição da solução proposta e os objetivos do trabalho. O Capítulo 2 apresenta a fundamentação teórica necessária para compreensão dos conceitos, padrões e tecnologias envolvidos na solução proposta. O estudo bibliográfico realizado compreendeu os temas: gestão de identidades, o modelo de gestão de identidades federados, o padrão SAML, e, por fim, os componentes e funcionalidades do *framework* Shibboleth. O Capítulo 3 descreve a federação CAFe, seus objetivos, sua participação no cenário mundial, a lista de alguns serviços disponíveis para usuários da federação CAFe e o esquema brEduPerson. O Capítulo 4 apresenta uma visão geral da CAFe Expresso, assim como as tecnologias e ferramentas (*softwares*) utilizados para implantação e funciomento da federação. Em seguida, os resultados de uma avaliação de uso da CAFe Expresso são apresentados, avaliação realizada com pesquisadores, participantes do CT-GId da RNP e conhecedores de tecnologias de gestão de identidades federadas. Esta seção também aborda sucintamente a execução do projeto, citando os procedimentos realizados, para o completo funcionamento do trabalho proposto. Por fim, o Capítulo 5 apresenta a conclusão deste trabalho.

2 *Fundamentação teórica*

2.1 Introdução

Este capítulo aborda fundamentos teóricos sobre Gestão de Identidade. Os tópicos descritos nesse documento são: conceitos básicos de Gestão de Identidade, os modelos de Gestão de Identidade descritos na literatura, o padrão *Security Assertion Markup Language* (SAML), e, por fim, a estrutura do *framework* Shibboleth, principal componente de estudo deste trabalho.

2.2 Gestão de Identidade

De acordo com o Dicionário Aurélio, dentre os significados para palavra identidade, têm-se: **Identidade** [*Do Lat. escolástico identitate*]: *S. f.* 2. Conjunto de caracteres próprios e exclusivo de uma pessoa, tais como nome, profissão, sexo, impressões digitais, defeitos físicos etc., o qual é considerado exclusivo dela e, consequentemente, considerado, quando ela precisa ser reconhecida. I. *pessoal*: consciência que uma pessoa tem de si mesma (FERREIRA, 1986).

Segundo Cao e Yang (2010), é difícil descrever o conceito de identidade uma vez que a definição de identidade está relacionada ao ambiente no qual esta é empregada, a contextos semânticos e a casos de uso. Como uma definição mais geral, tem-se que uma identidade é uma representação de uma entidade ou sujeito que seja suficiente para identificar esta entidade em um contexto particular (MALIKI; SEIGNEUR, 2007). Uma entidade, por sua vez, é qualquer coisa existente no mundo real.

De acordo com a norma ITU-T Y.2720 (ITU-T, 2009), uma identidade pode consistir de:

- Identificador – conjunto de caracteres e símbolos ou qualquer outra forma de dados usada para identificar unicamente uma identidade. Este pode ser delimitado pelo tempo e/ou espaço. Por exemplo, uma *Uniform Resource Locator* (URL) que é única ao longo do tempo. Também são exemplos de identificadores o CPF, o RG, o número de matrícula de uma instituição de ensino e o número do passaporte, etc.;

- Credenciais – uma credencial é um atestado de qualificação, competência ou autoridade, que pode ser expedida por terceiros com autoridade relevante ou competência para tal ato e que atesta a veracidade da identidade. No âmbito da computação, exemplo de credenciais incluem certificados digitais X.509 assinados por uma autoridade certificadora, *Certificate Authority* (CA), senhas, asserções SAML, entre outras;

- Atributos – um conjunto de dados que descreve as características fundamentais de uma identidade. Como exemplo, tem-se o nome completo, o endereço de domicílio, a data de nascimento e papeis (*roles*).

A Gestão de Identidade pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade ou de um objeto, garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) e para prover procedimentos de autenticacão, autorização, contabilização e auditoria (ITU-T, 2009). A Gestão de Identidade também envolve aspectos relacionados com a definição, certificação e gerenciamento do ciclo de vida das identidades digitais, infraestruturas para troca e validação dessas informaçãoes, juntamente com os aspectos legais (JøSANG; POPE, 2005; CHADWICK, 2009).

Para a realização da Gestão de Identidade, 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).

De acordo com Bhargav-Spantzel et al. (apud WANGHAM et al., 2010b), um sistema de gerenciamento de identidades é caracterizado pelos seguintes elementos:

- Usuário – quem deseja acessar algum serviço.

- Identidade – conjunto de atributos de um usuário. Por exemplo, nome, filiação, data de nascimento, endereço, etc.;

- Provedor de identidade (IdP) – responsável por manter as informações sobre as pessoas vinculadas a um domínio. O provedor de identidade estabelece seu método de autenticação interno e deve garantir que cada pessoa da instituição tenha um identificador único (MOREIRA et al., 2011);

- Provedor de serviço (SP) – oferece recursos a usuários autorizados, após verificar a autenticidade de sua identidade e após comprovar que a mesma carrega todos os atributos necessários para o acesso.

Segundo Damiani, Vimercati e Samarati (apud WANGHAM et al., 2010b), um sistema de gerenciamento de identidades necessita que um conjunto de requisitos seja contemplado, com o intuito de garantir uma melhor experiência para os usuários, porém, estas facilidades oferecidas ao usuário, não devem afetar a segurança das informações pessoais. A seguir, têm-se os requisitos listados por Damiani, Vimercati e Samarati (2003):

- Interoperabilidade – As identidades dos usuários devem ser representadas em um formato comum, possibilitando que estas possam ser compreendidas e validadas em diferentes domínios administrativos e de segurança;
- Mecanismo para revogação de identidades – O sistema deverá prover uma forma para que os usuários possam gerenciar as informações contidas em suas identidades, assim como revogá-las quando desejado;
- Gerenciamento de confiança – Relações de confiança entre provedores de serviços e de identidades de diferentes domínios permitem que identidades emitidas em um sejam aceitas em outro. Para esse tipo de interação, é preciso prover uma forma de indicar o nível de confiança associado a cada relação, sendo que este influenciará no comportamento dos provedores de serviço;
- Privacidade – Os usuários devem possuir meios de expressar suas preferências de privacidade sobre as informações pessoais presentes em suas identidades, e quais serão disponibilizadas na relação entre os diferentes provedores;
- Anonimato – Aos usuários deve ser garantido o direito de permanecerem anônimos de forma que as informações fornecidades com sua identidade digital não possam ser usadas para obter dados de suas outras identidades. Para garantir o anonimato, pode-se utilizar pseudônimos.

2.2.1 Modelos de Gestão de Identidade

Os modelos de Gestão de Identidade são classificados de acordo com a sua arquitetura. Em Jøsang e Pope (2005) e Bhargav-Spantzel et al. (2007), os modelos de Gestão de Identidade são classificados como: tradicional, federado, centralizado e centrado no usuário. Cada um desses modelos apresenta uma forma diferente de interação.

A Figura 2.1 ilustra os modelos de Gestão de Identidade e uma breve descrição destes modelos é apresentada a seguir (WANGHAM et al., 2010a):

- Tradicional (ou isolado) – a identificação do usuário é tratada de forma isolada por cada provedor de serviços, o qual também atua como provedor de identidades (ver Figura 2.1 (a)). Cabe ao usuário criar uma identidade digital para cada provedor de serviço que deseja interagir, não havendo assim o compartilhamento das identidades desses usuários entre diferentes provedores de serviços;

- Federado – os provedores de identidades e provedores de serviços podem estar em domínios diferentes, permitindo que usuários que possuam suas credenciais em um provedor de identidade acessem um serviço disponível em um provedor de serviço em outro domínio (ver Figura 2.1 (b)). Este modelo permite que os usuários possuam uma única identidade e não precisem lidar com o processo de autenticação diversas vezes, graças ao conceito de autenticação única (SSO);

- Centralizado – só existe um provedor de identidades, o qual é responsável por autenticar os usuários, fornecer aos provedores de serviços informações sobre estes, sendo que todos os provedores de serviços devem confiar plenamente nas informações fornecidas por este provedor de identidades (ver Figura 2.1 (c));

- Centrado no usuário – tem por objetivo dar ao usuário total controle sobre suas identidades digitais. Na proposta de Jøsang e Pope (2005) as identidades de um usuário, destinadas a diferentes provedores de serviços, são armazenadas em um dispositivo físico que fica em poder do usuário, como um *smartcard* ou mesmo um telefone celular (ver Figura 2.1 (d)), e permite que o usuário possa escolher que tipo de informações deseja liberar para um determinado provedor de serviços (FELICIANO et al., 2011). As principais implementações deste modelo fazem uso de um dos modelos descritos anteriormente, sendo o modelo federado o mais comum a ser utilizado (WANGHAM et al., 2010a).

Dentre os modelos apresentados, é possível realizar algumas considerações quanto suas características. Por exemplo, o modelo tradicional é amplamente utilizado nos atuais sistemas computacionais presentes na Internet. No entanto, apesar de ser amplamente utilizado, seu uso tende a ser custoso tanto para o usuário quanto para os provedores de serviços. Devido a isto os usuários devem possuir múltiplas identidades para interagir entre os diferentes serviços, como o servidor de e-mails, *site* de notícias, livrarias, e outros. Além disso, cada provedor de serviços pode exigir um conjunto próprio de atributos para compor a identidade digital do usuário (MELLO; FRAGA; WANGHAM, 2009).

O modelo centralizado trata destes problemas apontados sobre o modelo tradicional. O modelo centralizado fundamentalmente tem o compartilhamento de identidades dos usuários

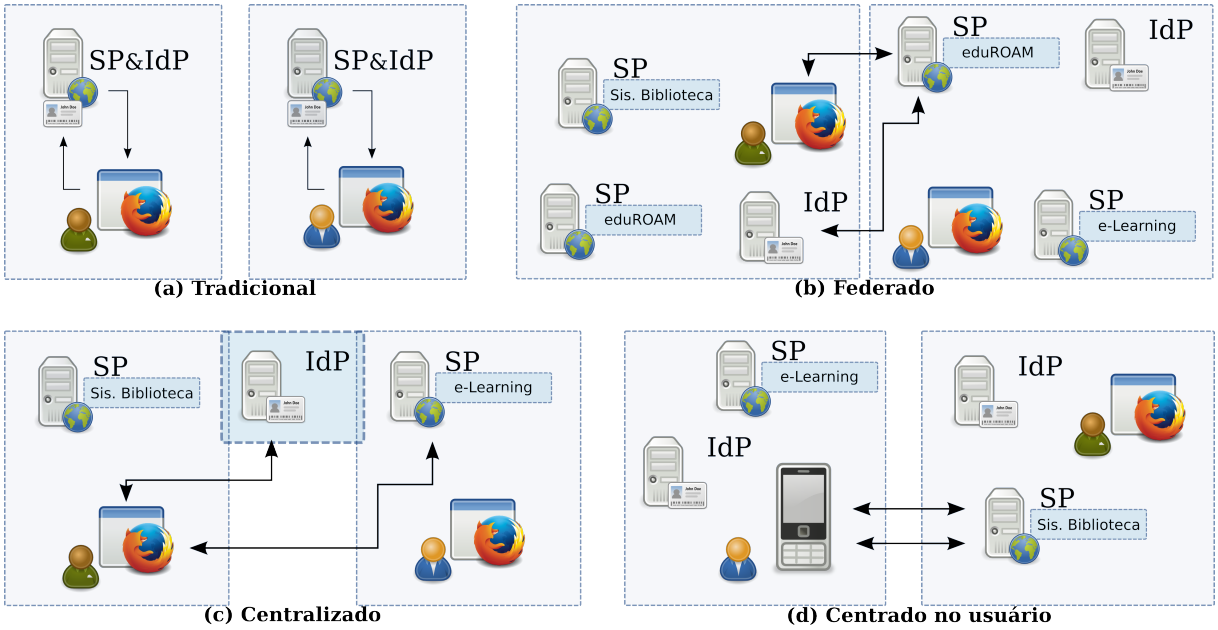


Figura 2.1: Modelos de Gestão de Identidade. Fonte: (WANGHAM et al., 2010a)

entre os provedores de serviços e permite o uso da autenticação única *Single Sign-On* (SSO), porém, todas as identidades estão centralizadas em um único provedor de identidade e todos os provedores de serviços devem confiar plenamente nas informações que este primeiro fornece (WANGHAM et al., 2010b). Segundo Maliki e Seigneur (apud WANGHAM et al., 2010a), o ponto fraco deste modelo é o poder que o provedor de identidade detém sobre as informações de seus usuários, podendo utilizá-las da forma que bem entender.

No final da década de 90, e ainda nos dias atuais, a infraestrutura de Gestão de Identidade se destina à provisão de serviços, especialmente serviços centralizados de autenticação. Neste cenário, as organizações (empresas ou universidades) empregam serviços de diretórios baseados em *Lightweight Directory Access Protocol* (LDAP). Esses serviços são destinados a fornecer mecanismos de autenticação de forma centralizada, com o objetivo de facilitar a gerência deste ambiente e prover uma forma de autenticação única (SSO) (SUESS; MOROONEY, 2009).

O modelo de gestão identidades federadas é uma abordagem que visa otimizar a troca de informações relacionadas a identidade por meio de relações de confiança construídas nas federações (CAMENISCH; PFITZMANN, 2007). Os acordos estabelecidos entre provedores de identidades e de serviços garantem que identidades emitidas em um domínio sejam reconhecidas por provedores de serviços de outros domínios e o conceito de autenticação única é garantido mesmo diante de diferentes domínios (WANGHAM et al., 2010b).

As principais propostas e implementações do modelo centrado no usuário fazem uso de um dos modelos apresentados anteriormente, sendo o modelo de identidade federadas o mais usado.

O usuário se autentica através de um dispositivo físico, podendo ser um telefone celular ou um *smartcard*, e cabe a este liberar as informações do usuário para cada provedor de serviços que o usuário acessar, respeitando totalmente as preferências de privacidade do usuário (WANGHAM et al., 2010b).

2.3 Especificações SAML

A *Security Assertion Markup Language* (SAML) é um conjunto de especificações que define uma infraestrutura para troca de informações seguras da autenticação do usuário, seus direitos e atributos entre parceiros (instituições) na rede de computadores. As especificaçãos SAML são elaboradas pelo *Security Services Technical Committee* (SSTC) que faz parte da *Organization for the Advancement of Structured Information Standard* (OASIS). No padrão SAML, as informações de segurança são apresentadas na forma de asserções (declarações). O padrão define as regras e a sintaxe para geração, requisição, transferências e uso destas asserções (WANGHAM et al., 2010b; OASIS, 2008).

As mensagens SAML são codificadas em arquivos XML que geralmente são incorporados em outras estruturas para o transporte, como por exemplo, o HTTP POST ou mensagens *Simple Object Access Protocol* (SOAP) codificadas. Esse tipo de transporte é denominado na especificação como *binding*. A especificação SAML fornece um conjunto base de perfis para o uso de afirmações e protocolos, visando possibilitar a interoperabilidade no uso dos recursos SAML (OASIS, 2008; MAçANEIRO, 2013).

Atualmente, a especificação SAML está na versão 2.0 (lançada em 2005) e é o padrão mais adotado que concretiza o modelo de identidades federadas. Os sistemas de gerenciamento de identidades que utilizam a especificação SAML o fazem por funcionalidades que estão disponíveis no padrão. A especificação SAML é utilizada de diferentes maneiras, as mais relevantes estão descritas em OASIS (2008), tais como:

- Web SSO – a SAML possibilita o SSO por meio da comunicação de uma asserção de autenticação em um primeiro local para um segundo local que confia na origem da autenticação;
- Autorização baseada em atributos – a especificação SAML permite a autorização baseada em atributos para comunicar informações de uma identidade entre diferentes *web sites*, possibilitando desta forma apoio em algumas transações;

- Segurança em Serviços Web – as asserções SAML podem ser usadas dentro das mensagens SOAP, afim de realizar operações com segurança de informações e identidade entre agentes em um serviço *web*.

2.3.1 Componentes SAML

A especificação SAML é constituida por alguns componentes que funcionam como blocos que podem ser combinados em configurações diferentes para suportar implementações de cenários diferentes. Os componentes primeiramente permitem transferência de identidade, autenticação, atributos e informações de autorização entre provedores de identidades e de serviços que possuem uma relação de confiança estabelecida. O núcleo da especificação SAML define a estrutura e o conteúdo das asserções e mensagens de protocolo usado para transferir essas informações (OASIS, 2008).

Segundo OASIS (2008), a especificação SAML possui componentes responsáveis por tratar informações específicas, protocolos utilizados para troca dessas informações assim como os tipos de ligações (*bindings*) que podem ser realizadas para o estabelecimento da comunicação entre elementos de uma federação.

A SAML define três tipos diferentes de declarações de afirmações (asserções) que podem ser criadas por uma autoridade SAML. A estrutura e o conteúdo de uma asserção são definidos por meio de um esquema XML. A asserção é usualmente criada por uma parte declarante (*asserting party*) baseada em uma requisição da parte confiante (*relying party*). No entanto, sob certas circunstâncias a asserção pode ser encaminhada para um parte confiante mesmo se não foi solicitada. Uma asserção fornece uma ou mais declarações feitas por uma autoridade SAML e é composta basicamente por um conjunto de informações que são: a entidade da asserção, as condições usadas para validar a asserção e as declarações sobre o sujeito. Uma asserção pode conter três tipos de declarações:

- Autenticação – são geradas pela entidade que autentica o usuário. Possuem pelo menos o método de autenticação e a data e hora da autenticação;
- Decisão de autorização – mensagens de requisição e resposta para permitir que uma asserção possa acessar um determinado recurso, a decisão é baseada na URL, que permite ou nega o acesso;
- Atributos – que contêm informações específicas do usuário.

