doi: http://dx.doi.org/10.5892/RUVRV.91.211219

UM SISTEMA DE GERENCIAMENTO ACADÊMICO GEOGRAFICAMENTE DISTRIBUÍDO COM SUPORTE A UM ÚNICO PONTO DE AUTENTICAÇÃO

Alfredo DEL FABRO NETO[1]
Rogério TURCHETTI[2]
Célio TROIS[3]
Walter PRIESNITZ FILHO[4]
Eunice PALMEIRA[5]
Eugênio SIMONETTO[6]

RESUMO: Este artigo apresenta uma proposta para autenticação em aplicação pertencentes a domínios distintos, através de um único ponto de acesso. A solução está sendo implementada para um sistema open-source de gerenciamento acadêmico (SIGA-EPCT). No contexto deste projeto, com uso do Shibboleth e do SAML, será possível racionalizar os recursos oferecidos pelos Institutos Federais, Integrar os diferentes módulos do SIGA-EPCT e compartilhar a base de dados com o Ministério da Educação.

ABSTRACT: This paper presents a proposal for application's authenticaton, allowing different domains to authenticate in a single access point. This solution is being implemented into an peon-source Academic Management System called SIGA-EPCT. By using Shibboleth and SAML, it will be possible to share computational resources between Federal Institutes, integrating the different modules of SIGA-EPCT and, also, share information with the Ministry of Education.

[1] Graduando em Tecnologia em Redes de Computadores, Universidade Federal de Santa Maria (UFSM).
[2] Mestre em Engenharia de Produção ênfase em Tec de Informação, Universidade Federal de Santa Maria (UFSM). Professor Assistente da Universidade Federal de Santa Maria (UFSM).
[3] Mestre em Systèmes Embarques, Universite Nice Sophia Antipolis (UM), França. Professor Assistente da Universidade Federal de Santa Maria (UFSM).
[4] Mestre em Ciências da Computação, Universidade Federal de Santa Catarina (UFSC). Professor Assistente da Universidade Federal de Santa Maria (UFSM).
[5] Mestre em Modelagem Computacional de Conhecimento, Universidade Federal de Alagoas (UFAL). Professora do Instituto Federal de Educação, Ciência e Tecnologia de Alagoas.
[6] Pós-Doutor, Universidade Tecnológica Federal do Paraná (UFTPR). Doutor em Administração - Área:Sistemas de Informação, Universidade Federal do Rio Grande do Sul (UFRGS). Mestre em Ciência da Computação, Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Professor Adjunto da Universidade Federal de Santa Maria (UFSM). E-mail: eosimonetto@gmail.com

1 Introdução

Em aplicações distribuídas que necessitam realizar relações de confiança entre diferentes domínios administrativos, há a exigência de aumentar a confiabilidade na troca de dados entre as entidades desconhecidas. Além disso, é preciso melhorar a flexibilidade entre as organizações permitido a autenticação de usuários em diferentes aplicações e domínios, oferecendo interoperabilidade entre estas aplicações. Os modelos tradicionais de autenticação em domínios, não suprem as necessidades das aplicações distribuídas. O principal motivo são as distintas políticas de segurança adotadas por cada domínio administrativo, além disso, surge o inconveniente de fazer o usuário se autenticar várias vazes nos sistemas. Uma solução eminente para resolver este problema é o uso da arquitetura Shibboleth (SCAVO; CANTOR, 2005) com o SAML (*Security Assertion Markup Language*).

