Capítulo 3

Segurança em Redes Colaborativas: Desafios e Propostas de Soluções[1]

Michelle S. Wangham[◇], Emerson Ribeiro de Mello[†], Davi da Silva Böger[⋆], Ramicés dos Santos Silva[⋆], Diego Ricardo Holler[◇], Joni da Silva Fraga[⋆]

[◇] Universidade do Vale do Itajaí

[⋆] Universidade Federal de Santa Catarina

[†] Instituto Federal de Santa Catarina

email:wangham@univali.br, mello@ifsc.edu.br,
{dsboger, ramices, fraga }@das.ufsc.br, diego.holler@univali.br

Abstract

The infrastructure provided by Internet stimulated the creation of different forms of collaborative networks. This Chapter introduces an analysis about security challenges in colaborative networks based on service oriented architecture, in particular, virtual organizations and national research and education networks. Dynamic trust establishment, quality of protection policies, privacy and single sign on in heterogeneous infrastructure are the main challenges in this environment. This Chapter also presents some security proposals to colaborative networks and some problems that are not covered yet.

Resumo

A realização de negócios que usufruem da infra-estrutura de colaboração oferecida pela Internet impulsionou a criação de diversas formas de redes colaborativas. Este Capítulo apresenta uma análise sobre os desafios de segurança presentes nas redes colaborativas baseadas na arquitetura orientada a serviço, em especial, organizações virtuais e redes nacionais de pesquisa e educação. Entre os desafios, destacam-se o estabelecimento dinâmico da confiança, a definição de políticas globais de qualidade de proteção, a privacidade das informações das entidades que compõem tais redes e a concretização da autenticação única e da autorização diante de infra-estruturas de segurança heterogêneas. Soluções para prover segurança às redes colaborativas voltadas para tratar cada um destes desafios são analisadas e, por fim, são apresentadas questões ainda em aberto.

[1]Financiado pelo CNPq (Projeto 484740/2007-5)

3.1. Introdução

Com o seu amadurecimento, a Internet alcançou índices de desempenho e confiabilidade que permitiram que esta deixasse de ser uma rede apenas acadêmica para transformar-se em uma importante plataforma de comunicação e colaboração para pessoas e organizações em todos os ramos de atividades. Essa evolução não só permitiu que as comunicações se tornassem mais rápidas e baratas, mas também oportunizou o desenvolvimento de novas formas de interação através das redes colaborativas. Dentre essas formas, destacam-se as redes colaborativas de organizações (*Collaborative Networks of Organizations* - CNO), que são sistemas constituídos por componentes autônomos, geograficamente distribuídos, que colaboram através da rede para alcançar um objetivo comum [Camarinha-Matos e Afsarmanesh 2005] e 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].

As redes colaborativas de pesquisa e de organizações possuem uma série de requisitos de interoperabilidade e segurança, que estão presentes em todas as fases do seu ciclo de vida. A interoperabilidade é necessária para tratar vários aspectos de heterogeneidade entre os membros da rede, que incluem as diversas plataformas computacionais (hardware, sistemas operacionais, linguagens de programação) utilizadas, as várias políticas (administrativas, de segurança, de negócios) 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 rede colaborativa possam depositar confiança nas suas interações com outros membros.

Uma vez que as redes colaborativas exigem que as organizações participantes tenham relações de confiança com um amplo domínio de parceiros, apesar da tendência para trabalhos colaborativos, muitas organizações ainda têm receios em compartilhar informações sensíveis, principalmente, quando há a necessidade de colaboração com parceiros desconhecidos [Wangham et al. 2005]. Do ponto de vista de políticas de segurança, cada organização possui suas próprias políticas, ou seja, havendo a necessidade de colaboração há ainda a necessidade de um acordo entre os parceiros envolvidos.

Os desafios de segurança que envolvem as redes colaborativas iniciam-se na sua fase de criação. Dentre estes, destacam-se o estabelecimento dinâmico de relações de confiança, a definição de políticas globais de qualidade de proteção e, no caso das organizações virtuais, a privacidade na busca e seleção de parceiros. Durante a fase de operação das redes colaborativas, como as entidades participantes estão dispostas por diferentes domínios administrativos e de segurança, os desafios consistem em concretizar a autenticação SSO (*Single Sign On*) e a autorização distribuída de forma transparente, devido principalmente à heterogeneidade das infra-estruturas de segurança. Na comunicação entre os participantes das redes colaborativas, deve-se garantir a confidencialidade, a integridade e a autenticidade das informações transmitidas, de acordo com a política de qualidade de proteção (QoP) estabelecida. A manutenção de uma rede está relacionada à evolução da composição da mesma. As redes colaborativas que serão tratadas neste capítulo possuem diferentes níveis de dinamismo. O grande desafio nestes ambientes é

manter o progresso das aplicações mesmo diante do que é identificado na literatura como churn [Godfrey et al. 2006], recursos entram e saem do sistema em tempos arbitrários, e muitas vezes durante os processamentos distribuídos.

O objetivo deste capítulo é analisar os desafios e as propostas de soluções para prover segurança às redes colaborativas orientadas a serviços, em especial, para as organizações virtuais e para as redes nacionais de pesquisa e educação. As questões chaves de segurança analisadas são: autenticação SSO, estabelecimento dinâmico de relações de confiança, casamento de políticas de qualidade de proteção e controle de acesso distribuído. Os conceitos, problemas e soluções de segurança apresentados neste capítulo são complementados com a apresentação de cenários de uso em redes colaborativas que demonstram a aplicabilidade das soluções de segurança apresentadas.

Este capítulo está dividido em cinco seções. Nesta primeira Seção foi apresentado o contexto geral em que o trabalho está inserido, destacando os objetivos do documento e a motivação para a escolha do tema. Na Seção 3.2, os tipos de redes colaborativas são descritos e alguns conceitos básicos relacionados à Arquitetura Orientada a Serviços são introduzidos. Ainda nesta seção, dois cenários de uso de redes colaborativas são descritos. A Seção 3.3 apresenta os principais desafios de segurança presentes nas redes colaborativas e, retomando os cenários apresentados na seção anterior, são apresentadas as principais ameaças de segurança nestes cenários. A Seção 3.4 tem por objetivo apresentar o estado da arte relativo à segurança em redes colaborativas orientadas a serviços, ou seja, as soluções atuais para os problemas apontados na Seção 3.3 . Por fim, a seção 3.5 traz uma síntese dos principais aspectos de segurança analisados e das tendências das soluções de segurança apresentadas.

3.2. Redes colaborativas: tipos e infra-estruturas de serviços

Segundo [Camarinha-Matos et al. 2008], um novo ambiente competitivo para as indústrias de manufatura, de software e de serviços vem se desenvolvendo nos últimos anos e a tendência para negócios colaborativos está forçando um mudança na forma na qual estas indústrias são gerenciadas. Segundo os autores, a participação em redes colaborativas tem sido muito importante para a organização que anseia encontrar uma vantagem competitiva diferenciada, especialmente se esta for uma pequena ou média empresa.

Neste Capítulo, está sendo adotado o seguinte conceito para rede colaborativa: "é uma rede que consiste de várias entidades (p.ex., organizações pessoas e máquinas) 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]. Dois tipos de redes colaborativas serão abordados neste trabalho: as redes colaborativas de organizações (*Collaborative Networks of Organizations* - CNO) e as redes nacionais de pesquisa e educação (*National Research and Education Network* - NREN).

3.2.1. Redes Colaborativas de Organização

Uma grande variedade de redes colaborativas de organizações tem sido formada nos últimos anos, como por exemplo, Empresas Estendidas (*Extended Enterprises*), Cadeias de Fornecimento Dinâmicas (*Supply Chain*), Empresas Virtuais (*Virtual Enterprises*) e

Organizações Virtuais (*Virtual Organizations*)[Camarinha-Matos e Afsarmanesh 2005]. No cenário das redes de organizações, a cooperação na forma de organizações virtuais (OVs) é a estratégia que mais se destaca e que vem sendo adotada por muitas empresas, por profissionais e laboratórios espalhados ao redor do mundo, visando atender novas oportunidades de negócios (ONs), bem como ampliar sua participação em novos mercados e/ou alcançar excelência científica para o desenvolvimento de projetos inovadores [Kürümlüoglu et al. 2005].

Uma OV corresponde a uma união temporária de organizações independentes que se agregam visando compartilhar recursos e funcionalidades para alcançar objetivos que estas não alcançariam sozinhas. A cooperação destas organizações é garantida pela automação e informatização de grande parte de suas infra-estruturas, deixando-as acessíveis via Internet. A seleção dos membros da OV é, geralmente, provida por sistemas de busca e seleção de parceiros que são aplicados sobre um conjunto pré-definido de organizações, chamado de ambiente de geração de OVs (*Virtual Organization Breeding Enviromment - VBE*), que é uma evolução do conceito tradicional de *cluster* de empresas [Wangham et al. 2005].

Conforme ilustrado na Figura 3.1, o ciclo de vida de uma organização virtual é um processo circular composto dos estágios de criação, operação, evolução e dissolução cujas funcionalidades são [Camarinha-Matos et al. 2008]:

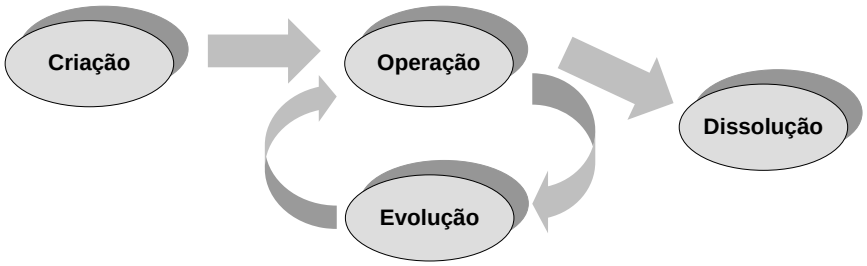

Figura 3.1. Ciclo de Vida de Vida de uma Organização Virtual

- Criação: identificar as competências necessárias para atender a uma oportunidade de negócio, modelar o projeto cooperativo com base nestas competências e identificar os parceiros que melhor se enquadram neste projeto (busca e seleção). Regras comuns de cooperação, riscos e o como ocorrerá compartilhamento dos resultados também são definidos neste estágio;

- Operação: executar o projeto cooperativo de forma eficiente e efetiva. Mecanismos de cooperação e medidas de desempenho tem papel importante neste estágio;

- Evolução: permitir uma pequena alteração de membros ou redistribuição de competências entre os membros. Mudanças maiores em objetivos, princípios ou mudanças de muitos parceiros levam a uma nova formação;

- Dissolução: como os projetos dentro de uma OV tem tempos de vida limitados, quando finalizados as relações de cooperação precisam ser dissolvidas.

Para a realização do conceito de redes colaborativas de organizações, três pré-condições são essenciais: a colaboração entre os parceiros envolvidos em um nível que vai além da simples troca de mensagens de correio eletrônico; a confiança, pois parceiros desejam compartilhar informações; e que todas (ou quase todas) as atividades colaborativas realizadas sejam feitas via rede de computadores [Rabelo 2008].

No cenário das redes de organizações, onde as alianças são voláteis e o fluxo de colaboração algumas vezes é gerado e conhecido dinamicamente, de acordo com o processo de negócio requerido, infra-estruturas para negócios colaborativos mais flexíveis são necessárias. A infra-estrutura deve ser transparente e adaptativa, de acordo com as condições do ambiente de negócio e o nível de autonomia das organizações. Segurança e interoperabilidade são dois requisitos não funcionais que também devem ser considerados nesta infra-estrutura [Rabelo 2008].

3.2.2. Redes Nacionais de Pesquisa e Educação

As Redes Nacionais de Pesquisa e Educação (*National Research and Education Network* - NREN) são caracterizas por interconectar principalmente entidades de educação superior (universidades e institutos de pesquisas), porém outras quatro exceções podem pertencer a uma NREN, escolas de ensino médio e fundamental, museus e bibliotecas, hospitais e departamentos do governo.

Segundo a associação TERENA (*Trans-European Research and Education Networking Association*)[2] (2008), é crescente, não só na Europa, o número de países interessados em desenvolver e aprimorar suas redes nacionais (NRENs). Na Europa, catalogados na associação TERENA, são 46 países que possuem estas redes. Dados do consórcio da APAN (*Asia-Pacific Advanced Network*)[3] indicam 15 redes acadêmicas na Ásia e Pacífico, já na América Latina 15 países são membros da Rede *Clara* (*Cooperación Latino Americana de Redes Avanzadas*)[4]. Outras duas importantes redes nacionais são a *Internet2* (Estados Unidados)[5] e a *CANARIE* (Canadá)[6].

No Brasil, tem-se a Rede Nacional de Ensino e Pesquisa (RNP) que oferece uma infra-estrutura de rede Internet (rede Ipê) que conecta as principais universidades e institutos de pesquisa do país, cerca de 600 instituições, beneficiando-se de um canal de comunicação rápido e com suporte a serviços e aplicações avançadas. Baseada em tecnologia de transmissão óptica, a rede Ipê está entre as mais avançadas do mundo e possui conexão com redes acadêmicas estrangeiras, tais como *Clara* (América Latina), *Internet2* (Estados Unidos) e *Géant* (Europa) [7].

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, Telefonia IP e *help desk*; centro de

[2] http://www.terena.org
[3] http://www.apan.net
[4] http://www.redeclara.net
[5] http://www.internet2.edu
[6] http://www.canarie.ca
[7] http://www.rnp.br

atendimentos a incidentes de Segurança; serviços de vídeo digital, tais como vídeo sob demanda e transmissões de vídeo ao vivo; ferramentas de planejamento e operação de redes que monitoram o funcionamento de todos os enlaces da NREN; infra-estrutura de chaves públicas (ICP), serviços de autenticação e de autorização para federações de serviços; serviços de sincronização de relógios e *Grid Services*. O portfolio de serviços oferecidos pelas NREN tem crescido a cada ano.

Na RNP, os serviços básicos de conectividade oferecidos para as instituições usuárias da rede Ipê incluem ampla largura de banda de acesso, com uso de tecnologias avançadas como IPv6 e *multicast* e atendimento a incidentes de segurança. A RNP também disponibiliza ferramentas avançadas de comunicação, tais como videoconferência e telefonia pela Internet (voz sobre IP), serviços de vídeo digital (vídeo sob demanda, transmissão de vídeo ao vivo e transmissão de sinal de TV), *service desk*, serviço de sincronização de relógio e *Internet Data Center*[8]. Desde 2008, a RNP reúne instituições de ensino e pesquisa brasileiras em uma rede de confiança chamada Federação CAFe - Comunidade Acadêmica Federada, na qual cada instituição parceira é responsável por autenticar e prover informações de seus usuários para provedores de serviços autorizados pertencentes a esta federação[9].

3.2.3. Redes Colaborativas Orientadas a Serviço

Arquitetura Orientada a Serviços

Um conceito que vem se solidificando para a construção de redes colaborativas é o de Arquitetura Orientada a Serviços (AOS) [Rabelo 2008]. Os componentes fundamentais de uma AOS são os serviços que implementam interfaces bem definidas. As aplicações distribuídas são construídas então através da composição e combinação dos vários serviços disponíveis [Weerawarana et al. 2005].