Os protocolos (*protocols*) são mensagens de solicitações e respostas que os provedores de serviços podem utilizar. Os protocolos descritos na especificação SAML são (OASIS, 2008):

- Protocolo de consulta e pedido de asserção (*Assertion Query and Request Protocol*) – usado para requisições por referência (por meio de artefatos) ou consultas por asserções pelo usuário e tipos de declarações;

- Protocolo de pedidos de autenticação (*Authentication Request Protocol*) – protocolo para obtenção de uma asserção contendo declarações de autenticação para o estabelecimento de um contexto de segurança, com uma ou mais partes confiantes que envia uma requisição de autenticação e recebe uma resposta, contendo uma ou mais asserções;

- Protocolo para resolução de artefatos (*Artifact Resolution Protocol*) – mecanismo para troca de mensagens SAML por referência, usando um identificador de tamanho fixo denominado artefato. Utiliza o protocolo de comunicação HTTP POST, para comunicação entre entidades SAML;

- Protocolo de gerenciamento de identificador de nome (*Name Identifier Management Protocol*) – depois do estabelecimento de um identificador para um usuário, um IdP pode mudar ou formatar o valor do identificador que será utilizado para referenciar o usuário, ou indicar que um identificador não será mais usado para referenciar este usuário, informando ao SP desta mudança usando este protocolo;

- Protocolo para encerramento único de sessão (*Single Logout Protocol*) – permite a troca de mensagens informando que todas as sessões disponíveis para uma determinada sessão serão simultaneamente finalizadas. A requisição de *logout* pode ser feita na entidade responsável pela sessão ou por uma entidade participante. Quando o *logout* é solicitado na entidade participante, esta precisa enviar uma requisição de *logout* para entidade principal que provê a declaração de autenticação relacionada à entidade participante e esta finaliza a sessão com todas as sessões ativas;

- Protocolo de mapeamento de identificador de nome (*Name Identifier Mapping Protocol*) – usado quando uma entidade que compartilha o identificador de um usuário com um IdP deseja obter o nome do identificador para o mesmo usuário em um formato particular para compartilhar com outra entidade. Exemplo, um SP que deseja se comunicar com outro SP, pode solicitar o identificador de um usuário a um IdP que compartilha o identificador com ambos os SP, para mapear seus próprios identificadores para um novo identificador, normalmente encriptado.

O mapeamento das mensagens de requisição e resposta trocadas entre protocolos de comunicação padrão, usando padrões de comunicação já estabelecidos como HTTP e SOAP, são chamados procolos de ligação (*bindings*). As ligações SAML, são utilizadas pelos protocolos para transporte de mensagens entre as partes do sistema, por exemplo, uma ligação SAML SOAP descreve como uma troca de mensagens de requisição e resposta SAML são mapeados dentro de mensagens SOAP (OASIS, 2008). Na versão 2.0 da SAML, estão disponíveis diversas ligações, dentre estas, as mais comuns são:

- HTTP *Redirect Binding* – fornece um meio para transmitir asserções SAML dentro da URL de uma solicitação HTTP. Esta opção pode ser utilizada quando não é possível um caminho direto entre um provedor de identidade e um provedor de serviços. Neste caso, a mensagem SAML será transportada de maneira indireta, normalmente, via o navegador *web* do usuário final;

- HTTP POST *Binding* – nesse *binding*, as mensagens SAML são transmitidas dentro do conteúdo de um formulário HTML, utilizando do método HTTP POST para postar a asserção em um provedor de serviços;

- HTTP *Artifact Binding* – fornece um mecanismo que permite a comunicação por intermédio de um agente do usuário (navegador *web*) HTTP intermediário, no qual a requisição ou a resposta SAML podem ser transmitidas usando referências, ou artefatos, um conceito do SAML. Esta ligação tem o objetivo de reduzir o fluxo de mensagens por meio do protocolo;

- URI *Binding* – este modelo de *binding* possibilita que uma asserção SAML específica seja repassada ao provedor de serviços por intermédio de uma HTTP URI;

- SOAP *Binding* – o SOAP é um protocolo de comunicação baseado no formato XML. É um protocolo simples, extensível e flexível, desenvolvido como um padrão W3C. Uma mensagem SOAP é composta pela seguinte estrutura: encapsulamento, cabeçalho e corpo da mensagem. Nesta última, o corpo da mensagem SOAP, é onde ficam as informações dos protocolos de requisição/resposta SAML. O modelo de mensagem SOAP é um modelo simples de requisição e resposta no qual não pode haver mais de uma requição SAML por mensagem SOAP.

Os perfis (*profiles*) SAML possibilitam que os protocolos SAML e suas asserções trabalhem em fluxos de dados específicos, por exemplo, com a finalidade de promover a funcionalidade de gerenciamento de identidades e autenticação única (SSO). Existem também perfis de atributos

(*Attribute Profiles*) que não se referem a nenhuma mensagem de protocolo ou ligação, que definem como realizar a transmissão de informações de atributos usando asserções, de forma que se enquandre em usos comuns para diferentes tipos de ambientes (ex. X500, LDAP, etc.).

Alguns dos perfis mais importantes descritos na especificação SAML que podem ser citados, são (OASIS, 2008):

- Navegador *web* SSO – O perfil (*Web Browser* SSO) é um dos mais utilizados. Um usuário através de um navegador *web* acessa um recurso (serviço) no SP ou acessa um IdP que faz parte de uma federação. O cliente se autentica no IdP, que gera uma asserção de autenticação já com as declarações para o SP. O SP então consome esta asserção gerada e estabelece um contexto de segurança para o cliente. Neste processo, um identificador para o cliente é estabelecido entre os provedores e o cliente, sujeitos aos parâmetros da interação e do consentimento do cliente. Este perfil é utilizado especificamente com o auxílio do perfil do Protocolo de Solicitação de Autenticação em conjunto com o HTTP *Redirect*, HTTP POST e HTTP *artifact binding*. Assume-se que o usuário está utilizando um navegador *web* e tem uma identidade válida para se autenticar;

- Cliente ou proxy melhorado (*Enhanced Client or Proxy* – ECP) – Este perfil é similar ao perfil *Web* SSO, no entanto, o cliente é um sistema cliente ativo, um navegador, um proxy ou outro dispositivo configurado para estabelecer comunicação com um determinado IdP, dependendo do contexto. Este perfil é baseado no protocolo de Solicitação de Autorização e da ligação reversa SOAP *Reverse SOAP (PAOS) binding*. A diferença deste perfil para o *Web* SSO é que não precisa de um navegador *web* para realizar as interações e estabelecimento de uma sessão federada;

- Encerramento único de sessão, (*Single Logout* – SLO) – Uma vez que o usuário tenha se autenticado com um IdP, este estabelece uma sessão, normalmente por meio de *cookie*, reescrita de URL ou outra implementação específica. O IdP emite uma asserção para o SP ou outra parte confiante baseado nesta autenticação e então o SP usa esta asserção para estabelecer sua própria sessão com o usuário. Em algumas situações, o IdP pode atuar como um autor de sessão e o SP como um participante da sessão, mas isto não é muito comum. Então o usuário, em um dado momento, decide finalizar sua sessão ou a sessão com um SP específico, ou com todos os SPs da sessão atual, gerenciada pela autoridade da sessão. Neste segundo caso, o padrão SAML define o perfil de encerramento único de sessão (SLO). Este pefil permite o uso de protocolos com ligações síncronas, como ligações SOAP para finalizar a sessão do usuário, ou o uso de ligações assíncronas, usando HTTP

Redirect, POST ou ligações por artefatos, que são ditas ligações ” textitfront-channel”. No entanto, é recomendável o uso das ligações ”*front-channel*”nos casos em que a sessão principal está somente no navegador *web* na forma de *cookie*, assim uma interação direta entre o navegador e os participantes da sessão é requisitada, garantindo maior probabilidade do encerramento único de sessão SLO ser realizada com sucesso.

Na Figura 2.2 é possível visualizar a pilha de componentes SAML conforme descritos anteriormente.

Figura 2.2: Pilha de componentes SAML. Fonte: (OASIS, 2008)

Dois outros componentes bastante utilizados para composição de ambientes SAML, são:

- Metadado – que define como informar e compartilhar informações entre entidades SAML e papéis (como IdP, SP, etc.). O metadado contém informações sobre ligações SAML, identificadores de identidade, protocolos de transportes suportados, certificados digitais e chaves criptográficas; e

- Contexto de Autenticação – em inúmeras ocasiões um provedor de serviço pode necessitar de informações detalhadas referente ao mecanismo de autenticação que é empregado pelo provedor de identidade do usuário. O contexto de autenticação SAML é usado para

comunicação entre o provedor de serviços e o de identidades, permitindo ao primeiro solicitar uma forma específica de autenticação e ao segundo permitir o acesso do usuário em seus serviços (OASIS, 2008).

2.4 Framework Shibboleth

O termo "shibboleth" denota uma palavra usada para distinguir pessoas de grupos distintos. A origem do termo remete ao velho testamento (Juízes, 12:1-15), no qual ele foi usado para distinguir duas tribos semitas, os gileaditas e os efremitas, que travaram uma grande batalha. Os gileaditas, vencedores, bloquearam a passagem do Jordão para evitar que os efremitas sobreviventes pudessem escapar. As sentinelas exigiam que todos os passantes dissessem "shibboleth". Como os efremitas não tinham o fonema x em seu dialeto, só conseguiam pronunciar "siboleth" (com si na primeira sílaba), estes eram identificos e executados (MOREIRA et al., 2011).

O projeto *Shibboleth* (SCAVO; CANTOR, 2005) foi uma iniciativa do consórcio americano Internet2[1] que teve como principal objetivo lançar uma implementação de código aberto, baseada em padrões abertos, para tratar desafios relacionados ao gerenciamento de identidades e controle de acesso em instituições acadêmicas (WANGHAM et al., 2010a).

O projeto *Shibboleth* teve inicio em 2000 no comitê *Middleware Architecture Committee for Education* (MACE). O *framework* Shibboleth 1.0 foi lançado em Julho de 2003. Em Agosto de 2005, foi lançada a versão 1.3 e em Março de 2008 foi lançada a versão 2.0 (MANUEL; SEABRA, 2009). Em Julho de 2014 as últimas versões eram: Shibboleth IdP v2.4.0[2], e Shibboleth SP v2.5.3[3].

De acordo o *site* do Shibboleth[4], existem informações oficiais de desenvolvimento de uma nova versão, com melhorias e novas implementações. Segundo o *Roadmap*[5] do projeto, não existe uma data de lançamento oficial, mas prevê-se que até o segundo semestre de 2015 seja lançada a versão Shibboleth IdP v3.0.

Uma federação *Shibboleth* é composta por um grupo de organizações que usa um conjunto comum de atributos, práticas e mecanismos de segurança e permissões previamentes definidas e que permite a troca de informações e compartilhamento de serviços, possibilitando a cooperação entre membros da federação (CARMODY et al., 2005).

[1] http://www.internet2.edu/
[2] http://shibboleth.net/downloads/identity-provider/latest/
[3] http://shibboleth.net/downloads/service-provider/latest/
[4] http://shibboleth.net/documents/business-case.pdf
[5] https://wiki.shibboleth.net/confluence/display/DEV/Project+Roadmap#ProjectRoadmap-PlannedWork

O framework está fundamentado sobre padrões abertos como o XML e SAML e provê uma forma fácil para que aplicações *web* usufruam das facilidades providas pelo modelo de identidades federadas, como o conceito de autenticação única (SSO) e a troca segura de atributos dos usuários por todos provedores de serviços que compõem a federação (WANGHAM et al., 2010b).

O *framework* Shibboleth provê suporte a uma classe de atributos (*Object Class*) chamada *eduPerson*, que é um esquema LDAP, originalmente desenvolvida por (INTERNET2, 2008) baseada nas RFCs 2256[6] e 2798[7] (WAHL, 1997; SMITH, 2000). O esquema *eduPerson* é um conjunto padrão de atributos de identidades comuns para federações acadêmicas. Esta classe define quais atributos e informações do usuário são necessários para um funcionamento harmonioso entre IdP e SP dentro do escopo de uma instituição acadêmica.

Em um ambiente federado, a padronização destes atributos é fundamental para que provedores de serviços saibam quais atributos poderão requisitar e para que provedores de identidades saibam quais atributos deverão fornecer (WANGHAM et al., 2010a).

2.4.1 Provedores Shibboleth

Por estar baseado no padrão SAML, o *framework* Shibboleth é composto também pelos provedores de identidades e provedores de serviços. Estes são os principais compontes do framework. O IdP é a entidade responsável pelo gerenciamento das identidades dos usuários, seus atributos, gerenciamento da autenticação e declarações de atributos. Enquanto o SP, é a entidade responsável pelo gerenciamento de segurança dos serviços disponibilizados que, com base nas declarações de atributos recebidas do IdP, permite o acesso a estes serviços. A autorização para acesso ao serviço requisitado ainda passa por um conceito utilizado pelo *framework* Shibboleth, dito contexto de segurança, que precisa ser estabelecido para um usuário, por meio da relação de confiança estabelecida entre SP e IdP, que permitirá o acesso seguro ao serviço (KALLELA, 2008).

No *framework* Shibboleth, o processo de autenticação é executado na instituição de origem do usuário, por meio de seu provedor de identidades, fazendo uso dos mecanismos de autenticação presentes nesta instituição. A autenticação de usuários pode ser feita por meio de senhas, de tickets Kerberos, certificados X.509, entre outros mecanismos (CHADWICK, 2009; WANGHAM et al., 2010b).

[6] https://www.ietf.org/rfc/rfc2256.txt
[7] https://www.ietf.org/rfc/rfc2798.txt

Um IdP é dividido em quatro subcomponentes, como descrito abaixo (SCAVO; CANTOR, 2005; FELICIANO et al., 2011):

- Autoridade de autenticação – responsável por emitir pedidos de autenticação requisitado pela parte confiante (*relying parties*), neste caso, o SP;
- Serviço de autenticação única (SSO) – responsável pela manipulação de requisições do processo de autenticação e verificação de existência de *cookie* de sessão válido. Interage com o componente de Autoridade de Autenticação, este componente obtém as requisições de asserção e gera um fomulário HTML que é redicionado para o SP;
- Serviço de resolução de artefatos – responsável pela resolução dos artefatos utilizados para troca de asserções entre componentes. Por exemplo, quando o SP define um perfil que utiliza a troca de asserções por ligações por referência, (*artifact binding*), ao invés de enviar a asserção de resposta de autenticação via o browser do usuário, é enviada uma referência à asserção expedida;
- Autoridade de atributos – componente responsável pela emissão de asserções de atributos baseadas nas requisições dos provedores de serviços.

A Figura 2.3 representa graficamente a distribuição dos subcomponentes de um IdP.

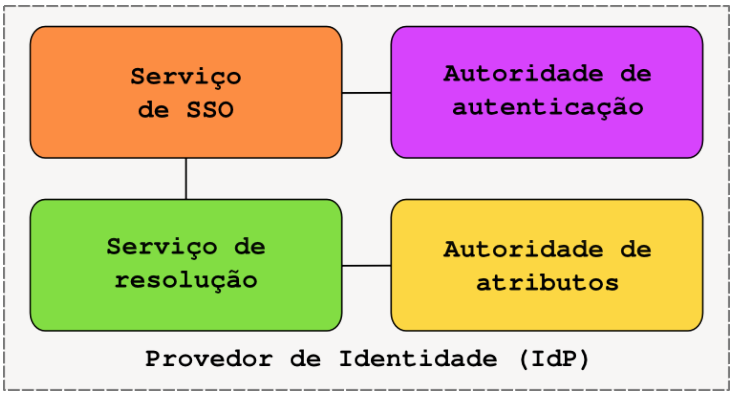


Figura 2.3: Subcomponentes IdP Shibboleth. Fonte: (FELICIANO et al., 2011)

Um SP assim como o IdP é formado por subcomponentes, são estes (SCAVO; CANTOR, 2005):

- Recurso alvo – os recursos (serviços) são protegidos no SP por meio do Controle de Acesso (mod_shib, módulo do Apache), o que impede usuários não autenticados/autorizados de acessarem esses recursos;

- Serviço consumidor de asserção – gerencia as funções de SSO no provedor de serviço. Processa a asserção de atributos recebida ou o artefato, podendo elaborar requisições de asserções de atributos adicionais, estabele o contexto de segurança e redireciona o usuário para o recurso desejado;

- Requisitante de atributos – realiza interações com a Autoridade de Atributos do IdP, para realizar trocas adicionais de atributos, uma vez que um contexto de segurança tenha sido estabelecido. Esse tipo de interação ocorre diretamente entre os provedores, por meio dos protocolos de ligação (*binding*) SAML (como HTTP e SOAP), e não utilizam o navegador Web do cliente.

A Figura 2.4 representa graficamente a distribuição dos subcomponentes de um SP.

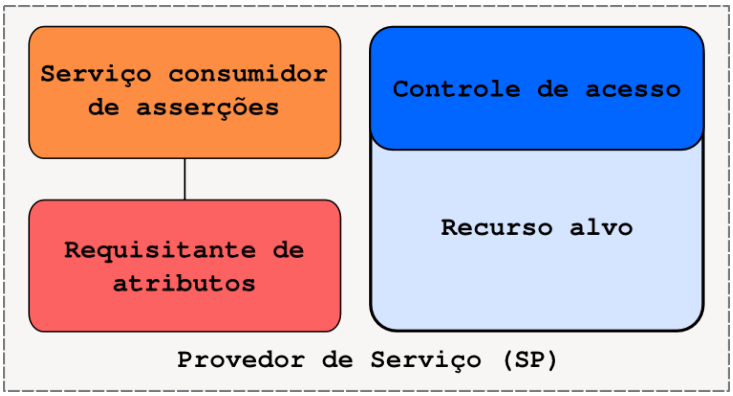


Figura 2.4: Subcomponentes SP Shibboleth. Fonte: (FELICIANO et al., 2011)

A Figura 2.5 exemplifica o fluxo de mensagens trocadas entre os provedores e o WAYF (um serviço de descoberta que permite ao usuário escolher seu IdP em uma lista, para assim poder ser redirecionado e realizar a autenticação) para o acesso quando um usuário realiza a requisição de um serviço a um provedor de serviços da federação, conforme descritos a seguir (FELICIANO et al., 2011). O serviço WAYF será descrito com mais detalhes na Seção 2.4.2.

