Uma Infraestrutura para Tradução de Credenciais de Autenticação para Federações *Shibboleth*[*]

Michelle S. Wangham[1], Emerson Ribeiro de Mello[2], Davi da Silva Böger[3], Joni da Silva Fraga[3], Marlon Candido Guérios[4]

[1] Grupo de Sistemas Embarcados e Distribuídos–GSED/CTTMAR
Universidade do Vale do Itajaí (UNIVALI) – São José – SC – Brasil

[2]Instituto Federal de Santa Catarina – São José – SC –Brasil

[3]Departamento de Automação e Sistemas (DAS)
Universidade Federal de Santa Catarina (UFSC) – Florianópolis – SC – Brasil

[4]Inohaus Consultoria e Desenvolvimento de Sistemas- Florianópolis – SC– Brasil

wangham@univali.br, mello@ifsc.edu.br

{dsboger,fraga}@das.ufsc.br, marlonguerios@inohaus.com.br

Abstract. *Academic institutions are creating federations aiming to bring facilities to their users through resource sharing. The Shibboleth project, widely used in academic federations, was designed exclusively to operate with web applications. Academic communities make use of desktop applications that do not necessarily make use of browsers making them unsuitable to operate in a Shibboleth federation. This paper proposes an infrastructure that enables these desktop applications operate in a Shibboleth federation and it allows translation of credentials from different security technologies. Another feature of this proposal is to allow Shibboleth's users to access non Shibboleth service providers.*

Resumo. *Instituições acadêmicas estão formando federações com o intuito de compartilhar seus recursos, trazendo assim facilidades aos usuários. O projeto Shibboleth, amplamente usado para concepção de federações acadêmicas, é voltado exclusivamente para aplicações web. Comunidades acadêmicas fazem uso de aplicações desktop que não necessariamente fazem uso de navegadores tornando-as inadequadas para operar em uma federação Shibboleth. O presente trabalho propõe uma infraestrutura que permite a essas aplicações desktop autenticarem seus usuários através do Shibboleth além de permitir a tradução de credenciais de diferentes tecnologias de segurança. Outra característica desta proposta é permitir que usuários de uma federação Shibboleth possam acessar provedores de serviços não Shibboleth.*

1. Introdução

Com o seu amadurecimento, a Internet alcançou índices de desempenho e confiabilidade que não só permitiram que as comunicações se tornassem mais rápidas e baratas, mas também oportunizou o desenvolvimento de novas formas de interação através das

[*]Desenvolvido dentro do escopo do projeto "Serviços para Transposição de Credenciais de Autenticação Federadas", GT-STCFed financiado pela RNP.

redes colaborativas. Dentre essas formas, destacam-se as redes nacionais de pesquisa e educação (*National Research and Education Network* - **NREN**), provedores de serviço de Internet especializados que oferecem serviços de comunicação avançada para comunidade científica e canais dedicados para projetos de pesquisa [TERENA 2008].

Além do serviço de conectividade de rede com uso de tecnologias avançadas, as NREN oferecem uma diversidade de serviços para os parceiros que participam destas redes colaborativas, entre estes destacam-se: ferramentas avançadas para comunicação instantânea interativa, tais como videoconferência e Telefonia IP; centro de atendimentos a incidentes de segurança; serviços de vídeo digital; ferramentas de planejamento e operação de redes que monitoram o funcionamento de todos os enlaces da NREN; serviços de sincronização de relógios, *Grid Services* e serviços de comércio eletrônico. O portfolio de serviços oferecidos pelas NREN tem crescido a cada ano [TERENA 2008].

As NREN possuem uma série de requisitos de interoperabilidade e segurança. A interoperabilidade é necessária para tratar vários aspectos de heterogeneidade entre os membros da rede, que incluem as diversas plataformas computacionais utilizadas, as várias políticas às quais esses membros estão sujeitos e as diferentes tecnologias de segurança adotadas. Um suporte a essa heterogeneidade é essencial para garantir que a rede possa atender o maior número possível de participantes. A segurança, por sua vez, é fundamental para que os membros de uma NREN possam depositar confiança nas suas interações com outros membros [Wangham et al. 2009].

Nas atuais redes nacionais de pesquisa, o aumento de provedores de serviços e a crescente necessidade de compartilhar recursos para usuários de diferentes instituições que possuam algum tipo de afinidade motivaram a constituição de **federações acadêmicas** [Carmody et al. 2005]. Uma federação é uma forma de associação de parceiros de uma rede colaborativa que usa um conjunto comum de atributos, práticas e políticas para trocar informações e compartilhar serviços, possibilitando a cooperação e transações entre os membros da federação [Carmody et al. 2005]. A noção de federação é construída a partir do gerenciamento de identidades obtido com o uso de uma Infraestrutura de Autenticação e Autorização (AAI). No contexto das NRENs, o *framework Shibboleth* é a infraestrutura mais empregada para constituição de federações acadêmicas. As federações *Incommon*[1], da rede norte-americana *Internet 2*, e a *CAFe*[2], da Rede Nacional de Pesquisa (RNP) do Brasil, são exemplos de federações construídas tendo como base este framework. Estas federações agrupam pessoas do meio acadêmico que vão desde alunos, técnicos administrativos e professores. Tal comunidade é o principal público alvo de muitas empresas, o que torna interessante a essas empresas o ingresso nas federações acadêmicas também como provedores de serviços.