A AOS é constituída de relações entre três tipos de participantes: o diretório para registro de serviços, repositório que é utilizado para publicar e localizar as interfaces dos serviços; o provedor de serviços, entidade responsável por publicar as interfaces dos serviços providos por esta no registro de serviços e também responsável por atender as requisições originadas pelos clientes; e o cliente, aplicação ou um outro serviço que efetua requisições a um serviço. Cada participante da arquitetura pode ainda assumir um ou mais papéis, podendo ser, por exemplo, um provedor e um cliente de serviços [de Mello et al. 2006].

Os participantes se relacionam através de três operações: publicar, localizar e invocar, como pode ser visto na Figura 3.2. Inicialmente, o provedor de serviços publica a interface do seu serviço junto ao diretório para registro de serviços. Desta forma, em algum momento posterior, o cliente pode efetuar uma busca por um determinado serviço (operação localizar), especificando as características desejadas, no diretório de registros. Se o serviço existir, a interface e a localização do respectivo serviço são retornados para o cliente. Por fim, o cliente efetua uma invocação ao provedor do serviço (operação invocar) [de Mello et al. 2006].

[8]Mais detalhes sobre esses serviços podem ser obtidos em `http://www.rnp.br/servicos`

[9]`http://eaa-ufc.ufc.br/wiki/index.php/Federa%C3%A7%C3%A3o_CAFe`

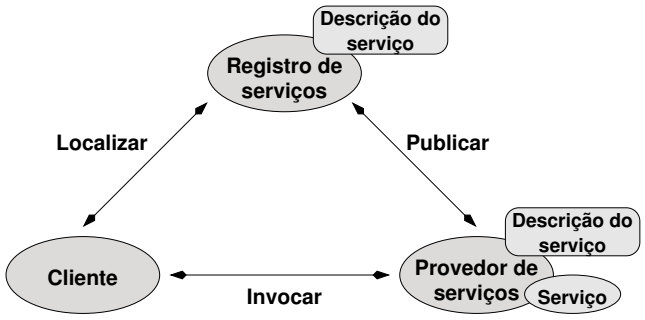

Figura 3.2. Interação entre as entidades da AOS[de Mello et al. 2006]

[Erl 2006] apresenta uma série de princípios que os serviços devem atender:

- serviços abstraem a lógica de implementação. Devido a isto, o contrato do serviço (sua interface) é a única parte visível para o mundo externo;
- serviços compartilham um contrato formal que descreve o que o serviço faz e quais os termos da troca de informações entre os serviços;
- serviços são fracamente acoplados pois são projetados pra interagir sem a necessidade de dependências fortes e o conhecimento interno de suas estruturas;
- serviços são autônomos já que a lógica governada por um serviço permanece em um contorno explícito e este não é dependente de outros serviços para executar sua governança;
- serviços podem ser compostos;
- serviços permitem serem descobertos, pois seus contratos podem estar expostos em um repositório;
- serviços são reutilizáveis;
- serviços não fazem o gerenciamento de estado (*stateless*).

Os Serviços *Web* (*Web Services*) são uma das principais tecnologias existentes para a implementação de aplicações seguindo a AOS e são componentes de software projetados para prover suporte às interações entre aplicações heterogêneas sobre a Internet. As principais características que tornam os Serviços *Web* uma tecnologia integradora e promissora são [de Mello et al. 2006]: (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) são auto-contidos[10] e auto-descritivos[11]; (3) usam padrões abertos como o

[10]A adoção dos Serviços *Web* não implica uso de qualquer aplicativo adicional no cliente ou no servidor. Para o cliente, basta uma linguagem de programação que dê suporte a XML e ao HTTP, por exemplo. Para o servidor, basta que o mesmo possua um servidor de aplicação para disponibilizar os serviços.

[11]Tanto o cliente como o servidor só precisam se preocupar com o formato e com o conteúdo das mensagens a serem trocadas, abstraindo os detalhes de implementação (fraco acoplamento).

HTTP e o XML, permitindo assim que aplicações sejam integradas através de linguagens e protocolos amplamente aceitos, e (4) tornam mais fácil a composição ou a combinação de diferentes provedores, visando formar serviços mais complexos e sofisticados.

Para tornar possível as três operações fundamentais de uma AOS - publicar, localizar e invocar - a arquitetura de Serviços *Web* adota as seguintes tecnologias baseadas em XML: a *Web Services Description Language* (WSDL) [Booth e Liu 2007], linguagem padrão usada para descrever as funcionalidades dos Serviços *Web*; o *Universal Description, Discovery and Integration* (UDDI) [Clement et al. 2004], serviço padrão para publicação e localização de Serviços *Web*; e o SOAP [Mitra e Lafon 2003], protocolo usado para a invocação do serviço.

Segundo [Rabelo 2008], como as redes colaborativas são caracterizadas como um sistema aberto, que faz uso da Internet, as vantagens inerentes dos Serviços *Web* tornam esta tecnologia ideal para compor a camada de infra-estrutura que dará o suporte para as trocas de informações, que fornecerá as funcionalidades de coordenação e de colaboração e que permitirá que relações de negócios e de parcerias entre empresas e instituições de ensino e pesquisa sejam estabelecidas de maneira simples e dinâmica. Com o uso desta tecnologia, as aplicações podem executar múltiplos saltos, envolvendo múltiplas operações em vários serviços, e, além disso, estas podem ultrapassar os limites impostos pelos filtros de pacotes tradicionais (*firewalls*).

Um conceito fundamental para a compreensão das infra-estruturas de suporte às redes colaborativas é o de **federação de serviços**, definido no contexto deste trabalho como: uma forma de associação dos parceiros de uma rede colaborativa que usa um conjunto comum de atributos, práticas e políticas para trocar informações e compartilhar serviços, possibilitando a cooperação entre os membros da federação[12]. Uma federação é basicamente composta por consumidores de serviços (clientes), provedores de serviços (*Service Provider* - SP) e provedores de identidades (*Identity Provider* - IdP). Provedores de serviços são entidades que disponibilizam serviços para os parceiros da federação, consumidores de serviços são entidades ou serviços que usufruem dos serviços disponibilizados nos provedores de serviços e provedores de identidade são entidades que atuam como um serviço de autenticação para consumidores de serviços e como serviço de autenticação da origem do dado para provedores de serviços. IdPs atuam como Terceiras-Partes Confiáveis (TPC) tanto para o consumidor quanto para o provedor de serviços.

Conceitos e Modelos de Computação usados em Redes Colaborativas

Segundo [Camarinha-Matos 2005], a ampla adoção da arquitetura orientada a serviços, a difusão das redes colaborativas, a popularização dos conceitos Web 2.0 e Enterprise 2.0 e o sucesso das tecnologias associadas e estes conceitos tem impactado profundamente nas atividades colaborativas das organizações e no processo de desenvolvimento de software.

O termo **Web 2.0** foi criado em 2004 pela empresa *O'Reilly Media* para designar uma segunda geração de comunidades e serviços que tem como conceito a "*Web* como

[12]Baseado nas definições de federação encontradas na Federação *Incommon* (`http://www.incommonfederation.org/`), WS-Federation[WS-FEDERATION 2006] e [Rabelo 2008].

plataforma e o software com serviço"[13]. A Web 2.0 visa expandir radicalmente a idéia do acesso à informação através de um conjunto transparente de plataformas computacionais que permite uma fácil, rápida e inteligente forma de encontrar o que se deseja independentemente de onde, em que formato e com qual semântica a informação se encontra [Cancian 2009]. Segundo o precursor do uso do termo, Web 2.0 pode ser definida como:

> "[...] é a mudança para uma Internet como plataforma e um entendimento das regras para obter sucesso nesta nova plataforma. Entre outras, a regra mais importante é desenvolver aplicativos (serviços) que aproveitem os efeitos de rede para se tornarem melhores quanto mais são usados pelas pessoas, aproveitando a inteligência coletiva" [O'Reilly 2005].

Na Web 2.0, os *softwares* funcionam pela Internet (via Web), não somente instalados no computador local, de forma que vários programas podem se integrar formando uma grande plataforma. Exemplos de tecnologias e ferramentas Web 2.0 são: wikis, blogs, as redes sociais, *social bookmarks*, RSS e os serviços do Google, tais como GoogleDocs, GoogleMaps e Gmail. Na Web 2.0, os softwares funcionam como um serviço. Neste modelo de negócio o software, oferecido como um serviço (***Software as a Service*** - **SaaS**), está hospedado em um provedor de serviços e é acessado pelos usuários através da Internet (ver Figura 3.3), sem a necessidade que estes implantem ou mantenham uma infra-estrutura de TI para utilizá-lo [Cancian 2009]. O cliente possui direitos sobre seus dados e sobre o uso do software, mas em nenhum momento precisa adquirir uma licença ou comprar o software como se fosse um produto [Ma 2007]. O acordo comercial é estabelecido através de um contrato em de nível de serviço (SLA - *Service Level Agreement*), onde são definidas as condições, valores e responsabilidades entre clientes e provedores.

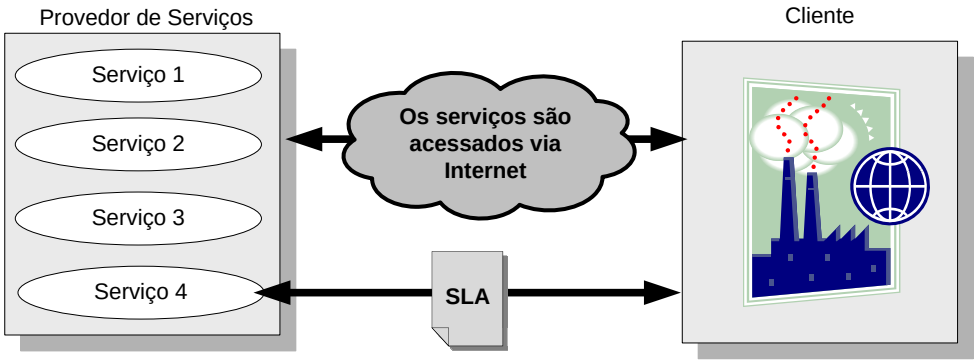

Figura 3.3. Exemplo do Modelo de Negócio *SaaS*[Cancian 2009]

Aprimorando a tecnologia ASP (*Application Service Provider*), que também oferece serviços via Internet, o modelo SaaS envolve também conceitos de arquitetura (funcionamento, desempenho, segurança) típicos de um serviço bem construído. Na tecnologia ASP, um servidor provê serviços de *software* baseados em contratos que envolvem a utilização, armazenamento e acesso a aplicações, através de um gerenciamento centralizado.

[13] Alguns críticos do termo, tais como Tim Berners-Lee, afirmam que este é apenas uma jogada de marketing (*buzzword*).

Enquanto no modelo SaaS o acesso é feito aos serviços, ou seja, pode-se selecionar o que será acessado de maneira desacoplada, no ASP o acesso é feito a toda aplicação.

Segundo [Mcafee 2006], o termo **Enterprise 2.0** refere-se a trazer para as empresas (organizações) as tecnologias e ferramentas da Web 2.0, possibilitando que parceiros colaborem e compartilhem informações, provendo a informação certa na hora certa através de redes de aplicação, de serviços e de dispositivos interconectados. Na Enterprise 2.0, o uso das emergentes plataformas de software social, torna acessível a inteligência coletiva transformando-a em uma enorme vantagem competitiva. Siemens e IBM são exemplos de empresas que implantaram em suas redes colaborativas o conceito Enterprise 2.0.

De acordo com [Armbrust et al. 2009], no contexto da Web 2.0 e Enterprise 2.0, há uma tendência de que os dados de usuários - inclusive os próprios sistemas operacionais – sejam disponibilizados em servidores remotos, tornando desnecessário o uso de dispositivos de armazenamento e possibilitando o compartilhamento de tal conteúdo com qualquer plataforma de acesso à *Web*. Este recente conceito de computação, chamado ***cloud computing***, tem o potencial para transformar uma grande parte da indústria de TI, tornando o software como um serviço ainda mais atraente e moldando a forma como o hardware é concebido e adquirido [Armbrust et al. 2009].

Cloud computing é um termo usado para descrever um ambiente de computação baseado em uma rede massiva de servidores, sejam virtuais ou físicos e refere-se à distribuição de aplicações como serviços (SaaS) através da Internet. Essa rede massiva de servidores (hospedada em datacenters) e a infra-estrutura de gerenciamento destes servidores constituem a nuvem (*cloud*) e os softwares (serviços) residem nesta nuvem [Armbrust et al. 2009]. Quando uma nuvem se torna disponível, um serviço é vendido como uma "utility computing". *Utility computing*[14] é modelo de provisionamento de serviços em que um prestador de serviços torna recursos de computação e gestão das infra-estruturas disponíveis para o cliente, conforme necessário, sem cobrar uma taxa fixa, mas sim o quanto foi consumido e utilizado [Buyya et al. 2008]. Segundo [Armbrust et al. 2009], *cloud computing* é a soma de SaaS com utility computing. Para [Hayes 2008], os conceitos *cloud computing*, *utility computing*, *software as a service*, *Internet as platform* (Web 2.0), tem um elemento em comum, a mudança na geografia da computação. Esta mudança irá afetar todo o ecossistema computacional, usuários, desenvolvedores de software, gerentes de TI e até mesmo a indústria de *hardware*.

Visto como uma plataforma essencial para distribuição de serviços, *cloud computing* oferece um ambiente que permite o compartilhamento de recursos, tais como o compartilhamento de infra-estruturas escaláveis, *middleware* e plataformas de desenvolvimento de aplicações e processos de negócios (aplicações de valor agregado).

Um dos principais objetivos da *cloud computing* é usufruir da Internet e da Intranet para compartilhar recursos para os seus usuários. Segundo [Zhang e Zhou 2009], tipicamente, quatro tipos de recursos podem ser providos e consumidos na Internet: recursos de infra-estrutura, que incluem poder computacional, capacidade de armazenamento (*storage*); recursos de *software*, incluindo recursos de *middleware* e plataformas de desenvol-

[14]Também conhecido como *on-demand computing*.

vimento de aplicações; recursos de aplicações (serviços ou *mashups*[15]), que são providos através do modelo de SaaS ou *mashups* de aplicações de valor agregado; e processos de negócios, que inclui os Serviços *Web* compostos e aplicações orientadas a negócios que possibilitem reuso, provisionamento e composição.

De acordo com [Zhang e Zhou 2009], a virtualização e a AOS são as duas tecnologias chaves para o sucesso da *cloud computing*. A virtualização é a tecnologia central que permite compartilhar recursos na nuvem, esta tecnologia trata como as imagens de sistemas operacionais, *middlewares* e aplicações são criadas e alocadas corretamente em máquinas ou em fatia de pilhas de servidores. As imagens poderão ser transferidas e colocadas no ambiente de produção sob demanda. Como AOS é apropriada para tratar a componentização, a reusabilidade e a flexibilidade de *softwares*, com intuito de conceber plataformas de *Cloud Computing* escaláveis, a AOS deve ser adotada para prover componentes reutilizáveis, interfaces padronizadas e soluções arquiteturais extensíveis. Segundo os autores, conceber plataformas de *cloud computing* simples (compartilhamento de um único tipo de recurso) é fácil, entretanto, construir uma arquitetura de *cloud computing* escalável e que suporte o compartilhamento dos quatros tipos de recursos ainda é uma tarefa desafiadora.