- Passo 1 – O usuário através do navegador web solicita acesso a um serviço protegido por um provedor de serviços da federação. Caso já exista um contexto de segurança válido, segue para o Passo 8;

- Passo 2 – O provedor de serviços recebe a requisição e redireciona o navegador do usuário para o serviço de descoberta ou DS (representado pelo WAYF);

- Passo 3 – O DS verifica se existe um *cookie* de sessão e a sua validade e processa uma requisição de autenticação do usuário. Caso o usuário tenha um *cookie* válido os Passos 4 e 5 não são executados;

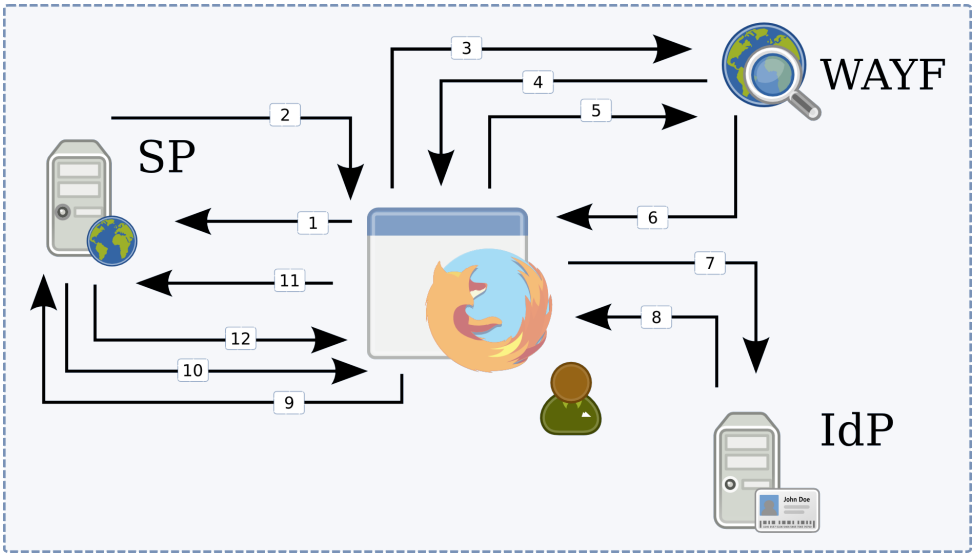


Figura 2.5: Fluxo de mensagens entre usuário e provedores Shibboleth. Fonte: (WANGHAM et al., 2010a)

- Passo 4 – O DS apresenta uma lista com IdPs disponíveis na federação;
- Passo 5 – O usuário seleciona o seu IdP de origem e uma requisição HTTP GET é enviada para o DS;
- Passo 6 – O DS atualiza o cookie de sessão com as informações do IdP escolhido e redireciona o navegador do usuário para o IdP indicado;
- Passo 7 – O serviço de SSO é requisitado no IdP escolhido e este adquire uma declaração de autenticação (asserção SAML) da Autoridade de Autenticação;
- Passo 8 – A asserção SAML é retornada após o usuário fornecer as suas credenciais por meio de uma mensagem HTTP POST
- Passo 9 – O serviço consumidor de asserções do SP consulta a asserção gerada e enviada pelo IdP;
- Passo 10 – O serviço consumidor de asserções processa a resposta da autenticação (além de outras verificações), cria um contexto de segurança e redireciona o navegador do usuário para o recurso protegido;
- Passo 11 – O navegador requisita novamente acesso ao recurso protegido;
- Passo 12 – Com um contexto de segurança válido o usuário é redirecionado para o recurso solicitado no início do processo.

2.4.2 Serviços adicionais

Além dos componentes IdP e SP do *framework* Shibboleth, é possível agregar a estes primeiros alguns serviços, pois só IdP e SP não resolvem todo o ambiente. É necessário também um serviço que ofereça ao usuário uma lista de IdPs, para que o usuário escolha dentre os apresentados, o seu IdP de origem. O padrão SAML possui um protocolo para descoberta de serviços chamado (*Discovery Service* – DS), que possibilita a descoberta de provedores de serviços e de identidades. No *framework* Shibboleth, é possível o uso de dois serviços de descoberta: o *Where Are You From* (WAYF) e o *Embedded Discovery Service* (EDS).

Os serviços WAYF e EDS realizam o redirecionamento do usuário entre o provedor de serviços e o provedor de identidades, uma vez que o provedor de serviço não sabe qual o provedor de identidades que o usuário utiliza para validar seus credenciais de autenticação.

O WAYF é um provedor de serviços que mantém um base dos metadados SAML dos provedores, que além de realizar o estabelecimento de relação de confiança entre os provedores, provê o redirecionamento do usuário para seu provedor de identidade de origem (SHIBBOLETH, 2005; KALLELA, 2008; WANGHAM et al., 2010b).

O EDS, no entanto, permite o uso da mesma base disponibilizada pelo WAYF, porém, o processo de redirecionamento do usuário entre SP, EDS e IdP é transparente, isto porque o EDS é embutido diretamente na página do SP, diminuindo os redirecionamentos entre páginas *web* vistas pelo usuário.

Outro serviço que pode ser agregado ao Shibboleth, especificamente ao IdP, é o *uApprove*, um *plug-in* que solicita o consentimento de liberação do usuário para os atributos que estão sendo solicitados pelo SP, quando o usuário tenta acessar um recurso (serviço) deste segundo.

Where Are You From (WAYF)

A especificação SAML tem descrita quais são os requisitos para se implementar um serviço de descoberta (*Discovery Service* – DS). No entanto, WAYF e DS podem ser usados como sinônimos, mas o WAYF implementa o protocolo DS com algumas diferenças.

Basicamente, WAYF ou DS, tem somente o propósito de apresentar para o usuário uma lista de provedores de identidades e redirecionar o navegador web para o IdP selecionado e depois retornando para o provedor de serviço. A diferença entre os WAYF e o protocolo DS se resume nas interações entre provedores e WAYF ou DS. O WAYF, após apresentar a lista de IdPs para o usuário e receber a sua escolha, redireciona para o IdP escolhido a sessão do usuário. Já o

DS, também apresenta a lista de IdPs para o usuário, mas ao receber a resposta, reencaminha o usuário para o SP, que se encarregará pelo resto do processo de redirecionar o usuário para o seu IdP de origem até o estabelecimento do contexto de segurança. Esta diferança pode ser vista na Figura 2.6.

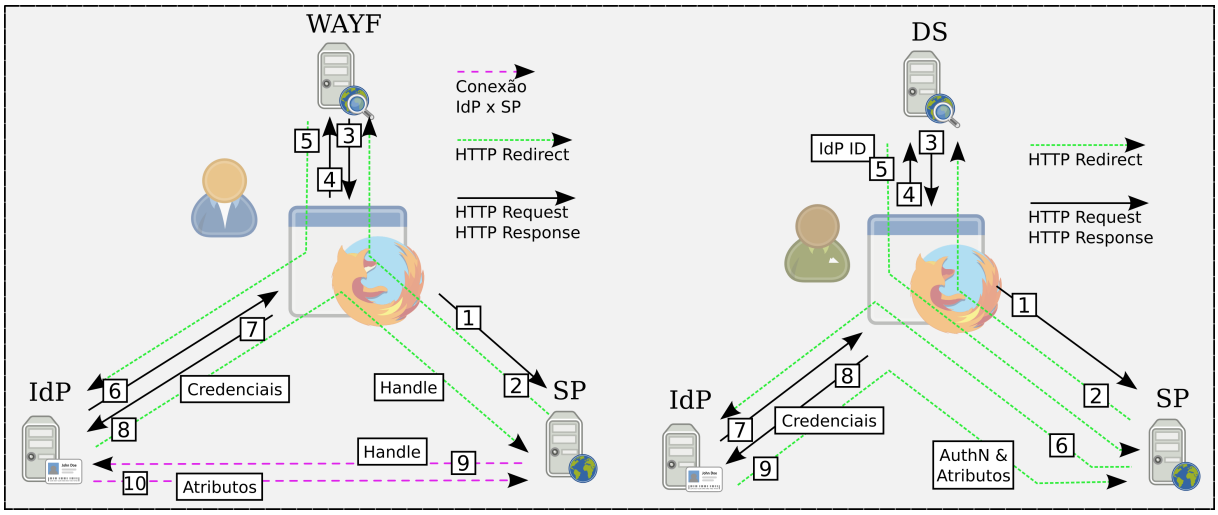


Figura 2.6: Diferenças entre fluxo de mensagens do WAYF e DS

A implementação desenvolvida pela SWITCH[8] foi feita em PHP que permite suporte a muitos idiomas, diversas formas de selecionar um provedor de identidade e permite fácil atualização de metadados para inclusão de novos provedores na federação.

Algumas características destsa implementação são:

- *Open Source* disponibilizado sob licença BSD;
- Leitura de metadados SAML2;
- Redirecionamento automático para o IdP selecionado na sessão ativa do navegador;
- Implementação de um WAYF embarcado.

Existem outras alternativas que implementam o protocolo DS. Uma delas é a implementação desenvolvida pelo projeto do Shibboleth e está descrita logo em seguida. A outra implementação não foi disponibilizada na CAFe Expresso, mas é desenvolvida e mantida pela GRNET[9] criado em 2009 e implementado usando Python através do *framework* Django.

[8] https://www.switch.ch/aai
[9] http://www.grnet.gr/

***Embedded Discovery Service* (EDS)**

Desenvolvido pela equipe do projeto Shibboleth, o Embedded DS pode ser facilmente implementado no SP Shibboleth. A grande diferença entre o EDS e o WAYF é que para o usuário o processo de redirecionamento é transparente. Ou seja, o SP possui um *applet* dentro da própria página que permite ao usuário a escolha do seu IdP de origem, é como se ele não saísse da página do serviço.

Outra característica do EDS é prover uma forma fácil de disponibilizar para um SP o protocolo DS embutido direto no próprio SP. Isso permite que a rede se descentralize mais. O elemento DS está presente e sempre necessitará de um servidor próprio para o mesmo, pois este é responsável por fazer o intermédio entre IdP e SP, constituindo a relação de confiança entre estes. Sendo assim, pode-se dizer que o DS se torna a terceira parte confiante, num ambiente federado.

A wiki do Shibboleth[10], desenvolvedor oficial do EDS, cita dois principais objetivos do EDS:

- Melhorar a experiência durante o processo de *login* do usuário;
- Disponibilizar um DS embutido para SP de forma fácil.

De acordo com a wiki[11] do projeto Shibboleth, onde podem ser encontrados procedimentos de instalação, configuração e relatos do desenvolvimento do *framework* Shibboleth, algumas recomendações são dadas referente a como melhorar a experiência do usuário durante o processo de *login*. Estas recomendações tratam do processo inicial, o botão de *login*, a localização deste dentro do *layout* da página *web* fazendo a referência somente ao processo de identificação e não à federação. Outras recomendações são sobre a página de seleção do IdP, o painel de IdPs preferidos, entre outras recomendações.

A equipe de desenvolvimento do Shibboleth simplificou a implementação do EDS na página do SP. O EDS é composto basicamente por dois arquivos em Javascript, que tratam os metadados extraindo as informações necessárias de cada IdP para exibição e um *Cascading Style Sheets* (CSS) que define um ID específico para uma *tag div*, que será agregado ao arquivo HTML da página do SP.

[10] https://wiki.shibboleth.net/confluence/display/DEV/EDSDetails
[11] https://wiki.shibboleth.net

uApprove

O uApprove[12] é uma extensão para o IdP Shibboleth desenvolvido pela SWITCH[13] que possibilita ao usuário saber quais atributos estão sendo liberados para o SP que este deseja acessar, e permitir que o usuário permita ou não a liberação destes atributos para o SP. O uApprove atua em conjunto com o IdP, no processo de autenticação do usuário, assegurando o processo de aceitação dos Termos de Uso impostos pelo IdP, e o consentimento de liberação dos atributos solicitados pelo SP.

Este processo tem como objetivo informar ao usuário sobre a liberação dos seus dados (atributos) para um SP, quando este acesssa o SP pela primeira vez, ou, uma vez que seus seus dados tenham sofrido alterações, por exemplo, um novo atributo foi adicionado no IdP. Além disto, o uApprove permite que o administrador de um IdP informe ao usuário seus direitos e deveres, ao apresentar para este os Termos de Uso do IdP, permitindo ao administrador implementar leis de proteção de dados e ao solicitar ao usuário seu consentimento antes que seus dados pessoais sejam liberados para um SP, quando este tenta acessar qualquer serviço da federação. Permite ao administrador ter conhecimento quando um usuário deu permissões de acesso e quais atributos foram liberados para um determinado SP.

Do ponto de vista do usuário, o uApprove é uma aplicação que:

- Pode aceitar ou negar o termo de uso do IdP Shibboleth num primeiro acesso ao sistema (esta configuração pode ser desabilitada);
- Pode aceitar liberar todos os atributo para qualquer SP, sempre que este ou outro SP solicitar;
- Deve aceitar a liberação dos seus atributos num primeiro acesso à um SP (se a liberação de todos os atributos não foi aprovada).

O uApprove não permite escolher quais atributos serão liberados, somente se serão ou não liberados para o SP que o usuário está tentando acessar. Na Figura 2.7, é possível visualizar como é o fluxo do uApprove, quais condições são necessárias para que a aplicação apareça para o usuário e permita visualizar os atributos que estão sendo liberados assim como o Termo de Uso do IdP de origem do usuário.

Como o uApprove é um *plug-in* para o IdP é necessário configurá-lo como tal, inserir as chamadas do uApprove dentro das configurações do IdP possibilitando que o primeiro possa

[12] https://www.switch.ch/aai/support/tools/uApprove.html
[13] http://www.switch.ch/

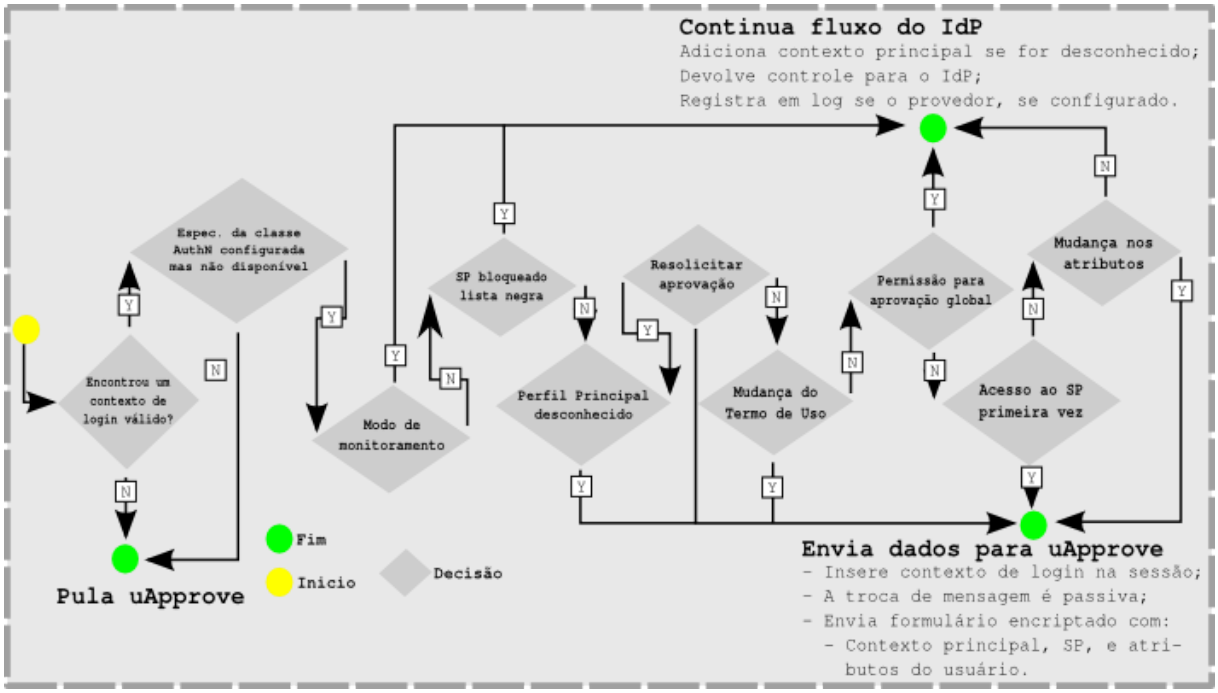


Figura 2.7: Fluxo de mensagens que definem o funcionamento do uApprove

interceptar o fluxo normal do IdP e verificar se o usuário possui um contexto de *login* válido, para então obter os atributos e mostrar no navegador *web* do usuário o que está sendo solicitado pelo SP e o que está sendo liberado dos atributos solicitados. Ao término do fluxo, se o usuário aceitar o Termo de Uso e aprovar a liberação dos atributos, o uApprove regitra esta interação no banco de dados. Caso tenha alterações no Termo de Uso ou mais atributos sejam liberados para o usuário, o uApprove verifica estas informações novamente e solicita novo consentimento do usuário.

Os requisitos de *software* para instalação do *uApprove* estão listados na Tabela 2.1.

Software	Versão utilizada	Fornecedor
IdP Shibboleth	2.4.0	Internet2
uApprove	2.5	SWITCHaai
MySQL	5.5.37	Oracle
MySQL JDBC Connector	2.5.25	Oracle

Tabela 2.1: Requisitos de *software* para implantação do uApprove.

O uApprove proporciona algumas funcionalidades: permite que o usuário limpe os atributos liberados anteriormente e força que o uApprove verifique novamente as informações dos atributos do usuário que estão sendo solicitados pelo SP. Além disto, o administrador do IdP que tenha o uApprove, pode habilitar que, em casos de falha de conexão com Banco de Dados, o uApprove aja como se estivesse realizando o registro das informações liberadas pelo usuário, no entanto, a aprovação do consentimento do usuário não será registrada no banco, mas mostrará

ao usuário os dados solicitados pelo SP, porém num próximo *login*, será solicitado novamente o consentimento de liberação de atributos do usuário para aquele SP.

2.5 Considerações finais

Entre os diversos modelos de Gestão de Identidade, atualmente, o modelo federado vem sendo amplamente adotado por instituições de ensino e por grandes empresas. Para possibilitar isto o padrão SAML define mecanismos para criação de infraestruturas de Gestão de Identidades federadas e especifica uma série de perfis e ligações para trocas de mensagens *bindings* o que permite diferentes cenários de uso. Além disto, define um conjunto de metadados que especificam que tipos de atributos devem ser utilizados, permitindo que sejam definidos entre os participantes de uma federação. O Shibboleth é um sistema de gerenciamento de identidades federadas que aplica os conceitos e especificações do padrão SAML e provê os componentes necessários para estabelecimento de um ambiente federado entre organizações.

Com o amadurecimento do *framework* Shibboleth, constata-se que este provê um sistema de gerenciamento de identidades federadas possível de ser adotado não só no âmbito acadêmico, como é o exemplo da CAFe, mas também no governamental e privado.

3 *Federação CAFe*

Em Julho de 2007, a RNP com a colaboração das instituições CEFET-MG, UFC, UFF, UFMG e UFRGS, dentro do escopo do projeto Infraestrutura de Autenticação e Autorização Eletrônica (e-AA), tinham como objetivo criar condições necessárias para a implantação de uma comunidade acadêmica federada no Brasil, a CAFe. Uma federação acadêmica envolve instituições de ensino e pesquisa e permite que as pessoas vinculadas a estas instituições compartilhem informações e recursos e tenham acesso a serviços restritos, usando o vínculo institucional como critério básico para esse compartilhamento (MOREIRA et al., 2011). A partir destes esforços, surgiu a Comunidade Acadêmica Federada (CAFe).