Em uma federação acadêmica, uma vez autenticado em sua instituição, é desejável que um usuário possa acessar qualquer serviço da federação sem novas autenticações, caracterizando o que é chamado de autenticação única (*Single Sign-On* - SSO). A instituição que desejar trazer tal facilidade para seus usuários deve implantar um provedor de identidades *Shibboleth* e cumprir as políticas para o ingresso na Federação [Carmody et al. 2005]. Um outro passo necessário está na adaptação das atuais aplicações Web desta instituição e de provedores de serviços, para que estas usufruam do *Shibboleth*

[1] `http://www.incommonfederation.org`
[2] `http://www.cafe.rnp.br`

em seus processos de autenticação de usuários, sendo que o cliente sempre necessitará de um navegador Web [Shibboleth 2005a]. Para provedores de serviços cujo público alvo não se restringe exclusivamente à comunidade acadêmica, a implementação da pilha *Shibboleth* pode ser um impeditivo, analisando custos *vs* benefícios. É importante ressaltar ainda que, mesmo partindo do pressuposto de que as relações de confiança já estejam previamente estabelecidas, ainda assim, há diversos desafios para transpor as credenciais de autenticação em uma federação, pois provedores de serviços possuem autonomia para decidir quais políticas e tecnologias de segurança serão utilizadas, ou seja, uma federação precisa prover uma infraestrutura que suporte a autenticação SSO mesmo diante de parceiros que usem credenciais de segurança diferentes da usada no *Shibboleth*.

Este artigo tem por objetivo descrever uma infraestrutura para tradução de credenciais de autenticação que garanta, aos membros de uma federação *Shibboleth*, (i) o acesso a provedores de serviços que estão fora do domínio *Shibboleth* e (ii) a transposição de credenciais de autenticação entre diferentes tecnologias de autenticação. A infraestrutura proposta neste trabalho adapta a solução proposta em [de Mello et al. 2009] de forma que seja possível que membros de uma federação *Shibboleth* possam interagir com aplicações não *Shibboleth*, não necessariamente via navegador Web. De forma a comprovar a sua aplicabilidade, um protótipo da infraestrutura foi implementado e integrado a um portal de serviços não *Shibboleth*.

2. *Framework Shibboleth*

O projeto *Shibboleth* [Shibboleth 2005a] foi uma proposta conjunta do grupo Internet2 e IBM com o intuito de permitir que usuários de instituições acadêmicas pudessem interagir com serviços providos por outras instituições, bastando que essas façam parte de uma mesma federação acadêmica. O *framework Shibboleth* está baseado em padrões abertos como o XML e SAML e fornece um pacote de software, de código aberto, para a construção de aplicações Web. Este *framework* provê suporte ao conceito de autenticação única (*Single Sign-On*), transposição de credenciais de autenticação e preserva a privacidade e o anonimato dos usuários do sistema.

Dentro de um domínio *Shibboleth* existem dois papéis: provedor de identidades (*Identity Provider* – IdP) e provedor de serviços (*Service Provider* – SP). O primeiro é responsável por autenticar seus usuários, antes que estes possam usufruir dos serviços oferecidos pelo segundo. O ponto comum entre estes papéis é que ambos devem implementar toda a pilha de software fornecida pelo projeto *Shibboleth*, permitindo assim o transporte das credenciais dos usuários do provedor de identidades até o provedor de serviços [Shibboleth 2005a].

A Figura 1 ilustra os passos para que um usuário, ainda não autenticado, consiga acessar um recurso disponibilizado pelo provedor de serviços. O usuário, através de seu navegador, aponta para a `URL` da aplicação Web desejada. Este pedido é interceptado pela pilha *Shibboleth* que, através de redirecionamentos HTTP, encaminha-o a um serviço que o questiona sobre qual instituição acadêmica este usuário faz parte. Uma vez informada a instituição, este usuário é encaminhado, novamente através de redirecionamentos HTTP, ao provedor de identidades (IdP) de sua instituição, o qual irá autenticá-lo e, uma vez que o processo tenha ocorrido com sucesso, o usuário é finalmente redirecionado ao recurso Web desejado (SP). Cabe ao detentor deste recurso, aplicar o controle de acesso, conside-

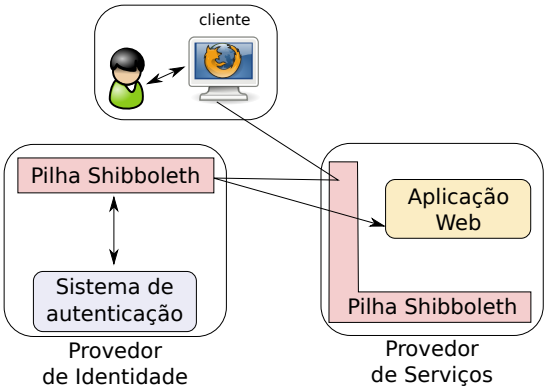

Figura 1. Interação de um usuário com um provedor de serviços *Shibboleth*

rando as credenciais do usuário que foram fornecidas com essa tentativa de acesso.

O provedor de serviços pode requisitar outros atributos do usuário junto ao seu provedor de identidades, como por exemplo o número do registro acadêmico, o endereço de email, etc. Os provedores de identidade respeitam um conjunto de políticas para revelação de atributos de seus usuários, preservando assim a privacidade dos mesmos. O *Shibboleth* define uma forma padronizada para troca de atributos, através de asserções SAML, porém, não especifica como deverão ser tais atributos, deixando tal função livre para os desenvolvedores.

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. Em [Internet2 2008, Wahl 1997, Smith 2000], foi proposto o `eduPerson`, um conjunto padrão de atributos de identidade comuns para federações acadêmicas, sendo que 6 atributos são altamente recomendados, 10 são sugeridos e 25 são opcionais. A comunidade federada CAFe que reúne instituições acadêmicas brasileiras, além de implementar esse conjunto de atributos, definiu ainda seu próprio conjunto de atributos (chamado `brEduPerson`).

A Infraestrutura para Tradução de Credenciais de Autenticação proposta neste trabalho contribui em três aspectos com as NRENs que implementam suas federações acadêmicas utilizando o *framework Shibboleth*: (i) possibilita que os membros de uma federação, após serem autenticados em seus IdPs, possam acessar provedores de serviços afiliados à federação mas que não são SPs *Shibboleth*; (ii) permite que estes SPs afiliados possam exigir credenciais de autenticação diferentes das suportadas no *Shibboleth*[3], uma vez que a infraestrutura provê o suporte à transposição de credenciais mesmo diante do uso de diferentes credenciais de autenticação; e (iii) possibilita que um membro da federação se autentique em seu IdP não somente via navegador Web.

