ACROSS: um Framework de Autenticação e Autorização Baseado em Políticas e Atributos para Organizações Virtuais*

Edelberto Franco Silva[1], Débora Christina Muchaluat-Saade[2], Natalia Castro Fernandes[2]

[1]Universidade Federal de Juiz de Fora – Juiz de Fora - MG - Brasil
edelberto@ice.ufjf.br

[2]MídiaCom Laboratory – Universidade Federal Fluminense – Niterói - RJ - Brasil
{debora, natalia}@midiacom.uff.br

Resumo. *Esta tese contribui ao estado da arte em gerência de organizações virtuais, propondo um novo framework que facilita, tanto a entrada de instituições em uma organização virtual (OV) quanto a criação de uma nova OV, colaborando para a solução de problemas importantes na gestão de identidade e acesso. Além de propor a especificação, documentação e implementação de um framework que integra um conjunto mais amplo de funcionalidades do que aqueles presentes na literatura, a solução permite a gerência e integração de uma organização virtual a soluções de gestão de identidade e acesso amplamente difundidas, como é o caso das federações de identidade e o conceito de controle de acesso baseado em atributos. O framework proposto suporta diversos métodos de autenticação, permite a gerência de atributos específicos à OV, realiza a transposição de credenciais e provê controle de acesso a recursos utilizando políticas distribuídas e padrões baseados em papel e atributos. Além disso, é genérico em relação ao tipo de recurso compartilhado pela OV. Outra contribuição do trabalho é o auxílio na integração a quaisquer ambientes de organização virtual, independentemente de características particulares, como tipos específicos de credenciais ou mensagens de gerência de recursos.*

Abstract. *This thesis contributes to the state-of-the-art in virtual organization (VO) management, proposing a new framework that facilitates both the ingress of institutions into a VO and the creation of a new VO, collaborating to solve important problems in identity and access management. Beyond to propose a framework – introducing its specification, documentation and implementation – this proposal allows the management and integration of a VO to widely distributed identity and access management solutions, such as identity federations and concepts of access control based on attributes. The framework supports several authentication methods, allows to manage specific attributes of each VO, performs the credential translation and provides access control in resource level using distributed policies. In addition, it is generic in terms of shared resources' characteristics by VO. Another contribution of this work is to assist institutions to ingress in any VO – regardless of its particular characteristics, such as specific types of credentials or resource management messages.*

*__A tese encontra-se disponível no endereço web:__ `http://www.ic.uff.br/PosGraduacao/frontend-tesesdissertacoes/download.php?id=744.pdf&tipo=trabalho`

1. Introdução

O termo GId (Gestão de Identidade) vem sendo usado para descrever os mecanismos e processos de Autenticação e Autorização (A&A) utilizados para garantir o uso seguro de recursos arbitrários. Da mesma forma, é comum encontrarmos o termo IAM (*Identity and Access Management*) para definir os mesmos conceitos. A comunidade acadêmica apresenta requisitos especiais de compartilhamento de recursos, dada a necessidade de colaboração e integração gerada por projetos, intercâmbios, cursos remotos e outras atividades. Há alguns anos, a comunidade acadêmica vem utilizando identidades federadas, que permitem regular o acesso a recursos disponíveis para todos os membros de uma instituição ou para toda a comunidade, como, por exemplo, repositórios de periódicos, sem a necessidade de duplicação de informações e de bases de dados. No entanto, há também recursos que devem ser compartilhados apenas por determinados membros de diferentes instituições, como por exemplo os participantes de um projeto interinstitucional. Esses grupos são muitas vezes chamados de OV (Organizações Virtuais).