A CAFe tem como objetivo congregar todas as universidades e instituições de pesquisa brasileiras. A metodologia adotada para construção da infraestrutura básica de federação consiste na utilização de padrões e soluções de software já disponíveis e adotados por outras federações, e da implementação e experimentação de ferramentas auxiliares para apoiar a implantação de provedores de identidades e de serviços. O projeto de criação da Federação CAFe incluia ainda o estudo, a proposição, a análise e a validação de políticas para regular o funcionamento da federação (MOREIRA et al., 2011).

Atualmente, o padrão SAML se firmou como um padrão para a troca de informações de autenticação e autorização entre provedores de identidade e de serviço. Entre as tecnologias baseadas no SAML, o *framework* Shibboleth, desenvolvido no âmbito do projeto Internet2, vem sendo utilizado por diversas federações acadêmicas. A CAFe, que reúne as instituições de ensino e pesquisa brasileiras, utiliza o Shibboleth como sistema de Gestão de Identidades (WANGHAM et al., 2013).

3.1 Como funciona

As instituições pertencentes à CAFe podem atuar como provedores de identidade (IdP) ou como provedores de serviço (SP), ou ainda podem ter ambos os provedores dentro das suas

dependências. As organizações usuárias da RNP que atuam como provedores de identidade têm atualmente um subsídio completo no preço associado ao uso do serviço da CAFe. Além disso, nenhum dos acordos atuais prevê qualquer custo para os provedores de serviço. A RNP é responsável pela gestão do serviço e por manter o repositório centralizado com dados sobre integrantes da federação (RNP, 2009b).

Na CAFe, cada usuário tem uma conta única em sua instituição de origem, que é válida para todos os serviços oferecidos na federação. Isto é possível devido a relação de confiança entre as instituições participantes da CAFe e permite que o usuário use as credenciais de acesso da sua instituição de origem para acesso aos serviços disponibilizados na federação (RNP, 2009b).

Outro aspecto positivo é o controle sobre a privacidade dos dados. Ao invés de ter um cadastro individual em cada serviço, a federação permite que o provedor de identidade forneça ao provedor de serviço apenas o mínimo de informação necessária para o controle de autorizações. Isto pode variar da simples garantia de que aquele usuário é reconhecido e autenticado pela instituição até informações sobre seu status ou tempo de serviço junto a essa instituição. Os acordos firmados pelos provedores de serviço com a CAFe garantem que os dados serão usados apenas para os fins combinados[1].

Diversos países já têm federações em funcionamento ou em implantação. Dentro das redes de instituições de ensino, os serviços de ensino a distância e atividades de colaboração estão entre os maiores beneficiários das infraestruturas oferecidas por federações (RNP, 2009b).

3.2 Serviços disponíveis

Os principais serviços disponíveis na CAFe são:

- video@RNP – O portal de Vídeo Digital da RNP agrega três diferentes serviços (Vídeo Sob Demanda, Transmissão de Vídeo ao Vivo e Transmissão de Sinal de TV) e se integra ao conteúdo do serviço Videoaula@RNP;
- Portal de Periódicos CAPES - O portal de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) é uma biblioteca virtual, que reúne e disponibiliza a instituições de ensino e pesquisa no Brasil o melhor da produção científica internacional;
- JEMS – O *Journal and Event Management System* (JEMS) é um sistema para submissão,

[1] http://portal.rnp.br/web/servicos/beneficios

revisão, discussão e seleção de artigos para eventos científicos da Sociedade Brasileira de Computação (SBC), mantido pela Universidade Federal do Rio Grande do Sul (UFRGS). Seu principal objetivo é disponibilizar para acadêmicos participantes de eventos da SBC uma infraestrutura para envio de artigos e resumos para avaliação. Assim, é possível a análise de tais documentos por parte da organização do evento e a decisão de quais deles serão selecionados para participação;

- GENI – O *Global Environment for Network Innovations* (GENI)[2] é um portal de infraestrutura de pesquisa patrocinado pela *National Science Foundation* (NSF), órgão dos Estados Unidos de fomento ao desenvolvimento científico. O portal disponibiliza um ambiente laboratorial para redes e sistemas distribuídos para ensino e pesquisa com múltiplos *testbeds*. O laboratório virtual possibilita pesquisas sobre o futuro das redes de grande porte, criando oportunidades de compreensão, inovação e transformação das redes globais e suas interações com a sociedade;

- RedCLARA – Os serviços que operam sobre a infraestrutura da RedCLARA[3] são destinados a promover o desenvolvimento de iniciativas de colaboração científica e acadêmica na América Latina, oportunidades reais para pesquisadores, cientistas e acadêmicos da região;

- GISELA – O Gisela Science Gateway é um portal de aplicações científicas do projeto *Grid Initiatives for e-Science virtual Communities in Europe and Latin America* (GISELA), que funciona como uma interface para um ambiente de grid;

- Atlases – O Atlases é uma biblioteca de imagens de patologia em alta resolução. É voltado para estudantes de Medicina e profissionais da área médica;

- PADBR – A grade computacional PADBR oferece acesso integrado aos recursos de alto desempenho distribuídos geograficamente entre os Centros Nacionais de Processamento de Alto Desempenho (CENAPAD) geograficamente distribuídos. São nove unidades, operadas respectivamente pela UFRGS, UFMG, UFC, UNICAMP, UFRJ, UFPE, INPE, INPA e LNCC. Este último coordena o sistema por delegação do Ministério da Ciência, Tecnologia e Inovação (MCTI).

Todos os serviços descritos acima estão disponíveis para acesso gratuito. A lista de serviços pode ser encontrada no *site* da CAFe[4]

[2] https://portal.geni.net/
[3] http://www.redclara.net/index.php
[4] http://portal.rnp.br/web/servicos/servicos-disponiveis

3.3 Acordos internacionais

A disponibilização ou criação de novas infraestruturas de autenticação e autorização federadas para as suas comunidades acadêmicas está se tornando uma prática comum em vários países. Tipicamente, as iniciativas de criação de infraestruturas federadas são coordenadas pelas redes nacionais de ensino e pesquisa, *National Research and Education Network* (NREN), como a RNP. A CAFe se tornou um projeto pioneiro no Brasil e estabeleceu acordos internacionais, que permitem a integração com diferentes federações do Mundo (RNP, 2009b).

3.3.1 EduGAIN

A CAFe integra, desde Dezembro de 2012, o serviço eduGAIN[5], que reúne, em uma rede de confiança, as federações de Gestão de Identidade sócias da *pan-European Research and Education Network* (GEANT)[6] (Rede de Pesquisa pan-Européia). A organização é uma rede de alta capacidade que engloba mais de três mil instituições de ensino e pesquisa em 32 países, através de 28 redes nacionais e regionais de ensino e pesquisa.

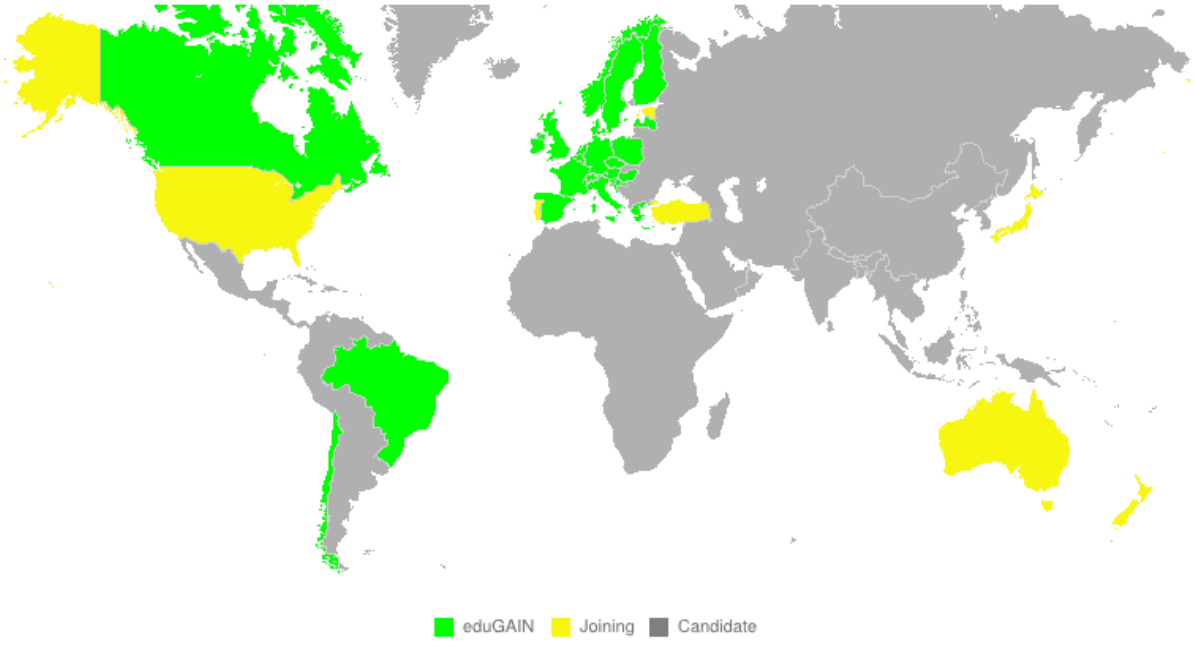


Figura 3.1: Mapa de países com federações participantes da EduGAIN. Fonte: EduGAIN (http://edugain.org/technical/status.php)

Além do Brasil, representado pela CAFe, fazem parte da eduGAIN federações da Croácia, Finlândia, Hungria, Itália, Noruega, Espanha, Suécia e Suíça. Constam também na lista de

[5]http://www.geant.net/service/edugain/pages/home.aspx
[6]http://www.geant.net/pages/home.aspx

candidatos a integrar a confederação os seguintes países: República Tcheca, França, Alemanha, Grécia, Letônia e Holanda. A CAFe foi, portanto, a primeira federação das Américas a fazer parte desta rede de confiança.

O principal benefício para os clientes da CAFe é a possibilidade de utilizar os diversos serviços disponibilizados pelas inúmeras organizações que integram a eduGAIN.

3.3.2 REFEDS

Desde Março de 2011, a CAFe integra o mapa das federações de identidade mundiais de educação e pesquisa mantido pela *Research and Education Federations* (REFEDS)[7].

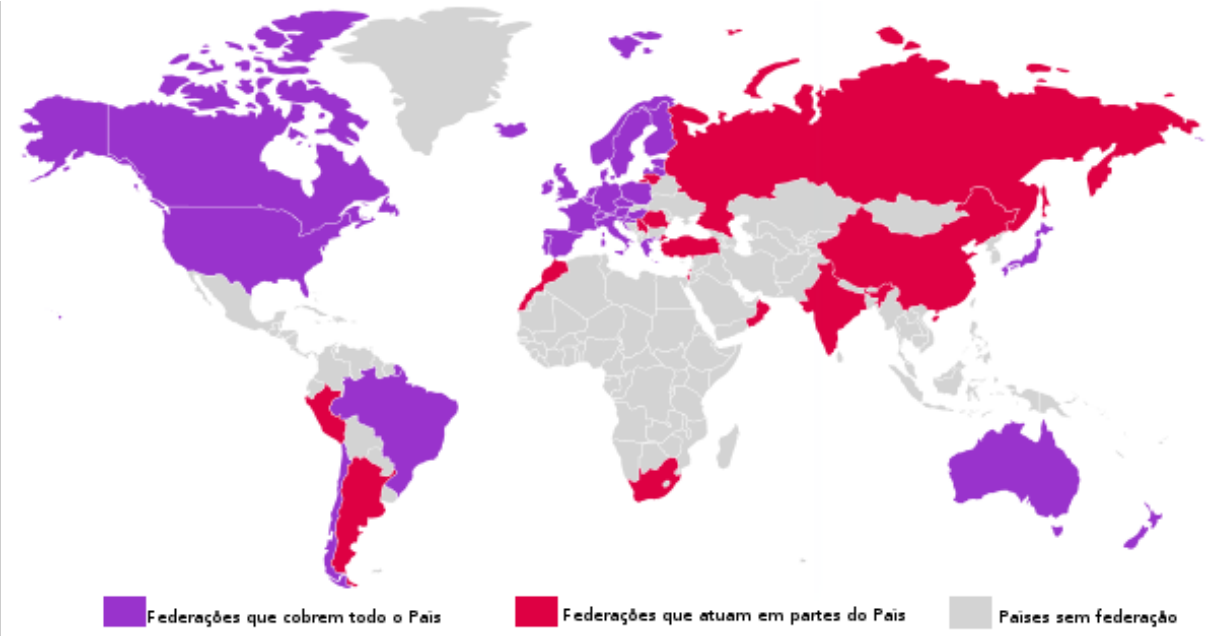


Figura 3.2: Mapa de países com federações participantes da REFEDS. Fonte: REFEDS (https://refeds.org/resources/)

Assim, a CAFe se tornou a primeira federação da América Latina a ser reconhecida internacionalmente pela iniciativa, gerenciada pela *Trans-European Research and Education Networking* (TERENA)[8], que articula as necessidades de federações de identidade para educação e pesquisa em todo o mundo.

Os participantes da REFEDS compartilham o interesse de desenvolver tecnologias, políticas e processos de Gestão de Identidade. Muitos destes representam redes nacionais de ensino e pesquisa, NREN, como é o caso da RNP.

[7] http://www.terena.org/activities/refeds
[8] http://www.terena.org/

3.4 Esquema brEduPerson

Usando como base o conjunto de atributos *eduPerson*, a RNP propôs uma adaptação deste esquema para as universidades e instituições brasileiras e o denominou *brEduPerson*. O esquema *brEduPerson* visa complementar o conjunto original de esquemas que descrevem informações sobre pessoas, o *inetOrgPerson*, o *eduPerson* e o esquema *SCHema for ACademia* (SCHAC) definido por (TERENA, 2009). Este esquema armazena informações específicas para a realidade do país, tais como informações genéricas de qualquer cidadão residente no Brasil, (como CPF, Endereço, Passaporte), informações gerais sobre os membros de uma instituição (e-mail, cargo entre outros) além de informações específicas sobre os funcionários e alunos destas instituições. Tendo estas características definidas, a RNP definiu que 6 atributos são altamente recomendados, 10 são sugeridos e 25 são opcionais[9].

A gestão do esquema brEduPerson ocorre da seguinte maneira: as instituições de ensino e pesquisa juntamente com a RNP participam do desenvolvimento para melhorias do esquema brEduPerson, onde a comunidade e o comitê gestor, atraves de fóruns, discutem e geram demandas de alterações que são discutidas em workshops, gerando as alterações que são posteriormente implementadas pelo comitê gestor no esquema, sendo então publicado no site da CAFe. A Figura 3.3 demonstra como fica o fluxo de interações até publicação das alterações.

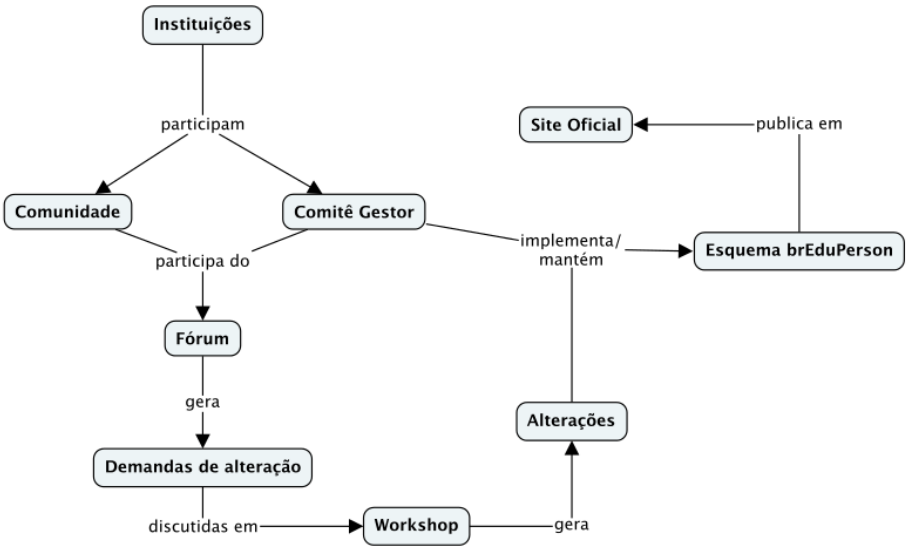


Figura 3.3: Gestão do esquema brEduPerson. Fonte: (RNP, 2009a)

[9]http://wiki.rnp.br/download/attachments/41190038/BrEduPersonv1_0.pdf

3.4.1 Estrutura do esquema eduPerson

Para o uso de um esquema em instituições de ensino e pesquisa, é necessário modelar relacionamentos entre conjuntos de informações. É preciso poder capturar na estrutura de uma base de dados, como uma estrutura de diretórios LDAP, o fato de uma mesma pessoa poder desempenhar diferentes papéis, por exemplo, aluno, e a cada um destes está associada uma data de ingresso, um código de curso, uma matrícula, e outras informações, ou um funcionário que pode ter direito a vários números VoIP, cada um deles com suas características (RNP, 2009a). Para modelar esses relacionamentos, a RNP optou por usar uma solução hierárquica. Os nós em um diretório LDAP formam uma árvore. Cada nó, independentemente de originar algum outro nó na árvore, é uma entrada com suas próprias informações (atributos). Esses nós são por vezes chamados de *containers* na terminologia X.500.

O item principal (uma pessoa) tem uma ligação com uma instituição de ensino e/ou pesquisa com o qual se deseja relacionar as demais informações deste vínculo. Este item será tratado como um *container* e abaixo deste aparecerão nós com as informações relacionadas. As informações genéricas (nome, data de nascimento, CPF, e-mail, tipo de vínculo, etc), aparecerão como entradas, sobre ela, pois cada pessoa pode ter diferentes vínculos com a instituição, como vínculo de estudante em curso, vínculo de funcionário, etc. Abaixo da entrada com os dados gerais podem aparecer diversas entradas descrevendo telefones VoIP, dados biométricos, formas de contato, tais como: e-mail, telefone pessoal etc. (RNP, 2009a).