Exemplos de Redes Colaborativas Orientadas a Serviço

Conforme descrito [Rabelo et al. 2008], o projeto ECOLEAD desenvolveu um *middleware* para redes colaborativas de organização baseado no modelo de negócio SaaS. A infra-estrutura desenvolvida no projeto aplica a abordagem de AOS e a tecnologia de serviços web foi a escolhida para implementar a infra-estrutura proposta. Um conceito fundamental na infra-estrutura ECOLEAD é o de federação de serviços, sendo que todos os serviços relacionados com uma rede colaborativa são membros da federação . Logo, serviços podem ser encontrados, usados e compartilhados entre os parceiros da rede colaborativa. Os conceitos Web 2.0 e Enterprise 2.0 também foram adotados na concepção da infra-estrutura do projeto ECOLEAD uma vez que os serviços compartilhados pela Internet (via *web*) são fáceis de serem localizados, podem ser combinados em processos de negócios complexos, são acessados e contabilizados sob demanda (*utility computing*), proveem suporte a computação móvel e alguns serviços oferecidos são específicos para trabalhos colaborativos que contribuem para a inteligência coletiva [Rabelo 2008].

No contexto das Redes Nacionais de Pesquisa e Educação, pode-se citar como exemplo de infra-estrutura orientada a serviço para redes colaborativas o *middleware* para gerenciamento de acesso e identidade da rede colaborativa Internet2[16] que garante que somente pessoas autorizadas terão acessos aos serviços da rede. Neste *middleware*, o mesmo serviço de gerenciamento de identidade é usado para acessar todas as aplicações. Os principais projetos em desenvolvimento no contexto deste *middleware* são: o Shibbol-

[15]Um *mashup* é um novo gênero de aplicação *web* interativa ou *web site* que usa conteúdo de mais de uma fonte de dados externa para criar um novo serviço completo, pode ser considerada uma aplicação da Web 2.0 [Merrill 2006].

[16]`http://www.internet2.edu/middleware`

let[17], a ferramenta de gerenciamento de grupos Gouper[18] e a plataforma para trabalhos colaborativos COmanage[19]. Os membros da rede colaborativa da Internet2, já usufruem das funcionalidades deste *middleware* através da federação de serviços InCommon. A missão desta federação é criar e prover suporte a um *framework* comum para o gerenciamento confiável de acesso a recursos compartilhados para os parceiros da Internet2. Em abril de 2009, a comunidade desta federação era formada por mais de 3.6 milhões de usuários finais. Como a base do *middleware* Internet2 e da federação InCommon consistem em sistemas de gerenciamento de identidade federada, estes estão descritos em mais detalhes na seção que trata deste assunto (Seção 3.4.1).

3.2.4. Estudos de casos

Esta seção descreve dois cenários de uso fictícios de redes colaborativas. O primeiro consiste na seleção de parceiros para composição de uma organização virtual e outro envolve o provimento de serviços de acesso a bibliotecas digitais em redes nacionais de pesquisa e ensino. Aspectos de segurança nestes cenários serão analisados nas Seções 3.3 e 3.4.

Cenário 1: Rede Colaborativa TechPlast - Busca e Seleção de Parceiros

A rede colaborativa de organizações *TechPlast* é um cluster de pequenas e médias indústrias do setor de plásticos do Sul do Brasil que colaboram para aprimorar sua participação de mercado. Entre estas estão indústrias de embalagens plásticas, de peças plásticas injetadas, de máquinas injetoras de plástico, prestadoras de serviços e fornecedoras de matéria prima. Esta rede colaborativa foi criada como uma solução estratégica para atender ao mercado que demanda tempos de entrega curtos, preços baixos e produção acima da capacidade das micros e pequenas empresas da região. Na *TechPlast*, um ambiente para geração de Organizações Virtuais (OVs) propicia o estabelecimento de alianças temporárias e a condução de negócios colaborativos de forma mais eficiente, ágil, flexível e confiável. Este ambiente não é estático sendo que novas organizações podem entrar e outras podem deixar a rede. Cada OV criada atua como uma entidade de grande porte capaz de atender uma oportunidade negócio que não poderia ser atendida por somente uma das organizações. Cada membro da OV mantém sua independência e autonomia podendo inclusive fazer negócios fora da rede *TechPlast*.

A infra-estrutura para negócios colaborativos da *TechPlast* está baseada nos conceitos e tecnologias mais modernos da área de TI, tais como Enterprise 2.0, *SaaS*, Federação de Serviços e Serviços *Web* . Como as alianças nas OVs são voláteis e o fluxo de colaborações em alguns casos é definido dinamicamente de acordo com os requisitos do processo de negócios, a infra-estrutura oferece diferentes funcionalidades (modeladas como serviços) que podem ser selecionados sob demanda para cada tipo de negócio. Os participantes da rede *TechPlast* fazem parte da Federação de Serviços e podem tanto desenvolver e disponibilizar serviços (atuando como provedores de serviços), quanto usu-

[17] `http://shibboleth.internet2.edu`
[18] `http://grouper.internet2.edu/`
[19] `http://middleware.internet2.edu/co/`

fruir dos serviços básicos desenvolvidos para prover suporte as atividades chaves das fases do ciclo de vida de uma OV (consumidores de serviços), tais como: o serviço de busca e seleção de parceiros da OV, os serviços CSCW (*Computer Supported Cooperative Work*)[20], o motor de busca de conhecimentos, o motor de execução de processos de negócios (automáticos) e o serviço de gerenciamento de processo de negócio interativo (processos automáticos combinados com processos que requerem interação humana). No ambiente de geração de OVs da TechPlast, todas as organizações estão aptas a receber uma oportunidade de negócios (ON) e a organização que a recebe assume a função de Gerente da OV. O gerente da OV atua como broker independente e é este que inicia o processo de busca e seleção de parceiros, o que significa que diversas oportunidades de negócios podem estar sendo tratadas na rede e que um parceiro pode estar envolvido em diferentes ONs simultaneamente (ver Figura 3.4).

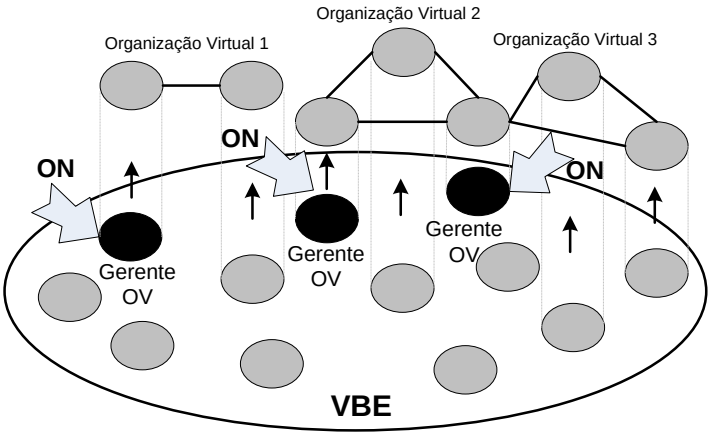

Figura 3.4. Formação de Organizações Virtuais na TechPlast

Com base na tecnologia de Serviços *Web*, o serviço *Universal Description, Discovery and Integration* (UDDI) [Clement et al. 2004] é utilizado para localizar parceiros potenciais para formação de uma OV. Cada organização publica no UDDI informações detalhadas sobre os serviços que esta provê, como funcionalidades, competências e áreas de negócio relacionadas com cada serviço (p.ex., fabricantes de peças plásticas injetadas, fabricantes de embalagens plásticas, fornecedoras de matéria prima, etc), possibilitando assim ao gerente da OV localizar quais organizações poderão vir a ser parceiros de negócios. O gerente da OV é responsável por gerar um conjunto de possíveis combinações de OVs, avaliar cada possibilidade de combinação e um representante humano da organização elege a combinação mais apropriada usando como critério, por exemplo, prazo de entrega mais curto, preço baixo e confiança nos parceiros (reputação).

Uma vez selecionados os parceiros da OV, é necessário o estabelecimento de relações de confiança entre os mesmos. Essas relações garantirão a autenticação dos parceiros, permitindo que o gerente da OV atribua os papéis que cada organização desempenhará.

[20]Por exemplo, videoconferência, telefonia IP, gerenciadores de projetos, *Wikis*, *Web syndication* e fóruns de discussão.

Cenário 2: Rede Colaborativa de Ensino e Pesquisa do Brasil (RNP) - Acesso a Serviços de Bibliotecas Digitais

A RNP é a rede nacional de ensino e pesquisa que congrega as principais instituições de ensino e pesquisa do Brasil e que mantém cooperação com redes nacionais de outros países. Esta rede colaborativa possui uma Federação de Serviços (CAFe) que reúne os provedores de identidades das instituições participantes da rede e provedores de serviços que são as próprias instituições e outras entidades parceiras tais como órgãos de fomento, editoras e empresas que oferecem descontos para estudantes e professores. Atualmente, 13 instituições são membros da federação e outras 7 estão em fase de preparação. Dentre os serviços que podem ser oferecidos na federação destacam-se: serviço de acesso às bibliotecas digitais das instituições, serviços de trabalhos colaborativos (telefonia IP, videoconferência), serviços de ensino a distância, serviço de acesso ao Portal Periódico da CAPES, serviço de monitoramento de rede, serviço de grids e serviço de hospedagem de equipamentos e servidores. Um cenário de uso desta rede colaborativa é exemplificado a seguir.

Cada membro da federação possui um provedor de identidade responsável por auxiliar o gerenciamento de identidades da instituição. Os membros da federação, através de provedores de serviços, podem oferecer serviços de acesso as suas bibliotecas digitais. Neste exemplo, a própria RNP pode ter um provedor de serviços que ofereça um Serviço *Web* para a busca avançada de artigos, monografias e teses em todas as bibliotecas digitais da federação, retornando assim o maior número de ocorrências possíveis. O serviço consiste basicamente de uma interface, a qual interage com o usuário, um motor de buscas avançado, responsável por realizar consultas em bases locais, remotas ou ainda invocando outros Serviços Web, e um visualizador de conteúdos.

3.3. Questões de segurança em redes colaborativas

A colaboração entre diferentes parceiros passa pela ativação de uma série de funcionalidades dessas organizações, isto é, envolve o atravessamento de várias camadas de segurança. Como os limites administrativos precisam ser transpassados, os processos de negócios estarão sob **diversos modelos administrativos** e também sob diversos mecanismos e tecnologias de segurança. Cada domínio transposto por um processo de negócio, pode prover seu próprio conjunto de credenciais de segurança, tomando como base suas tecnologias subjacentes de segurança e suas políticas de segurança e de negócios [de Mello et al. 2005].

Além dos Serviços Web desempenharem um papel importante para prover interoperabilidade na concepção de sistemas distribuídos, estes possuem uma série de mecanismos, definidos através de especificações padronizadas e abertas, que visam agregar segurança e confiabilidade às aplicações que os utilizam. Entretanto, as especificações atualmente existentes são insuficientes para atender aos requisitos de segurança de sistemas dinâmicos. Em particular, os aspectos mais ligados ao dinamismo das redes colaborativas – como autenticação e autorização através de diferentes domínios de segurança, a negociação de políticas de QoP e a incidência de *churn* – requerem a concepção de novos mecanismos para oferecer um nível mais adequado de proteção aos sistemas.

Em redes colaborativas, o uso de padrões para o formato e o transporte das mensagens, ou até mesmo para implementar mecanismos de segurança não garante interoperabilidade. Sempre que houver organizações autônomas envolvidas, estas podem impor diversas restrições adicionais que podem dificultar ou até mesmo impedir a comunicação. Em particular, tipicamente, cada organização de uma rede colaborativa possui autonomia para definir seus requisitos de segurança. Quais dados são considerados sensíveis, quais os tipos de credenciais que devem ser apresentados pelos parceiros, quais os algoritmos criptográficos que devem ser usados para quais informações, são algumas das variáveis que podem ser definidas pelas organizações.

No cenário descrito acima, fica claro que quando duas organizações precisam se comunicar, mesmo que usem uma tecnologia que permita interoperabilidade, como os Serviços Web, pode ser que a comunicação seja impedida porque os requisitos de segurança das organizações não são compatíveis. Por exemplo, uma organização pode considerar uma certa informação altamente sensível e exigir que as mensagens contendo essa informação sejam cifradas, enquanto a outra pode ter o suporte ao mesmo algoritmo criptográfico, ou nem sequer considerar a mesma informação sigilosa.

A situação pode ficar ainda mais complexa se não forem apenas duas organizações mas sim um conjunto de colaboradores provendo serviços para uma composição. Nessa situação, gerenciar a compatibilidade de requisitos de segurança se torna uma tarefa ainda mais difícil, principalmente quando se deseja um alto dinamismo na formação dessas composições de serviços [Böger et al. 2009].

O uso de políticas de qualidade de proteção (QoP) apresenta-se como solução para amenizar tais dificuldades. A definição de política de QoP empregada neste trabalho é a de um documento emitido por uma organização que expressa formalmente um conjunto de requisitos de segurança (confidencialidade, integridade e autenticidade) que deve ser satisfeito a fim de utilizar um dado serviço provido pela organização. Há outros tipos de políticas relacionadas a segurança, que no entanto não devem ser confundidas com QoP, como as políticas de autorização ou controle de acesso. Soluções para o problema da verificação de compatibilidade entre os requisitos de segurança dos parceiros que necessitam cooperar em uma rede colaborativa serão apresentadas em detalhes na Seção 3.4.3.

Um outro problema importante relacionado à verificação de compatibilidade de requisitos de segurança, e que também pode ser facilitado com o uso de políticas, é a aplicação dinâmica dos mecanismos de segurança. Enquanto no momento da formação da composição de serviços é preciso verificar se os colaboradores possuem suporte e permitem as mesmas tecnologias de proteção, durante a execução da composição é preciso garantir que em cada comunicação os parceiros apliquem os mecanismos de segurança corretamente, dependendo do serviço que for invocado, isto é, a configuração dinâmica da aplicação dos mecanismos de segurança.

Concretizar a autenticação e a autorização distribuída de forma transparente em sistemas complexos como as redes colaborativas é uma tarefa muito árdua, diretamente afetada pela escalabilidade. Em tais sistemas as entidades, sejam estas clientes ou provedores de serviços, se fazem presentes através de diferentes domínios administrativos e de segurança. Neste cenário, três barreiras a serem transpostas são: a heterogeneidade das infra-estruturas de segurança, presentes nos diversos domínios corporativos, o estabeleci-

mento de relações de confiança entre entidades desconhecidas e o gerenciamento de identidades feito tanto por provedores de serviços quanto por clientes [Camargo et al. 2007]. Para isto, são necessários tanto padrões altamente difundidos, com abstrações suficientes para esconder as diferentes tecnologias, quanto modelos que contribuam para integração de tais padrões.