Um exemplo prático de uma OV é o projeto FIBRE (*Future Internet Testbeds Experimentation Between Brazil and Europe*) [Sallent et al. 2012] para experimentação e validação de soluções para a Internet do Futuro (IF), que conta com diversas instituições no Brasil e em diversos outros países que, juntas, têm um interesse em comum. O objetivo principal do FIBRE é a interconexão de ambientes de experimentação geograficamente distribuídos, chamados de *testbeds*, com a finalidade de oferecer suporte para a experimentação em IF, criando assim um ambiente de testes de larga escala e grande diversidade de equipamentos. Neste ambiente, um pesquisador pode realizar seu experimento alocando recursos de diferentes *testbeds* em diferentes instituições. Para tanto, é necessário tratar o compartilhamento de recursos, de tal forma que um pesquisador possa verificar quais são os recursos disponíveis em todos os *testbeds*, assim como aplicar soluções de A&A para o uso desses recursos. Nesse caso, é preciso garantir que a autenticação de um usuário de uma rede de testes sirva como identificação para o uso dos recursos de qualquer outra rede de teste federada, desde que o usuário atenda às políticas locais de controle de acesso de cada um dos ambientes (instituições/ilhas) envolvidos e às políticas globais do projeto (que representa a OV neste cenário) como um todo.

Contudo, apesar da forte demanda por OVs, criar tais organizações representa um grande desafio. De fato, além de questões práticas específicas de cada OV – sobre como gerenciar recursos ou estabelecer cooperações, por exemplo – o gerente de uma OV precisa também ter grande conhecimento na área de gestão de identidade para estabelecer formas de autenticação e controle de acesso que atendam a todos os requisitos da OV e também de cada instituição participante. Uma vez que, em geral, os potenciais gerentes de OV possuem apenas conhecimento específico sobre o ambiente que desejam criar, acabam sendo desestimulados a criar a OV devido ao alto grau de dificuldade para estabelecer uma gestão de identidade bem elaborada como deveria ser.

2. Motivação

Este trabalho foi desenvolvido tendo como um dos cenários de maior motivação aqueles relacionados a ambientes de experimentação para IF. Estes ambientes apresentam características cruciais à criação de uma OV, onde a gestão de identidade e acesso é fundamental para operação e compartilhamento de seus recursos distribuídos. Pode-se destacar os

seguintes requisitos para essas OVs: (I) **ambiente heterogêneo:** uma vez que essa OV tem como característica a utilização de recursos de tipos diferentes, como nós sem fio, máquinas virtuais, equipamentos de roteamento definidos por software etc; (II) **OV formada por diversas entidades parceiras:** já que o ambiente de experimentação deve ser geograficamente distribuído, e isso só é possível por meio da interconexão entre diversos parceiros, que incorporam seus recursos ao ambiente; (III) **alocação dinâmica dos recursos distribuídos:** com os recursos sendo utilizados hora por certo usuário, hora por outro, devendo ser escalonado esse processo de alocação conforme os pedidos dos participantes da OV; (IV) **usuário pode assumir funções diferentes em instantes diferentes de tempo:** já que em um dado momento o mesmo usuário pode assumir a função de gerente de um projeto, e em outro apenas um integrante de um outro grupo de trabalho; (V)**autonomia para políticas de controle de acesso:** onde cada entidade parceira que oferece acesso a seus recursos, pode descrever seu controle de acesso de forma independente sobre seus recursos oferecidos, respeitando a política geral da OV.

Ao propor um *framework* para A&A para esse ambiente, tais requisitos deverão ser atendidos. Em linhas gerais, esse *framework* deve suportar a heterogeneidade dos recursos do ambiente, suportar as políticas distribuídas e hierárquicas da OV, permitir a reserva de recursos de forma dinâmica e independente a partir do resgate de atributos do usuário de forma dinâmica para a visão atual do ambiente. Deve ainda, permitir que as políticas de controle de acesso a serem descritas sejam independentes entre as entidades que oferecem recursos, mas que respeitem as políticas gerais da OV. Os pontos destacados, são identificados em diversos ambientes de OV, e podem também ser aplicados a eles, mas fica clara a motivação do desenvolvimento deste trabalho no escopo do cenário de um ambiente de IF.

