UNIVALI

FORMULÁRIO DE PROJETO DE TRABALHO - PIBIC

1. TÍTULO DO PROJETO DE TRABALHO:

Mecanismo de Tradução de Credenciais de Autenticação para Portais de Negócios

2. ÁREA DE CONHECIMENTO: Ciência da Computação (1.03.00.00-7)

2.1 Sub-área de conhecimento: Sistemas de Computação (1.03.04.00-2)

2.2 Grupo de Pesquisa: Grupo de Sistemas Embarcados e Distribuídos (GSED)

2.2.1 Linha de Pesquisa ou Área: Sistemas Distribuídos

3. RESUMO

Nos portais de negócios, por onde circulam informações importantes para as corporações e, muitas vezes, sigilosas, garantir o gerenciamento de identidades e a autenticação única (*Single Sign On*) são requisitos desejáveis. Este projeto de pesquisa tem por objetivo prover a autenticação única para portais de negócio do tipo *marketplace*, mesmo diante de credenciais de autenticação heterogêneas, através de um mecanismo de tradução de credenciais. O projeto envolverá (1) a análise dos mecanismos que oferecem autenticação única (SSO) em portais de negócios e do problema da falta de compatibilidade entre credenciais de autenticação, (2) a definição e modelagem do mecanismo de tradução de credenciais para portais de negócios, (3) a implementação de um protótipo do mecanismo e a sua integração em um estudo de caso para verificação da sua aplicabilidade, (4) os testes de software e de desempenho que contribuirão para aferir a qualidade e eficiência do protótipo desenvolvido. Por fim, (5) a divulgação dos resultados desta pesquisa na forma de artigos e na apresentação de seminários a serem realizados pelo grupo de pesquisa.

Palavras-chaves: 1: Gerenciamento de Identidades 2:Tradução Credenciais. 3: Portais de Negócios

4. INTRODUÇÃO

Segundo Camarinha-Matos et al. (2008), um novo ambiente competitivo para as diversas organizações vem se desenvolvendo nos últimos anos e a tendência para negócios colaborativos está forçando um mudança na forma na qual estas organizações são gerenciadas. Segundo os autores, a participação em redes colaborativas tem sido muito importante para as organizações privadas que anseiam encontrar uma vantagem competitiva diferenciada, especialmente se estas forem pequenas ou médias empresas.

Uma rede colaborativa consiste de várias entidades autônomas, heterogêneas e geograficamente distribuídas, que colaboram para encontrar um objetivo comum e compatível e cujas interações são suportadas pelas redes de computadores (CAMARINHA-MATOS et al, 2008). Nas redes colaborativas

organizacionais, os portais de negócios do tipo *marketplace*, que seguem uma arquitetura orientada a serviços, tem sido excelentes oportunidades para que pequenas e médias empresas se tornem mais competitivas e possam aumentar sua participação no mercado visando atender novas oportunidades de negócios (ONs), bem como ampliar sua participação em novos mercados (WEGE, 2002).

Os portais de negócio possuem características comuns, tais como: a customização de serviços de acordo com os interesses específicos de cada usuário, a agregação de conteúdo e serviços proveniente de diferentes fontes e para diferentes interesses, a proliferação de informações resumidas através de protocolos padronizados, por exemplo, via RSS (*Really Simple Syndication*) ou XML (*eXtensible Markup Language*) e o suporte a múltiplos dispositivos (conteúdos e serviços preparados para diferentes dispositivos) (WEGE, 2002). Além destas características, os portais devem ainda oferecer (1) autenticação única (*Single Sign On* - SSO), que permite que um usuário se autentique apenas uma vez (no portal) e use desta autenticação nos demais serviços acessados via portal de negócios e (2) gerenciamento de usuários e de permissões de acesso a informações e serviços disponibilizados via portal, mas que são suportados por diferentes provedores. É importante destacar que há uma tendência para que o controle de acesso seja baseado nas credencias (atributos) dos usuários (BARTON, 2006).