Em sistemas distribuídos, 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 provedor) são alcançadas pela apresentação de credenciais emitidas por uma autoridade de autenticação em quem ambas as partes confiam. Em ambientes mais complexos como as redes colaborativas, este modelo de simples intermediação se apresenta como limitado, já que cada domínio possui suas próprias políticas, infra-estruturas de segurança e ainda uma forma particular de gerenciar as identidades dos principais [Jøsang et al. 2005]. Por exemplo, quando um membro de uma rede acadêmica de ensino e pesquisa deseja acessar, de forma segura, recursos presentes em provedores de serviços em diferentes universidades, este deve se filiar a cada um desses provedores e fornecer dados de identificação e atributos próprios por meio dos quais o cliente terá sua identidade autenticada ao tentar acessar os recursos.

Para evitar esses problemas, os provedores e clientes que usem a mesma tecnologia de segurança podem se agrupar em domínios (federações de serviços) para compartilhar informações e confiar em uma terceira parte para mediar a autenticação. Além disso, domínios distintos podem formar relações de confiança entre si, permitindo que a autenticação em um possa ser transposta para os domínios associados. Essa forma da autenticação segue a abordagem *Single Sign On* (SSO), contudo, 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, pois domínios administrativos possuem autonomia para decidir quais políticas e tecnologias de segurança serão utilizadas, ou seja, precisa haver suporte a autenticação SSO mesmo diante de parceiros que usem diferentes tecnologias de segurança [de Mello et al. 2009b].

Um problema a ser tratado no gerenciamento de identidades é a questão da privacidade das informações. Em um cenário ideal, os usuários poderiam exercer o direito de determinar como suas informações serão manipuladas, informando quais informações poderão ser compartilhadas com terceiros, como esse compartilhamento deve ser feito e também indicando o período de tempo o qual essas informações poderão ficar disponíveis nos sistemas. O projeto Shibboleth [Shibboleth 2005] apresenta uma preocupação com a privacidade das informações dos usuários, definindo como requisitos da arquitetura, meios para gerenciar quais informações um sítio origem irá transferir para um sítio destino, com o consentimento do usuário. Com o crescimento do uso de Serviços Web, a questão da privacidade ganha um foco ainda maior, visto que um fluxo de negócios pode ser composto por diversos Serviços Web, ultrapassando assim diversos domínios administrativos e de segurança. Por exemplo, para fazer parte de uma organização virtual, uma organização precisa satisfazer a requisitos especificados, como ter uma certa capacidade de produção disponível ou ser capaz de atender a determinados prazos ou orçamento. Em casos como este, surge naturalmente uma preocupação com a privacidade dos atributos usados na busca e seleção de parceiros de uma OV, particularmente quando existem infor-

mações sensíveis cuja revelação pode prejudicar a organização face a seus concorrentes ou colaboradores. Nesse contexto, torna-se importante oferecer mecanismos que possibilitem a uma organização tomar parte no processo de busca e seleção de parceiros sem com isso comprometer sua posição perante os demais. A especificação *Web Services Architecture* da W3C [W3C 2004a] apresenta algumas considerações sobre a privacidade na arquitetura dos Serviços Web, indicando que tal assunto ainda não está completamente solucionado e necessita de um estudo mais aprofundado.

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 um processo de negócio. Em uma aplicação distribuída o termo confiança pode assumir diferentes interpretações. Em segurança o mais usual é como garantir que as informações foram enviadas por uma origem confiável, ou seja, a preocupação recai sobre as propriedades de autenticidade e integridade das mensagens. Porém, a confiança pode ser entendida como a probabilidade subjetiva que um indivíduo "A" espera que um indivíduo "B" execute uma dada ação na qual depende o bem-estar de "A" [Gambetta 1988, Sabater e Sierra 2005].

A confiança possui papel fundamental tanto na fase de criação quanto nas fases de operação e manutenção das redes colaborativas. A dinâmica intrínseca das Organizações Virtuais torna a seleção de parceiros uma tarefa difícil do ponto de vista da segurança. Além da necessidade de combinar políticas e adequação dos mecanismos de segurança, é necessário garantir que somente entidades confiáveis deverão ser selecionadas para compor a OV. Para o gerente de uma OV, selecionar entidades com as quais este interagiu anteriormente não chega a ser uma tarefa complexa, porém selecionar uma entidade com quem este nunca interagiu e determinar se esta é confiável ao ponto de incluí-la em uma OV é uma decisão difícil de ser tomada. Por este motivo, sistemas de reputações geralmente são combinados com modelos de redes de confiança permitindo assim, por exemplo, que um gerente possa consultar em entidades confiáveis a reputação de uma determinada entidade.

Em algumas redes colaborativas, assume-se que o estabelecimento de confiança é um processo manual que exige o cumprimento de diversos requisitos burocráticos antes da criação da relação de confiança. Por exemplo, para que uma Universidade seja um Provedor de Identidade em uma federação de serviços de um rede de ensino e pesquisa, como a InCommon, é necessário que a entidade cumpra um conjunto de requisitos, sendo alguns destes relacionados à necessidade de certificados digitais emitidos pela Autoridade Certificadora da Federação. Outros trabalhos tratam a confiança de uma maneira mais dinâmica e volátil. Por exemplo, em OV para executar um determinado processo de negócios é necessário que diversos provedores de serviços se agrupem e, uma vez que o processo tenha sido cumprido, tal relação é desfeita.

A manutenção de uma rede colaborativa está relacionada à evolução da composição do sistema. Estas redes possuem diferentes níveis de dinamismo sendo algumas formadas por entidades que entram e saem da rede com uma grande frequência e outras que mantêm suas entidades quase que inalteradas. O grande desafio nestes ambientes é manter o progresso das aplicações mesmo diante do *churn*, o que requer mecanismos que permitam detectar a saída ou a falha de membros, com conseqüente redistribuição de

tarefas no sistema e eventual renegociação de parâmetros de segurança. Como visto na seção 3.2, as redes colaborativas são geralmente constituídas para atender uma determinada necessidade de negócio e, no caso das Organizações Virtuais (OV), são desfeitas tão logo esta necessidade tenha sido satisfeita. Por outro lado, redes de pesquisa e educação, como a Internet2 e a RNP, constituem redes colaborativas com relações mais duradoras e com poucas modificações em sua lista de participantes.

Durante o ciclo de vida das redes colaborativas é importante garantir que todos os participantes, e somente estes, possam usufruir dos recursos ali presentes. Os modelos discricionários garantem o acesso de usuários às informações com base na identidade e nas autorizações que determinam a forma de acesso que cada usuário está autorizado a realizar sobre cada objeto [Sandhu e Samarati 1994]. Em redes acadêmicas tal modelo poderia ser empregado sem grandes transtornos uma vez que a lista de participantes sofre poucas modificações.

Segundo [Blaze et al. 1996], apesar do modelo discricionário ser amplamente adotado, não é o mais adequado para os atuais sistemas computacionais devido a dinâmica inerente destes sistemas, com a lista de sujeitos e de recursos em constante modificação, como no caso das Organizações Virtuais. Por exemplo, uma entidade pode ingressar em diversas OV em intervalos de tempo diferentes ou de forma concorrente. Desta forma, uma entidade precisa garantir aos demais participantes o acesso aos seus recursos, de acordo com a política de negócio, enquanto durar a OV.

Um membro de uma organização virtual, além de autenticar os serviços parceiros, costuma, com base nas credenciais apresentadas, definir regras de acesso para limitar as ações desses parceiros. Ou seja, uma **política de autorização local** pode ser definida e concretizada em cada serviço/organização. Segundo [Lorch et al. 2003a], a maioria das organizações utiliza linguagens de políticas proprietárias ou que se direcionam somente a algumas aplicações, causando assim problemas de **interoperabilidade** para produzir, aceitar e interpretar a informação de autorização proveniente de diferentes organizações. Ou seja, modelos fortemente dependentes de um padrão de descrição de política (casamento sintático de políticas) não podem ser aplicados nestes ambientes heterogêneos [Patterson e Miller 2006]. A Figura 3.5 exemplifica um problema de casamento de políticas de autorização onde se tem declarações equivalentes mas a comparação entre elas (casamento) só é possível se houver o conhecimento do domínio da aplicação (semântica) pois uma comparação puramente sintática irá negar o acesso ao recurso [Patterson e Miller 2006]. Tal problema é facilmente encontrado no cenário de redes colaborativas pois envolvem ambientes heterogêneos e de domínios administrativos, logo semânticos, distintos. Para que possam colaborar, os serviços precisam entrar em um acordo quanto aos protocolos, sintaxes e semânticas de autorização.

No contexto de OV´s (Organizações Virtuais), podem-se considerar três macro problemas ligados a autorização e controle de acesso: um relacionado com a definição e casamento semântico de políticas de controle de acesso, a composição e transposição de políticas em serviços compostos e a qualidade de proteção da política global nestes ambientes colaborativos.

Entre as soluções mais citadas na literatura estão aquelas baseadas em mapeamento semântico das políticas de segurança usando ontologias, [Patterson et al. 2008],

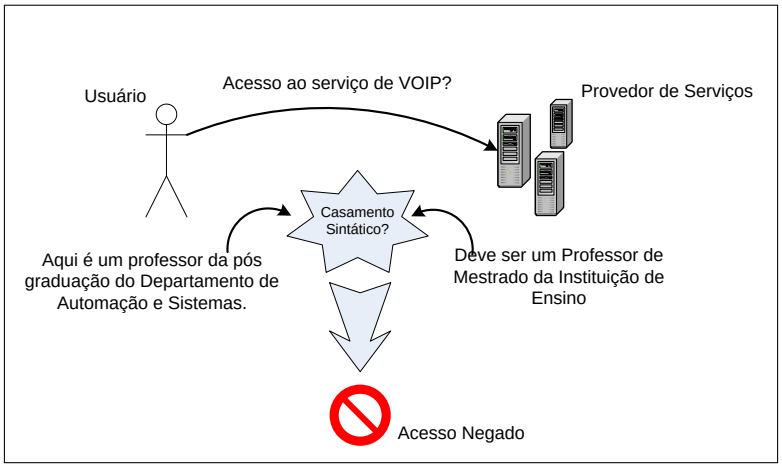

Figura 3.5. *Exemplo de um problema de casamento sintático de política de autorização*

[Patterson e Miller 2006] [Muthaiyah e Kerschberg 2007] ou de um *framework* baseado em UCON (*Usage Control*) para uma solução que provê suporte a autenticação baseada em contexto em redes colaborativas *ad-hoc* [Zhang et al. 2006, Zhang et al. 2008]. Estas soluções são descritas na Seção 3.4.5.

Outros requisitos de segurança trazem a qualidade de proteção necessária para um ambiente de negócios. São estes: a autenticidade, a confidencialidade, a integridade e a não-repudiação das transações entre os serviços parceiros [Charfi e Mezini 2005]. As partes envolvidas necessitam de suporte apropriado para garantir esta qualidade de proteção. Tradicionalmente, o *Secure Sockets Layer* (SSL), o *Transport Layer Security* (TLS) e o *Internet Protocol Security* (IPSec) são algumas das tecnologias que permitem o transporte seguro de informações. Estas são tecnologias ponto a ponto que criam um canal seguro, através do quais os dados podem trafegar. No entanto, em processos de negócios, o roteamento entre múltiplos Serviços *Web* é essencial, uma vez que uma mensagem, para atingir o destinatário final, passa por diversos nós intermediários que devem ter acesso apenas a partes específicas das mensagens. Ou seja, a **segurança fim a fim** é outra necessidade de segurança crítica para redes colaborativas.

Segundo [Demchenko et al. 2005], apesar da adoção do padrão XML ter sido apontado como uma vantagem para o sucesso dos Serviços *Web*, este traz alguns riscos à segurança. A análise das mensagens XML com entradas volumosas e complexas pode requerer um consumo de recursos computacionais consideráveis, e por isso esta característica pode ser explorada por ataques de negação de serviço. Além disso, documentos XML podem conter instruções maliciosas[21] que podem alterar o processo de análise do XML ou conter comandos maliciosos que carregam ameaças às aplicações finais.

Na composição de Serviços Web, os processos de negócios executados das redes colaborativas tornam-se ainda mais visíveis, expondo suas funcionalidades, seus fluxos de negócios, processos, políticas e arquiteturas internas. Como a WSDL exibe os parâmetros e métodos utilizados para acessar os Serviços Web, bem como as possíveis exceções que podem ocorrer, estas, muitas vezes, expõem informações importantes sobre a estrutura

[21] Extensões *XML Schema* e instruções *XQuery* ou *XPath* maliciosas.

interna dos serviços, trazendo riscos à segurança dos Serviços Web compostos. Mecanismos de segurança estão sendo propostos para Serviços Web, porém, tais mecanismos ainda não contemplam todas as necessidades exigidas na composição de Serviços Web [Charfi e Mezini 2005, Carminati et al. 2005].

Os cenários apresentados na Seção 3.2.4 compartilham algumas das questões de segurança apresentadas nesta seção. No caso 1, após encontrar os possíveis parceiros que contemplam os requisitos para a determinada oportunidade de negócio, resta selecionar aqueles que possuam boa reputação, podendo estar diretamente relacionada a honestidade dos parceiros ou relacionada a capacidade destes em realizar a tarefa com uma certa qualidade. Uma vez que a confiança esteja estabelecida resta ainda decidir sobre os mecanismos e políticas de segurança, presentes em cada um dos parceiros. Mecanismos para gerenciamento de identidades são necessários para permitir que os mecanismos de autenticação e autorização dos participantes de uma OV possam lidar com a dinâmica inerente deste ambiente.

No caso 2, apresentado na Seção 3.2.4, as relações entre os participantes desta rede colaborativa são mais duradouras e geralmente estão envolvidas entidades renomadas e publicamente respeitadas. Dessa forma, o estabelecimento da confiança não chega a ser um grande desafio, podendo este ser realizado de forma estática e em momento que antecede o ingresso da entidade na rede colaborativa. Contudo, neste caso ainda é necessário modelos para gerenciamento de identidade e de atributos. A autenticação única (*Single Sign-On*) é algo bastante desejável e isto implica em adaptações dos mecanismos de autorização e até casamento de políticas de segurança.

Esta seção apresentou os principais desafios de segurança presentes nas redes colaborativas, entre estes, destacam-se: a autenticação SSO em federações de serviços, a preservação da privacidade na busca e seleção de parceiros, o estabelecimento dinâmico de relações de confiança entre os membros da rede e provedores de serviços. O casamento de políticas de qualidade de proteção diante de domínios administrativos heterogêneos, a garantia da segurança das informações que trafegam entre os membros da rede e autorização distribuída e flexível são também pontos importantes nos desafios de segurança nestes ambientes.

3.4. Soluções de Segurança para Redes Colaborativas

Esta seção tem por objetivo apresentar uma síntese do estado da arte relativo à segurança em redes colaborativas orientadas a serviços. As soluções analisadas estão divididas nas seguintes subseções: gerenciamento de identidade (Seção 3.4.1), gerenciamento de confiança (Seção 3.4.2), gerenciamento de políticas de qualidade de proteção (Seção 3.4.3), provisionamento de canais seguros (Seção 3.4.4) e autorização e modelos de controle de acesso (Seção 3.4.5).