3. Objetivos

A partir do estudo do estado da arte, e conforme [Afsarmanesh and Camarinha-Matos 2005], definiu-se os seguintes objetivos aos quais o trabalho deve contemplar para se firmar como mais completo que as demais soluções propostas na literatura: **(I)** ser integrado a uma solução de autenticação com suporte à federação de identidade e não exigir nenhuma mudança nessa federação; **(II)** realizar autorização baseada em atributos e políticas; **(III)** permitir a transposição de credenciais para diferentes tipos de ambiente de recursos; **(IV)** respeitar a privacidade dos usuários e **(V)** ser aplicável a diferentes federações, ou ambientes, de recursos distribuídos.

4. Resultados Obtidos

Este trabalho contribui ao estado da arte em gerência de OVs, propondo um novo *framework* que facilita, tanto a entrada de instituições em uma OV, quanto a criação de uma nova OV, colaborando para a solução de problemas importantes em IAM. Esse *framework* tem o nome de ACROSS, ***A**ttribute-based access **C**ont**RO**l and di**S**tributed policie**S***.

Além de propor a especificação, documentação e implementação de um *framework* que integra um conjunto mais amplo de funcionalidades do que aqueles presentes na literatura, o ACROSS permite a gerência e integração de uma organização virtual a soluções de gestão de identidade e acesso amplamente difundidas, como é o caso das

federações de identidade e o conceito de controle de acesso baseado em atributos. Diferentemente dos demais trabalhos propostos na literatura, o ACROSS utiliza uma ampla e diversificada gama de conceitos de gestão de identidade e acesso em um único *framework* modularizado, integrado e extensível. Além de suportar a autenticação por federações de identidade e outros métodos, facilita a gerência de atributos específicos a uma organização virtual, através do conceito de provedores de atributos adicionais. Permite a transposição de credenciais entre o ambiente da federação de identidade e a organização virtual de forma simples e ainda realiza controle de acesso utilizando políticas distribuídas e padrões baseados em papel e atributos. Além disso, permite que quaisquer que sejam os tipos de recursos compartilhados pela organização virtual, esses sejam facilmente integrados ao *framework* para a aplicação do controle de acesso.

O ACROSS trata tanto da autenticação [Fernandes et al. 2013, Silva et al. 2013, Silva et al. 2014a] como da autorização em OVs [Silva et al. 2014b, Silva et al. 2015a] , possibilitando a criação de políticas locais e globais para uso de seus recursos. O ingresso de qualquer entidade em uma OV é facilitado a partir de uma federação de identidade, sendo a federação de identidade responsável por manter os principais atributos de um usuário de forma confiável. Além disso, a partir da utilização do ACROSS, esta OV pode armazenar atributos adicionais, ou particulares ao seu ambiente. Através de uma solução de agregação de atributos proposta em [Silva et al. 2015a], o ACROSS possibilita a geração de uma identidade de usuário completa, sem a necessidade de qualquer alteração dos dados do usuário na federação de identidade, nem duplicação de atributos dessa federação de identidade na organização virtual. O *framework* auxilia na instalação e configuração de todos os serviços de uma forma simplificada para quem deseja gerir uma OV, criando uma abstração de detalhes da gestão de identidade que não interessam diretamente ao gerente da OV. Todas essas funcionalidades do *framework* proposto são detalhadas através da modelagem em *Unified Modeling Language* (UML)[1] [Silva et al. 2015b]. Além disso, é proposta uma nova forma de abstração e generalização de pontuação de atributos para classificação de usuários em níveis, que são usados na definição de políticas de acesso. Com este conceito, o ACROSS implementa o *Attribute-Based Access Control* (ABAC) [Hu et al. 2013] e esconde aspectos mais custosos de configuração e gerenciamento dos atributos dos usuários, facilitando a gerência de acesso em OVs.