O SAML é um conjunto de aplicações que permite a troca de atributos de usuários entre diferentes domínios. As informações utilizam um padrão XML (*extensible Markup Language*) para a troca de dados de autenticação e autorização. O principio do SAML está baseado no conceito de Federação, onde um grupo de serviços e identidades trabalham juntos para simplificar e resolver problemas como SSO (*Single Sign On: um único ponto para autenticação*) (WISNIEWSKI, 2004). O Shibboleth é um projeto open-source que possibilita realizar o gerenciamento das identidades participantes, criando e controlando as informações dos usuários através do padrão SAML. O sistema Shibboleth otimiza a autenticação nas aplicações que ele gerencia, redirecionando o acesso do usuário para autenticá-lo na instituição escolhida. Cada instituição possui um Provedor de Identidade (IdP) que gera uma referência do usuário para Provedor de Serviço, este por sua vez decide, baseado nos atributos, se o usuário utiliza ou não os recursos. Diversas aplicações têm sido oferecidas com a arquitetura Shibboleth, como exemplo: uso para autenticação em GRIDs (SPENCE et al., 2006), gerenciamento de recursos para um sistema e-learning (RASOOLZADEH, 2008) Federação CAFe (Comunidade Acadêmica Federada) reúne instituições de ensino brasileiras em uma rede de confiança (MELLO, 2010), entre outros.

Neste sentido, o presente trabalho objetiva implementar o uso do padrão SAML para controlas e trocar atributos dos usuários entre diferentes domínios. Esta funcionalidade será aplicada a um sistema integrado de gestão acadêmica desenvolvido com tecnologias de software livre e de forma colaborativa por várias instituições federais do Brasil. O referido projeto denomina-se SIGA-EPCT (Sistemas Integrado de Gestão Acadêmica- Educação Profissional, Cientifica

e Tecnológica) (RENAPI) e atualmente está dividido em dois sistemas, um Administrativo e outro Educacional. O objetivo é criar um único ponto de autenticação unindo os dois sistemas e conseqüentemente integrar as diferentes Instituições, possibilitando o compartilhamento de seus recursos. O gerenciamento destas Instituições será realizado com a utilização do Shibboleth.

Com o Compartilhamento de atributos dos usuários através do uso dos recursos do SAML, tanto acadêmicos como docentes, poderão utilizar recursos de qualquer Instituição participantes do projeto, se assim o quiserem. Como exemplo, considere o seguinte cenário: um discente pertencente a uma Instituição localizada no sul do país, está fazendo um estágio em uma empresa instalada no norte do país. Este estudante ao necessitar de bibliografias, poderá se deslocar até a Instituição mais próxima para adquirir os livros desejados, além disso, o aluo poderá também fazer o uso do refeitório da Instituição. Em síntese, deseja-se que com a implementação da abordagem exposta, os recursos dispostos pelas Instituições possam ser utilizados por qualquer usuário, desde que possuam uma conta ativa no sistema independente de seu local físico.

O restante deste trabalho está organizado da seguinte forma: Na seção 2 é descrito o sistema acadêmico SIGA-EPCT, tanto a parte educacional como a administrativa, onde será incorporado o sistema de um único ponto de autenticação. A seção 3 discorre sobre o atual processo de autenticação e as mudanças propostas para agregar uma maior flexibilidade para o usuário. Por fim, na seção 4 são apresentadas as condições finais sobre o trabalho, ressaltando as necessidades atuais do sistema SIGA-EPCT e como a arquitetura de autenticação proposta resolveu o problema.

2 O sistema SIGA-EPCT

O SIGA-EPCT é um sistema de gestão acadêmica desenvolvido com a filosofia de software livre sendo por isso *open-source*, podendo ser baixado e testado via repositório *apt-get(*RENAPI) conforme GNU *General Public License* como publicada pela Fundação do Software Livre (FSF). O SIGA-EPCT automiza a gestão dos processos institucionais acadêmicos através do SIGA-EDU e , administrativos pelo SIGA-ADM. Um dos objetivos do projeto é compartilhar os dados de todas as Instituições Federais facilitando o acesso destas informações ao Ministério da Educação. De forma resumida, serão descritos os módulos desenvolvidos ou que estão em fase de desenvolvimento do SIGA-ADM e do SIGA-EDU, respectivamente. Ressalta-se que o processo de desenvolvimento e gerenciamento é realizado com o auxílio de ferramentas *open-source* na plataforma Linx Ubuntu.