3.4.1. Gerenciamento de Identidade

O *gerenciamento de identidades*[22] consiste de um sistema integrado de políticas, processos de negócios e tecnologias que permite às organizações proverem recursos de forma

[22]Uma identidade digital consiste na representação de uma entidade em um domínio específico e geralmente está relacionada a domínios do mundo real.

segura, somente aos seus usuários. O gerenciamento de identidade 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 e em [Jøsang e Pope 2005, Jøsang et al. 2005] é apresentada uma breve descrição de alguns modelos.

O ***modelo tradicional*** de gerenciamento trata a identificação de forma isolada, sendo que o provedor de serviços também atua como o provedor de identidades e de credenciais (senhas associadas com os identificadores). Neste modelo, os usuários possuem identificadores únicos e específicos para cada serviço com o qual interajam. E como consequência diferentes credenciais são associadas com cada identificador.

Com o crescimento da oferta de serviços, o gerenciamento de identidades digitais, por parte dos usuários e organizações, tornou-se uma tarefa árdua. Cada sistema exige um conjunto próprio de informações para que se possa criar uma identidade digital. Para os usuários é muito custoso alimentar bases de dados de diferentes serviços, repetindo sempre as mesmas informações, entretanto a principal dificuldade é gerenciar o identificador e a senha escolhidos para cada sistema.

O modelo de ***gerenciamento de identidades federadas*** surgiu para suprir as necessidades apresentadas pelo modelo de gerenciamento tradicional. Neste tipo de ambiente, é definido o conceito de domínio, nos quais estão presentes os provedores de serviço, de identidades e de credenciais, por exemplo, relacionados a uma determinada empresa. O projeto *Liberty Alliance* [Liberty 2003a] e o projeto *Shibolleth* [Shibboleth 2005] são implementações abertas de modelos de gerenciamento de identidade federada.

No ambiente de identidades federadas, são estabelecidos acordos entre os domínios, os quais permitem que identidades locais a um domínio sejam reconhecidas nos demais domínios participantes do acordo. A federação de domínios de identificação dá a impressão aos usuários de possuírem um identificador único para todos os domínios que compõem a federação. Os usuários poderão continuar a manter identificadores locais a cada serviço ou mesmo domínio, porém o simples fato de possuírem tal identificador permite que estes usuários possam acessar serviços presentes em qualquer domínio da federação.

No ***modelo centralizado*** de gerenciamento, considera-se a existência de um único provedor de identidades e de credenciais em uma federação, o qual é utilizado por todos os provedores de serviços da mesma. Neste modelo um usuário pode acessar todos os serviços presentes na federação utilizando um mesmo identificador. Em tese, o modelo se assemelha ao modelo de identidade federada, porém com a diferença de não necessitar do mapeamento de identificadores. A *WS-Federation* [WS-FEDERATION 2006] é um exemplo deste tipo de modelo. A WS-Federation especifica o provedor de identidade que tem o objetivo de autenticar os usuários, permitindo que estes usufruam desta autenticação em todos os serviço da federação.

Em redes de ensino e pesquisa que possuem federação de serviços, como por exemplo no cenário descrito na Seção 3.2.4, a facilidade de uma única autenticação (*Single Sign-On - SSO*), permite ao cliente (membro de um domínio da federação) efetuar o

processo de autenticação uma única vez, seja em provedores de serviços ou de identidades ou em uma entidade autenticadora centralizada, e usufruir deste processo de autenticação nos demais serviços disponíveis na rede.

Juntamente com a facilidade trazida pela autenticação única tem-se novos desafios. Do ponto de vista da segurança dos usuários deste sistema, a autenticação única permite, por exemplo, que provedores de serviços entrem em comum acordo para rastrear as atividades de um determinado usuário, ferindo assim sua privacidade. Já para os provedores de serviços, os novos desafios apresentados estão voltados para a gerência das relações de negócio entre os provedores parceiros, visto que cada sistema participante do negócio possui suas próprias políticas de negócio, de segurança e administrativas. Por exemplo, como garantir que os controles de autenticação e de acesso aplicados em um domínio serão equivalentes aos controles aplicados em um outro domínio?

[Damiani et al. 2003] apresenta um estudo sobre os problemas inerentes ao gerenciamento de múltiplas identidades, descrevendo os requisitos necessários que um sistema de gerenciamento de identidades deve atender. Dentre os requisitos apresentados, alguns estão diretamente preocupados com as necessidades de segurança dos clientes [W3C 2002, Rannenberg 2000], tais como a privacidade, o anonimato, a responsabilidade, a interoperabilidade das identidades, etc.

Projeto Shibboleth

O projeto Shibboleth[23] é uma proposta conjunta da Internet2 e IBM que investiga arquiteturas, estruturas e tecnologias para permitir o compartilhamento e controle de acesso inter-institucional de serviços disponíveis através da Internet, tendo como cenário de uso o ambiente acadêmico[Carmody 2001]. O projeto visa a troca de informações, de forma segura e interoperável, entre sítios web, permitindo que usuários de um determinado campus possam usufruir de recursos presentes em outros campi, garantindo ainda a privacidade dos usuários. O Shibboleth requer que cada sítio possua um mecanismo para autenticar seus usuários e usando como suporte tecnologias de segurança subjacentes que já estejam em uso pelas instituições[24].

O Shibboleth visa ser uma solução completa para permitir a transposição de domínios administrativos e de segurança, usufruindo do conceito de uma única autenticação (SSO) e das relações de confiança. Visando ser uma solução prática e não somente um modelo conceitual, a arquitetura do Shibboleth é construída sobre padrões que já possuem seu uso consolidado, como HTTP, XML, esquema XML, XMLDSign [Bartel et al. 2002], SOAP e SAML (*Security Assertion Markup Language*). A arquitetura estende o mecanismo para troca de atributos e o SSO do SAML[OASIS 2005b], especificando um provedor de serviços SSO e provendo melhorias para a privacidade dos usuários.

De acordo com a especificação [Shibboleth 2005], a implementação de um sítio é composta por três principais componentes: provedor de identidade - formalmente chamado de "origem", responsável pela manutenção das credenciais e atributos dos usuários;

[23] http://shibbolet.internet2.edu

[24] Sendo o ideal o uso de certificados de ICPs, tanto pelos clientes quanto pelos sítios

provedor de serviço - formalmente chamado de "destino", gerencia os recursos protegidos, sabendo que os usuários poderão acessar os recursos através da apresentação de asserções emitidas por um provedor de identidade; o *Where Are You From*? (WAYF) é um serviço opcional que pode ser usado pelo provedor de serviço para determinar o provedor de identidade preferencial do usuário, interagindo ou não com o usuário para obter tal informação. O WAYF geralmente faz parte do próprio provedor de serviço.

Projeto Liberty Alliance

O projeto *Liberty Alliance* consiste em um conjunto de especificações produzidas por um consórcio de empresas atuantes nas mais diferentes áreas, como em telecomunicações, transportes, universidades, bancos, empresas de *software*, etc. Tem como principal objetivo criar especificações abertas para tratar o gerenciamento de identidades, usufruindo do conceito de *federação de identidades*. Os principais objetivos do projeto são [Liberty 2003a]: (1) prover um padrão aberto para permitir uma única autenticação (SSO), o que inclui a autenticação descentralizada e a autorização em múltiplos provedores de serviços; (2) garantir a privacidade e a segurança das informações pessoais dos usuários; e, (3)prover especificações, compatíveis com uma grande variedade de dispositivos.

Esses objetivos podem ser alcançados quando provedores de serviços e clientes agrupam-se baseados em acordos comerciais e nas tecnologias propostas pela *Liberty*, formando assim os *círculos de confiança*. Tais círculos consistem na federação de provedores de serviços e serviços de identidade, juntamente com os clientes.

No contexto deste projeto, visando garantir a segurança e a privacidade dos clientes, em [Liberty 2003b], um guia de "boas práticas" para provedores de serviços é apresentado, frisando que cada empresa ainda deverá estar de acordo com a jurisdição a qual está submetida. Neste guia é descrito que os serviços deverão informar, de forma clara, aos usuários quem está coletando suas informações pessoais, quais informações estão sendo coletadas e de que forma estão sendo coletadas. Os serviços deverão acatar as escolhas do usuário, com relação a privacidade de suas informações pessoais. O usuário deve ter o direito de escolher quais atributos um provedor de serviços terá acesso, bem como os meios para indicar o tempo de vida das informações fornecidas.

Identificadores opacos ou pseudônimos foram propostos nas especificações da *Liberty* com o intuito de garantir a privacidade dos usuários dos serviços. Para cada provedor de serviços, o provedor de identidade poderá atribuir diferentes pseudônimos relacionados a um mesmo usuário. Dessa forma, o mesmo usuário pode ser representado por diferentes pseudônimos para cada serviço que este acessa, garantindo assim a proteção contra o rastreamento de suas transações.

Transposição de Credenciais de Autenticação

Conforme visto anteriormente, as abordagens que proveem suporte a autenticação *Single Sign On* (SSO) 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 infra-estruturas de segurança.

Em [de Mello et al. 2009b], é descrito um modelo com suporte a autenticação SSO, isto é a transposição de credenciais de autenticação, mesmo diante de domínios administrativos com diferentes tecnologias de segurança. Neste modelo, um principal[25] 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 [de Mello et al. 2009b]. 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. Essa credencial pode ser expressa em um formato neutro e flexível, como o SAML, a fim de facilitar tradução. Ao receber a requisição juntamente com a credencial do cliente, o serviço pode invocar um **Serviço de Tradução de Credenciais** (STC) presente no seu domínio para que este traduza a credencial do cliente para o formato suportado pelo serviço. De posse da credencial na tecnologia do seu próprio domínio, o serviço pode decidir se permite ou não o acesso do cliente [de Mello et al. 2009b].

O STC deve possuir conhecimento de diversos formatos de credenciais de autenticação e das regras para a tradução entre os diversos formatos. Concentrar esses requisitos no STC visa permitir aos serviços dos provedores pertencentes ao domínio operar apenas com a tecnologia que for mais conveniente.

Os serviços de atributos desempenham um papel importante na transposição de credenciais, pois para realizar a tradução de uma credencial para o formato suportado no domínio do provedor, pode ser necessário obter outras informações requeridas pela credencial. Esses atributos podem ser requisitados pelo STC a um serviço de atributos no domínio do cliente para que os campos da credencial possam ser preenchidos. Os serviços de atributos devem ser capazes de gerenciar pseudônimos que são usados pelos clientes para aumentar a sua privacidade e dificultar o rastreamento por parte dos provedores de serviços [de Mello et al. 2009b].

Há outras abordagens para a transposição de credenciais de autenticação entre diferentes domínios como o Serviço de Conversão de Credenciais [Canovas et al. 2004, Lopez et al. 2005], que converte credenciais de diferentes formatos para SAML, o CredEx [Vecchio et al. 2005], que fornece armazenamento e troca dinâmica de credenciais de diversos tipos mas sem realizar a tradução, os projetos ShibGrid [Spence et al. 2006] e SHEBANGS [Jones e Pickles 2007], que provêem autenticação baseada em Shibboleth, usando SAML, para uma infra-estrutura de *grids* que usa certificados X.509. Há ainda outros trabalhos de transposição de credenciais, mas que não lidam com heterogeneidade [Winslett et al. 2002, Lorch et al. 2003b].

3.4.2. Gerenciamento de Confiança

Em sistemas distribuídos a confiança assume papel fundamental nas interações entre as diversas partes que compõem o sistema. O estabelecimento da confiança nessas aplica-

[25] Usuários, processos ou máquinas autorizados pelas políticas do sistema.

ções pode ser simples quando a aplicação só abrange um único domínio administrativo, ou seja, quando todas as partes do sistema estão dentro dos limites de uma única instituição. Porém, para casos em que a aplicação atravesse diversos domínios o estabelecimento da confiança entre tais partes torna-se um desafio [de Mello 2009].

O estabelecimento da confiança pode se dar de forma estática ou dinâmica. No estabelecimento estático, a confiança entre as partes se dá em um momento prévio à execução da aplicação e geralmente consiste em uma interação direta entre os administradores de cada parte. As redes acadêmicas de pesquisa em sua maioria seguem este tipo de abordagem. Por outro lado, o estabelecimento dinâmico da confiança ocorre durante a execução da aplicação, sendo este caso o mais comum em Organizações Virtuais.

Para ambos os casos, estabelecimento estático ou dinâmico, a principal dificuldade se faz quando uma das partes envolvidas não possui qualquer informação sobre a outra. Assim, o estabelecimento da confiança estaria sendo realizado sem qualquer tipo de respaldo ou garantia, o que poderia desencorajar as partes em estabelecer uma relação de confiança e por consequência, deixariam de atender oportunidades de negócio. Na literatura, as soluções apresentadas para tal problema geralmente combinam modelos de confiança à sistemas de reputações, que através de provedores de opiniões permitem às partes verificar se a reputação da outra é boa o suficiente para que possam estabelecer uma relação de confiança.

Em [Sabater e Sierra 2005] é dito que modelos de confiança e reputação podem ser caracterizados como cognitivos ou baseados na teoria dos jogos. Os modelos cognitivos baseiam-se nas noções humanas sobre confiança, risco e reconhecimento para assim obter um grau de confiança sobre uma certa entidade. Os modelos baseados na teoria dos jogos consideram a confiança e a reputação como probabilidades subjetivas. Em ambos os modelos é previsto que as informações de confiança colhidas por uma parte possam ser divulgadas para outras partes interessadas, criando assim uma rede de informações para expressar noções de confiança.

Em [Gray et al. 2003] é apresentada uma arquitetura de segurança que faz uso dos conceitos do *mundo pequeno*[26] [Milgram 1967] e tem por objetivo otimizar a formação e a propagação da confiança. A arquitetura apresentada por [Gray et al. 2003] tem como foco aplicações colaborativas em redes móveis *ad hoc* e baseia-se nas noções humanas sobre confiança, risco e conhecimento. Uma entidade p_0 só irá interagir com uma entidade p_m se o grau de confiança calculado por p_0 sobre p_m for suficiente para superar o risco envolvido em interagir com p_m. O cálculo da confiança, de uma entidade p_0 sobre uma entidade p_m é apresentado pela equação 1:

$$Tp_0(p_m) = \frac{\sum_{k=1}^{m} (Tp_{k-1}(p_k))w_k}{m} \quad (1)$$

sendo $Tp_0(p_m)$ o valor de confiança que p_0 irá formar sobre um p_m qualquer. p_m é uma entidade que está m saltos distante de p_0, ou seja, entre p_0 e p_m existem $m-1$

[26]Cada entidade em um sistema de larga escala pode estar separada de qualquer outra entidade por somente algumas entidades intermediárias.

entidades intermediárias. k é a $k-esima$ entidade intermediária entre p_0 e p_m e w_k é o peso associado a distância entre p_0 e p_k, e quanto menor for o valor de k maior será a influência do peso w_k.

Dessa forma, o valor final da confiança calculado por p_0 sobre p_m é constituído pela soma de valores parciais, sendo que os valores obtidos de entidades mais próximas a p_0 terão maior influência no cálculo da confiança. Para o caso de existirem múltiplos caminhos de confiança ligando p_0 ao p_m, é assumido que p_0 sempre irá escolher o caminho mais confiável para assim obter o valor de confiança para p_m mais legítimo.