3. Trabalhos Relacionados

As abordagens que proveem suporte a autenticação *Single Sign On* (SSO), como o *framework Shibboleth*, surgiram, justamente, para tornar mais simples as interações entre clientes e provedores de serviços. No entanto, devido a problemas de interoperabilidade, essa abordagem é deficiente em domínios com diferentes infraestruturas de segurança.

[3]Por exemplo, um SP afiliado pode exigir um certificado X.509 como credencial de autenticação.

O modelo de confiança nos Serviços Web e a autenticação SSO nestes serviços é definida na especificação WS-Trust [OASIS 2009]. A WS-Trust define um serviço, o *Security Token Service* (STS), que representa uma terceira parte confiável capaz de emitir e validar credenciais. Os protocolos para emissão e validação de credenciais de autenticação, autorização ou atributos definidos na WS-Trust não restringem as tecnologias de segurança e os tipos de credenciais que podem ser usados. A WS-Trust define também meios para estabelecer, gerenciar e verificar relações de confiança existentes por meio de emissão e validação de credenciais. No entanto, essa especificação não aborda como traduzir as informações contidas na credencial de segurança do principal, diante de diferentes tecnologias de autenticação.

Em [de Mello et al. 2009], é descrito um modelo com suporte a autenticação SSO mesmo diante de domínios administrativos com diferentes tecnologias de segurança. Neste modelo, um cliente pode acessar recursos em domínios com tecnologias de segurança diferentes do seu domínio de origem, usando para isto as credenciais fornecidas em seu próprio domínio. Para que a transposição possa ocorrer, é preciso que haja uma relação de confiança entre o domínio de origem e o domínio do provedor do serviço. Se este for o caso, o cliente pode se autenticar no seu domínio de origem e usar essa credencial para acessar o serviço no domínio de destino. Ao receber a requisição juntamente com a credencial do cliente, o serviço alvo pode invocar o *Credential Translation Service* (CTS) presente no seu domínio para que este traduza a credencial do cliente para o formato suportado pelo serviço. O CTS deve possuir conhecimento de diversos formatos de credenciais de autenticação e das regras para a tradução entre os diversos formatos. O modelo de transposição de credenciais de autenticação proposto em [de Mello et al. 2009] foi avaliado considerando duas tecnologias de segurança: certificados X.509 e SPKI.

É importante destacar um que um Serviço Web, mesmo utilizando os serviços propostos em [de Mello et al. 2009], não pode usufruir diretamente dos mecanismos de segurança providos pelo *framework Shibboleth*, devido a exigência do uso de navegadores web. Ou seja, apesar dos resultados obtidos em [de Mello et al. 2009], constatou-se que para prover também às Federações *Shibboleth* uma infraestrutura orientada a serviços que suporte a autenticação SSO mesmo diante de diferentes credencias de autenticação, objetivo da infraestrutura aqui proposta, o modelo [de Mello et al. 2009] precisava ser adaptado para que os membros da federação pudessem acessar provedores de serviços com tecnologias de autenticação diferentes da provida no *Shibboleth* e que também não implementam a pilha de software *Shibboleth*.

Com o intuito de encorajar que mais usuários, em especial acadêmicos vinculados às redes nacionais de pesquisa e educação (NREN), utilizem os *Grid Services*, diversos projetos surgiram tendo como proposta integrar o *framework Shibboleth* ao modelo de segurança comumente utilizado em *grid services*. Dentre estes projetos, destacam-se os projetos conduzidos pelo *Joint Information Systems Committee* (JISC) da Grã-Bretanha, que visam permitir que usuários autenticados por IdPs *Shibboleth* confiáveis obtenham credenciais temporárias para acessar recursos do *National Grid Service* da Grã-Bretanha (um *grid service* ou um *grid portal*). O projeto mais recente do JISC, chamado SARONGs [Wang et al. 2010], que se ocupa da integração *Shibboleth* e a *Grid Security Infrastructure* baseada no X.509, definiu um serviço intermediário, chamado CTS (*Credential Translation Service*), com o objetivo de traduzir as credenciais Shibboleth em credenciais GSI

temporárias aceitas no NGS. As credenciais GSI temporárias, mais conhecidas como *X.509 proxy certificates*, são certificados de tempo limitado (*low assurance certificates*) assinados por autoridades certificadoras *online*. É importante destacar que o serviço CTS do SARONGs não oferece uma interface padronizada para emissão de novas credenciais de autenticação como a oferecida no modelo proposto em [de Mello et al. 2009], que utiliza o STS da especificação WS-Trust.

Outro importante projeto que integra o *Shibboleth* ao modelo computacional de grid é o projeto GridShib[4]. A principal motivação deste projeto é estender o modelo de autorização do Globus Toolkit para que atributos *Shibboleth* possam ser utilizados para autorização em grids construídos com o Globus. Neste projeto, foi desenvolvido um par de *plugins* de software, um para o Globus Toolkit e outro para o *Shibboleth*, que permite que um *GT Grid Service Provider* (SP) solicite atributos de um usuário a um provedor de identidades (IdP) *Shibboleth* [Scavo e Welch, 2008]. No GridShib, ao invés de usar um serviço tradutor de credenciais, este adapta tanto o mecanismo de autenticação do *Shibboleth* quanto o Globus Toolkit para ligar uma asserção de autenticação do *Shibboleth* (asserção SAML) com um certificado X.509. É importante destacar que tanto o projeto SARONGs quanto o GridShib, a tradução de credenciais de autenticação ocorre somente entre dois domínios de segurança (*Shibboleth*/SAML e *Grid Security Infrastructure*/X.509).

4. Infraestrutura para Tradução de Credenciais de Autenticação para Federações *Shibboleth*

Na Federação *Incommon*[5], existem duas categorias de organizações colaboradoras: as participantes, que são as organizações com interesse em utilizar os serviços de confiança da Federação *InCommon*, que hospedam IdP e/ou SPs *Shibboleth* e que participam ativamente dos grupos de colaboração da comunidade federada, e as afiliadas, organizações com interesse em usufruir da abrangência da *InCommon* para comercializar os seus produtos e serviços relacionados à federação, mas que não são tão ativas na mesma. Na infraestrutura proposta neste trabalho, define-se como **organizações afiliadas** os provedores que não implementam a pilha de software *Shibboleth*, porém que cumprem os critérios necessários para serem afiliados a federação para prover serviços aos seus participantes. Estas podem ser instituições públicas não acadêmicas, entidades sem fins lucrativos ou organizações comercias que desejam fornecer conteúdos, produtos, softwares, consultoria, suporte e/ou serviços aos membros de uma federação acadêmica.