A seguir estão relacionados os módulos acadêmicos implementados no SIGA-EDU: **Infra-Estrutura:** Informações sobre a instituição; discentes, docentes e técnico administrativos; gerencias/ departamentos/ coordenações; Regras acadêmicas. **Período Letivo:** Definição de calendário acadêmico; Definição de docentes/ disciplinas para o período; Definição e criação de turmas; Definição de vagas para transferência externa/ interna e reingresso. **Registros Acadêmicos:** ofertar vagas; manutenção de cursos; matriz curricular de curso; regras acadêmicas especificas das unidades de ensino; dados detalhados do elemento curricular. **Registro Diário**: todas as atividades sobre registro das aulas, notas de alunos, diário de classe. **Matricula:** manutenção das matrículas de alunos; tratamento de isenção em disciplinas; vínculo de alunos as turmas; **Extensão:** todas as atividades envolvendo projetos de extensão; programa e fonte de financiamento;convênios; instituições externas; **Segurança:** incluir usuários e gerenciar perfis. Apesar de alguns módulos estarem em fase de construção, em geral, a parte acadêmica encontra-se em estado avançado de desenvolvimento.

Os módulos do SIGA-ADM possuem, resumidamente, as seguintes funcionalidades: Requisições on-line do Almoxarifado, Compras, Diárias, Hotel, Passagens; Restaurantes, Serviços externos e veículos; Controle de pagamento de bolsas oferecidas pela instituição; Licitação e serviços; Controle orçamentário e controle contábil; Controle de empenhos; Controle de pagamentos; Patrimônio; Protocolo e Recursos Humanos.

Como já relatado neste artigo, os processos Administrativos encontram-se, no momento, implementados em arquiteturas distintas dos processos Educacionais. Não havendo qualquer integração entre as duas soluções. Neste sentido, um dos objetivos do presente trabalho é implementar o uso do SAML para integrar as duas arquiteturas com um único ponto para autenticação, de forma a tornar transparente para o usuário a integração da parte Educacional (EDU) com parte Administrativa (ADM).

3 Arquitetura Proposta

A utilização do Shibboleth com SAML no SIGA-EPCT, permitira racionalizar os recursos oferecidos pelas Instituições e integrar a parte administrativa com a parte acadêmica. Neste sentido, esta seção apresenta o processo de autenticar também via LDAP, para possibilitar a integração com o SAML. Posteriormente apresenta-se como a autenticação será efetuada utilizando o SAML.

3.1 **Processo de Autenticação Localizada**

O processo local de controle de acesso do SIGA-EPCT tem como método de autenticação o LDAP. Basicamente, o LDAP é responsável por autenticar o usuário através de um *login e senha*, uma vez que o banco de dados se encarrega de fazer a consulta para obter os perfis para controle de acesso da aplicação de cada usuário. A figura 1 mostra o diagrama de classe dos sistema atual de autenticação.