Cada usuário tem uma entrada principal no esquema, e esta entrada é um objeto de classe estrutural *inetOrgPerson* e das classes auxiliares *schacPersonalCharacteristics*, *eduPerson* e *brPerson*. Abaixo desta classe é recomendável que exista pelo menos uma entrada de classe estrutural *brEduPerson*, que descreve os vínculos de uma pessoa com uma instituição. Cada vínculo será descrito como uma entrada em separado dentro da entrada principal, podendo haver uma quantidade arbitrária de entradas (RNP, 2009a).

O *eduPerson*, no entanto, supõe que uma pessoa possua um único vínculo com uma instituição, com campos multivalorados descrevendo os atributos. Esse modelo não satisfez as necessidades da Federação CAFe, pois era necessário associar a cada vínculo existente (professor, estudante, funcionário, coordenador, pós-graduando, pesquisador, e outros) outras informações, como a data de entrada e saída. No esquema *brEduPerson*, tanto a entrada principal de cada indivíduo (de classe estrutural *brPerson*) como cada entrada abaixo dessa que descreve um vínculo (de classe estrutural *brEduPerson*) têm a classe *eduPerson* como auxiliar, pois atributos gerais do indivíduo ficam na entrada principal enquanto que os atributos relativos a um de seus vínculos ficam na entrada específica de vínculo (RNP, 2009a). Na Figura 3.4, é possível

visualizar a distribuição dos atributos de uma pessoa e seus vínculos.

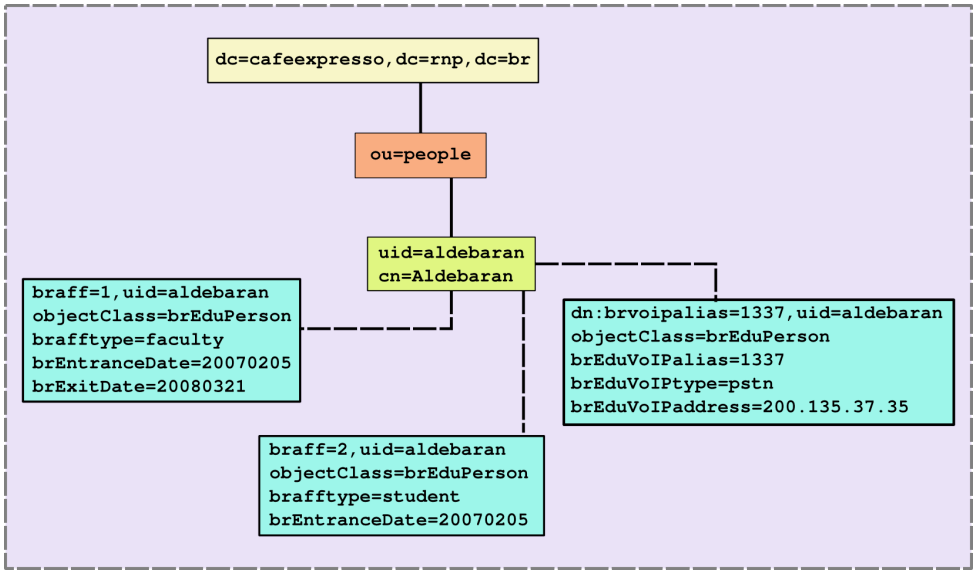


Figura 3.4: Árvore de atributos do brEduPerson. Fonte: (RNP, 2009a)

3.5 Conclusões do capítulo

A CAFe é um importante serviço que proporcionou a disponibilização de diversos serviços para as suas instituições participantes, além de permitir que o acesso a estes serviços seja realizado usando autenticação única, através das credenciais dos usuários, registros, já presentes nas instituições de ensino e pesquisa que participam da federação. Serviços como o JEMS ou o Portal de Periódicos da CAPES são de grande importância para a comunidade acadêmica, e permitir que estes sejam acessados usando a matrícula ou o registro de uma instituição de ensino ao qual o usuário já está matriculado, é uma das facilidades que a CAFe provê para a comunidade.

Além disso, os acordos internacionais firmados pela CAFe com outras federações tendem a melhorar o ambiente de pesquisa e ensino, possibilitando uma maior interação e participação de pesquisas e desenvolvimento tecnológico no cenário mundial. Mas, mais importante, a CAFe permite que o resultado de pesquisas possam ser disponibilizados para a comunidade, que buscam facilitar o desenvolvimento de novas pesquisas em Gestão de Identidades Federadas.

4 *Federação CAFe Expresso*

Gestão de Identidades Federadas é uma área ativa de pesquisa, sendo que muitos trabalhos desenvolvidos nesta área precisam realizar experimentos com soluções e frameworks consolidados e adotados por empresas ou instituições acadêmicas. Desenvolver pesquisas aplicadas na área de gestão de identidades federadas exige que os experimentos sejam conduzidos em um ambiente que implemente uma federação em sua totalidade. A complexidade e trabalho para implantar uma federação, usando o *framework* Shibboleth por exemplo, é muito alta (WANGHAM et al., 2013). A Federação CAFe Expresso é uma resposta da RNP às necessidades de pesquisadores que atuam na área de gestão de identidades federadas.

A RNP mantém no Brasil a Comunidade Acadêmica Federada (CAFe) baseada no framework Shibboleth, porém sua política de uso não permite que pesquisadores a utilizem para realizar seus experimentos. Sendo assim, os pesquisadores devem dedicar uma quantidade razoável de seu tempo para construir seu próprio ambiente federado, executar seus experimentos e depois se desfazer do ambiente, uma vez que seria custoso manter disponível a federação, em termos de recursos computacionais, aplicação de correções de segurança, evolução dos softwares utilizados, etc. Em suma, configurar uma federação para realizar experimentos de uma pesquisa, pode ser uma tarefa mais árdua e demorada do que a implementação da pesquisa propriamente dita.

Motivada por esta necessidade, a RNP criou em 2013 o Laboratório de Experimentação em Gestão de Identidades (GId Lab)[1], um projeto que tem por objetivo disponibilizar para a comunidade acadêmica um ambiente virtual no qual os pesquisadores possam realizar testes com Infraestruturas de Autenticação e Autorização (IAA) e também Infraestruturas de Chaves Públicas (ICPs).

Mantido pela RNP como plataforma de apoio aos pesquisadores brasileiros, principalmente os participantes do Programa de Gestão de Identidade (PGID) e dos Grupo de Trabalhos (GTs) da RNP (WANGHAM et al., 2013), o projeto GId Lab provê uma Infraestrutura de Autenticação

[1] http://wiki.rnp.br/display/gidlab

e Autorização, que trata da especificação de uma federação para experimentos permitindo que desenvolvedores e pesquisadores de qualquer instituição de ensino do Brasil possam desenvolver serviços ou disponibilizar um provedor de identidade, tendo como base o *framework* Shibboleth.

O projeto GId Lab provê ainda o Sistema de Gerenciamento de Certificados Digitais ICPEdu (SGCI)[2] da Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu)[3], um software desenvolvido para o âmbito acadêmico, em uso em diversas universidades e centros de pesquisas brasileiros, que permite a implantação e gerenciamento de Autoridades Certificadoras (CAs), para emissão de certificados digitais. Este provê as funcionalidades necessárias para o gerenciamento da Infraestrutura de Chave Pública (ICP) (WANGHAM et al., 2013).

4.1 Visão geral da CAFe Expresso

A Figura 4.1 ilustra a infraestrutura de autenticação e de autorização disponível dentro do GId Lab, assim como as máquinas virtuais que serão disponibilizadas para os pesquisadores interessados.

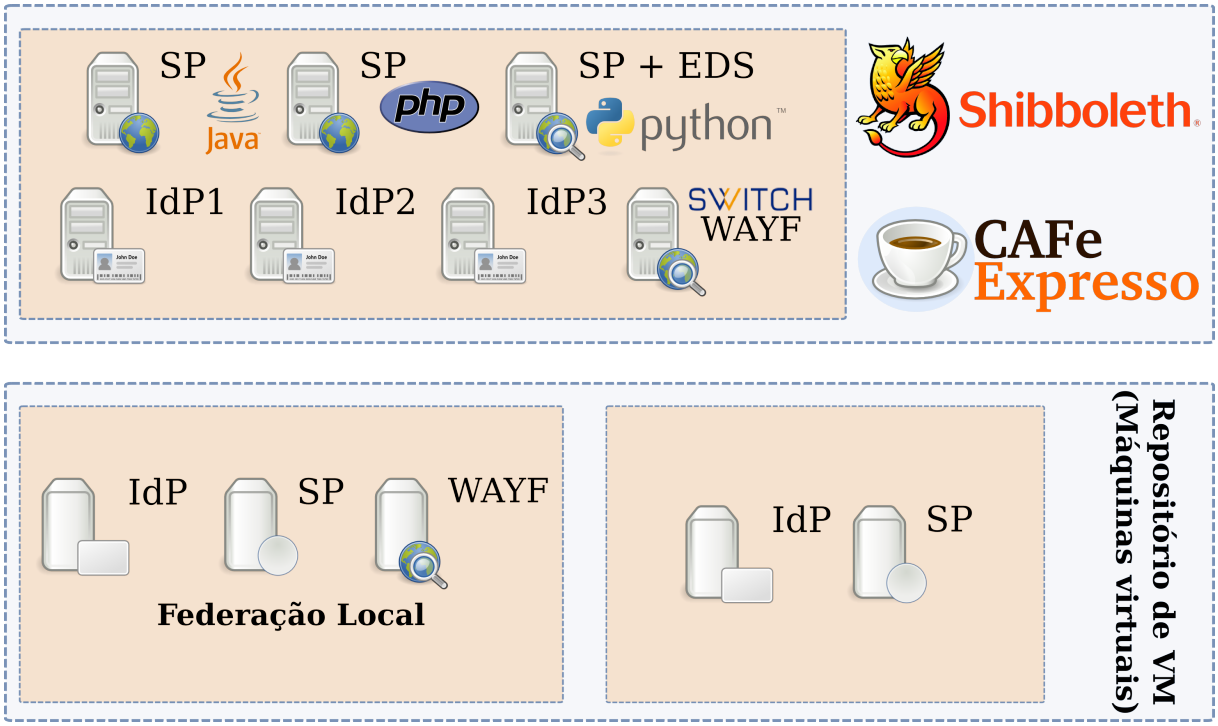


Figura 4.1: Estrutura da CAFe Expresso no GId Lab.

Dentro do contexto do projeto GId Lab a CAFe Expresso oferece três *Identity Providers*

[2]https://projetos.labsec.ufsc.br/sgci
[3]http://www.rnp.br/servicos/icpedu.html

(IdPs) alimentados com usuários com diferentes perfis e atributos e três *Service Providers (SPs)* configurados para proteger aplicações web em PHP, Java e Python. Desta forma, pesquisadores poderão implementar suas soluções em uma dessas linguagens e só precisarão disponibilizá-las por meio destes SPs. Estes provedores de serviços e de identidades estão espalhados[4] pelos Ponto de Presenças (PoPs) da Rede Ipê[5] da RNP.

Em um dos IdPs da CAFe Expresso, o módulo de consentimento do usuário, conhecido como *uApprove*[6] foi integrado. Este módulo tem como objetivo informar ao usuário quais atributos estão sendo liberados para o SP, no momento que está sendo solicitado a autenticação do usuário no IdP da sua instituição e o encaminhamento, por meio da asserção de atributos SAML, para o SP no qual está sendo solicitado o serviço.

Conforme indicado na Figura 4.1, o projeto GId Lab disponibiliza aos pesquisadores um repositório com máquinas virtuais (*Virtual Machine*s (VMs)). Com estas máquinas virtuais, é possível criar um federação local completa (um IdP, um SP e um WAYF) ou implantar um IdP ou um SP a partir de máquinas virtuais pré-configuras e prontas para serem incluídas na CAFe Expresso.

O serviço *Where Are You From* (WAYF) ou *Discovery Service* (DS) está disponível na CAFe Expresso como uma máquina virtual separada. Além do WAYF, foi integrado em um dos SP um serviço de descoberta (*Embedded Discovery Service* – EDS) que tem o mesmo objetivo do WAYF, porém o EDS está embutido na página do SP, diminuindo a transição entre diferentes páginas *web* para escolha do IdP, como ilustrado na Figura 2.5.

Serão também disponibilizados na CAFe Expresso dois serviços adicionais que foram resultado de pesquisas realizadas na área de Gestão de Identidades e IAA, dentro do escopo de projeto de pesquisa e desenvolvimento da RNP chamado Grupo de Trabalho Serviços para Transposição de Credenciais de Autenticação Federadas (GT-STCFed) do Comitê Técnico de Gestão de Identidade (CT-GId)[7] da RNP, para possibilitar integrações entre ambientes diferentes do provido pelo *framework* Shibboleth. Devido a grande complexidade de implantação destes serviços, estes serviços não foram inclusos no contexto deste trabalho.

[4] http://wiki.rnp.br/display/gidlab/Infraestrutura
[5] http://www.rnp.br/ipe/
[6] http://www.switch.ch/aai/support/tools/uApprove.html
[7] http://portal.rnp.br/web/servicos/comite-tecnico-de-gestao-e-autorizacao-de-identidade-ct-gia

4.1.1 Tecnologias e ferramentas utilizadas

Para implantação de uma infraestrutura em ambientes computacionais, é comum que sejam necessários muitos serviços, aplicações e/ou bibliotecas para que esta infraestrutura esteja disponível. A seguir, será apresentada uma breve descrição dos *softwares* necessários para implementação da uma Infraestrutura de Gestão de Identidade Federada para uso do *framework* Shibboleth.

Framework Shibboleth

O *framework* Shibboleth (SHIBBOLETH, 2005) é utilizado por federacões acadêmicas de diversos países, incluindo a Comunidade Acadêmica Federada (CAFe). É um conjunto de *softwares* Open Source mantido pelo consórcio Internet2[8]. O *framework* Shibboleth implementa amplamente o padrão SAML da OASIS. O conjunto é formado por dois componentes, o Shibboleth IdP e o Shibboleth SP. A versão mais atual do *framework* Shibboleth é a versão 2.5.2 para o Shibboleth SP e a versão 2.5.1 para o *Shibboleth IdP*, porém, como a federação CAFe utiliza a versão 2.1.5 do *Shibboleth IdP* e a versão 2.4.3 para o *Shibboleth SP* estas serão as versão utilizadas na CAFe Expresso.

O sistema operacional utilizado em todas as máquinas da CAFe Expresso é o Ubuntu Linux versão 12.04 LTS. A documentação do Shibboleth disponibiliza versão do *framework* para as plataformas GNU/Linux, Windows e MacOS. A escolha da plataforma GNU/Linux foi feita por ser *software* livre. Além disto, é a mesma distribuição escolhida para estar alinhada a usada na federação CAFe.

O *framework* Shibboleth por si só não contempla todos os serviços necessários para o uso como uma federação completa. Além do *framework* Shibboleth é necessário ter nos servidores o Apache, o Apache-Tomcat, o OpenJDK, o OpenSSL, o OpenLDAP, e outros. Além destes elementos, foi implantado o serviço WAYF, responsável por oferecer ao usuário uma página web onde o usuário pode escolher o seu provedor de identidade. Estes são os elementos necessários para implantação de uma Federação Shibboleth completa.

Usando a CAFe Expresso o pesquisador não necessita implantar todos os elementos chaves de uma federação, permitindo que seja implementado um IdP ou um SP, dependendo da necessidade da pesquisa. Cada um possui um processo de instalação e configuração próprio, com níveis de complexidade diferentes.

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

O processo de implantação destes elementos, assim como os serviços adicionais que cada um destes precisará para funcionar foram simplificados com o objetivo de incentivar o uso e as pesquisas em Gestão de Identidade. Com isso o processo de configuração completo para cada elemento não será descrito, somente as partes mais importantes que são específicas de cada instituição ou que o pesquisador tiver disponível.

Nos tópicos seguintes serão descritos os requistos de *softwares* e *hardware* utilizados para implantação da CAFe Expresso. Assim como orientações para gerenciamento do ambiente, e onde esta infraestrutura está disponível.

4.1.2 Infraestrutura

Foram utilizadas 8 máquinas virtuais para realização deste trabalho, que estão espalhadas pelos Pontos de Presença (PoPs) da RNP. As especificações de *hardware* das máquinas virtuais utilizadas podem ser vistas na tabela abaixo. Entre os servidores que estão alocados nos PoPs, além dos os IdPs e SPs, duas delas tem propósitos diferentes, e são descritas a seguir:

- Repo (repositório) – Servidor que armazena arquivos de configurações específicos e pré-editados, assim como as máquinas virtuais que foram disponibilizadas;
- DS (*Discovery Service*)– Servidor que faz papel de WAYF para a federação CAFe Expresso.

As configurações das VMs utilizadas na implantação do ambiente da CAFe Expresso foram baseadas na recomendação de Hardware para um IdP, disponível na Wiki[9] do Shibboleth e pode ser vista na Tabela 4.1:

Processador	Espaço em Disco	Memória RAM
1GHz	150 MB	1 GB

Tabela 4.1: Requisitos de Hardware recomendado para IdP Shibboleth

Conforme descrito na Wiki do projeto Shibboleth, estas configurações são recomendadas para um ambiente de demonstração, que suporta de 25 à 40 requisições de acesso por minuto. Para uma configuração de ambiente de produção a configuração necessita ser um pouco mais robusta. Baseado nessa recomendação a Tabela 4.2, descreve as configurações de Hardware disponível para os servidores, tanto IdPs quanto SPs da CAFe Expresso. Além do Sistema

[9]https://wiki.shibboleth.net/confluence/display/SHIB/IdPPlatform

Operacional utilizado e a configuração de Hardware de cada servidor, está descrito também o Hostname (nome) definido para cada servidor.

Sistema Operacional	Espaço em Disco	Memória RAM	Hostname
Ubuntu Linux 12.04 LTS 64bits	15 GB	1 GB	IdP1 IdP2 IdP3 SP-Python SP-PHP SP-Java DS Repo

Tabela 4.2: Configuração de *hardware* dos servidores da CAFe Expresso

Na Figura 4.2 é possível visualizar quais PoPs de quais Estados do Brasil estão alocadas as máquinas virtuais que compõem a federação para experimentação.

Figura 4.2: PoPs da RNP onde estão alocadas as VMs da CAFe Expresso

4.1.3 Identity Provider - IdP

O provedor de identidade é responsável por manter as informações sobre as pessoas vinculadas a uma instituição. Estas informações incluem: Nome, Data de nascimento, Filiação, Sexo, CPF, entre outros. Assim como os tipos de informações internas: Data de admissão, Cargo ocupado, Matrícula, Contato telefônico, Vínculo que as pessoas possuem com a instituição (estudante, técnico administrativo, professor e outros). O IdP estabelece seu método de autenticação interno e deve garantir que cada pessoa tenha um identificador único (MOREIRA et al., 2011).