A infraestrutura proposta neste trabalho possibilita a emissão e tradução de credenciais de autenticação e atua como um *gateway* confiável entre os IdPs e os provedores de serviços afiliados de uma federação *Shibboleth* e entre os membros da federação e os seus IdPs. Visando oferecer interoperabilidade, requisito necessário para as federações acadêmicas e para seus parceiros de negócio, a infraestrutura proposta segue uma arquitetura orientada a serviços e está baseada nas principais especificações relacionadas aos Serviços Web.

A infraestrutura é composta por dois serviços: o STS e o CTS (ver Figura 2). O *Security Token Service* (STS) tem como funções a emissão e validação de credenciais

[4]`http://gridshib.globus.org`
[5]`http://www.incommonfederation.org/affiliate/`

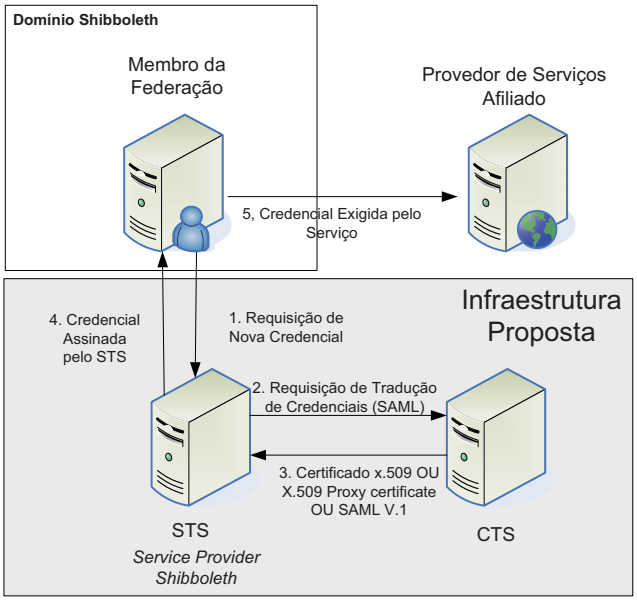

Figura 2. Visão Geral dos Serviços Providos na Infraestrutura Proposta

de segurança, de acordo com a especificação WS-Trust [OASIS 2009]. O *Credential Translation Service* (CTS), por sua vez, trata de aspectos de tradução de credenciais entre diferentes tecnologias de segurança. Na infraestrutura proposta, estão sendo considerados quatro possíveis tipos de credenciais de autenticação (certificado X509v.3, credenciais GSI temporárias - *X.509 proxy certificates*, SAMLv.1 ou SAMLv.2).

É importante ressaltar que o serviço STS atua como um mediador entre serviços não *Shibboleth* (serviços afiliados da federação) e usuários de federações *Shibboleth*, com isso, é papel do STS criar novas credencias de autenticação para o usuário, a partir da credencial SAML do usuário gerada durante o processo de autenticação deste usuário em seu IdP (ver passos de 1 a 4 da Figura 2). Esta nova credencial é que será a apresentada para o serviço afiliado (passo 5). Os serviços afiliados devem possuir uma relação de confiança com o serviço STS e podem prover suporte a tipos de credencias diferentes daqueles providos pelo framework *Shibboleth*.

4.1. Security Token Service (STS)

O STS é um Serviço Web que deve atuar como um provedor de serviços dentro de um domínio *Shibboleth*. A especificação WS-Trust define os protocolos para emissão e validação de credenciais de autenticação (passos 1 e 4 da Figura 2) e não restringe as tecnologias de autenticação e tipos de credenciais que podem ser usados, ou seja, qualquer tecnologia que seja suportada pelas partes envolvidas pode ser usada. Segundo o modelo da WS-Trust, todas as requisições (*RequestSecurityToken* - RST) feitas ao STS são para emissão de asserções de segurança.

Os principais campos de uma requisição ao STS são `wst:RequestType`, `wst:TokenType` e `wst:Claims`. Em todas as requisições, o elemento `wst:RequestType` da mensagem de requisição RST contém o URI de emissão definido na WS-Trust. Além disso, todas as requisições STS devem conter a credencial de autenticação SAMLv2 do cliente emitida pelo IdP *Shibboleth*. A diferença entre os tipos

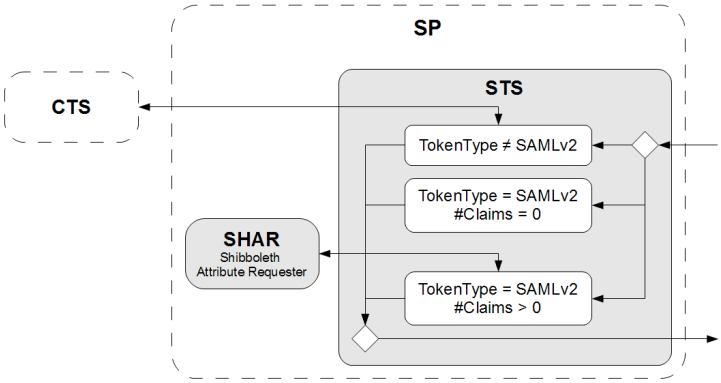

Figura 3. Diferença entre os tipos de requisições ao STS

de requisições está nos demais campos da mensagem, conforme ilustrado na Figura 3.