O conceito de mundo pequeno fora observado em diversos sistemas computacionais, como em redes par a par para compartilhamento de arquivos [Capkun et al. 2002] e em redes de confiança do *Pretty Good Privacy* (PGP) [Penning 2006]. No modelo proposto por [Gray et al. 2003], a rede de confiança aliada ao sistema de reputações visa o estabelecimento de novas relações de confiança entre partes que nunca interagiram previamente. Na fase de criação de uma Organização Virtual, o gerente da OV poderá se deparar com parceiros de negócio que estão aptos a atender uma oportunidade de negócio, mas ainda não possui um valor de confiança formado sobre tal parceiro. A proposta de [Gray et al. 2003] poderia ser empregada nesse caso.

Um problema inerente aos sistemas de reputações está na filtragem das opiniões recebidas. Ao assumir que os provedores de opiniões são corretos e nunca irão prover opiniões diferentes daquilo que de fato observaram, ainda assim é possível que diferentes provedores apresentem diferentes opiniões, que apesar de não serem maliciosas são inconsistentes, gerando dúvida para a parte que as requisitou.

Em [Wang e Vassileva 2003] é apresentado um modelo de confiança, aliado a um sistema de reputações, baseado em redes bayesianas, tendo como aplicação exemplo uma rede par a par para o compartilhamento de arquivos. Cada par na rede pode assumir dois papéis, o primeiro destinado ao provimento de arquivos, denominado *provedor* e o segundo destinado ao provimento de opiniões, denominado *agente*. A proposta de [Wang e Vassileva 2003] apresenta uma solução para situações em que diferentes agentes possuem diferentes opiniões sobre um mesmo par. Os autores assumem que todos os agentes sempre irão emitir pareceres verdadeiros sobre a reputação de outros pares, ou seja, os agentes nunca irão assumir um comportamento malicioso. Neste caso, diferentes agentes apenas possuem diferentes critérios para classificar outros pares.

A rede bayesiana serve de apoio para que um par, ao pesquisar por arquivos, possa escolher os melhores provedores, ou seja, provedores que anteriormente se mostraram capazes em prover arquivos e por consequência possuem uma maior probabilidade de continuar provendo arquivos de forma satisfatória. Para os casos em que um agente não possua qualquer experiência anterior com um provedor é proposto um sistema de reputação onde os agentes passam a atuar como *provedores de recomendações*. Assim, um agente ao ser consultado sobre a competência de um determinado provedor de arquivos, este irá verificar em sua rede bayesiana se existe alguma opinião formada a respeito e irá responder com o valor ali presente.

Para formar uma opinião sobre um determinado provedor de arquivos, um agente pode questionar diversos outros agentes e como consequência irá receber diversas respos-

tas, as quais podem ser oriundas de agentes confiáveis, não confiáveis e até de agentes desconhecidos, ou seja, agentes com quem este não teve qualquer interação prévia. As recomendações oriundas de agentes não confiáveis são imediatamente descartadas. As recomendações oriundas de agentes confiáveis e de agentes desconhecidos são combinadas de acordo com a equação 2:

$$r_{ij} = w_t * \frac{\sum_{l=1}^{k} tr_{il} * t_{lj}}{\sum_{l=1}^{k} tr_{il}} + w_s * \frac{\sum_{z=1}^{g} t_{zj}}{g}, w_t + w_s = 1 \quad (2)$$

sendo r_{ij} o total de recomendações que o *i-ésimo* agente obteve sobre o *j-ésimo* provedor de arquivos. k é o número de recomendações de agentes confiáveis e g é o número de recomendações de desconhecidos. tr_{il} é o grau de confiança que o *i-ésimo* agente possui sobre o *l-ésimo* agente confiável. t_{lj} é o grau de confiança que o *l-ésimo* agente confiável possui sobre o *j-ésimo* provedor de arquivos. t_{zj} é o grau de confiança que o *z-ésimo* agente desconhecido possui sobre o *j-ésimo* provedor de arquivos. w_t e w_s são pesos definidos por cada agente para determinar a importância das recomendações feitas por agentes confiáveis e por agentes desconhecidos, respectivamente.

Após ser calculado o grau de confiança para um determinado provedor de arquivos, é verificado se este valor é suficiente para interagir com este provedor, sendo cada agente o responsável por definir o valor mínimo necessário para isto. Após cada interação, o agente irá atualizar sua rede bayesiana para o provedor de arquivos em questão e também irá atualizar sua confiança nos agentes que proveram as recomendações através da técnica de aprendizado por reforço [Sutton e Barto 1998], de acordo com a equação 3:

$$tr_{ij}^{n} = \alpha * tr_{ij}^{o} + (1 - \alpha) * e_{\alpha} \quad (3)$$

sendo tr_{ij}^{n} o novo grau de confiança que o *i-ésimo* agente irá possuir sobre o *j-ésimo* provedor de opiniões após a atualização. tr_{ij}^{o} representa o grau de confiança anterior. α é a taxa de aprendizado, um número real no intervalo de $[0,1]$. e_{α} é o valor da nova evidência, o qual pode ser -1 ou 1. Se o valor recomendado for maior que o necessário para iniciar a interação com o provedor de arquivo e se a interação ocorrer de forma satisfatória, então e_{α} é igual a 1 e caso a interação ocorra de forma insatisfatória, e_{α} é igual a -1.

A equação 3 garante aos agentes que forneceram recomendações verdadeiras um aumento em seu grau de confiança e aqueles que apresentaram recomendações falsas serão punidos gradativamente até atingir um limiar para serem considerados como não confiáveis. O modelo de [Wang e Vassileva 2003] poderia ser empregado na fase de criação de uma Organização Virtual (OV) e assim evitar a inclusão de entidades que não honraram alguma interação no passado em alguma outra Organização Virtual. Durante a execução de uma OV, o modelo poderia ser empregado para aumentar ou diminuir o grau de confiança sobre as entidades participantes, garantindo assim uma visão sempre atualizada o que facilitaria o processo de criação de OV subsequentes.

Os trabalhos [Gray et al. 2003, Wang e Vassileva 2003, Sabater e Sierra 2001] fazem uso de médias ponderadas para calcular a probabilidade de uma entidade honrar a negociação. Para cada provedor de opiniões é atribuído um peso, diferenciando assim a influência de cada opinião no cálculo do valor da confiança sobre uma determinada entidade. Nos trabalhos [Buchegger e Boudec 2003, Whitby et al. 2005, Teacy et al. 2006, de Mello et al. 2009a], a probabilidade é calculada através de métodos estatísticos os quais fazem uso das interações passadas para prever como será o comportamento futuro, tanto dos provedores de opiniões quanto da entidade para qual se deseja formar um valor de confiança. Tais trabalhos fazem uso da análise bayesiana e assim para determinar a probabilidade (*a posteriori*) é necessário conhecer a probabilidade *a priori*, podendo esta ser obtida através de uma *função densidade de probabilidade* de uma *distribuição beta*[27][de Mello et al. 2009a], veja equação 4.

$$f(p) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1}, \text{ sendo } \alpha,\beta > 0 \tag{4}$$

$$\Gamma(x) = \int_0^\infty e^{-t}t^{x-1}dt \tag{5}$$

sendo $\Gamma(x)$ a função Gama de Euler que estende a noção de fatorial para valores não inteiros.

Todos trabalhos usam de maneira semelhante a *distribuição beta* para determinar a probabilidade de uma entidade vir a honrar a interação. Os parâmetros α e β são usados como probabilidade *a priori* e registram o total de interações que resultaram em sucesso e em insucesso, respectivamente. Sistemas de reputações tornam-se mais precisos a partir do momento que suas bases possuam um grande número de registros. Em seu início, quando não existem registros nas bases, tem-se uma distribuição uniforme, ou seja, a probabilidade de qualquer interação ocorrer com sucesso ou insucesso é exatamente igual.

Os trabalhos de [Whitby et al. 2005] e [Teacy et al. 2006] diferem entre si na forma como tratam a detecção de opiniões não confiáveis. Em [Whitby et al. 2005] as opiniões de provedores que se desviarem da maioria são descartadas. Em [Teacy et al. 2006] é comparado o histórico de opiniões fornecidas por um provedor com o que de fato foi observado nas interações diretas com a entidade sobre quem este provedor opiniou. Se o provedor de opiniões fornecer de forma continuada opiniões semelhantes, então assume-se que o provedor é preciso, caso contrário, assume-se que este é impreciso e suas opiniões são descartadas.

O modelo apresentado em [de Mello et al. 2009a] também faz uso da média ponderada, porém os pesos são obtidos através de métodos estatísticos, com base nas experiências observadas pela entidade que está solicitando as opiniões. Neste modelo, como em [Teacy et al. 2006] as opiniões recebidas consideram o histórico do provedor de opiniões, permitindo assim que as opiniões dos bons provedores prevaleçam sobre as opiniões de provedores maliciosos.

[27]Determinada pelos parâmetros α e β, é usada para representar variáveis aleatórias limitadas a um intervalo, por exemplo, entre 0 e 1 [Jain 1991].

Determinar o grau de confiança sobre uma entidade consiste também em observar em qual contexto tal entidade está inserida. A delimitação do contexto serve para expressar a confiança com uma maior precisão, haja visto que uma entidade pode atuar em diferentes contextos e para cada um desses a mesma pode assumir diferentes comportamentos. Em [de Mello et al. 2009a] cada entidade possui uma base de experiências diretas que contém os históricos das interações que realizou com as demais entidades. Para cada entidade presente nesta base, são registradas as experiências separadas por contexto. Essa separação permite determinar em quais contextos a entidade, para a qual se está calculando a confiança, se mostrou mais correta e no caso de não houver ainda qualquer experiência em um determinado contexto, a combinação de todas as experiências, não importando o contexto, pode ajudar a prever o comportamento para o contexto desejado. As interações seguintes, dentro do contexto desejado, iriam então aprimorar esta visão inicial da confiança.

A separação por contextos de confiança pode ajudar um gerente de uma Organização Virtual a verificar quais parceiros atenderiam melhor uma oportunidade de negócio. O grau de confiança deixaria de estar relacionado a honestidade de uma entidade e passaria agora estar relacionado a capacidade daquela entidade realizar uma negociação de forma satisfatória. Assim, as entidades candidatas a parceiro de negócio, além de atuarem no contexto como parceiro de negócio em uma OV, poderiam também atuar no contexto de provedoras de opiniões.

O uso de um modelo de confiança aliado a um sistema de reputação, atende as necessidades relacionadas as fases de criação e execução, por exemplo, de uma Organização Virtual. O sistema de reputação pode ser usado para classificar o grau de competência dos possíveis parceiros de negócio além de permitir classificar o quão precisos são no provimento de opiniões, pois as entidades que já atuaram como parceiros de negócio poderiam agora ser também provedores de opiniões, formando assim as redes de confiança.

Com os sistemas de reputação, é possível calcular a probabilidade de uma dada entidade honrar uma futura negociação, porém não é possível ter certeza que essa negociação ocorrerá com sucesso. O estabelecimento dinâmico de redes colaborativas exigem meios para garantir que nenhuma entidade participante obtenha benefícios em detrimento das demais partes. Em [Asokan et al. 2000], é apresentado um protocolo para troca de assinaturas digitais, de forma justa, sobre um conteúdo eletrônico (definido como *contrato*), sendo que nenhuma parte será prejudicada caso a transação não possa ser terminada com sucesso.

O protocolo garante que sempre uma parte poderá forçar o término de uma transação, de forma justa e com base em um limite temporal, sem que necessite da cooperação da outra parte e mesmo em uma rede assíncrona. A solução tradicional para este problema sempre envolve uma Terceira Parte Confiável (TPC). Cada parte envia seu item (p.e. assinatura sobre o contrato) para a TPC e esta só efetuará a troca dos itens assim que receber os itens de todas as partes envolvidas. O fato de acionar a TCP em todas as transações torna a solução ineficiente. Em [Asokan et al. 2000] é apresentada uma versão otimista do protocolo em que a TPC só é acionada em casos onde uma parte tenha um comportamento indesejado, proposital ou não.

A combinação de modelos de confiança e mecanismos parecidos com o protocolo

proposto por [Asokan et al. 2000] permitem assim o estabelecimento dinâmico da confiança para a concepção de redes colaborativas, além de prover ferramentas para melhorar o funcionamento de uma rede que já esteja na fase de execução.

3.4.3. Gerenciamento de Políticas de Qualidade de Proteção

As políticas de qualidade de proteção (QoP) são expressões formais, processáveis por computador, declaradas por organizações e anexadas aos seus serviços, que indicam quais mecanismos de segurança a organização suporta ou requer para acessar os serviços [Böger et al. 2009]. Essas políticas devem ser aplicada às mensagens trocadas com serviço para garantir que os requisitos de segurança da organização serão respeitados.

Tratando-se de uma política de QoP, os requisitos de segurança podem ser indicações de quais informações são sigilosas e precisam ser cifradas, quais informações devem ser assinadas, os algoritmos criptográficos suportados ou requeridos, os mecanismos e os tipos de credenciais de autenticação suportados ou requeridos, ou outros requisitos de segurança necessários para que a comunicação possa ocorrer de forma segura de acordo com as necessidades da organização.

Se as organizações desejam se comunicar dinamicamente de forma segura, estas podem declarar políticas de QoP e publicar essas políticas juntamente com a descrição dos serviços providos. Colaboradores que desejarem invocar o serviço poderão então avaliar a possibilidade de cumprir a política anexada. Essa verificação pode ser feita automaticamente se o colaborador que deseja invocar o serviço possui seus requisitos ou capacidades também especificados em uma política. As duas políticas, uma anexada pelo provedor de serviço e outra definida pelo cliente podem ser comparadas automaticamente para verificar se há acordo entre os requisitos [Böger et al. 2009].

Em situações mais complexas, como em um processo de negócio, ou durante a criação de uma OV, onde pode haver várias organizações envolvidas, as políticas de QoP são ainda mais importantes. Com essas políticas, é possível automatizar a verificação da compatibilidade dos requisitos de segurança de todas as comunicações, desde que todas as organizações declararem seus requisitos em políticas expressas em uma linguagem padrão e que uma descrição formal do processo de negócio esteja disponível e indique quais as invocações de serviços serão realizadas.

Para os serviços *Web*, a linguagem padrão para expressar políticas é a *WS-Policy* [WS-POLICY 2007]. A *WS-Policy* é uma linguagem altamente extensível que permite expressar diversos tipos de requisitos não funcionais de serviços *Web*, como segurança, confiabilidade e otimização nas trocas de mensagens. A seguir, tem-se a descrição desta linguagem e do padrão *WS-SecurityPolicy*. Na seqüência, alguns aspectos de gerenciamento de políticas *WS-Policy* são apresentados e, por fim, um estudo de caso é descrito.

WS-Policy

WS-Policy é um padrão W3C que "define um *framework* e um modelo para expressar políticas que se referem a capacidades, requisitos e características gerais de entidades em um sistema baseado em serviços *Web*" [WS-POLICY 2007]. É um padrão de ampla

aceitação e presente na maioria das ferramentas para desenvolvimento de soluções em Serviços *Web*.