Para implantação do IdP, são necessários alguns softwares e serviços adicionais. Na tabela 4.3, é possível verificar os requisitos de *software* necessários para implantação do IdP.

Software	Versão utilizada	Fornecedor
IdP Shibboleth	2.1.5 e 2.4.0	Internet2
OpenJDK	6b31-1	Oracle
Apache	2.2.22	Apache Software Foundation
Tomcat	6.0.35	Apache Software Foundation
OpenLDAP	2.4.28	OpenLDAP Foundation
OpenSSL	1.0.1	OpenSSL Project

Tabela 4.3: Requisitos de *software* para implantação do IdP.

Para a instalação do IdP, são necessários diversos procedimentos, configurações de arquivos, de serviços, sendo um processo complexo e demorado. Neste trabalho, foi utilizada a documentação gerada pela RNP disponível na wiki[10]. Este processo foi simplificado para a configuração das máquinas virtuais que foram disponibilizadas, para que os pesquisadores não precisassem se preocupar com a instalação do IdP Shibboleth, esta documentação também está disponibilizada na wiki do Gid Lab[11].

Na Figura 4.3, é possível visualizar como fica o encapsulamento dos serviços envolvidos para prover o IdP Shibboleth.

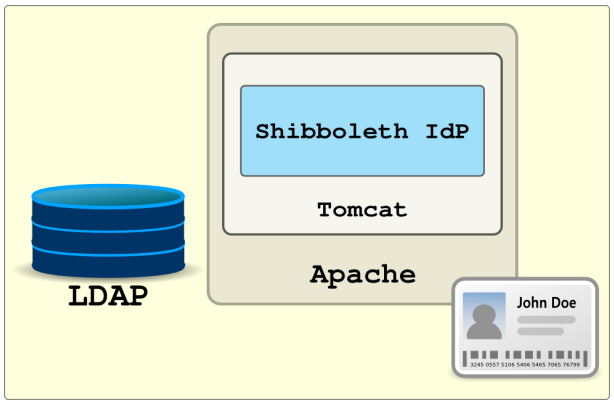


Figura 4.3: Encapsulamento dos serviços envolvidos para prover o IdP Shibboleth

O servidor Apache é responsável por interpretar as requisições HTTP do navegador do usuário e por dar suporte ao Apache-Tomcat, o *container* Java, que permite a troca de mensagens e faz a interface entre as requisições HTTP e o Shibboleth IdP. O Shibboleth IdP é uma aplicação Java com componentes em C. É possível utilizar outros *containers*, como Jetty[12]. O LDAP é responsável por armazenar as informações dos usuários e é consultado pelo IdP sempre que este recebe uma solicitação de autenticação.

[10] https://wiki.rnp.br/display/cafewebsite/Roteiro+de+Atividades+para+Entrada+de+um+IDP
[11] https://wiki.rnp.br/display/gidlab/Procedimentos+operacionais+da+CAFe+Expresso
[12] http://download.eclipse.org/jetty/

4.1.4 Service Provider - SP

O provedor de serviço é responsável por fazer a autorização do usuário e disponibilizar o acesso ao recurso que o usuário deseja através da autenticação e dos atributos disponibilizados pelo IdP.

A instalação padrão de um Provedor de Serviço é baseada no Shibboleth SP. O foco do SP é proteger a aplicação desenvolvida pelo pesquisador. O processo consiste na instalação de dois elementos:

- mod_shib – módulo do Apache, responsável por controlar a autorização e o acesso ao recurso;
- shibd – *daemon* (serviço), responsável por intermediar a solicitação de autenticação e de atributos (MOREIRA et al., 2011).

Software	Versão utilizada	Fornecedor
SP Shibboleth	2.4.3	Internet2
Apache com módulo Shibboleth	2.2.22	Apache Software Foundation
OpenSSL	1.0.1	OpenSSL Project

Tabela 4.4: Requisitos de *software* para implantação do SP.

Na Figura 4.4, é possível visualizar como é o encapsulamento dos serviços envolvidos para provimento do SP Shibboleth.

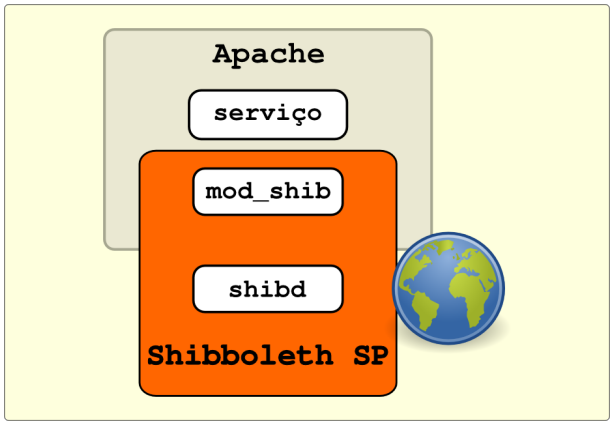


Figura 4.4: Encapsulamento dos serviços envolvidos para prover o SP Shibboleth

Assim como no IdP, no processo de instalação do SP também foi usado a documentação disponibilizada pela RNP disponível na wiki[13]. Na CAFe Expresso, este processo foi simplificado para que pesquisadores só se preocupassem com algumas configurações específicas

[13]https://wiki.rnp.br/display/cafewebsite/Roteiro+de+Atividades+para+Entrada+de+um+SP

referentes ao serviço e ao *host* (ou nome) que irá responder ao navegador. Os procedimentos para configuração do SP da CAFe Expresso podem ser obtidos na wiki do Gid Lab[14].

Para ambos os elementos, é necessário gerar um certificado digital para identificação única, garantindo assim a segurança de cada provedor. No trabalho, foram utilizados certificados auto-assinados.

4.2 Relação de projetos usuários da CAFe Expresso

A seguir, estão descritos os projetos que fizeram uso da infraestrutura da CAFe Expresso, seja usando os provedores IdP ou SP, ou fazendo uso das máquinas virtuais pré-configuradas.

Nome projeto:	**Transposição de Credenciais para uso de Testbeds para a Internet do Futuro**
Programa relacionado:	Projeto FIBRE
Instituições envolvidas:	UFF
Coordenador:	Débora Christina Muchaluat Saade
Responsável técnico:	Edelberto Franco Silva
Serviço da CAFe Expresso:	IdP, SP-PHP, SP-Java, Máquinas Virtuais pré-configuradas (SP e IdP)
Tempo de duração:	13 meses (finalizado)

Nome projeto:	**Testes com autenticação federada em uma nuvem OpenStack**
Programa relacionado:	GT-CNC
Instituições envolvidas:	UFRN
Coordenador:	Carlos Eduardo da Silva
Responsável técnico:	Carlos Eduardo da Silva
Serviço da CAFe Expresso:	IdP, IdP+
Tempo de duração:	6 meses (finalizado)

Nome projeto:	**Análise da integração de infraestrutura de nuvem privada com federação CAFe e serviço OpenID**
Programa relacionado:	PGId 2013
Instituições envolvidas:	UFPE
Coordenador:	Carlos André Guimarães Ferraz
Responsável técnico:	Ioram Schechtman Sette
Serviço da CAFe Expresso:	IdP e IdP+
Tempo de duração:	6 meses (finalizado)

[14]https://wiki.rnp.br/display/gidlab/Procedimentos+operacionais+da+CAFe+Expresso

Nome projeto:	**Interoperabilidade entre Shibboleth e OpenAM**
Programa relacionado:	Não informado
Instituições envolvidas:	UFMA
Coordenador:	Zair Abdelouahab
Responsável técnico:	Luiz Aurélio
Serviço da CAFe Expresso:	Máquinas Virtuais pré-configuradas (SP e IdP)
Tempo de duração:	5 meses (finalizado)

Nome projeto:	**Módulo Web de visualização de dados coletados de redes sem fio usando identidades federadas**
Programa relacionado:	Não informado
Instituições envolvidas:	UFRGS
Coordenador:	Cristiano Bonato Both
Responsável técnico:	Leonardo Roveda Faganello
Serviço da CAFe Expresso:	SP-PHP, Máquina Virtual pré-configurada (SP)
Tempo de duração:	6 meses (finalizado)

Nome projeto:	**Teste em ambiente federado para homologação para Federação CAFe**
Programa relacionado:	GT-CoLisEU
Instituições envolvidas:	UFRGS
Coordenador:	Lisandro Zambenedetti Granville
Responsável técnico:	Cristiano Bonato Both
Serviço da CAFe Expresso:	SP-PHP, Máquina Virtual pré-configurada (SP)
Tempo de duração:	3 meses (finalizado)

Nome projeto:	**Experimentos com Gestão de Identidades usando Shibboleth**
Programa relacionado:	GT-Tel
Instituições envolvidas:	PUC-Rio
Coordenador:	Noemi Rodriguez
Responsável técnico:	Ian Baldo
Serviço da CAFe Expresso:	IdP, SP-Java, Máquina Virtual pré-configurada (SP)
Tempo de duração:	10 meses (em andamento)

Nome projeto:	**Implantação de IdPs para uso em instituições de ensino para o projeto CENPC**
Programa relacionado:	GT-CNC
Instituições envolvidas:	UFPA
Coordenador:	Roberto Samarone
Responsável técnico:	Carlos Eduardo da Silva
Serviço da CAFe Expresso:	Máquinas Virtuais pré-configuradas (10 IdP)
Tempo de duração:	12 meses (em andamento)

Nome projeto:	**Experimentos com gerenciamento de identidades**
Programa relacionado:	Não informado
Instituições envolvidas:	UFSC
Coordenador:	Jorge Werner
Responsável técnico:	Jorge Werner
Serviço da CAFe Expresso:	Máquinas Virtuais pré-configuradas (SP e IdP)
Tempo de duração:	36 meses (em andamento)

Nome projeto:	**Infraestrutura do controle de acesso baseado em políticas**
Programa relacionado:	PGId 2014
Instituições envolvidas:	UFF
Coordenador:	Débora Christina Muchaluat Saade
Responsável técnico:	Edelberto Franco Silva
Serviço da CAFe Expresso:	Máquinas Virtuais pré-configuradas (IdP)
Tempo de duração:	1 ano (em andamento)

Nome projeto:	**Testes com perfil ECP para envio de credenciais e asserções SAML por meio da biblioteca libcurl**
Programa relacionado:	Projeto SFera – PGId 2014
Instituições envolvidas:	UFF
Coordenador:	Antônio Tadeu Azevedo Gomes
Responsável técnico:	Marcelo Monteiro Galheigo
Serviço da CAFe Expresso:	Máquinas Virtuais pré-configuradas (IdP)
Tempo de duração:	2 meses (em andamento)

4.3 Pesquisa de uso da CAFe Expresso

4.3.1 Objetivo da pesquisa

A pesquisa de uso foi aplicada para avaliar algumas funcionalidades oferecidas na federação CAFe Expresso, suas deficiências, e coletar sugestões de melhorias, verificar a importância de um ambiente para experimentação, assim como a importância de duas tecnologias que não são encontradas na CAFe, o EDS e o *uApprove*. Esta pesquisa foi realizada com pessoas que participam do Comitê Técnico de Gestão de Identidade (CT-GId) da RNP e mais 4 alunos do Mestrado de Computação Aplicada da UNIVALI. O email enviado para potenciais entrevistados encontra-se no Apêndice A. A pesquisa foi realizada período de 19 de Junho de 2014 até 29 de Junho 2014, obtendo um total de 19 respostas de um grupo de 37 pessoas, isto representa 51,35% dos entrevistados.

4.3.2 Resultados da pesquisa

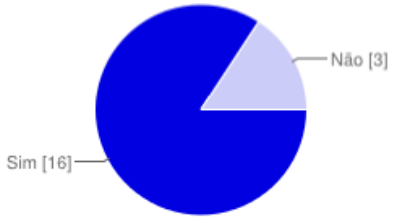
A pesquisa foi dividida em 3 partes. Na primeira parte, os entrevistados avaliam o acesso federado usando o *uApprove*, seguindo um roteiro do experimento. Na segunda parte, os entrevistados avaliam o acesso federado e a funcionalidade provida pelo *Embedded Discovery Service* (EDS), seguindo um segundo roteiro de experimento. Por fim, na terceira parte os entrevistados avaliam a CAFe Expresso como um todo, assim como o roteiro, a linguagem utilizada, se as mensagens de erro (quando aparecem) são claras e se o uso da aplicação foi satisfatório. A pesquisa é composta por perguntas objetivas e descritivas, neste último caso,

são solicitações de sugestões, ou descrições de problemas encontrados, caso haja. As respostas descritivas estão registradas no Apêndice D.

Experimento: Acesso federado com uApprove (e WAYF tradicional)

Nesta primeira avaliação, os entrevistados seguiram o experimento descrito no Apêndice B e, em seguida, responderam algumas questões. A pesquisa inicia com um levantamento se o entrevistado já realizou algum acesso através da federação CAFe e qual o nível de conhecimento referente CAFe.

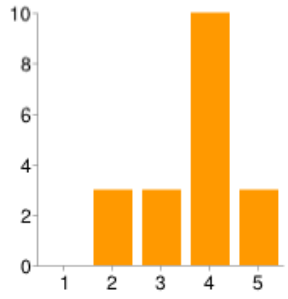
Você já se autenticou alguma vez em um provedor de identidades da Federação CAFe ou Chimarrão?



Sim	**16**	84%
Não	**3**	16%

Figura 4.5: Resultados da avaliação se entrevistado já se autenticou em algum IdP.

Como você avalia o seu conhecimento sobre autenticação federada na CAFe (Framework Shibboleth)?



1	**0**	0%
2	**3**	16%
3	**3**	16%
4	**10**	53%
5	**3**	16%

Figura 4.6: Resultados sobre nível de conhecimento do entrevistado.

Como é possível perceber na Figura 4.5, somente 3 dos entrevistados (16%) nunca acessou nenhum provedor de identidade da CAFe, ou da federação Chimarrão (federação de homologação da RNP, para aqueles que estão ingressando na CAFe). Dos entrevistados, 16% tem um nível de conhecimento sobre autenticação federada baixo, outros 16% se consideram com nível de conhecimento razoável. 53% dos entrevistados tem nível de conhecimento bom sobre autenticação federada e o Shibboleth. 16% dos entrevistados se consideram experientes.

As Figuras 4.7 e 4.8 ilustram os resultados referentes ao serviço uApprove. O objetivo

desta etapa do experimento foi avaliar o entendimento no uso deste serviço. Em 100% dos casos, a resposta sim indica que o serviço estava configurado e funcionando corretamente e que os entrevistados entenderam a função de liberação de atributos.

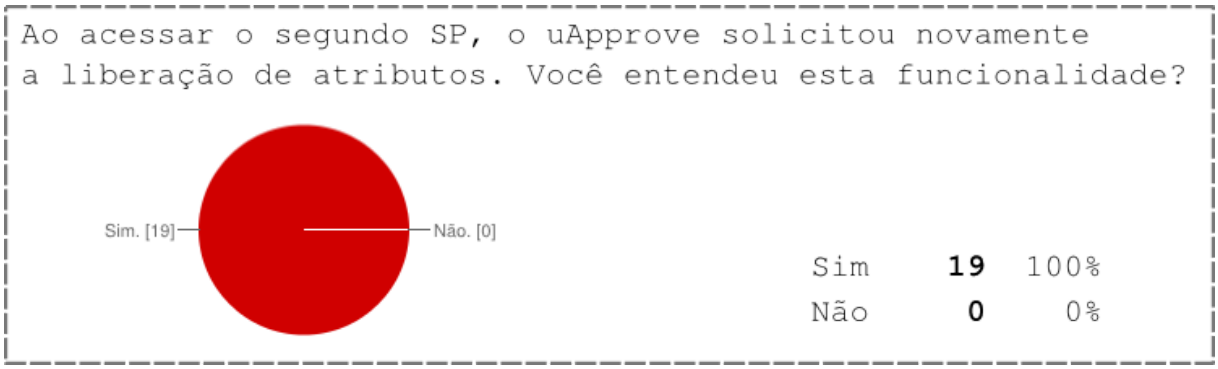


Figura 4.7: Resultados sobre apresentação da solicitação de liberação de atributos do usuário pelo *uApprove*.

Na Figura 4.8 é possível constatar que todos os entrevistados entenderam a funcionalidade do Termo de Uso apresentado pelo *uApprove*. O Termo de Uso é responsável por apresentar quais os direitos e deveres do usuário e do IdP onde este se autentica.

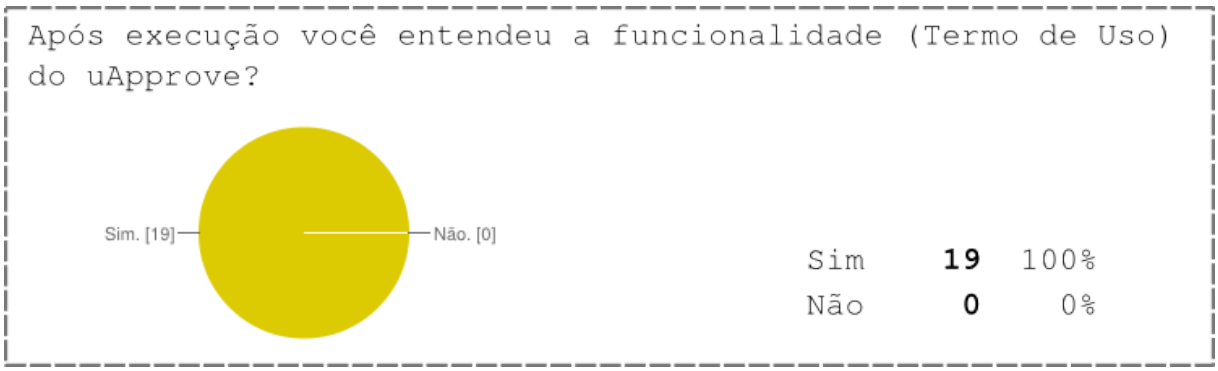


Figura 4.8: Resultados sobre a entendimento da funcionalidade do Termo de Uso do *uApprove*.

De acordo com os comentários registrados pelos entrevistados, não foi encontrado nenhum problema ou dúvida referente ao funcionamento do *uApprove*. Uma sugestão foi registrada: disponibilizar diferentes serviços para o usuário entender melhor o funcionamento e o objetivo do *uApprove*.