Os portais de negócios possuem uma série de requisitos de interoperabilidade e de segurança. A interoperabilidade é necessária para tratar vários aspectos de heterogeneidade entre os participantes do portal (organizações e usuários), que incluem as diversas plataformas computacionais utilizadas, as várias políticas (administrativas, de segurança, de negócios) às quais esses participantes estão sujeitos e as diferentes tecnologias de segurança adotadas. Um suporte a essa heterogeneidade é essencial para garantir que um portal possa atender o maior número possível de participantes. A segurança, por sua vez, é fundamental para que os participantes deste ambiente colaborativo possam depositar confiança nas suas interações com outros participantes.

Os modelos usuais de autorização se apóiam em uma autoridade de autenticação para mediar a confiança entre partes desconhecidas (terceira parte confiável). Desta forma, as interações entre partes distintas (cliente e provedores de serviços) são alcançadas pela apresentação de credenciais emitidas por uma autoridade de autenticação em quem ambas as partes confiam. Em ambientes mais complexos como os portais de negócios, este modelo de simples intermediação se apresenta como limitado, já que cada organização possui suas próprias políticas, infra-estruturas de segurança e ainda uma forma particular de gerenciar as identidades dos principais (JOSANG et al., 2005).

O gerenciamento de identidades consiste de um sistema integrado de políticas, processos de negócios e tecnologias que permite às organizações proverem recursos de forma segura, somente aos seus usuários. O gerenciamento de identidades também envolve aspectos relacionados com a definição, certificação e gerenciamento do ciclo de vida das identidades digitais, infra-estruturas para troca e validação dessas informações, juntamente com os aspectos legais. Diversos modelos foram propostos para o gerenciamento de identidades (JOSANG et al., 2005).

O aumento de provedores de serviços e a crescente necessidade de compartilhar recursos para usuários de diferentes organizações que possuam algum tipo de afinidade são fatores que motivam a constituição de federações. 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, 2009). A noção de federação é construída a partir do gerenciamento de identidades obtido com o uso de uma Infraestrutura de Autenticação e Autorização (AAI).

A autenticação única (*Single Sign On* – SSO) traz facilidade para os usuários, pois permite que esses passem pelo de processo de autenticação uma única vez e usufrua das credenciais obtidas por todos os serviços que desejar acessar. Garantir tal conceito dentro de um único domínio administrativo e de segurança não é algo complexo, porém garantir o SSO em uma federação de serviços (associadas a um portal de negócios) é algo desafiador. A dificuldade está no estabelecimento, manutenção e encerramento da sessão do usuário, a qual deverá ser mantida por todos os domínios que fazem parte da federação (MALER e REED, 2008) e na necessidade de tradução de credencias de autenticação, ou seja, prover um suporte a autenticação SSO mesmo diante de parceiros que usem diferentes tecnologias de segurança (MELLO et al, 2009). Como exemplo de infraestruturas de autenticação e autorização, tem-se o Shibboleth, Liberty Alliance, OpenAM, OpenID, Microsoft Identity Metasystem (Windows CardSpace).

5. PROBLEMA

A partir da contextualização apresentada anteriormente, pode-se formular as seguintes questões de pesquisa, indicando os desafios a serem enfrentados:

- Diante da heterogeneidade dos participantes/envolvidos (provedores e clientes) em portais de negócios, como prover autenticação única (SSO) tendo como base o gerenciamento de identidades federadas?
- Como garantir que a autenticação SSO provida em portais de negócios possa ser oferecida mesmo diante de diferentes credenciais de autenticação?

5.1. Solução Proposta

Para tratar o problema apresentado, a presente proposta de pesquisa pretende definir um mecanismo adequado as características dinâmicas de portais de negócios orientados a serviços. O mecanismo a ser desenvolvido neste trabalho serve para prover autenticação única em ambientes heterogêneos, atravessando domínios administrativos mesmo que usem tecnologias de segurança distintas. Para isso, o mecanismo proposto estará baseado no modelo de transposição de credenciais de autenticação descrito em (MELLO et al., 2009), porém, com substanciais alterações para que possa oferecer a tradução de credenciais adequada aos portais de negócio (p.ex. que utilizam processos de negócios executáveis).