Uma política expressa em *WS-Policy* é formada por um conjunto de alternativas de política, sendo que cada alternativa é formada por um conjunto de asserções de política. Cada asserção de política representa um requisito, uma capacidade ou outra propriedade de um comportamento específico de um domínio, como segurança [WS-POLICY 2007]. A *WS-Policy* define apenas o modelo geral das políticas, mas não define nenhuma asserção. As asserções são especificadas em outros padrões, como o *WS-SecurityPolicy* que define asserções de segurança.

Uma política que não contém nenhuma alternativa não pode ser satisfeita (chamaremos de política nula). Uma política que contém uma ou mais alternativas é satisfeita se exatamente uma dessas alternativas é satisfeita. Uma alternativa de política que não contém nenhuma asserção não indica nenhuma característica comportamental e é satisfeita trivialmente. Uma alternativa com uma ou mais asserções é satisfeita somente se todas as asserções são satisfeitas. A satisfação de uma asserção resulta em um comportamento que reflete a restrição indicada, que é específica do domínio.

A Figura 3.6 apresenta um exemplo simples de política em *WS-Policy*. A política contém duas alternativas, cada uma representada por um elemento `<wsp:All>` (linhas 5 a 7 e 8 a 10), contidas em um elemento `<wsp:ExactlyOne>` (linhas 4 a 11) que representa a escolha. As asserções representadas pelos elementos `<sp:Basic256Rsa15>` (linha 6) e `<sp:TripleDesRsa15>` (linha 9) são especificadas na *WS-SecurityPolicy* e representam, cada uma, um conjunto diferente de algoritmos criptográficos. Normalmente, essas asserções não são usadas sozinhas como no exemplo da Figura 3.6, mas em conjunto com outras asserções de segurança, como será explicado na próxima seção.

```
1  <wsp:Policy
2     xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy
          /200702"
3     xmlns:wsp=" http://www.w3.org/ns/ws-policy" >
4    <wsp:ExactlyOne>
5      <wsp:All>
6        <sp:Basic256Rsa15 />
7      </wsp:All>
8      <wsp:All>
9        <sp:TripleDesRsa15 />
10     </wsp:All>
11   </wsp:ExactlyOne>
12 </wsp:Policy>
```

Figura 3.6. Exemplo de política *WS-Policy*

A política da Figura 3.6 está na forma normal, definida na *WS-Policy*, em que as alternativas estão indicadas explicitamente na política. No entanto a linguagem permite construções mais complexas, como aninhamento de operadores, asserções marcadas como opcionais e referências de políticas, que permitem uma representação mais intuitiva e compacta da política. Toda política possui uma forma normal equivalente e a *WS-Policy*

apresenta um procedimento para realizar a transformação para tal forma.

Além de uma forma para expressar políticas, o padrão *WS-Policy* também define algumas operações sobre políticas, a normalização de política, a união de políticas e a intersecção de políticas, que permitem manipular políticas de forma consistente e independente das asserções e dos domínios utilizados.

A operação de normalização de políticas transforma uma política em uma outra na forma normal equivalente, que é um formato mais simples para a manipulação automática por computador. Notavelmente, a operação de intersecção é bastante simples de explicar em termos de alternativas de políticas e uma implementação básica poderá fazer uso da normalização para simplificar o processamento.

A união de políticas junta duas políticas em uma outra que representa a combinação das alternativas das duas. Em termos de alternativas, a política resultante da união conterá alternativas que são formadas pela concatenação de uma alternativa de uma política com uma alternativa da outra. Satisfazer a união é equivalente a satisfazer exatamente uma alternativa de cada uma das políticas unidas.

A operação de intersecção é a que permite a verificação de compatibilidade entre políticas [WS-POLICY 2007]. Assim como na união, a intersecção é formada pela concatenação de alternativas das políticas, no entanto a alternativa resultante da concatenação só é adicionada ao resultado se as duas alternativas forem compatíveis. Duas alternativas são consideradas compatíveis se e somente se cada asserção de uma alternativa for compatível com pelo menos uma asserção da outra. A compatibilidade de asserções é apenas parcialmente definida no padrão *WS-Policy*, de forma que as especificações podem estender o algoritmo de compatibilidade com informações específicas de domínio. A base do algoritmo de intersecção de asserções é comparar os nomes dos elementos XML que representam as asserções e verificar a compatibilidade das políticas aninhadas nessas asserções, se houver.

O resultado da intersecção de duas políticas conterá as alternativas compatíveis de ambas, ou nenhuma alternativa se as políticas forem incompatíveis. É essa característica que permite verificar se duas políticas declaradas por dois parceiros que desejam se comunicar são compatíveis, isto é, se um parceiro suporta os requisitos do outro. Além disso, o resultado da intersecção ainda indica quais as alternativas que foram satisfeitas e permite aos parceiros aplicar os mecanismos corretos no momento de se comunicar.

O padrão *WS-Policy* define três mecanismos de anexação de política, conforme ilustrados na Figura 3.7. Os dois primeiros mecanismos, mostrados respecivamente nos elementos das linhas 1 a 3 e 5 a 10, anexam políticas a um elemento XML qualquer simplesmente pela adição de um atributo `wsp:PolicyURIs`, no primeiro caso, ou de subelementos `<wsp:PolicyReference>`, no segundo caso. No terceiro tipo de anexo, ilustrado nas linhas 12 a 23 da Figura, o alvo da anexação está indicado no elemento `<wsp:AppliesTo>`, que é seguido pela indicação de quais políticas estão sendo anexadas e por um elemento opcional `<wsse:Security>`, que é definido na especificação *WS-Security* [WS-SECURITY 2006] e serve para prover características de segurança ao anexo de política, com uso assinaturas digitais e credenciais (*tokens*).

As políticas são geralmente anexadas aos elementos da descrição WSDL do ser-

```
1  <MyElement wsp:PolicyURIs="
2     http://example.com/policies/rm-policy
3     http://example.com/policies/X509-endpoint-policy" />
4
5  <MyElement>
6    <wsp:PolicyReference
7       URI="http://example.com/policies/rm-policy" />
8    <wsp:PolicyReference
9       URI="http://example.com/policies/X509-endpoint-policy" />
10 <MyElement/>
11
12 <wsp:PolicyAttachment>
13   <wsp:AppliesTo>
14     <wsp:URI>
15       http://example.com/services/srv.wsdl#wsdl.endpoint(srv/endp)
16     </wsp:URI>
17   </wsp:AppliesTo>
18   <wsp:PolicyReference
19      URI="http://example.com/policies/rm-policy" />
20   <wsp:PolicyReference
21      URI="http://example.com/policies/X509-endpoint-policy" />
22   <wsse:Security>...</wsse:Security>
23 </wsp:PolicyAttachment>
```

Figura 3.7. Exemplo de anexação de política *WS-Policy*

viço, como `<wsdl:operation>`. Nesse caso, a política é aplicada a todas as mensagens trocadas com o serviço relacionadas com a invocação dessa operação. O mesmo vale para os elementos `<wsdl:service>`, `<wsdl:endpoint>`, `<wsdl:binding>`, `<wsdl:interface>`, `<wsdl:operation>`, `<wsdl:input>`, `<wsdl:output>`, `<wsdl:fault>`, `<wsdl:infault>` e `<wsdl:outfault>` e a política aplicada a uma mensagem é a união de todas as políticas anexadas aos elementos com os quais a mensagem está relacionada.

WS-SecurityPolicy

O *WS-SecurityPolicy* [WS-SECURITYPOLICY 2007] define um conjunto de asserções, para serem usadas em políticas *WS-Policy*, que indicam a capacidade ou o requerimento da aplicação dos padrões de segurança para serviços *Web* (*WS-Security*, *WS-Trust* e *WS-SecureConversation*) às mensagens trocadas com um serviço. São essas asserções, em conjunto com a linguagem *WS-Policy*, que definem o formato padrão para expressar políticas de qualidade de proteção para Serviços *Web*.

Por questão de espaço e objetividade, não será possível abordar todas as asserções definidas na *WS-SecurityPolicy*. Ao invés, um exemplo simples de política de QoP expressa em *WS-Policy* e *WS-SecurityPolicy* está apresentado na Figura 3.8 e explicado a seguir.

As asserções `SignedParts` e `EncryptedParts` (linhas 2 e 3) indicam que

```
<wsp:Policy xmlns:wsp="..." xmlns:sp="...">
 <sp:SignedParts><sp:Body /></sp:SignedParts>
 <sp:EncryptedParts><sp:Body /></sp:EncryptedParts>
 <sp:AsymmetricBinding>
  <wsp:Policy>
   <sp:InitiatorToken>
    <wsp:Policy>
     <wsp:ExactlyOne>
      <sp:SamlToken
       sp:IncludeToken=".../IncludeToken/Always">
       <sp:IssuerName>saml-authority</sp:IssuerName>
      </sp:SamlToken>
      <sp:X509Token
       sp:IncludeToken=".../IncludeToken/Always">
       <sp:IssuerName>x509-ca</sp:IssuerName>
      </sp:X509Token>
     </wsp:ExactlyOne>
    </wsp:Policy>
   </sp:InitiatorToken>
   <sp:RecipientToken>
    <wsp:Policy>
     <wsp:ExactlyOne>
      <sp:SamlToken
       sp:IncludeToken=".../IncludeToken/Always">
       <sp:IssuerName>other-saml-authority</sp:IssuerName>
      </sp:SamlToken>
      <sp:X509Token
       sp:IncludeToken=".../IncludeToken/Always">
       <sp:IssuerName>other-x509-ca</sp:IssuerName>
      </sp:X509Token>
     </wsp:ExactlyOne>
    </wsp:Policy>
   </sp:RecipientToken>
   <sp:AlgorithmSuite>
    <wsp:Policy>
     <wsp:ExactlyOne>
      <sp:Basic256 />
      <sp:Basic192 />
     </wsp:ExactlyOne>
    </wsp:Policy>
   </sp:AlgorithmSuite>
   <sp:ProtectTokens />
   <sp:Layout><wsp:Policy><sp:Strict /></wsp:Policy></sp:Layout>
  </wsp:Policy>
 </sp:AsymmetricBinding>
</wsp:Policy>
```

Figura 3.8. Exemplo de política de QoP expressa em *WS-Policy* e *WS-SecurityPolicy*

o corpo das mensagens deve ser cifrado e assinado. A asserção `AsymmetricBinding` indica que criptografia assimétrica será usada, sendo que as credenciais do emissor e receptor (`InitiatorToken`, nas linhas 6 a 19, e `RecipientToken`, nas linhas 20 a 33) da mensagem podem ser ou uma asserção SAML emitida pela autoridade de nome *saml-authority* (asserções `SamlToken`, nas linhas 9 a 12 e 23 a 26) ou um certificado X.509 emitido pela CA *x509-ca* (asserções X509Token, nas linhas 13 a 16 e 27 a 30). Os algoritmos criptográficos aceitos são indicados dentro da asserção `AlgorithmSuite` (linhas 34 a 41) e, nesse exemplo, dois conjuntos de algoritmos são suportados, *Basic256* (asserção `Basic256`, na linha 37) e *Basic192* (asserção `Basic192`, na linha 38).

A política nesse exemplo não está na forma normal, no entanto é fácil perceber que esta contém oito alternativas formadas com as possíveis combinações das opções de credencial do emissor, credencial do receptor e conjunto de algoritmos criptográficos. Um cliente que deseje se comunicar com um serviço que use essa política deve satisfazer apenas uma dessas alternativas.

Há muitas outras asserções definidas na *WS-SecurityPolicy*. Há outras formas de declarar quais partes das mensagens devem ser protegidas, outras asserções de *token*, outros conjuntos de algoritmos criptográficos, há asserções para usar criptografia simétrica ou usar HTTPS, asserções que exigem ou permitem o uso de credenciais adicionais na mensagem, e ainda outras. O melhor documento para obter informações detalhadas sobre essas asserções é a própria especificação *WS-SecurityPolicy*.

Aspectos de Gerenciamento

Além de definir os requisitos de segurança dos serviços providos na forma de políticas, para alcançar todo o dinamismo proposto pelas AOSs, as organizações precisam fazer com que essas políticas estejam acessíveis aos potenciais parceiros. Além disso, os colaboradores que obtiverem as políticas devem ser capazes de avaliar a autenticidade e a integridade dessas políticas.

Nos serviços *Web*, há diversas formas de disponibilizar as políticas *WS-Policy* de um serviço. A mais simples delas é adicionar as políticas diretamente como elementos de extensão na WSDL do serviço e, com isso, aproveitar os mecanismos de descoberta existentes para WSDL, como os serviços de registro UDDI. Em algumas situações, no entanto, outros mecanismos podem ser mais interessantes. Por exemplo, se a política de um serviço deve ser atualizada com certo dinamismo, talvez os registros não ofereçam a agilidade necessária. Nesse caso, algum dos mecanismos definido na especificação *WS-MetadataExchange* [WS-METADATAEXCHANGE 2009] pode ser usado, como a operação *GetMetadata*, para obter a última versão da política.

Na *WS-Policy*, mecanismos para prover características de segurança podem ser adicionados aos anexos de política no elemento `<wsse:Security>` conforme apresentado anteriormente. Esse elemento poderá conter assinaturas digitais e credenciais de segurança a fim de garantir a autenticidade e a integridade tanto das políticas, que podem estar incluídas diretamente no anexo, quanto do próprio anexo. Se a operação *GetMetadata* for implementada, a *WS-Security* pode ser usada para assinar o conteúdo da mensagem com as políticas.

Estudo de caso

Para ilustrar as possibilidades das políticas de QoP abordadas anteriormente, nessa seção será apresentado um exemplo de ciclo de vida de uma organização virtual no contexto da rede *TechPlast* definida na Seção 3.2.4.

Para fins de exemplo, suponhamos que uma empresa participante da rede *TechPlast*, a *Plasmax*, que produz peças plásticas de uso doméstico, recebe uma encomenda de peças acima da sua capacidade usual, de forma que não conseguirá atender ao pedido sozinha. Está situação configura, então, uma oportunidade de negócio (ON) e, neste caso, a *Plasmax* será o gerente da OV que se formará. De acordo com a ON, a empresa *Plasmax* organiza um *workflow* para cumprir a demanda da seguinte forma: a empresa *Plasmax* produzirá as peças do pedido segundo a sua capacidade máxima, e para tal deverá realizar compras de matéria-prima adicional; o restante do pedido será repassado a uma outra empresa que produza a mesma categoria de objetos plásticos e que suporte o mesmo formato de peça.

Depois de definir o *workflow* para a lógica de negócio, a *Plasmax* iniciará o processo de busca e seleção de parceiros. Nessa etapa serão escolhidos os parceiros que participarão da OV e os serviços que serão invocados no processo de negócio para atender a ON. Nessa etapa, além dos requisitos funcionais, das relações de confiança e outros fatores relacionados ao negócio, a seleção deve levar em conta também os requisitos de segurança das empresas a serem selecionadas. Por exemplo, a empresa *Plasmax* considera a informação de seus pedidos de matéria-prima altamente sigilosa, pois um espião de outra empresa poderia usar essa informação para tentar descobrir fórmulas químicas de substâncias usadas nos seus produtos. Dessa forma, a *Plasmax* só fará pedidos de matérias-primas por meio de serviços providos por fornecedores se esses serviços suportarem a encriptação das mensagens de pedido.