Este *framework* introduz uma solução de autenticação e autorização flexível e adaptável para OV, suportando diversos conceitos de gestão de identidade e recursos. Entre os benefícios da utilização do ACROSS, destacam-se as contribuições científicas: **(I)** criação de um *framework* de A&A com controle de acesso baseado em atributos e políticas distribuídas para organizações virtuais; **(II)** criação de um agregador de atributos que respeita a privacidade do usuário através da utilização de um atributo opaco único de criação flexível; **(III)** proposta de um novo modelo de classificação de usuário em níveis a partir de seus atributos;

O *framework* ACROSS também oferece as seguintes facilidades: **(I)** desenvolvimento baseado na utilização de padrões, uma vez que se baseia em X.812 , ABAC [Hu et al. 2013], XACML (*eXtensible Access Control Markup Language*), SAML (*Security Assertion Markup Language*), SOAP (*Simple Object Access Protocol*), UML, etc, que facilitam a extensão e integração com outras soluções; **(II)** autenticação baseada em

[1] `http://www.uml.org/`

SAML, herdando todos os benefícios das federações de identidade e facilitando a entrada de novos membros; **(III)** especificação e implementação de forma modularizada, onde cada módulo tem características específicas, facilitando sua extensão e uso; **(IV)** instalação e configuração facilitada através de guias (*wizards*); **(V)** facilidade de gestão das instituições, dos atributos de usuário, políticas e recursos, através de uma *interface web*.

Para obtenção de seus resultados práticos *framework* ACROSS foi implementado em um espelho do GIdLab, o laboratório de experimentação em gestão de identidade real suportado pela RNP, sendo validado por uma organização virtual hipotética com suporte a recursos distribuídos e também no FIBRE.

5. Produção Científica

As publicações listadas nesta seção ocorreram regularmente durante o desenvolvimento da pesquisa até a conclusão do doutorado. Os resultados da tese foram publicados, por fim, no periódico de extrato superior: *Future Generation Computer Systems*.

- 2013
    1. SILVA, E. F.; FERNANDES, N. C. ; RODRIGUEZ, N. ; MAGALHAES, L. C. S. ; SAADE, D. C. M. . Gestão de Identidade em Organizações Virtuais. Minicursos do JAI - XXXIII CSBC. 1ed.Porto Alegre - RS: SBC, 2013, v. 33, p. 1-47.
    2. SILVA, E. F.; FERNANDES, N. C. ; RODRIGUEZ, N. ; MAGALHAES, L. C. S. . Gestão de Identidade em Redes Experimentais para a Internet do Futuro. In: Joni da Silva Fraga; Jacir Luiz Bordim; RafaTimóteo de Sousa Júnior; William Ferreira Giozza. (Org.). Livro de Minicursos do SBRC 2013. 1ed.Porto Alegre - RS: SBC, 2013, v. 31, p. 165-209.
    3. FERNANDES, N. C. ; SILVA, E. F. ; SAADE, D. C. M. . Gestão de Identidade em Testbeds Brasileiros para a Internet do Futuro. In: IV Workshop de Pesquisa Experimental da Internet do Futuro (WPEIF), 2013, Brasília - DF. 31o Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2013.
    4. SILVA, E. F.; SAADE, D. C. M. ; FERNANDES, N. C. . Transposição de Credenciais para uso de Testbeds para a Internet do Futuro. In: II WGID Programa de Gestão de Identidades, 2013, Manaus - AM. XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2013.
- 2014
    1. SILVA, E. F.; FERNANDES, N. C. ; RODRIGUEZ, N. ; MUCHALUAT-SAADE, D. C. . Credential translations in Future Internet testbeds federation. In: IEEE/IFIP Network Operations and Management Symposium (NOMS), 2014, Krakow.
    2. SILVA, E. F.; SAADE, D. C. M. ; FERNANDES, N. C. . Controle de Acesso Baseado em Políticas e Atributos para Federações de Recursos. In: IV Workshop de Gestão de identidade, 2014, Belo Horizonte - MG. XIV SBSeg, 2014.
    3. SILVA, E. F.; FERNANDES, N. C. ; RODRIGUEZ, N. ; SAADE, D. C. M. . Gestão de Identidade em Testbeds de Internet do Futuro baseada em Federações A&A Acadêmicas. In: SEMISH - XLI Seminário Integrado de Software e Hardware, 2014, Brasília / DF. XXXIV CSBC, 2014.
- 2015
    1. SILVA, E. F.; FERNANDES, N. C. ; MUCHALUAT-SAADE, D. . ACROSS-FI: Attribute-Based Access Control with Distributed Policies for Future Internet Testbeds. In: International Conference on Networking, 2015, Barcelona. 14th International Conference on Networking - ICN, 2015. p. 198-204.