O campo `wst:TokenType` da mensagem indica qual o tipo da credencial requerida. Se a credencial requerida for de um tipo diferente de SAMLv2, o STS invocará o CTS para tradução da asserção recebida. Se a credencial requerida for uma asserção SAMLv2, o STS irá validar a asserção recebida para autenticação do cliente e emitirá uma nova asserção com os mesmos valores, porém assinada pelo STS. O campo `wst:Claims` deve ser usado em conjunto com um tipo de credencial SAML e serve para especificar um conjunto de atributos do cliente que devem ser incluídos na asserção. Esses atributos podem ser usados pela aplicação invocada pelo cliente de maneira similar aos atributos providos pelo *Shibboleth*.

4.2. Credential Translation Service (CTS)

Na infraestrutura proposta, o *Credential Translation Service* (CTS) trata de aspectos de tradução de credenciais entre diferentes tecnologias de segurança. Ou seja, quando o STS necessita traduzir a credencial SAML v.2 para um formato diferente, este necessita invocar o CTS (ver Figura 4).

A Figura 4 ilustra um exemplo do funcionamento interno do CTS. No passo 1, o CTS extrai da asserção SAML de autenticação enviada pelo STS as informações para compor a nova credencial de autenticação, no exemplo, um certificado X.509. Se os dados contidos na asserção SAML não forem suficientes para gerar um certificado X.509, o CTS invocará, no passo 2, o STS indicando no campo `wst:Claims` os atributos que faltam para que este último os obtenha junto ao serviço denominado *Attribute Authority*, através de uma requisição SAML contendo um elemento `AttributeQuery` [Shibboleth 2005b]. Após coletar os atributos necessários, no passo 3, o CTS, com o auxílio de uma Autoridade Certificadora *Online*, gera o certificado. Essa AC receberá o conjunto de atributos obtidos (nome X.500, chave pública) e devolverá um certificado X.509 devidamente assinado. Por fim, no passo 4, o CTS entregará o certificado ao STS.

4.3. Cenários de Uso da Infraestrutura Proposta

A seguir, de forma a elucidar a aplicabilidade da infraestrutura proposta, são apresentados alguns cenários de uso da Infraestrutura para Tradução de Credenciais de Autenticação.

O cenário ilustrado na Figura 5 consiste de um Portal de Serviços, pertencente a uma federação *Shibboleth*, um provedor de serviços fora do domínio *Shibboleth*, que

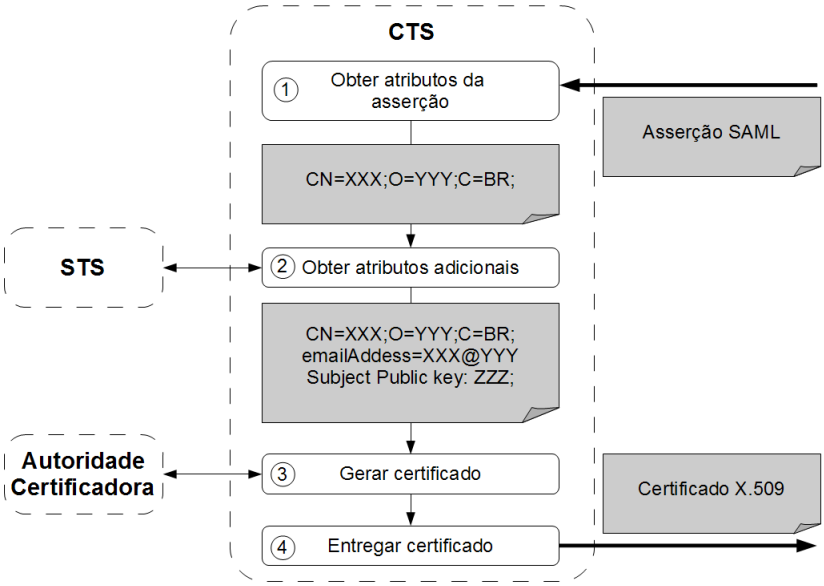

Figura 4. Diferença entre os tipos de requisições ao STS

hospeda um Serviço Web de uma Livraria, e os serviços STS e CTS. Considere neste cenário que um usuário do domínio *Shibboleth*, através de seu navegador Web deseja interagir com aplicações que não fazem parte deste domínio, usando para tal o portal. Este portal, do ponto de vista do cliente, é um provedor de serviços no domínio *Shibboleth*. Do ponto de vista da aplicação não *Shibboleth*, este portal atua como um cliente da aplicação.

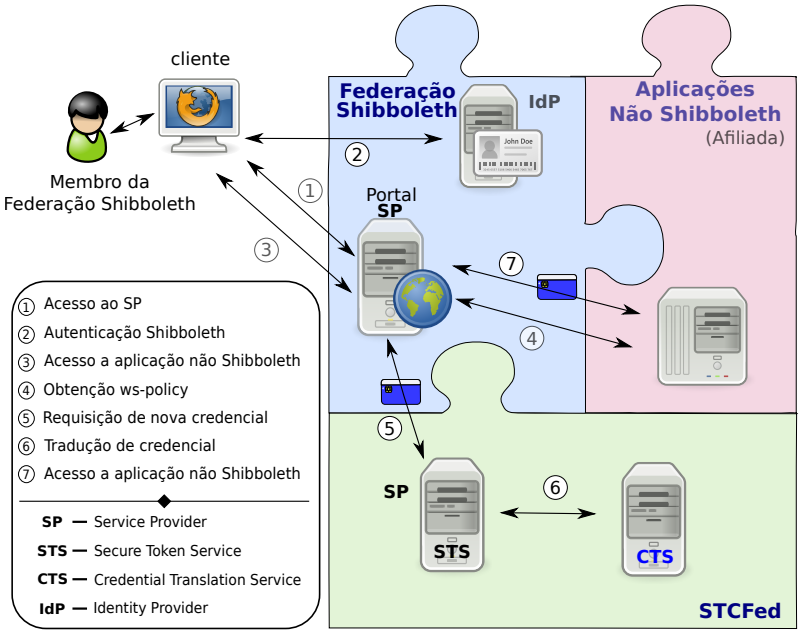

Figura 5. Cenário de Uso: Portal de Serviços Afiliados

A Figura 5 ilustra o processo de autenticação para que o usuário, através de seu navegador, possa acessar, através do portal, a aplicação da Livraria. O usuário usando a mesma conta e senha de sua instituição é autenticado (passos de 1 a 2). Pelo fato do portal ser também um SP dentro do domínio *Shibboleth*, este processo de autenticação do