A solução proposta está apoiada nas especificações *Web Services Remote Portals* – WSRP (OASIS, 2003), na especificação *Web Services Business Process Execution* - WSBPEL (JORDAN; EVDEMON, 2007), nas especificações de segurança para XML e Serviços Web amplamente aceitas e consolidadas, em especial as especificações: SAML (OASIS, 2005), WS-Trust (OASIS, 2009), WS-Policy (2007) e WS-Security (OASIS, 2006). O mecanismo a ser desenvolvido neste projeto ataca o problema das diferentes tecnologias de segurança por meio do gerenciamento de identidades federado e de um mecanismo que será um processo executável que verifica a compatibilidade das credenciais de autenticação e quando necessário traduz estas credenciais para o formato desejável (p.ex., traduzir um certificado X. 509 para uma asserção SAML).

6. OBJETIVOS

6.1. Objetivo geral

Prover a autenticação única (*Single Signo On* –SSO) para portais de negócio do tipo *marketplace*, mesmo diante de credenciais de autenticação heterogêneas, através de um mecanismo para tradução de credenciais de autenticação.

6.2. Objetivos específicos

De forma a alcançar o objetivo geral definido, os seguintes objetivos específicos serão perseguidos:

- analisar os mecanismos que oferecem autenticação única (SSO) em portais de negócios e o problema da falta de compatibilidade entre credenciais de autenticação;
- definir e modelar um mecanismo de transposição de credenciais de autenticação compatível com os requisitos de gerenciamento de identidades em portais de negócio do tipo *marketplace*;
- verificar a aplicabilidade do mecanismo proposto através da implementação de um protótipo e da sua integração a um estudo de caso - um portal de uma agência de viagens;
- verificar eficácia e eficiência do protótipo desenvolvido através de testes de software.

7. JUSTIFICATIVA

O uso de portais de negócios na Internet têm apresentado um crescimento muito acentuado nos últimos anos (BELLAS, 2004). Contribuem para estes avanços as novas tecnologias de rede colaborativa que aumentam as mesmas em escala, no desempenho e em interoperabilidade. Devido à dinamicidade e à heterogeneidade dos portais de negócios, prover o gerenciamento de identidades federadas com suporte a diferentes credenciais de autenticação via portal é uma atividade complexa.

O mecanismo de segurança proposto neste projeto deve prover meios que auxiliem clientes e provedores de serviços no gerenciamento de identidades (ou credenciais) e na tradução de credencias de autenticação. Mecanismos e *frameworks* que oferecem a autenticação SSO estão sendo propostos para Serviços Web (MELLO et al, 2009), porém, tais mecanismos ainda não contemplam todas as

necessidades exigidas em portais de negócios, como por exemplo, lidar com diferentes credenciais de autenticação de um processo de negócio executável (CARMINATI et al., 2005, MELLO et al, 2009). É importante que a criação sob demanda e customizada de processos de negócios (composição dinâmica de Serviços Web), realizada nos portais, seja ciente da segurança, levando em conta os riscos de segurança e os requisitos de todos os parceiros envolvidos (provedores e requisitantes), expressos em suas políticas de segurança. É desejável que processos de negócios não deixem de ser realizados por falta de compatibilidade das credenciais de autenticação entre os parceiros envolvidos.

Neste contexto, esta pesquisa afigura-se relevante uma vez que pretende contribuir com o estudo das implicações da autenticação única (*Single Sign On*) provenientes da execução de Serviços Web Compostos, em especial problemas decorrentes das diferentes credencias de autenticação que podem ser utilizadas pelos participantes da composição.