Experimento: Acesso federado com Embedded DS (WAYF embarcado)

A segunda parte da pesquisa, trata do acesso federado usando o EDS, ou WAYF Embarcado. Os entrevistados seguiram um segundo roteiro que os direcionou para o uso de uma facilidade que não está implementada na CAFe, o EDS. O EDS permite que o usuário faça a escolha do

seu IdP de origem diretamente na página do SP. O roteiro com os passos para o experimento estão descritos no Apêndice C.

Na Figura 4.9, 84% dos entrevistados acham que o EDS melhora a usabilidade e 16% dos entrevistados responde que o EDS não melhora a usabilidade das aplicações federadas.

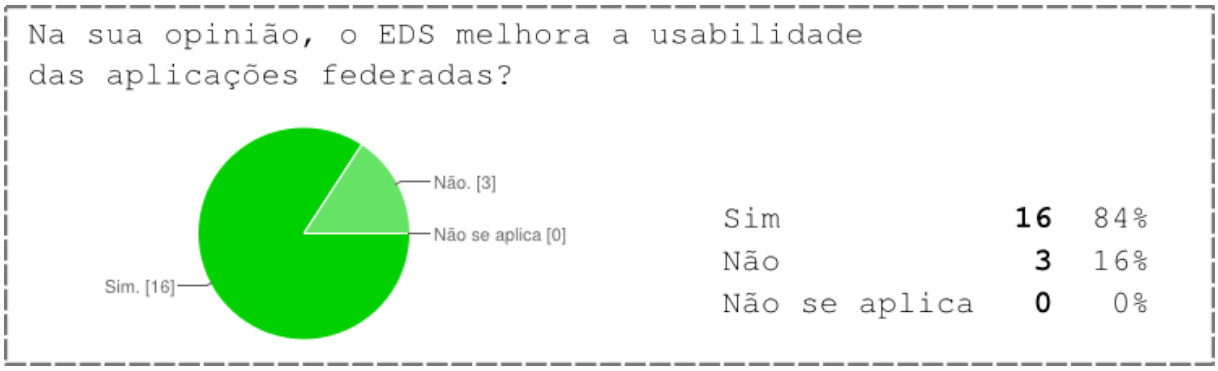


Figura 4.9: Resultados sobre a melhora na usabilidade para o usuário provida pelo EDS.

A Figura 4.10 mostra o resultado ao comparar as funcionalidades WAYF e EDS. 79% dos entrevistados responde que o EDS facilita a escolha do IdP e 21% responderam que não.

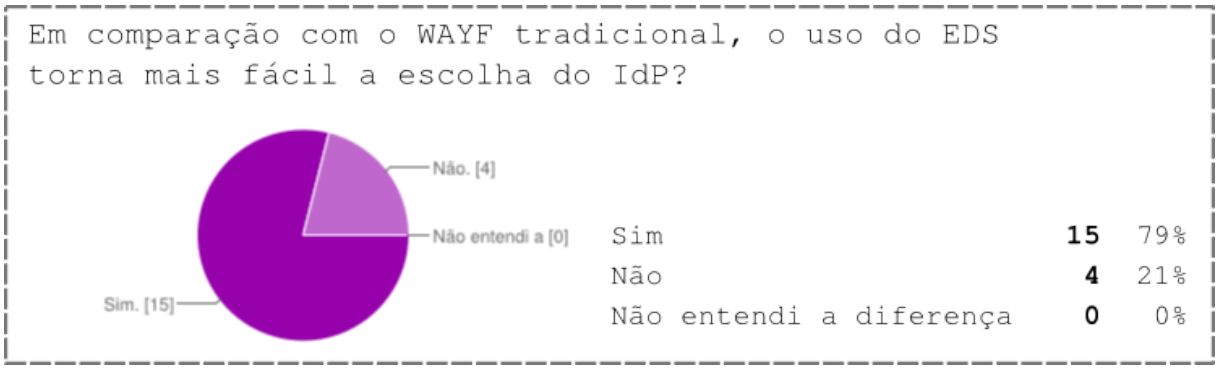


Figura 4.10: Resultados sobre a melhora na escolha do IdP pelo EDS.

Na Figura 4.11, somente uma pessoa não entendeu a funcionalidade do EDS.

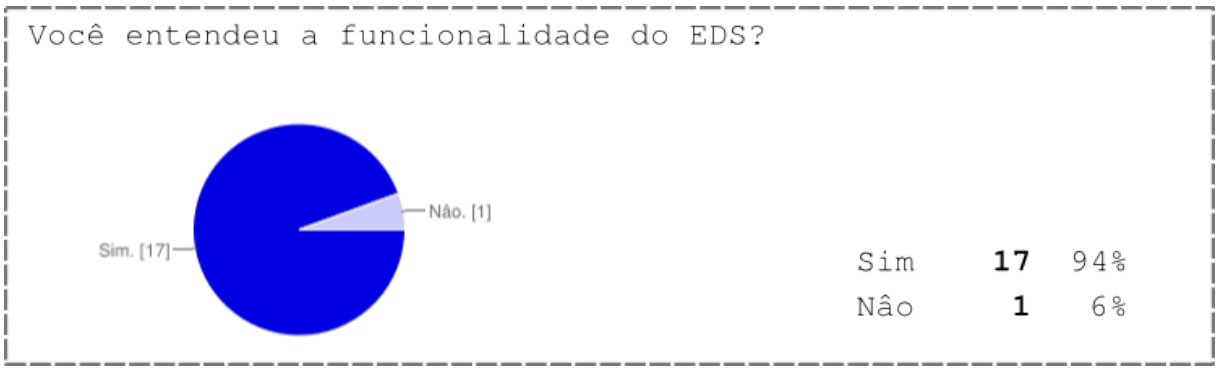


Figura 4.11: Resultados sobre entendimento da funcionalidade do EDS na CAFe Expresso.

Avaliação de uso da CAFe Expresso

Esta parte da avaliação trata de uma avaliação geral dos experimentos com a CAFe Expresso. Questões referentes ao vocabulário utilizado e mensagens de erros também foram avaliadas, assim como o grau de satisfação durante o período de uso. Foram disponibilizados campos de textos para que os entrevistados pudessem dar sugestões para operação da CAFExpresso e pudessem avaliar as contribuições que a federação de experimentação pode trazer para comunidade acadêmica.

A Figura 4.12 mostra que 3 pessoas, 16% dos entrevistados, teve algum problema ao realizar as atividades descritas nos roteiros de experimentos.

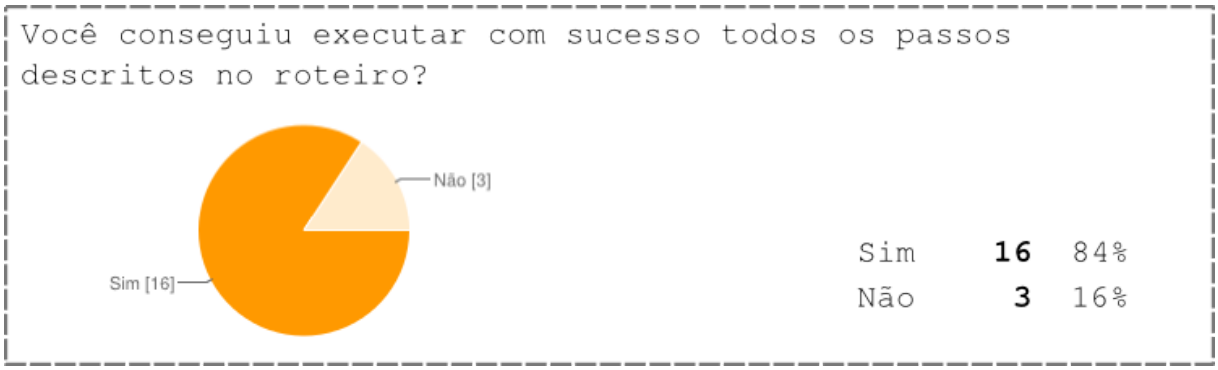


Figura 4.12: Resultados sobre erros ao realizar atividades do roteiro de avaliação.

O problemas encontrados foram referentes a uma falha no PoP-MS onde a máquina SP-Java, um dos SPs utilizados na avalição, estava hospedada. Isso foi resolvido ao entrar em contato com o Suporte GTI da RNP.

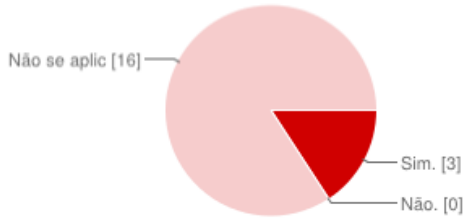
A Figura 4.13, trata das mensagens de erro e se a descrição destas mensagens foram claras. Somente 3 pessoas, 16%, informaram que Sim. Isso indica que as mensagens foram apresentadas. Os outros 84% dos entrevistados informou que "Não se aplica" o que mostra que as mensagens não apareceram.

De acordo com os entrevistados, 63% informaram que as informações estão legíveis e 37% responderam que as informações estão parcialmente legíveis, uma possibilidade para o resultado é que nem todas as mensagens foram traduzidas para o Português.

Apesar de todos os entrevistados possuírem algum conhecimento sobre gestão de identidades, 11% indicaram que o vocabulário utilizado no roteiro não está compatível com o usado pelo entrevistado, conforme mostra Figura 4.15.

26% dos entrevistados informam que encontraram parcialmente as informações necessárias para executar as ações na CAFe Expresso. 14 entrevistados, 74%, responderam que Sim, o

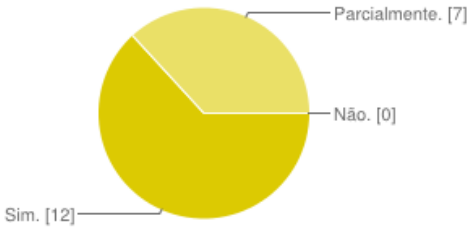
As mensagens de erro, caso tenham sido apresentadas, foram claras na sua descrição?



Sim	**3**	16%
Não	**0**	0%
Não se aplica	**16**	84%

Figura 4.13: Resultados sobre as mensagens de erros, se são claras, quando aparecem.

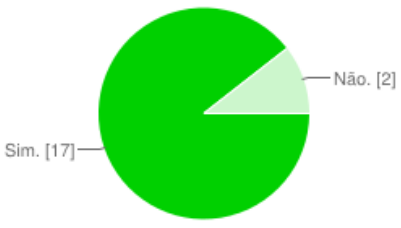
No seu ponto de vista, a apresentação das informações está legível?



Sim	**12**	63%
Parcialmente	**7**	37%
Não	**0**	0%

Figura 4.14: Resultados referente a legibilidade das informações.

O vocabulário utilizado no roteiro foi compatível com o seu vocabulário?



Sim	**17**	89%
Não	**2**	11%

Figura 4.15: Resultados sobre vocabulário utilizado no roteiro de avaliação.

usuário encontrou as informações disponíveis para executar as ações.

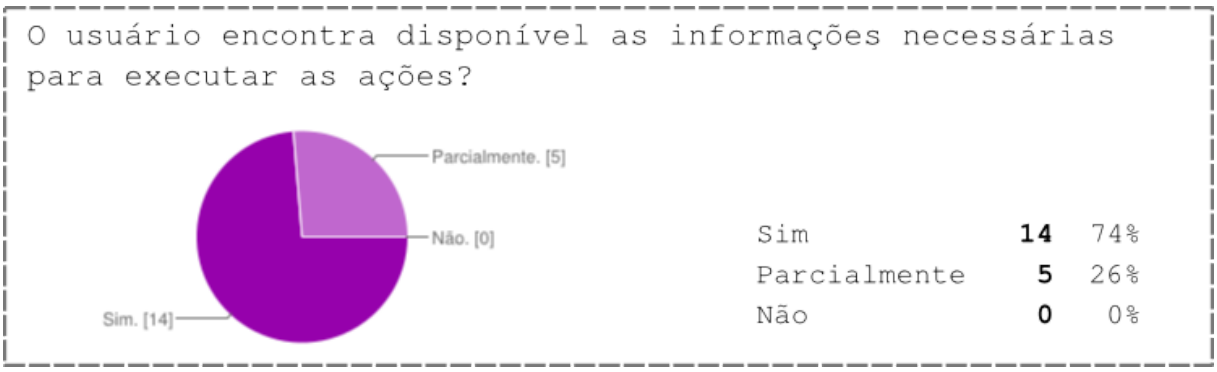


Figura 4.16: Resultados referente a encontrar informações necessárias para execução das ações na CAFe Expresso.

Dos 19 entrevistados, somente 1 não achou satisfatório a experiência de uso da CAFe Expresso durante o curto período de utilização. Todos os outros 18 entrevistados responderam que sim, que a experiência foi boa. Ver Figura 4.17

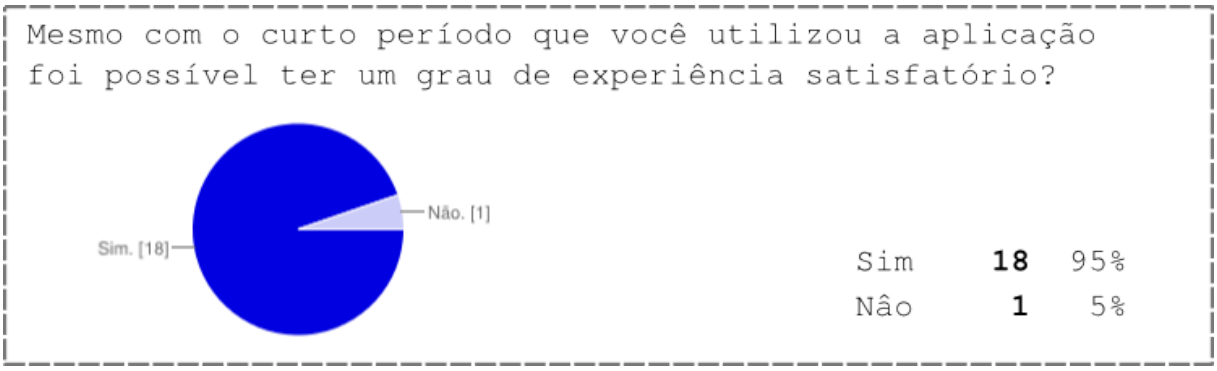


Figura 4.17: Resultados sobre satisfação durante período de utilização.

De todos os entrevistados, 63% deles fez uso da CAFe Expresso devido a algum projeto da RNP. Os outros 37% só usaram a CAFe para responder a avaliação. Ver Figura 4.18

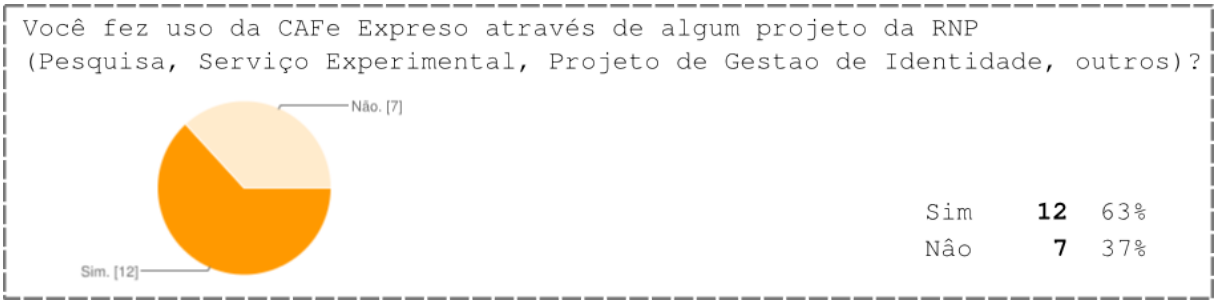


Figura 4.18: Resultados referente ao uso da CAFe Expresso devido a algum projeto da RNP.

Algumas considerações registradas nos comentários disponíveis na avaliação são muito relevantes, considerando a importância da CAFe Expreso para o entendimento sobre comunidade

acadêmica federada. Dentre eles a sugestão de disponibilizar outros serviços na CAFe Expresso além do serviço de teste de homologação de atributos poderia facilitar mais o entendimento da facilidade de autenticação única (SSO). Uma sugestão também é usar um vocabulário mais claro, simples e didático. O auxílio na validação de provedores antes de solicitar adesão para a CAFe foi um ponto forte citado. A importância do uso do *uApprove* na CAFe foi outra questão levantada, principalmente devido à privacidade do usuário, pois o *uApprove* permite ao usuário ter a consciência do que está sendo liberado para o SP.

4.4 Considerações finais

Foi possível perceber, durante o processo de implantação da infraestrutura da CAFe Expresso, a quantidade de conhecimento necessário para disponibilizar um ambiente de experimentação para Gestão de Identidade usando o *framework* Shibboleth, o mesmo *framework* utilizado na Federação CAFe. Este conhecimento engloba instalação e administração de serviços como Apache, Apache-Tomcat, OpenSSL e outros, usando por exemplo GNU/Linux, isto por que o *framework* está disponível para outras plataformas como Microsoft Windows e MacOS, mas que também precisam destes ou de serviços equivalentes aos citados anteriormente. Devido a estas grande dificuldades e quantidade de conhecimento necessário, a RNP, criou o projeto GId Lab, que tem como um dos objetivos disponibilizar uma infraestrutura para experimentação para pesquisas sobre Gestão de Identidades usando *framework* Shibboleth, originando também este trabalho.

Através da disponibilização do ambiente ou de máquinas virtuais para pesquisadores realizarem os experimentos foi possível perceber que a demanda para ambientes de experimentação para pesquisas voltadas para Gestão de Identidades existe, e isto está registrado através da relação de projetos atendidos e da pesquisa de satisfação realizada com pessoas que fazem pesquisas nesta área, e com isso alcançando seu objetivo geral, descrito na Seção 1.3.1 deste trabalho.

5 *Conclusões*

O crescimento da internet, como meio para realização de negócios, estudos, trocas de informações de forma geral, entre Homem X Máquina (*Human to Machine* – H2M) e Máquina X Máquina (*Machine to Machine* – M2M), criou uma necessidade natural de identificação das entidades que convivem na rede de computadores. Uma necessidade que é tratada no processo de gestão de identidades, por meio de diversos modelos.

O conceito de Gestão de Identidades Federadas tem se difundido nos últimos anos e refere-se a um conjunto de tecnologias e padrões que permite a interação do usuário com diversos serviços usando apenas uma credencial de acesso. A função básica da identidade federada, o SSO, possibilita ao usuário o uso da autenticação feita em um *site* e o uso desta mesma validação para acessar outros serviços protegidos (KALLELA, 2008).