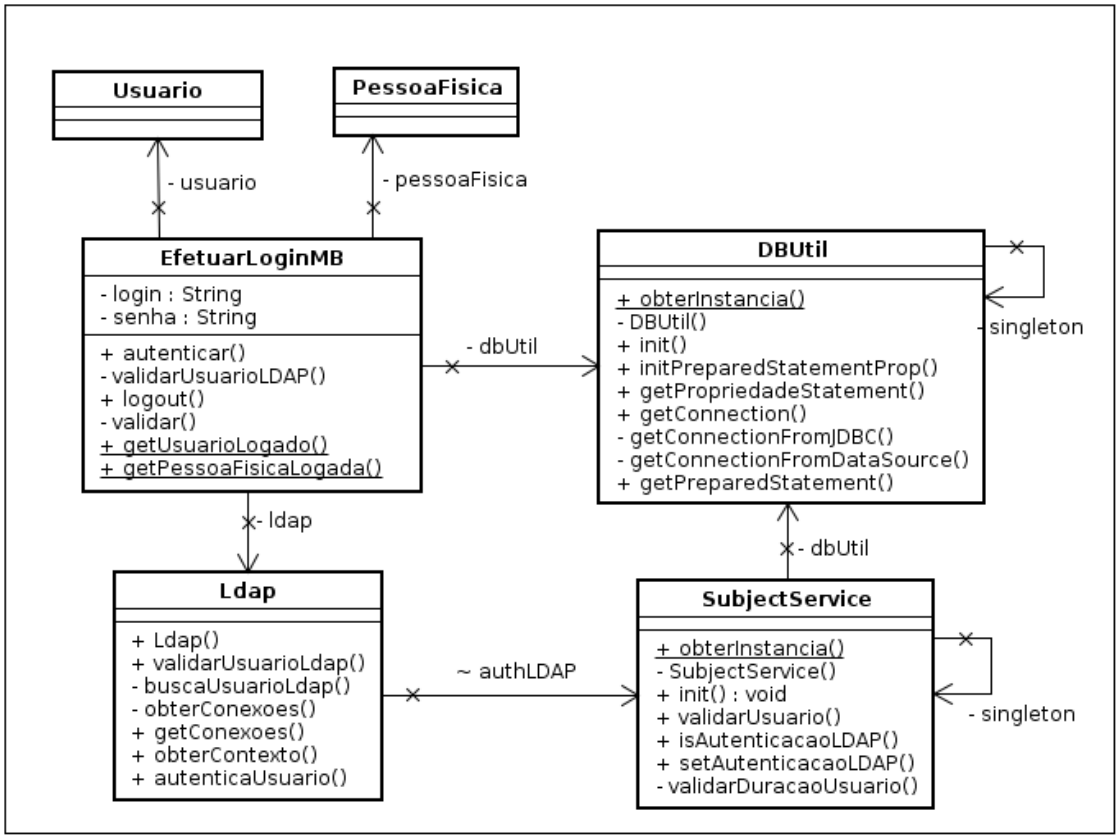

Figura 1: Diagrama de classe do Sistema de Autenticação do SIGA-EDU

Ao acessar a aplicação com as credenciais de usuário, são definidos os atributos *login e senha* da classe *EfetuarLoginMB* os valores digitados pelo usuário. Apos, é invocado o método *autenticar*(), responsável por enviar esses dados para a classe Ldap através do método *validarusuarioLDAP*(). Essa classe tem como função prover a autenticação do usuário no diretório *Ldap*, o qual possui um construtor que executa o método *obterconexoes*(), cuja função é pesquisar todas as conexões Ldap cadastradas no banco de dados pelo administrador do sistema.

O método *validarusuarioLDAP*(), acessado na classe *EfetuarLogin*, realiza uma busca pelo usuário identificado como *usuário* e executa o método *autenticarusuario*(), responsável por confrontar as informações com o Ldap. Caso a autenticação tenha sucesso, é enviado a classe SubjectService o valos da variável authLdap com o valor booleano verdadeiro através do método setAutenticacaoLDAp(). Porem, para ter acesso ao sistema um usuário precisa possuir uma Pessoa Física cadastrada, que é então verificado pelo método validarusuario() da classe SubjectService, que efetua a pesquisa de acordo com a classe DBUtil. Se todas essas condições forem preenchidas, o usuário poderá ter acesso ao sistema de acordo com as permissões do mesmo, obtidas da base de dados.

3.2 **Proposta do Processo de Autenticação Integrada**

A Arquitetura para comunicação e integração do SIGA-EDU é totalmente baseada no projeto *Shibboleth* [http://shibboleth.internet2.edu], visando a integração dos mesmos englobado as vantagens de um sistema federado como o uso de uma credencial única para acesso a diversos recursos pertencentes a federação (DUDCZAK et al ., 2008).

O sistema de autenticação do SIGA será composto por um servidor de autenticação (*Identily Provider*); diretórios LDAP no domínio do IdP (*Identily Provider*) para armazenar os dados dos usuários e validar-los; e um provedor de serviços (*Service Provider* ou SP). O servidor de autenticação interage com o usuário para validar o *login e senha* fornecendo informações sobre o usuário através do protocolo SAML. O SP tem com objetivo de redirecionar o usuário para um IdP, caso ele ainda não tenha sido autenticado, e confirmar as informações vindas IdP, caso ele ainda não tenha sido autenticado, e confirmar as informações vindas do Idp através de requisições SAML.