7.1. Viabilidade do Projeto

O projeto de pesquisa proposto é viável, pois as bibliotecas e as ferramentas necessárias para o desenvolvimento do protótipo do mecanismo de tradução de credenciais para portais de negócios são todos de código aberto, estão bem documentadas e a maioria já foi utilizada em outras pesquisas. Além disso, o projeto proposto continuará as pesquisas do projeto finalizado em 2010 intitulado “Mecanismos de Segurança para Processos de Negócios em Redes Colaborativas” (CNPq/Edital Universal 2007) e estará inserido em um projeto maior, já em andamento, que visa desenvolver serviços de tradução de credenciais para federações acadêmicas, baseadas no Shibboleth. Este último projeto está sendo desenvolvido por três instituições de pesquisa (UNIVALI/UFSC/IFSC). Diversos estudos bibliográficos e protótipos já foram desenvolvidos no contexto dos grupos de pesquisa destas instiuições, porém vale ressaltar que aspectos de autenticação SSO diante de diferentes credenciais de autenticação focada em portais de negócio serão, especificamente, tratados na pesquisa aqui proposta. Tanto o uso dos protótipos já desenvolvidos, quanto o repasse de conhecimentos das tecnologias de Serviços Web para o bolsista estão previstos de acontecer.

8. REVISÃO BIBLIOGRÁFICA/FUNDAMENTAÇÃO TEÓRICA

Em face da necessidade de reduzir os custos operacionais e de melhorar a produtividade, cada vez mais as organizações preocupam-se em desenvolver soluções para automatizar suas colaborações dentro ou através de seus domínios de confiança. A Internet provê uma poderosa infra-estrutura de comunicação e de colaboração e, devido a isto, a realização de negócios que usufruem desta cresceu muito nos últimos anos, impulsionando assim a criação de diversas formas de modelos de negócios e de redes colaborativas. Devido à necessidade de uma rápida adaptação dos negócios para atender novos consumidores e novas condições de mercado, cada vez mais as organizações procuram se unir para criar processos de negócios em portais para desenvolver serviços complexos. Processos de negócios descrevem serviços complexos (Serviços Web Compostos) que transpassam os limites organizacionais e são providos por diferentes parceiros (PELTZ, 2003). O desenvolvimento dos Serviços Web (*Web Services*), como uma tecnologia

modular de interoperabilidade global, coloca-os como uma peça fundamental para a área dos processos de negócios baseados em XML (BOOTH et al., 2004).

Os Serviços Web seguem uma arquitetura orientada a serviços (AOS) e são componentes de softwares projetados para suportar interações entre aplicações heterogêneas sobre a Internet. De acordo com Mello et al. (2006), as principais características que os tornam uma tecnologia emergente e promissora para a realização de transações comerciais, são: (1) possuem um modelo fracamente acoplado e transparente que garante a interoperabilidade entre os serviços, sem que estes necessitem ter o conhecimento prévio de quais tecnologias estão presentes em cada lado da comunicação; (2) usam um conjunto de padrões, como o HTTP e o XML, que permite a convergência de funcionalidades de negócios díspares através de linguagens e protocolos amplamente aceitos, resultando em uma redução significativa nos custos totais de desenvolvimento de aplicações de negócio; (3) usam interfaces de serviços que são auto-descritivas e baseadas no padrão XML; (4) tornam mais fácil a composição ou a combinação de diferentes provedores, visando formar serviços mais complexos e sofisticados.

A especificação WS-Security (OASIS 2006) define formas de prover integridade e confidencialidade às mensagens SOAP usando, respectivamente, os padrões XML-Signature (BARTEL ET AL., 2002) e XML-Encryption (IMAMURA et al., 2002). Esses dois padrões servem para representar assinaturas e cifras no formato XML (e não apenas assinar e cifrar documentos XML). Além disso, a WS-Security também estende o padrão SOAP para que as mensagens possam transportar diversos elementos de segurança como, por exemplo, pares usuário/senha, certificados X.509, Kerberos tickets ou asserções SAML.