usuário é executado com o auxilio dos redirecionamentos de URL do *Shibboleth*. Se a autenticação ocorrer com sucesso, o usuário é redirecionado para o portal. Neste cenário, o provedor afiliado exige, através de sua especificação de política de qualidade de proteção (WS-Policy), por exemplo, que o usuário apresente um certificado digital X.509 (passo 4) como credencial de autenticação. Sendo assim, o portal encaminha o pedido de acesso ao STS que, com o auxílio do CTS, fazem a emissão e conversão da credencial de segurança (passos 5 e 6), neste exemplo, converte a asserção SAML de autenticação (emitida pelo IdP *Shibboleth*) para um certificado digital X.509 esperado pelo provedor afiliado. Por fim, o certificado é encaminhado junto com o pedido de acesso ao provedor afiliado (passo 7).

Ainda neste cenário, pode ser considerado que o provedor afiliado exija uma asserção SAML v.1, já este não suporta SAML v.2. Neste caso, o CTS realizará apenas a tradução do formato das asserções SAML e assinará a asserção. Por fim, o STS pode ainda ser requisitado para emitir uma asserção SAML v.2, ou seja, somente para validar asserção recebida e assiná-la.

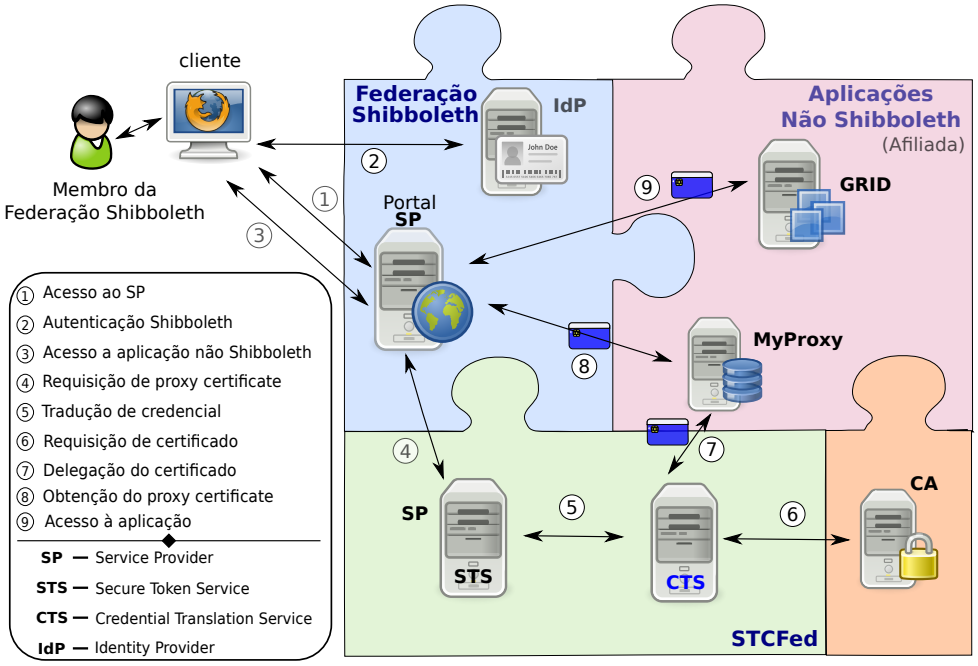

Figura 6. Cenário de Uso: *Grid Service* Afiliado

Outro cenário de uso da infraestrutura possibilita que um membro de uma federação acadêmica possa, com o auxílio da infraestrutura proposta, acessar um *grid portal* usando o mecanismo de autenticação do *Shibboleth*. Este cenário, ilustrado na Figura 6, é muito semelhante ao anterior, a principal diferença está na aplicação não *shibboleth* que é um *grid service* que exige *X.509 proxy certificates* como credenciais de autenticação. Ou seja, o STS e o CTS irão ser solicitados para emitir um X.509 proxy certificate a partir da tradução da asserção SAML resultante da autenticação no IdP. Conforme ilustrado na Figura 6, neste cenário, sugere-se o uso do serviço *MyProxy*, que faz parte do *Globus Project*, para auxiliar a gestão e proteção das credencias de segurança. Este serviço *online* possibilita que os usuários/portal recuperam as credenciais de curta duração (temporárias) geradas pela infraestrutura proposta.