No trabalho em questão, foi abordado o modelo de gestão de identidades federadas, como implementado no *framework* Shibboleth. Este modelo permite a descentralização dos provedores de identidade dos provedores de serviço, que além de facilitar o gerenciamento da infraestrutura dos provedores, para os administradores destes, também facilita para o usuário que precisará de somente uma identificação para acesso aos serviços disponibilizados pelos provedores de serviço. No modelo de gestão de identidades federadas a especificação mais utilizada é o SAML, que define que tipos de informações são trocadas pelos provedores de identidades e de serviços. O *framework* Shibboleth é o mais utilizado em ambientes acadêmicos.

Gestão de Identidades federadas é uma área ativa de pesquisa, sendo que muitos trabalhos desenvolvidos nesta área precisam realizar experimentos com soluções e frameworks consolidados como o Shibboleth. Desenvolver pesquisas aplicadas na área de gestão de identidades federadas exige que os experimentos sejam conduzidos em um ambiente que implemente uma federação em sua totalidade. Configurar uma federação para realizar experimentos de uma pesquisa pode ser uma tarefa mais árdua e demorada do que a implementação da pesquisa propriamente dita (WANGHAM et al., 2013).

O objetivo deste trabalho foi implantar uma parte do GId Lab, um ambiente virtual de apoio

aos pesquisadores brasileiros a fim de estimular e facilitar o desenvolvimento de novas soluções que possam vir a ser disponibilizadas na federação acadêmica, CAFe, ou como um serviço da RNP. Do objetivo proposto no início do trabalho, todas as atividades foram realizadas. De uma forma geral, a implantação da federação acadêmica foi realizada em sua plenitude, o ambiente é composto de três Provedores de Identidade *Identity Provider* (IdP), três Provedores de Serviço *Service Provider* (SP), dois serviços de descoberta, o WAYF e o EDS e um serviço que solicita o consentimento do usuário para liberação dos atributos solicitados pelo SP ao IdP, o *uApprove*. Além disto, foram disponibilizadas máquinas virtuais para *download* por pesquisadores interessados em implantar uma federação Shibboleth. Duas categorias de máquinas virtuais foram disponibilizadas, é possível realizar *download* dos elementos Shibboleth, separadamente, para fazer testes na CAFe Expresso, ou uma federação completa para uso local.

5.1 Trabalhos futuros

Para trabalhos futuros, sugere-se a implantação do IdP+, que é um IdP para tradução de credenciais de segurança, permitindo a geração de certificados X.509 e permitindo que aplicações não *web* possam fazer uso de autenticação federadas Shibboleth. Outra sugestão para trabalhos futuros é a implantação do Serviço Gerador de Certificados (SGC) que permite a tradução de credenciais Shibboleth em certificados digitais, que podem ser consumidas por serviços que requerem estes tipos de certificados. Mais uma sugestão de trabalho futuro é a implementação do SLO. Atualmente, a forma de se deslogar de uma sessão federada é fechar o navegador *web*. Com o SLO seria possível finalizar a sessão com um único clique. Uma última sugestão de trabalhos futuros é integração entre a federação CAFe Expresso, que utiliza a especificação SAML através do *framework* Shibboleth, e outras tecnologias de gestão de identidade federada, como OAuth[1] e OpenID Connect[2] que implementam outros padrões de comunicação, diferentes do SAML.

[1] http://oauth.net/
[2] http://openid.net/

Referências Bibliográficas

BHARGAV-SPANTZEL, A. et al. User Centric: A Taxonomy and Open Issues . *Journal of Computer Security*, p. 493–527, 2007.

CAMENISCH, J.; PFITZMANN, B. Security, Privacy, and Trust in Modern Data Management. In: ____. [S.l.]: Springer Verlag, 2007. cap. Federated Identity Management, p. 213–238.

CAO, Y.; YANG, L. A Survey of Identity Management Technology. *International Conference of Information Theory and Information Security (ICITIS)*, IEEE, 2010.

CARMODY, S. et al. *Incommon Technical Requirements and Information*. [S.l.], 2005.

CHADWICK, D. Federated Identity Management Solutions. *Foundations of Security Analysis and Design V*, p. 96–120, 2009.

DAMIANI, E.; VIMERCATI, S. D. C. di; SAMARATI, P. Managing Multiple and Dependable Identities. In: *Managing Multiple and Dependable Identities*. [S.l.]: IEEE, 2003. p. 29–37.

FELICIANO, G. et al. Gerência de Identidades Federadas em Nuvens: Enfoque na Utilização de Soluções Abertas. In: *Minicursos do XI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuidos*. Brasília: Sociedade Brasileira de Computação, 2011. p. 182–231.

FERREIRA, A. B. d. H. *Novo Dicionário da Língua Portuguesa*. 2a ed.. ed. Rio de Janeiro: Nova Fronteira, 1986.

GIL, A. C. *Métodos e Técnicas de Pesquisa Social*. 6ª. ed. [S.l.], 2008. Disponível em: <http://mba.eci.ufmg.br/downloads/metodologia.pdf>.

INTERNET2. *Middleware Architecture Committee for Education (MACE) - Internet2-mace-dir-eduperson-200806*. [S.l.], 2008.

ITU-T. *NGN Identity Management Framework - Recommendation Y.2720*. [S.l.], 2009.

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>.

JøSANG, A.; POPE, S. User Centric Identity Management. *AusCERT Asia Pacific Information Technology Security Conference*, 2005.

KALLELA, J. Federated Identity Management Solutions. *Seminar on Internetworking*, TKK T-110.5190, 2008.

MALIKI, T. E.; SEIGNEUR, J. M. A Survey of User-Centric Identity Management Technologies. *Proceedings of the International Conference on Emerging Security Information, Systems and Technology*, 2007.

MANUEL, E.; SEABRA, M. *Gestão de Identidades e Privacidade em Redes de Próxima Geração*. 2009.

MAçANEIRO, M. *Um Mecanismo Agregador de Atributos Mediado pelo Cliente Alinhado ao Programa de EGov.BR*. Dissertação (Mestrado) — Universidade do Valeo do Itajaí, 2013.

MELLO, E. R.; FRAGA, J. S.; WANGHAM, M. S. Uso de um Modelo de Confiança para Composição de Serviços Web. *XXVII - Simpósio Brasileiro de Redes de Computaods*, 2009.

MOREIRA, E. Q. et al. Federação CAFe: Implantação do Provedor de Identidade. In: *Federação CAFe: Implantação do Provedor de Identidade*. Rio de Janeiro: RNP, 2011.

OASIS. *Security Assertion Markup Language (SAML)*. v.2. [S.l.], mar. 2008.

RNP. *Federação CAFe - Esquema brEduPerson - versão 1.0*. [S.l.], 2009. Disponível em: <http://wiki.rnp.br/download/attachments/41190038/BrEduPersonv1>.

RNP. *Rede Nacional de Ensino e Pesquisa - CAFe - Comunidade Acadêmica Federada*. Rede Nacional de Ensino e Pesquisa - RNP, fev. 2009. Acessado em Maio de 2014. Disponível em: <http://portal.rnp.b/web/servicos/cafe>.

SCAVO, T.; CANTOR, S. *Shibboleth Architecture*. [S.l.], 2005. Disponível em: <http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf>.

SHIBBOLETH. *Shibboleth Architecture*. [S.l.], 2005. Disponível em: <http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf>.

SMITH, M. *Definition of the inetOrgPerson LDAP Object Class - RFC 2798 (Updated by RFCs 3698, 4519, 4524)*. [S.l.], 2000. Disponível em: <https://www.ietf.org/rfc/rfc2798.txt>.

SUESS, J.; MOROONEY, K. *Identity Management and Trust Services: Foundations for Cloud Computing*. [S.l.], 2009. Disponível em: <http://www.educause.edu/node/179404>.

TERENA, T. *SCHAC (SCHema for ACademia) – attribute definitions for individual data.* [S.l.], 2009. Disponível em: <http://www.terena.org/activities/tf-emc2/schacreleases.html>.

WAHL, M. *A Summary of the X.500(96) User Schema for use with LDAPv3 - RFC 2256*. [S.l.], dez. 1997.

WANGHAM, M. S. et al. Gerenciamento de Identidades Federadas. In: BARRETO, L. P. (Ed.). *Minicursos do Simpósio Brasileiro em Segurança da Informação e Sistemas Computacionais*. [S.l.]: Sociedade Brasileira de Computação, 2010. p. 3–52.

WANGHAM, M. S. et al. Uma Infraestrutura para Tradução de Credenciais de Autenticação para Federações Shibboleth. In: ____. *X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. Sbseg 2010. [S.l.]: Sociedade Brasileira de Computação, 2010. p. 360–447.

WANGHAM, M. S. et al. GIdLab: Laboratório de Experimentação em Gestão de Identidades. *Anais XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, Sociedade Brasileira de Computação, p. 481–486, 2013.

APÊNDICE A – Carta convite para pesquisa de uso

Abaixo, está reproduzido a carta de convite (enviado por e-mail) para pesquisadores realizarem a pesquisa de uso da CAFe Expresso. A pesquisa consistia em execução de um roteiro de uso e posteriormente, resposta de um fomulário com perguntas relacionadas a usabilidade do ambiente, entendimento sobre tecnologias como *Embedded Discovery Service* (EDS) e uApprove. Os pesquisadores convidados fazem parte do Comitê Técnico de Gestão de Identidade (CT-GId).

Caro Avaliador,

Esta pesquisa faz parte de um projeto de Trabalho de Conclusão de Curso e pretende avaliar a Comunidade Acadêmica Federada para Experimentação (CAFe Expresso). O experimento deve tomar cerca de 15 minutos do seu tempo. O questionário abrange a avaliação da CAFe Expresso.

Para iniciar o processo de avaliação acesse o link a seguir: http://bit.ly/formsCAFeExpresso

Pedimos que realize a avaliação até quinta-feira, dia 26 de junho de 2014.

Gostaríamos de contar com a sua colaboração.

Maykon Chagas de Souza (graduando - IFSC)
Michelle S. Wangham (orientadora - UNIVALI)
Emerson Ribeiro de Mello (co-orientador - IFSC)

IFSC - Instituto Federal de Santa Catarina
Graduação em Tecnologia em Sistemas de Telecomunicações

UNIVALI - Universidade do Vale do Itajaí

APÊNDICE B – Experimento: Uso federado com uApprove e WAYF

1.Acesse o serviço Homologa que está hospedado em um SP da CAFeExpresso via o endereço: http://sp-php.cafeexpresso.rnp.br

2.Na página inicial do SP clicar no botão Entrar;

3.Na página do WAYF, escolha a opção 'IdP3 – Universidade de Trantor' e clique no botão 'Selecione';

4.Na página do IdP3, informe usuário e senha (ver informações a seguir). Na página do IdP é possível marcar a opção "Limpar consentimento do usuário", que permite que os atributos já liberados para este SP sejam mostrados novamente. Para este experimento, não é necessário marcar esta opção;

usuário: camus

senha: camus

5.Aceite o Termo de Uso (ToU) clicando no botão 'Aceitar' no fim da página.

6.Veja a lista de atributos solicitada pelo SP e aceite a liberação da mesma clicando no botão 'Aceitar'. Observe que é possível também liberar os atributos de forma Global, para que não precise aceitar novamente os atributos liberados (não selecione esta opção);

7.Após o término do processo, você terá acesso ao Serviço Homologa do SP e verá os atributos do usuário. Este Serviço simplesmente exibe todos os atributos do usuário que o IdP pôde liberar.

8.Usando a identidade federada (Single Sign-on - SSO):

9.Ao término do primeiro acesso, para acessar outro SP, digite o endereço: http://sp-java.cafeexpresso.rnp.br

10. Escolha o IdP3 (o mesmo selecionado no Passo 3);

11. Observe que não será necessário se autenticar novamente, pois o SP alvo também está na CAFe Expresso. O IdP apenas apresentará para você os atributos que este SP está solicitando;

12. Aceite a liberação dos atributos clicando no botão 'Aceitar'. Você será redirecionado para o SP.

APÊNDICE C – Experimento: Acesso federado com Embedded DS (WAYF embarcado)

1.– Através de um navegador web acesse o Serviço Homologa no endereço: http://sp-python.cafeexpresso.rnp.br

2.– O Emdedded DS permite que você digite o nome do seu IdP ou que você escolha um em uma lista. Clique nesta última opção e selecione o IdP1 da Lista. Clique em “Continue”; https://idp1.cafeexpresso.rnp.br

3.– Na página do IdP1, informe o usuário e senha a seguir;

usuário: milo

senha: milo

4.– Ao realizar a autenticação, você será redirecionado para o serviço requisitado (SP indicado no início do processo);

5.– Usando a identidade federada (Single Sign-on - SSO):

6.– Ao término do primeiro acesso, para acessar outro SP, acesse o endereço: http://sp-php.cafeexpresso.rnp.br

7.– Escolha seu IdP de origem (o mesmo selecionado no Passo 2);

8.– Observe que não será necessário se autenticar novamente, pois o SP alvo também está na CAFe Expresso.

APÊNDICE D – Respostas descritivas da pesquisa realizada sobre a CAFe Expresso

D.1 Respostas referente ao funcionamento do uApprove

•Se não entendeu alguma das funcionalidades do uApprove, quais foram suas dúvidas?

1.“Entendi que existem 2 SPs (homologação de atributos) e que precisei liberar acesso aos meus atributos para os dois. No primeiro, precisei me autenticar no IdP. Mas no segundo não foi mais preciso (SSO). É isso? :)”;

2.“Minha sugestão é que a autenticação poderia ter sido testado em ambientes práticos. Por exemplo, foi legal ver a liberação dos atributos, mas o que o usuário quer mesmo é acessar diferentes serviços de forma rápida e segura !!! Acredito que assim o entendimento seria melhor ainda.”.

D.2 Respostas referente ao uso da CAFe Expresso

•Se não conseguiu, qual(is) passo(s) e qual(is) problemas você encontrou?

1.“Apenas o acesso ao SP java. Está fora do ar.”;

2.“O redirecionamento para http://sp-java.cafeexpresso.rnp.br falhou”;

3.“Ao executar o segundo procedimento e tentar usar o acesso federado, o segundo SP já redireciona diretamente para o Serviço Homologa, mas com as credenciais do primeiro acesso. Isso é decorrente pela sessão estar ativa primeiro (suponho).”.

•Registre aqui sua opinião sobre a contribuição da CAFe Expresso para seu entendimento sobre comunidade acadêmica federada.

1.“Foi a primeira comunidade acadêmica que tive acesso, de fato, e contribuiu para por conceitos de IdM em prática.”;

2.“Auxilia na validação das aplicações antes de efetivamente colocar em produção na CAFe. Uma vez validado na CAFe Expresso está pronta para a CAFe oficial, e isso é ótimo.”;

3.“Entendi que a principal vantagem do EDS é no caso do usuário possuir credenciais em IdPs diferentes. Fica mais fácil trocar o IdP acessando o site do SP. No primeiro caso, ele é automaticamente direcionado ao serviço. No caso do usuário possuir apenas 1 credencial, ele tem o ônus de fazer um clique a mais. Certo?”;

4.“O CAFE Expresso é bastante relevante, mas é necessário ter aplicações exemplo funcionando para aumentar a utilização dessa federação.”;

5.“É muito importante ter um test-bed para experimentação e para complementar o entendimento dos conceitos.”;

6.“Considerando um público-alvo leigo, é recomendável utilizar uma linguagem mais simples, clara e didática, restringindo o uso de termos técnicos, especialmente, os acrônimos.”;

7.“Muito importante já que nem todas as Universidades terão condições de realizar um estudo detalhado das soluções de IdM disponíveis e realizar os testes, preparando um pacote pronto pra deployment interno.”;

8.“A CAFe Expresso contribuiu com esclarecimentos via e-mail e com suporte técnico e tecnológico para o desenvolvimento de minha pesquisa sobre autenticação federada daqui do Laboratório de Sistemas em Arquiteturas Computacionais da Universidade Federal do Maranhão.”;

9.“A CAFe Expresso foi muito importante para mim não só no que se refere às comunidades acadêmicas federadas, mas também a processos de interoperabilidade dessas comunidades, caso usem middlewares distintos.”

•Use este campo para registrar qualquer outro comentário para a equipe da CAFe Expresso.

1.“Sugiro expandir o ambiente federado para suportar outros tecnologias, não só que implementam SAML (como a simplesaml) como também outros sistemas de identificação, OpenID, Oauth2 e etc”;

2.“Especificamente, sobre serviços da RNP. Sugiro uma análise sobre o tempo operacional, pois testar um serviço na CAFe expresso, Chimarão e posteriormente CAFe é requer bastante tempo dos desenvolvedores. Essa é a visão de um desenvolvedor que precisou passar por esses passos para federar um serviço na RNP.”;

3.“A utilização do EDS simplifica bastante o layout e proporciona ao usuário experiente na utilização dos serviços federados, a possibilidade de ganhar agilidade no processo de login, simplesmente digitando as siglas de sua instituição de origem. O uApprouve, na minha opinião, deveria ser adotado como padrão nestes processos de autenticação. Isto proporciona ao usuário a possibilidade de saber quais informações pessoais estão sendo disponibilizadas para o serviço a ser acessado. Embora para a grande maioria dos usuários o fator ”facilidade”seja o mais importante, para os poucos que prezam pela privacidade, este ”detalhe”pode ser o diferencial de usar ou não o serviço.”

4.“Sugiro que seja realizada a tradução das páginas para viabilizar um teste com alguns usuários finais. Além disso, gostaria de sugerir a criação de um documento de diretrizes arquiteturais para que os CIOs das IFES possam entender qual a melhor composição entre as federações de sistemas internos e de sistemas externos e qual o posicionamento da RNP em relação a isso. Tenho a seguinte dúvida e acho que outras pessoas também: devo utilizar uma Federação (como a CAFe Expresso) para federar o acesso aos meus sistemas internos? Como a Cafe Expresso deveria se encaixar na minha arquitetura corporativa?”;

5.“Acho que a ideia de um roteiro como esse é muito bacana. Notei que algumas vezes os textos que aparecem em botões são diferentes daqueles descritos no roteiro (por exemplo, um está em inglês outro em português). Isso atrapalha um pouco o usuário.”;

6.“Agradeço ao Maykon e sua equipe pelo apoio sempre que precisei.”.