A especificação SAML (*Security Assertion Markup Language*) (OASIS, 2005) define uma infraestrutura de segurança capaz de expressar, na forma de asserções, informações de autenticação, de autorização e de atributos acerca de um sujeito. Apesar de não prover a autenticação em si, o padrão SAML permite que, uma vez realizada a autenticação, esta possa ser usada em domínios diferentes por meio da troca de asserções. O modelo de confiança nos Serviços Web é definido na especificação WS-Trust (OASIS, 2007). Esta especificação pressupõe que, caso um sujeito que tente acessar um recurso não disponha das credenciais exigidas na política do provedor, o sujeito deve conhecer alguma autoridade que possa consultar (terceira parte confiável), na tentativa de obter tais credenciais. Na WS-Trust, essa autoridade é genericamente denominada de Serviço de *Tokens* de Segurança (*Security Token Service* - STS), que é responsável por emitir, validar e trocar credenciais de segurança. A WS-Trust prevê que as credenciais sejam transparentes ao sujeito que invocar o STS, no entanto, não provê informações sobre como credenciais de um tipo específico são transformadas para as credenciais exigidas no domínio do provedor de serviço.

Conforme constatado em Wege (2002), a tecnologia de Serviços Web, através da especificação *Web Services Remote Portals* – WSRP (OASIS, 2003), tem sido amplamente utilizada como infra-estrutura de comunicação, colaboração e coordenação em portais de informações e de aplicações, em especial, em portais de negócio do tipo *marketplace*.

Devido às características dos portais do tipo *marketplace*, que envolve vários domínios administrativos e ambientes heterogêneos, a utilização de uma tecnologia integradora tanto em nível de plataformas computacionais quanto de sistemas de informação se faz necessário. Nestes portais, para agilizar a criação de processos de negócios sob demanda e customizados, há a necessidade de uma composição dinâmica dos Serviços Web que participarão do processo de negócios. Na composição de Serviços Web, as aplicações tornam-se ainda mais visíveis, expondo suas funcionalidades, seus fluxos de negócios, processos, políticas e arquiteturas internas. Este cenário torna esta área um excelente ambiente para pesquisa.

Conforme constatado em (CARMINATI et al., 2005), geralmente, um provedor de serviços tem preocupações de segurança com relação aos provedores ou serviços com os quais este coopera durante uma transação comercial. É comum que os Serviços Web estejam acessíveis apenas para os parceiros de negócios que possuam credenciais de segurança apropriadas. Isto significa que o portal tem que conhecer as políticas de segurança dos serviços parceiros, antes de iniciar a comunicação com estes para verificar se as credencias exigidas e providas são compatíveis.

Para a realização de transações comerciais através de portais de negócio, por onde circulam informações importantes para as corporações e, muitas vezes, sigilosas, estabelecer o gerenciamento de identidades entre os parceiros envolvidos e traduzir credenciais de autenticação utilizadas na composição são necessidades críticas.

9. METODOLOGIA

A natureza deste trabalho é uma pesquisa aplicada. Será utilizado nesta pesquisa o método de experimentação através do desenvolvimento e avaliação de um protótipo que envolverá mecanismo para tradução de credenciais de autenticação para portais de negócio do tipo *marketplace* baseados em Serviços Web. A abordagem desta pesquisa é qualitativa, pois não requer o uso de métodos e técnicas estatísticas.

Para a construção do protótipo, até o momento, foram selecionados os seguintes softwares de código aberto: o ambiente de desenvolvimento Eclipse, a ferramenta de modelagem Enterprise Architecture, o *framework* para desenvolvimento de Serviços Web METRO e o servidor de aplicação Glassfish. A validação do mecanismo que será desenvolvido será realizada seguindo técnicas de engenharia de software. O protótipo implementado passará por testes tanto de software quanto de desempenho. A gestão desse projeto se dará através de reuniões periódicas entre orientador e bolsista. Além dessas reuniões, estão previstos seminários com a participação de alunos e demais pesquisadores que participam do GSED (Grupo de Sistemas Embarcados e Distribuídos) da Univali e o GCSEG (Grupo de Computação Segura e Confiável) da UFSC, grupos parceiros que já desenvolvem juntos pesquisas nesta área. A ferramenta de apoio a gestão de projetos DotProject será utilizada para acompanhamento de todas as etapas especificadas a seguir.