Com esta estratégia e considerando que cada Instituição tenha IdP implementado, os usuários do SIGA, tanto acadêmicos como docentes , poderão utilizar recursos de qualquer Instituição. Alem disso, o aluno poderá também se alimentar no refeitório da Instituição, e utilizar recursos que estejam compartilhados pelo IdP.

Para Implementar a estrutura de autenticação e autorização ao sistema, é importante definir como ocorre a comunicação entre as entidades que compõe.

O sistema permite que seja efetuada autenticação local e também de forma distribuída, no caso de obtenção de recursos de outra Instituição. A figura 2 descreve como comunicam-se as entidades nesse tipo de cenário (CAB=NTOR, 2005 a) (CANTOR, 2005b) (CANTOR ,2005 c) (HIRSCH, 2005).

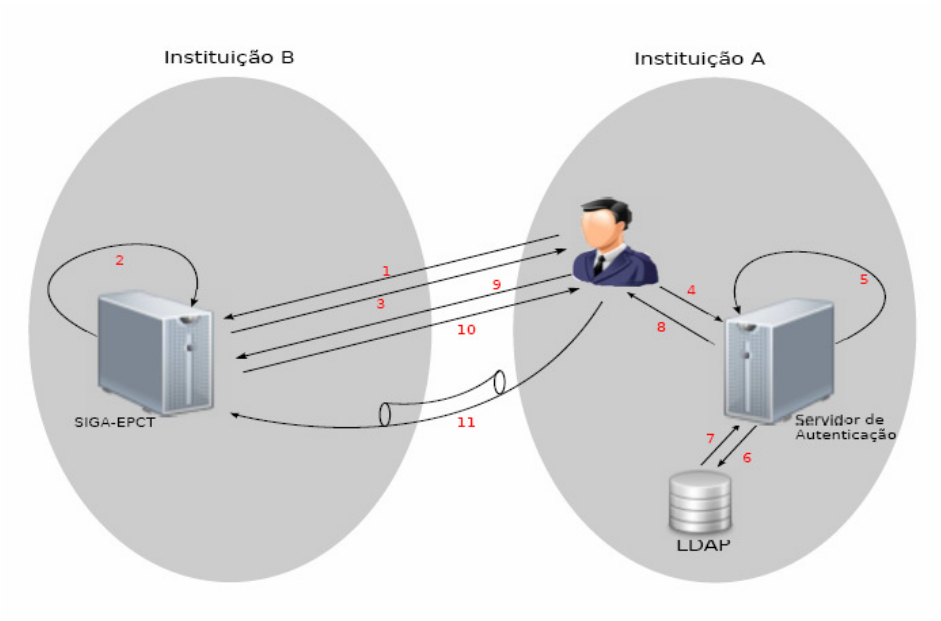

Figura 2: Autenticação em domínios administrativos diferentes

Como exemplo, tem-se um usuário localizado na Instituição B (1). Inicialmente, O SIGA-EPCT localizado na Instituição B verifica se não existe uma autenticação em nome do usuário que requisitou o acesso aos recursos (2). Caso Exista, o usuário já possuirá acesso ao recurso solicitado eu processo de autenticação ocorrera conforme descrito na Figura 1. Em caso negativo, o sistema gera uma requisição SAMl através de um formulário XHTML em direção ao usuário (3). O usuário então requisita autenticação no IdP da Instituição A (4), onde o serviço de Sso (*Single-Sing On)* processa a requisição.É então feita uma verificação para analisar as credenciais do usuário (5). Se o usuário não estiver autenticado, o sistema então efetua a autenticação (6)(7). Essa autenticação é feita através do LDAP, que também possui um atributo indicado o nível de permissões do usuário.