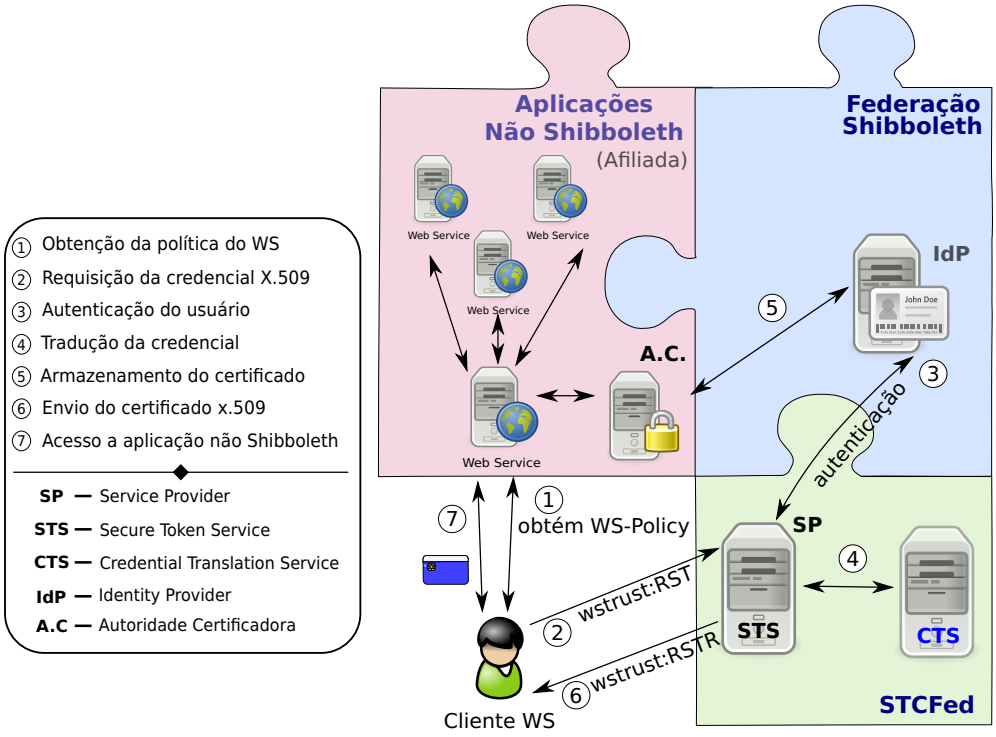

Figura 7. Cenário de Uso: Acesso via aplicação *desktop*

Um terceiro cenário de uso da infraestrutura ilustra como um usuário do domínio *Shibboleth*, através de uma aplicação desktop, pode acessar um Serviço Web fora domínio *Shibboleth*. Considere que um provedor de serviços afiliado hospeda uma aplicação distribuída baseada em Serviços Web. Para um usuário, membro de um domínio *Shibboleth*, que acessa uma aplicação desktop[6] e que é cliente de um serviço Web que está fora do domínio *Shibboleth*, é interessante que este possa usar a mesma conta de usuário e senha que possui em seu domínio *Shibboleth* para se autenticar na aplicação (ver Figura 7). Com isto sem expor seus dados pessoais, este usuário pode usufruir, sem o uso de um navegador Web, da autenticação no seu IdP no acesso a serviços afiliados da federação, sendo para tanto mediado por uma terceira parte confiável que é o STS.

5. Avaliação do Modelo Proposto

5.1. Implementação do Protótipo

O protótipo foi desenvolvido na linguagem Java devido principalmente a portabilidade implícita da plataforma Java e por oferecer facilidades para o desenvolvimento de aplicações web. Para o desenvolvimento dos serviços STS e CTS foi feito uso do *framework* Metro[7], o qual consiste em uma implementação de código aberto da pilha *Web Service*, incluindo a implementação de referência das APIs JAX-WS 2.1 e JAXB 2.1. A escolha do Metro 2.0 diante de outras opções de código aberto, como Apache Axis v1/v2 e Apache CXF, se deu principalmente por este implementar por meio do sub-projeto WSIT (Web Service Interoperability Technology) várias especificações WS-*, como WS-Trust e

[6]Que obrigatoriamente não é um navegador web.
[7]`https://metro.dev.java.net`

WS-Security e por incluir dentre suas APIs, ferramentas direcionadas ao desenvolvimento de serviços como STS e CTS.

O portal web foi disponibilizado em um provedor de serviços Shibboleth e para seu desenvolvimento foram usados os seguintes *frameworks*: Hibernate[8] para persistência de dados; JSF[9] combinado com o Richfaces[10] para a elaboração da parte de apresentação da aplicação, dentro do conceito *Model-View-Controller* (MVC).

Por fim, foi feito uso do Glassfish v3[11] como servidor de aplicação para hospedar os serviços STS e CTS e o Apache Tomcat para hospedar o portal web, simplesmente porque nosso provedor de serviços Shibboleth estava rodando sobre o Tomcat. Todas as trocas de mensagens entre serviços e portal web ocorrem sobre o protocolo SSL.

5.2. Análise da Segurança do Protótipo

Na infraestrutura proposta, tem-se como premissa que os serviços STS e CTS são confiáveis, assim como os provedores de identidade e de serviços da infraestrutura *Shibboleth*. Isso significa que essas entidades apresentarão as seguintes características:

- manterão suas chaves privadas em segredo;
- seguirão os protocolos da infraestrutura corretamente; e
- não revelarão o conteúdo de nenhuma mensagem trocada nos protocolos do modelo.

Todas as entidades participantes da infraestrutura possuem um par de chaves assimétricas que usarão para cifrar e assinar todas as mensagens trocadas. As relações de confiança são estabelecidas por meio da troca segura das chaves públicas entre o STS e os provedores de serviços afiliados e pela aceitação das mensagens assinadas com as respectivas chaves privadas.

No Shibboleth, provedores de serviços (SP) consultam o provedor de identidades (IdP) para obter atributos dos usuários. A liberação desses atributos segue a política de privacidade implementada por cada IdP, que dentro de uma federação tende ser a mesma em todos os IdPs. Cabe a cada SP, gerir seu próprio controle de acesso, indicando aos usuários quais atributos são necessários para que possam usufruir dos serviços providos. Na infraestrutura apresentada neste artigo, o serviço STS é um SP do Shibboleth e assim somente usuários autenticados e que possuírem os atributos necessários poderão fazer uso do mesmo.

Na infraestrutura proposta, preservando a solução implantada no *framework Shibboleth*, todas as mensagens trocadas entre um navegador Web e um IdP e um SP *Shibboleth* são protegidas por sessões SSL, garantindo a confidencialidade, integridade e autenticidade. Com o mesmo objetivo, todas as mensagens trocadas entre um cliente STS (p. exemplo, o portal de serviços da Figura 5 ou a aplicação *desktop* da Figura 7) e o serviço STS são protegidas com os mecanismos da WS-Security. Além disso, toda a comunicação com o provedor de serviços não Shibboleth pode ser protegida utilizando o protocolo SSL ou os mecanismos da WS-Security, conforme especificado na política do provedor. Com o

[8] `http://www.hibernate.org`
[9] `https://javaserverfaces.dev.java.net`
[10] `http://www.jboss.org/richfaces`
[11] `https://glassfish.dev.java.net`

uso destes mecanismos, fica garantido que nenhuma informação sensível possa ser obtida por um atacante ou alterada sem que isso seja detectado.