9.1 Plano de Trabalho

1. Estudo bibliográfico

Esta primeira etapa é destinada à formação do acadêmico-pesquisador, através do estudo das especificações relacionadas à arquitetura orientada a serviços, à arquitetura e desenvolvimento de portais (WSRP) e à segurança em Serviços Web. Textos de apoio serão indicados pela orientadora e reuniões periódicas serão realizadas para auxiliar a consolidação da base teórica da pesquisa. Faz parte desta etapa, analisar os *frameworks* para desenvolvimento de portais de código aberto e selecionar o mais adequado aos requisitos de segurança do projeto. Como resultado desta etapa, o bolsista deverá redigir um breve tutorial sobre como utilizar o portal escolhido destacando os mecanismos de segurança existentes no portal. Além disso, de forma a disseminar os conhecimentos entre os dois grupos de pesquisa, o bolsista participará de seminários e fará uma apresentação sobre portais de negócio do tipo *marketplace*.

2. Definição e Modelagem do Mecanismo de Tradução de Credenciais para Portais de Negócios

Nesta etapa, com base nas especificações WSRP, WS-BPEL e nas especificações de segurança para Serviços Web a arquitetura do mecanismo de tradução de crendenciais para portais de negócios será definida. Toda a modelagem do mecanismo será realizada utilizando UML. Os desenvolvimentos a serem realizados seguirão um processo de desenvolvimento de software e ferramentas de apoio serão utilizadas para este fim.

3. Implementação do Protótipo

Conforme mencionado, serão utilizadas somente ferramentas de código aberto no desenvolvimento do protótipo. Primeiramente, o bolsista investirá um tempo para fazer pequenos experimentos com o *framework* METRO/Glassfish e com as ferramentas para construção de portais para se familiarizar com a implementação de Serviços Web e com o uso dos portais baseados em uma arquitetura orientada a serviços. Em seguida, um protótipo do mecanismo de tradução de credenciais será implementado e integrado a um estudo de caso - um portal de uma agência de viagens.

4. Avaliação do Protótipo

Os softwares implementados passarão por testes de software (tanto de unidade quanto de integração) visando melhorar sua qualidade e sua conformidade com as especificações de Serviços Web. Além disso, testes de desempenho para avaliar o peso da inserção do mecanismo de tradução serão realizados.

5. Documentação e Divulgação de Resultados

Esta etapa compreenderá a produção dos relatórios parcial e final, bem como de um artigo discutindo os resultados alcançados com este projeto de pesquisa, a ser submetido para um evento de iniciação científica. Outra forma de divulgação dos resultados da pesquisa ocorrerá através de seminários a serem apresentados na UNIVALI. Estes seminários serão abertos a todos os pesquisadores e alunos interessados.

10. CRONOGRAMA DE ATIVIDADES DE PESQUISA

10.1 Cronograma físico da pesquisa

Atividades	08/08	09/08	10/08	11/08	12/08	01/09	02/09	03/09	04/09	05/09	06/09	07/09
1	●	●	●	●	●							
2				●	●	●	●					
3						●	●	●	●	●	●	●
4											●	●
5							●	●				●

10.2 Orçamento do projeto

Material de Consumo	**Quantidade**	**Preço Unitário**	**TOTAL**
Toner de impressora HP LJ1015	1	250,00	250,00
TOTAL			**250,00**
Material Permanente	**Quantidade**	**Preço Unitário**	**TOTAL**
Livros	2	100,00	200,00
TOTAL			**200,00**
Outros serviços e encargos	**Quantidade**	**Preço Unitário**	**TOTAL**
Inscrição em eventos	2	175,00	350,00
TOTAL			**350,00**
Material de Consumo			250,00
Material Permanente			200,00
Outros serviços e encargos			350,00
TOTAL GERAL			**800,00**

11. REFERÊNCIAS

BAJAJ, S. et al. **Web Services Policy 1.2** - Framework (WS-Policy). 2006. W3C Member Submission. Disponível em: <http://www.w3.org/Submission/2006/SUBM-WS-Policy-20060425/>. Acesso em: 13 maio 2008.

BARTEL M.; BOYER J.; FOX, B. **XML-Signature Syntax and Processing**. W3C, 2002.