O serviço SSO valida a requisição e envia um formulário XHTML contendo a resposta em direção ao usuário (8), que solicita uma requisição ao *Assertion Consurmer Service* (ACS) do SIGA-EPCT da Instituição B, para enviar as respostas obtidas do serviço Sso da Instituição A (9)(10). O ACS cria um contexto seguro, através do uso de Certificados Digitais de ambas as partes, com Instituição B e redireciona o usuário para o recurso desejado (11). Enquanto esse contexto seguro existir, as requisições feitas serão atendidas desde que o usuário tenha permissão para efetuá-las.

Durante esse processo, uma busca por atributos é feita ao domínio de autenticação do usuário, na Instituição A, para obter as

permissões de acesso ao sistema. O atributo só informará o nível de acesso do usuário, por exemplo *aluno*, mas suas permissões podem ainda ser diferentes do acordo com as normas administrativas da Instituição B, onde de fato as permissões serão atribuídas. As permissões que o usuário possuirá são responsabilidade do sistema da Instituição B. Em síntese, cada Instituição deverá gerenciar o perfil dos usuários que acessam o sistema a partir de outras bases remotas.

Conclusão

Este artigo apresentou uma aplicação para gestão acadêmica totalmente *open-source*. Tal aplicação encontra-se em fase avançada de implementação, onde seus módulos já estão sendo utilizados por algumas instituições Federais. Uma necessidade do sistema SIGA-EPCT é integrar a parte Acadêmica com a parte Educacional e, conseqüentemente compartilhar dados com o Ministério da Educação, como também, compartilhar os recursos oferecidos pela Instituições. Tais necessidades estão sendo absorvidas com a proposta do uso da arquitetura Shibboleth integrado ao SAML.

Concluiu-se que com o uso destas ferramentas é possível unificar diferentes sistemas autenticando uma única vez. Além disso, institucionalizando esta filosofia de controle de acesso para outras aplicações, é possível integrar o SIGA-EPCT com outros sistemas oferecidos pelo Ministério da Educação. Atualmente encontra-se em fase de implementação a utilização de bibliotecas que suportem o uso SAML para autenticação no SIGA-EPCT. O Shibboleth já está implementado como IdP, onde a dificuldade maior foi a integração deste como SP. Como a implementação ainda não foi finalizada, os experimentos práticos como testes de segurança e de desempenho ficam como trabalhos futuros.

Referências

CANTOR, e. a. S. Assertions and protocols for the oasis security assertin markup language (saml) v2.0. In : *Standard* [S. 1.: s.n.], 2005

CANTOR, e. a. S.Bindings for the oasis security assertion markup language (saml) v2.0. In: OASIS
Standard [S.1.: s.n.], 2005

CANTOR, e. a. S.Profiles for the oasis security assertions markup language (saml)v2.0. In: OASIS
Standard [S.1: s.n.], 2005

DUDCZAK, A.et al. Exending the shibboleth identity management model with a netoworked user profile. In: Information Tecnology, 2008. IT 2008. Ist Internacional Conference on. [S.l.: s.n.],2008. p.1 – 4.

HIRSCH, e. a. F. Security and privacy considerations for the oasis security assertion markup language (saml) v2.0. In : *Standard* [S.I.: s.n.], 2005

MELLO, E. e. a. F. J. W. M. Gerenciamento de identidades federadas. In: *X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais* [S.l.: s.n.], 2010.

RASOOLZADEH, L. Science faculty acess management of e-learning using shibboleth. In: *Departament of Informatics, University of Lisbon, Master Theses (Dissertation)*. [S.l.: s.n.], 2008.

RENAPI. Disponível em: <http//www.renapi.gov.br/sigaept/o-projeto>, Acesso em: 06 abril 2011.

SCAVO, T.; CANTOR, S. Shibboleth architecture technical overviem. In: *Internet 2 document: draft-mace-shibboleth-tech-overview-02*. [S.l.:s. n.], 2005.

SPENCE, D. et al. Shibgrid: Shibboleth access for the uk national grid service. In: *e-Sience and grig Computing, 2006. e-Science '06. Second IEEE Internacional Conference on.* [S.l.:s.n.], 2006. p. 75.

WISNIEWSKI, e. a. T. Saml v2.0 executove overvien. Committe draft. In: OASIS. [S.l.:s.n.], 2004.