2. SILVA, E. F.; SAADE, D. C. M. ; FERNANDES, N. C. . Modelagem do ACROSS: Um Arcabouço de A&A Baseado em Políticas e Atributos para Organizações Virtuais. In: SBSeg 2015 / WGID, 2015, Florianópolis / SC. XV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Porto Alegre / RS: Sociedade Brasileira de Computação, 2015.

- 2018

1. SILVA, E. FRANCO; MUCHALUAT-SAADE, DÉBORA CHRISTINA ; FERNANDES, NATALIA CASTRO . ACROSS: A generic framework for attribute-based access control with distributed policies for virtual organizations. Future Generation Computer Systems, v. 78, p. 1-17, 2018.

6. Conclusão

Comparado aos trabalhos relacionados, VOMS[2], CAS[3], PERMIS[4] e Akenti[5] [Alfieri et al. 2003, Pearlman et al. 2002, Chadwick et al. 2003], o ACROSS possui mais funcionalidades relacionadas à autenticação e autorização. Além de aplicar os conceitos mais atuais de IAM, ACROSS foi pensado para ser flexível e permitir sua extensão futura. Além disso, oferece funcionalidades adicionais como a instalação e configuração por meio de assistentes, o que agiliza e facilita a adesão de uma instituição a uma OV.

Para sumarizar a comparação e contribuições dese trabalho foram levantados os principais pontos de interesse atualmente para a proposta de um *framework* para VOs: para a **autenticação**, o suporte à federação de identidade (SAML/Shibboleth), o provedor de atributos adicionais e a agregação de atributos; para a **autorização**, o suporte aos mecanismos RBAC e ABAC, o uso de políticas distribuídas, globais e locais e o suporte ao XACML.

Os símbolos usados na comparação são apresentados pela Tabela 1. O *suporte nativo* é intuitivo; o *suporte parcial* é explicado nos próximos parágrafos para aqueles que têm ocorrência dessa característica. As *soluções de terceiros* são baseadas em ferramentas criadas por colaboradores ou outros projetos, adaptadas para funcionar com o *framework* em questão.

Tabela 1. Descrição dos símbolos

Símbolo	Significado
✓	Suporte nativo
□	Suporte parcial
■	Soluções de terceiros
	Sem suporte

O suporte à federação de identidade é nativo ao ACROSS e também ao PERMIS com o *Shibboleth and Apache Authorization Module* (SAAM) [Xu et al. 2005], e o CAS, com seu conceito natural de autorização e suporte às instituições distribuídas. Os demais sistemas têm soluções de terceiros. No VOMS, assim como para o Akenti, a solução

[2] *Virtual Organization Membership Service*
[3] *Community Authorization Service*
[4] *PrivilEge and Role Management Infrastructure Standard*
[5] `http://dst.lbl.gov/ACSSoftware/Akenti/`

Tabela 2. Comparação entre as propostas apresentadas

	ACROSS	CAS	VOMS	PERMIS	Akenti
Suporte à Federação de Identidade	✓	✓	■	✓	■
Suporte à Provedor de Atributos	✓	✓	✓	✓	✓
Suporte à Agregação de Atributos	✓				
Suporte ao RBAC	✓	✓	✓	✓	✓
Suporte ao ABAC	✓		□	□	□
Políticas Distribuídas	✓	✓	□	✓	✓
Suporte ao XACML	✓				

desenvolvida por terceiros foi o ShibGrid [Spence 2006], desenvolvida no contexto do *UK National Grid Service*.