5.3. Desempenho do Protótipo

No decorrer desta pesquisa, sabia-se que os protocolos desenvolvidos provocariam um aumento nos tempos de resposta do acesso dos usuários aos serviços. Visando avaliar os tempos de espera resultantes da execução do protótipo desenvolvido, experimentos para medição do desempenho foram realizados. No entanto, ressalta-se que o desempenho não foi comparado diretamente com os casos em que as funcionalidades oferecidas são mais limitadas. Ainda assim serão apresentados tempos de espera a fim de demonstrar que, de maneira geral, a solução é viável no sentido de que a espera do usuário não é proibitiva.

Há duas situações distintas durante a execução dos protocolos: antes e após a autenticação do usuário. No momento em que o usuário se autentica, a sobrecarga do protocolo é maior, porém essa autenticação ocorre apenas uma vez, mesmo que vários serviços distintos sejam acessados, ou seja, a sobrecarga da autenticação não existe em nenhum acesso posterior na mesma sessão. Além disso, no primeiro acesso a um provedor de serviços específico, é realizada uma chamada ao STS para que emita uma credencial de acordo com a política. Nas invocações posteriores, a mesma credencial poderá ser usada enquanto estiver dentro do prazo de validade, ocasionando um tempo de espera menor.

Para a medição dos tempos foi usado o cenário do Portal de Serviços (Figura 5). Dois tempos foram medidos no portal, (i) tempo entre a chegada da asserção SAML emitida pelo IdP e a resposta da invocação do SP agregado pelo portal, ou seja, no primeiro acesso do usuário; e o (ii) tempo entre o acesso do usuário ao SP e a resposta do SP agregado, nos demais acessos. O tempo entre o início do acesso pelo usuário e a chegada da asserção SAML no portal não foi medido, no entanto essa sobrecarga é parte do *Shibboleth* original e é simplesmente somada à sobrecarga medida.

A configuração do experimento foi a seguinte: foi usado um único computador com processador Intel Core 2 Duo 2,53 GHz, 4 GB de RAM DDR3 1067 MHz, sistema operacional MacOS X 10.6.4. Todos os serviços foram executados no mesmo local, o que significa que os tempos medidos não incluem latências de rede. Cada tempo foi medido 50 vezes, com 10 execuções de *warm-up* e com um intervalo de confiança de 95%. Foram calculados a média e o desvio padrão dos tempos medidos. A média para o tempo do primeiro acesso do usuário (medição (i)) foi de 1170ms, com desvio padrão 54ms. Para o tempo dos demais acessos (medição (ii)), a média foi 115ms, com desvio padrão 5ms.

Uma sobrecarga de pouco mais de um segundo não é muito alta quando comparada com tempos de espera típicos de acesso a serviços na Internet, muitas vezes da ordem de alguns segundos. Além disso, no caso frequente a sobrecarga é da ordem de 100 ms. Com isso, após a realização dos experimentos, foi possível confirmar a hipótese de que o tempo de espera do usuário para acessar o serviço afiliado não é proibitiva.

6. Conclusão

Visando atender as necessidades das instituições de ensino superior ligadas as NRENs dos países, diferentes federações acadêmicas, baseadas no *framework Shibboleth*, vem sendo estabelecidas, sendo que o número de participantes em cada federação é bastante expressivo. Por exemplo, em novembro de 2009, a comunidade de participantes da Federação

Incommon era de mais de 4 milhões de usuários, sendo que 153 instituições de ensino superior, seis agências e 51 parceiros patrocinadores faziam parte da federação.

A infraestrutura proposta neste trabalho visa garantir o conceito de autenticação única em Federações *Shibboleth*, mesmo diante de diferentes tecnologias de credenciais de segurança e ampliar a participação de provedores de serviços. Implementar a pilha *Shibboleth* pode ser um impedimento à participação de diversos provedores de serviços, o que diminui a gama de aplicações que os membros da federação *Shibboleth* podem acessar. Com a infraestrutura proposta, é possível fornecer os serviços de autenticação e de atributos da federação *Shibboleth* a partir do uso de um serviço STS padronizado [OASIS 2009], que atua como um gateway confiável para os membros da federação *Shibboleth*. Além de permitir a interoperabilidade com Serviços Web, a infraestrutura proposta suporta ainda outras funcionalidades, como a tradução de credenciais. Destaca-se que, apesar do uso do serviço STS, a autenticação ainda é realizada pelo provedor de identidades *Shibboleth* e as políticas aplicadas permanecem aquelas definidas na federação.

Referências

Carmody, S., Erdos, M., Hazelton, K., Hoehn, W., Morgan, B., Scavo, T., and Wasley, D. (2005). Incommon technical requirements and information. vol. 2005.

de Mello, E. R., Wangham, M. S., da Silva Fraga, J., Camargo, E., and da Silva Böger, D. (2009). Model for authentication credentials translation in service oriented architecture. *Transactions on Computational Sciences Journal*, 5430:68–86.

Internet2 (2008). eduPerson & eduOrg Object Classes. `http://middleware.internet2.edu/eduperson/`.

OASIS (2009). Ws-trust 1.4. OASIS Standard. `http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.pdf`.

Shibboleth (2005a). *Shibboleth Architecture*. `http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf`.

Shibboleth (2005b). *Shibboleth Architecture: Protocols and Profiles*. `http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-latest.pdf`.

Smith, M. (2000). *Definition of the inetOrgPerson LDAP Object Class*. IETF RFC 2798.

TERENA (2008). *TERENA Compendium of National Research and Education Networks In Europe*. TERENA.

Wahl, M. (1997). *A Summary of the X.500 User Schema for use with LDAPv3*. RFC 2256.

Wang, X., Jones, M., Jensen, J., Richards, A., Wallom, D., Ma, T., Frank, R., Spence, D., Young, S., Devereux, C., and Geddes, N. (2010). Sarongs: Shibboleth access for resources on the national grid service. *Journal of Information Assurance and Security*, 5:293–300.

Wangham, M. S., de Mello, E. R., da Silva Böger, D., dos Santos Silva, R., Holler, D. R., and da Silva Fraga, J. (2009). *Livro de Minicursos do IX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, chapter Segurança em Redes Colaborativas: Desafios e Propostas de Soluções, pages 99–148. Sociedade Brasileira de Computação.