BARTON, T. et al. Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy. In: ANNUAL PUBLIC KEY INFRASTRUCTURE R&D WORKSHOP, 5th, 2006, Gaithersburg, MA. **Proceedings…** Gaithersburg, National Institute of Standards and Technology Interagency Series (NISTIR 7313), 2006. p. 64-67.

BELLAS, F. Standards for Second-Generation Portals. **IEEE Internet Computing**, v. 8, n. 4, p. 54-60, Mar. 2004.

BOOTH, D. et al. **Web Services Architecture**. W3C Working Group Note, 2004. Disponível em: <http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/>. Acesso em: 25 jan 2007.

CAMARINHA-MATOS, L. M. e AFSARMANESH, H. Collaborative networks: a new scientific discipline. **Journal of Intelligent Manufacturing**, v. 16, n. 4-5, p. 439–452, 2005.

CARMINATI, B.; FERRARI, E.; HUNG, P. C. K. Web service composition: A security perspective. In: INTERNATIONAL WORKSHOP ON CHALLENGES IN WEB INFRMATION RETRIEVAL AND INTEGRATION (WIRI'05), 2005, Tokyo. **Proceedings…** Los Amitos, CA, IEEE Computer Society, 2005. p. 248 -253.

CARMODY, S., ERDOS, M., HAZELTON, W. HOEHN, B. MORGAN, T. SCAVO e D. WASLEY. **InCommon Technical Requirements and Information**. Last update 18.12.2009. Disponível em: <http://www.incommonfederation.org/technical.html>. Acesso em: 10 jul. 2010.

IMAMURA T.; DILLAWAY B.; SIMON E. **XML encryption syntax and processing**. W3C, 2002.

JORDAN, D.; EVDEMON, J. **Web Services Business Process Execution Language Version 2.0**. apr 2007. OASIS Standard. Disponível em: <http://docs.oasisopen.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html>.

JOSANG, A., FABRE, J., HAY, B., DALZIEL, J., e POPE, S. Trust requirements in identity management. In: AUSTRALASIAN WORKSHOP ON GRID COMPUTING AND E-RESEARCH (AusGRID'05), 3th, 2005, Newcastle, Australia. **Proceedings…** Australian Computer Society, Conferences in Research and Practice in Information Technology Series (CRPITS'44), pp. 99–108.

MALER, E. e REED, D. The Venn of Identity: Options and Issues in Federated Identity Management. **IEEE Security and Privacy**, v. 6, n. 2, p. 16-23, Mar. 2008.

MELLO, E. R. de; WANGHAM, M. S.; FRAGA, J.; CAMARGO, E. Segurança em Serviços Web. In: **Livro de Minicursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**. Santos: SBC, 2006. p. 1–48.

MELLO, E. R. de; WANGHAM, M. S.; FRAGA, J. S.; CAMARGO, E. T.; BOGER, D. S. . A Model for Authentication Credentials Translation in Service Oriented Architecture. **In Transactions on Computational Sciences Journal** - Security in Computing, v. 5430, p. 68-86, 2009.

OASIS. **Web Services for Remote Portlets (WSRP)**. Organization for the Advancement of Structured Information Standards (OASIS), 2003.

OASIS. **Security Assertion Markup Language (SAML) 2.0 Technical Overview**. Organization for the Advancement of Structured Information Standards (OASIS), 2005.

OASIS. **Web services security: Soap message security 1.1**. Organization for the Advancement of Structured Information Standards (OASIS) Standard Specification, 2006.

OASIS **WS-Trust 1.4**. Organization for the Advancement of Structured Information Standards (OASIS), 2009. Disponível em: <http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.pdf>.

WS-POLICY. **Web services policy 1.5 - framework**. W3C Recommendation, 2007. http://www.w3.org/TR/2007/REC-ws-policy-20070904/.

PELTZ, C. Web services orchestration and choreography. **IEEE Computer**, v. 36, n. 10, p. 46-52, 2003.

WEGE, C. Portal server technology. **IEEE Internet Computing**, v.6, n.3, p. 73–77, 2002.