Todos os *frameworks* apresentam suporte ao provedor de atributos. O CAS, o VOMS, o PERMIS e o Akenti suportam esses atributos adicionais em certificados de atributos, respeitando sua infraestrutura de chaves públicas e certificados herdados do Globus Toolkit. Porém, apenas o ACROSS apresenta suporte ao agregador de atributos, que, além de agregar os atributos da federação de identidade com os atributos do provedor de atributos adicionais, tem uma característica escalável, suportando diversos provedores de atributos adicionais. O ACROSS ainda provê a privacidade do usuário, através do atributo opaco.

Focando na autorização, o ACROSS apresenta dois mecanismos que merecem destaque: o RBAC e ABAC. O RBAC é suportado por todos os *frameworks* através de papéis. O ABAC é suportado nativamente pelo ACROSS e parcialmente pelo VOMS, PERMIS e Akenti. Diz-se que este suporte é parcial porque estes *frameworks* têm suporte a certificados de atributos, porém a análise desses atributos é sempre realizada na forma de papéis estáticos, associando-os a perfis pré-estabelecidos. Ou seja, esses *frameworks* poderiam ser estendidos para suportar o ABAC, porém teriam que levar em consideração todas as características das entidades desse mecanismo, como a adoção de políticas distribuídas e hierárquicas, a avaliação de atributos dinâmicos etc.

Para prover políticas distribuídas, diz-se que o *framework* deve suportar políticas globais e locais. O ACROSS tem um suporte nativo e de simples entendimento, se apoiando no XACML e X.812. O CAS, o PERMIS e o Akenti foram considerados como suporte nativo, contudo deve-se destacar que o Akenti tem limitações quanto ao suporte à escalabilidade de suas políticas. Já o VOMS tem apenas suporte parcial, por ter sua verificação apenas no nível global. Por ser o mais atual *framework* proposto dentre os comparados, o ACROSS é o único com suporte ao XACML.

Assim, concluimos este trabalho destacando suas principais características, o que demonstra claramente que o ACROSS se apresenta mais completo que os trabalhos do estado da arte.

Referências

Afsarmanesh, H. and Camarinha-Matos, L. M. (2005). *A Framework for Management of Virtual Organization Breeding Environments*, pages 35–48. Springer US, Boston, MA.

Alfieri, R. et al. (2003). Managing dynamic user communities in a grid of autonomous resources. *CoRR*, cs.DC/0306004.

Chadwick, D., Otenko, A., and Ball, E. (2003). Role-based access control with x.509 attribute certificates. *Internet Computing, IEEE*, 7(2):62–69.

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

Hu, V. C., Scarfone, K., and Cybersecurity, S. (2013). Guide to attribute based access control (abac) definition and considerations.

Pearlman, L., Welch, V., Foster, I., Kesselman, C., and Tuecke, S. (2002). A community authorization service for group collaboration. In *Policies for Distributed Systems and Networks, 2002. Proceedings. Third International Workshop on*, pages 50–59.

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

Silva, E., Fernandes, N. C., and Muchaluat-Saade, D. (2015a). Across-fi: Attribute-based access control with distributed policies for future internet testbeds. In *14th International Conference on Networking*, pages 198–204, Barcelona/Spain.

Silva, E., Fernandes, N. C., Rodriguez, N., and Muchaluat-Saade, D. (2014a). Gestão de identidade em testbeds de internet do futuro baseada em federacoes a&a academicas. In *CSBC 2014 - SEMISH ()*, Brasilia, Brazil.

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

Silva, E., Muchaluat-Saade, D., and Fernandes, N. C. (2014b). Controle de acesso baseado em políticas e atributos para federaćões de recursos. In *SBSeg 2014 - WGID*, Belo Horizonte.

Silva, E., Muchaluat-Saade, D., and Fernandes, N. C. (2015b). Modelagem do across: Um arcaboućo de a&a baseado em politicas e atributos para organizacoes virtuais. In *SBSeg 2015 WGID ()*, Florianopolis - SC.

Spence, D. (2006). ShibGrid: Shibboleth access for the UK National Grid Service. In *eScience 2006, Amsterdam*.

Xu, W., Chadwick, D., and Otenko, S. (2005). Development of a flexible permis authorisation module for shibboleth and apache server. In *Public Key Infrastructure*. Springer Berlin Heidelberg.