Supondo que cada empresa da *TechPlast* possui seus anexos de políticas de QoP disponibilizados no UDDI da *TechPlast*, o serviços de busca e seleção provido na rede colaborativa, no momento da avaliação de compatibilidade de um determinado serviço, obterá as políticas *WS-Policy* dos parceiros, verificará a autenticidade e integridade das mesmas, analisará o *workflow* para saber quais operações dos serviços serão invocadas e comparará, por meio da intersecção, as políticas *WS-Policy* dos serviços envolvidos. Se não houver compatibilidade o serviço é descartado e um outro parceiro é buscado. Se houver compatibilidade dos requisitos de segurança, a política resultante da intersecção é associada à troca de mensagem representada na descrição do *workflow*.

Se foi possível encontrar serviços adequados, o serviço de busca e seleção devolverá para a *Plasmax* a descrição do *workflow* juntamente com a lista dos serviços selecionados e com as políticas resultantes das intersecções realizadas. Com essas informações, a *Plasmax* pode configurar um motor de orquestração que implementará o *workflow* invocando os serviços selecionados anteriormente e aplicará, para cada troca de mensagem, a política comum aos serviços descoberta na etapa de busca e seleção. Além das políticas de QoP, para configurar corretamente o motor de orquestração é preciso que sejam definidos ainda vários parâmetros, como a localização das chaves criptográficas, os nomes de usuário, as senhas, etc..

A partir da configuração realizada, é possível executar o *workflow* e efetivar a oportunidade de negócio. Cada parceiro selecionado para a OV, receberá as requisições da *Plasmax* e desempenhará seu papel no *workflow*. Por fim, a OV pode ser desfeita, se não houver mais pedidos semelhantes.

3.4.4. Provisionamento de Canais Seguros

Nas redes colaborativas, a comunicação entre os integrantes do sistema deve garantir a confidencialidade, a integridade e a autenticidade das informações transmitidas, de acordo com a política de qualidade de proteção estabelecida. Em alguns sistemas surgem também requisitos de privacidade ou anonimato [Pfitzmann e Hansen 2007], que incluem a preservação da identidade de pares de nós comunicantes, a não vinculação de mensagens específicas aos seus nós de origem ou destino ou ainda a ocultação da identidade da real origem de uma requisição ou do nó que efetivamente atende a tal requisição.

A arquitetura dos Serviços *Web* está diretamente ligada ao XML e às extensões de segurança deste padrão definidas pela W3C, tais como as recomendações ***XML-Signature*** [Bartel et al. 2002] e ***XML-Encryption***[Imamura et al. 2002]. Estas recomendações permitem expressar assinaturas digitais e cifragem de dados em formato XML, sendo que os dados assinados e/ou cifrados podem ser ou não documentos XML. Estes mecanismos tornam possível a segurança fim-a-fim para os processos de negócios que usam o XML para troca e armazenamento de dados, garantindo assim: (1) a proteção da integridade com granularidade fina; (2) a autenticação da origem dos dados e, (3) a confidencialidade de campos específicos.

Padronizada pela OASIS, a especificação ***WS-Security*** [OASIS 2004] define aprimoramentos para garantir integridade, confidencialidade e autenticidades das mensagens SOAP, ou seja, garantir a segurança fim-a-fim no nível de mensagem e não somente no nível de transporte. Este padrão visa ser flexível, sendo possível utilizar uma grande variedade de mecanismos de segurança e tecnologias, como por exemplo Infra-estruturas de Chave Pública (ICP), Kerberos ou SSL. Mais especificamente, esta tecnologia provê suporte para diferentes tipos de credenciais de segurança (*security tokens*), possibilitando que um cliente utilize múltiplos formatos de credenciais para a autenticação e autorização, múltiplos formatos para assinatura e múltiplas tecnologias de cifragem de dados. Estas características são muito importantes para alcançar a interoperabilidade entre tecnologias de segurança de diferentes domínios administrativos. As especificações *XML Signature* e *XML Encryption* são utilizadas pela *WS-Security* para conseguir expressar assinaturas e cifragem no formato XML. O foco principal da WS-Security é promover trocas de mensagens SOAP seguras. Características como estabelecimento de relações de confiança, mecanismos de autenticação e troca de políticas de segurança não fazem parte do escopo desta especificação.

A especificação [W3C 2004a] apresenta algumas considerações sobre a privacidade na arquitetura dos Serviços *Web*, indicando que tal assunto ainda não está completamente solucionado e necessita de um estudo mais aprofundando. A *Platform for Privacy Preferences* (P3P) [W3C 2002] é um projeto do W3C que permite que os sítios *web* expressem suas políticas de privacidade de forma padronizada utilizando XML, dando aos usuários o conhecimento sobre como seus dados pessoais serão tratados. Se-

gundo [Hung et al. 2004], o uso do P3P não pode ser diretamente aplicado no contexto dos Serviços *Web*, visto que o P3P foi projetado para que usuários de sítios *web* possam ter controle sobre suas informações pessoais. Outro problema é que os vocabulários da P3P estão direcionados principalmente para descrever as práticas de privacidade dos sítios *web*, sobre quais dados irão coletar dos usuários e o que irão fazer com essas informações

O anonimato é uma propriedade que está diretamente relacionada com a privacidade, porém com significado distinto. O acesso anônimo de um usuário a um sistema indica que o usuário não será identificado, garantindo assim a privacidade de sua identidade real [de Mello et al. 2006]. Em [Cattaneo et al. 2004] é apresentada uma extensão ao SOAP para permitir o acesso anônimo aos Serviços *Web*. A solução está baseada no fato de que os usuários só precisam provar, para um provedor de serviços, que pertencem a um determinado grupo, autorizado pelas políticas do sistema, evitando assim revelar sua identidade pessoal. A especificação WS-Federation segue uma abordagem semelhante para o anonimato onde clientes podem usar pseudônimos para acessar serviços, seja dentro da mesma federação, seja entre federações com relação de confiança [WS-FEDERATION 2006].

Em [Papastergiou et al. 2008] é tratado o anonimato com os Serviços *Web*. Nesse trabalho, o anonimato é garantido pelo uso conjunto de uma rede Tor[28] com técnicas de atraso propositado e reordenação de mensagens para dificultar rastreamentos baseados em temporização.

3.4.5. Autorização e modelos de controle de acesso

Conforme analisado na Seção 3.3, nas redes colaborativas, a heterogeneidade das organizações e a distribuição dos recursos em domínios administrativos distintos, fazem surgir problemas relacionados a definição e gerenciamento de políticas globais de controle de acesso. Logo, as soluções clássicas de controle de acesso não atendem as necessidades dessas redes pois não são flexíveis o suficiente e nem se adequam, em termos de granularidade de definição de regras às necessidades que envolvem domínios semânticos distintos [Zhang et al. 2008].

Os participantes das redes colaborativas já possuem políticas de controle de acesso fortemente dependentes do domínio de aplicação e definições inerentes ao domínio administrativo, como a semântica da política definida. Ou seja, nestas redes, as políticas de controle de acesso não podem ser verificadas considerando somente o significado sintático uma vez que a identificação dos usuários e dos recursos podem ser diferentes por conta da heterogeneidade e a não existência de um acordo prévio entre os parceiros (feito de forma dinâmica) [Rao e Sadeh 2005].

As soluções de controle de acesso adequadas às redes colaborativas exigem que durante a composição dos serviços se tenha uma etapa de mediação, onde são feitas: a identificação das políticas, seleção dos serviços e o acesso e casamento de políticas baseado no contexto da aplicação (semântica). Além disso, a própria transposição de credenciais através dos domínios distintos (ver Seção 3.4.1) pode introduz problemas nestas redes. Algumas credenciais encapsulam a identificação/papel do usuário bem como os

[28] http://www.torproject.org/

recursos que este pretende acessar, logo a falta de padrão na representação destas identificações já não permite um casamento puramente sintático. Soluções de controle de acesso no contexto de redes colaborativas devem, então, tratar os problemas relacionados a representação, transposição e casamento de políticas de controle de acesso.

As soluções de segurança encontradas na literatura para tratar estes problemas podem ser classificadas em duas abordagens. Na primeira abordagem, as soluções adotam uma padronização prévia das políticas de controle de acesso (bases de autorização, usuários, níveis, recursos e hierarquias) e o desenvolvimento de um *framework* com base no modelo UCON proposta por [Zhang et al. 2006] e [Zhang et al. 2008]. A segunda abordagem, mais adequada para redes colaborativas com suporte a formação dinâmica (OVs), agrupam as soluções que fazem o mapeamento das políticas existentes para domínios de ontologias, com o objetivo de representar a semântica de cada domínio envolvido [Patterson et al. 2008, Patterson e Miller 2006, Muthaiyah e Kerschberg 2007].

Soluções de autorização baseadas em Serviços Web Semânticos

Diante da existência de diversas linguagens para definição de políticas de autorização, o que limita a concepção de sistemas distribuídos e abertos baseados em Serviços *Web*, a OASIS lançou a *eXtensible Access Control Markup Language* (XACML) [OASIS 2005a], um sistema de políticas de controle de acesso, baseado em XML. Os cenários que constituem as redes colaborativas caracterizados pela heterogeneidade e principalmente por envolver diferentes domínios administrativos e de segurança, faz com que a simples representação sintática desta linguagem não seja suficiente para as etapas de descoberta e casamento das políticas de controle de acesso [Damiani et al. 2004].

A linguagem XACML foi concebida visando garantir a interoperabilidade entre diversas aplicações, além de permitir extensões em sua linguagem de forma a permitir que desenvolvedores definam novas funções, tipos de dados, combinações lógicas, etc. As soluções de controle de acesso que envolvem aspectos semânticos, usam destas extensões para adequar o uso do XACML nas redes colaborativas.

Nos trabalhos [Damiani et al. 2004, Patterson e Miller 2006, Patterson et al. 2008, Muthaiyah e Kerschberg 2007] são propostas soluções para integração de políticas de controle de acesso através de anotações no XACML que apontam para instâncias de ontologias. A Figura 3.9 ilustra como são feitas as anotações que acrescentam uma descrição semântica ao WSDL de um Serviço *Web*. Tais anotações poderiam também ser usadas em conjunto com o WS-Policy [WS-POLICY 2007] para acrescentar significado semântico às políticas.

Observa-se na Figura 3.9 que as *tags* RDF (*Resource Description Framework*) são utilizadas para indicar a localização da descrição semântica do serviço. O uso em conjunto do RDF com a *Web Ontology Language* (OWL) possibilita a representação do conhecimento a partir de padrões (ontologias).

O controle de acesso baseado em papéis (RBAC) é um modelo onde a identidade no sistema é representada por um papel e todas as políticas de permissões estão associadas a este [Sandhu e Samarati 1994]. Segundo [Patterson e Miller 2006], o RBAC é o modelo

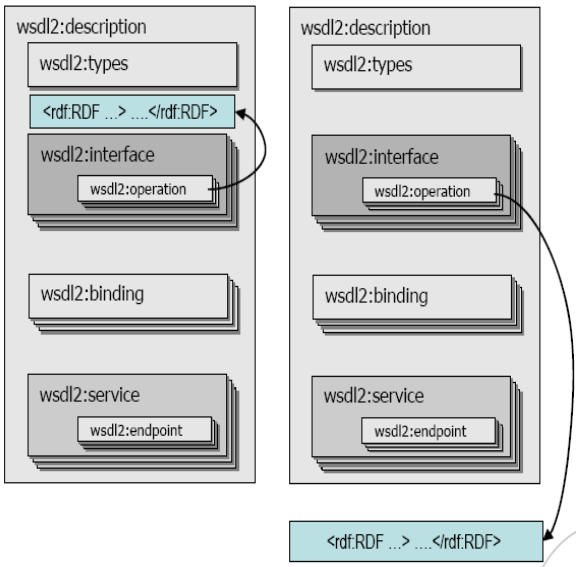

Figura 3.9. Acrescentando anotações semânticas em WSDL

de controle de acesso mais empregado em soluções que fazem uso de ontologia devido a sua facilidade de implementação, flexibilidade e por possuir um amplo repositório de papéis já mapeados por ontologias. Isto permite que se use um mecanismo RBAC com anotações semânticas para descrição de usuários, papéis, objetos e operações.

Com as informações semânticas compondo a descrição funcional e não funcional do Serviço *Web*, a descoberta e casamento dos serviços não é mais simplesmente uma busca sintática e sim uma inferência sobre as instâncias e domínios de ontologias. O fluxo básico de descoberta de serviços é exemplificado pelo diagrama da Figura 3.10.

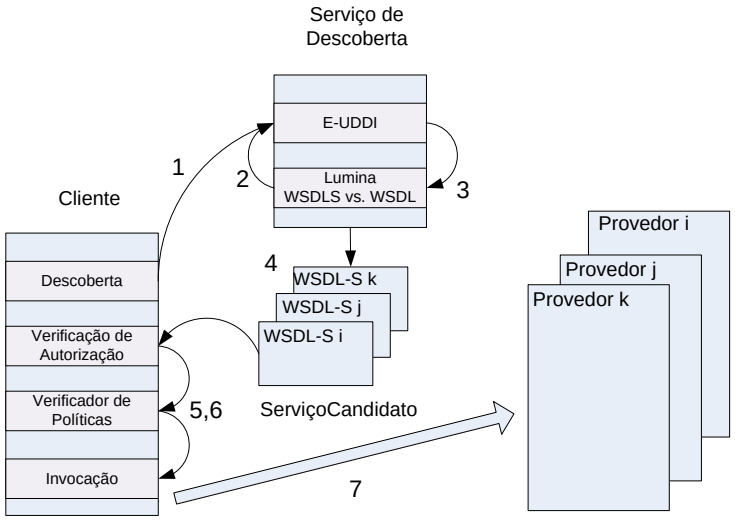

Figura 3.10. Fluxo de Descoberta de Serviços Web Semânticos. Adaptado de [Patterson e Miller 2006]

A Figura 3.10 mostra, no passo 1, um cliente enviando uma requisição de serviço

para o motor de descoberta semântica. Nos passos 2 e 3, é feita a busca por serviços a partir de anotações semânticas usando a ferramenta Lumina[29], que implementa um UDDI semântico. No passo 4, os serviços encontrados são retornados ao cliente, onde nos passos 5 e 6 é feita a verificação de autorização e análise de restrições bem como a invocação do serviço. No passo 7, são feitas as análises do *WS-Policy* quanto ao casamento dos requisitos funcionais e não funcionais da descoberta.

Soluções de autorização baseadas em Padronização das Políticas

Segundo [Zhang et al. 2006] e [Zhang et al. 2008], sistemas colaborativos e *ad hoc* se tornaram um novo desafio para o gerenciamento de autorização, pois não existe um acordo prévio para formação da organização virtual e as decisões de autorização dependem de informação de contexto. Para tal em [Zhang et al. 2006] e [Zhang et al. 2008] foi proposto um *framework* de autorização baseado em UCON (*Usage Control*) para sistemas colaborativos. UCON estende os modelos de controle de acesso clássicos e permite controlar uma ação instantânea, ou contínua, durante um determinado período de tempo. A decisão de acesso pode ser realizada antes e durante o processo de acesso. Duas características diferem o UCON dos modelos de controle de acesso clássicos: a continuidade do processo de decisão de acesso; e a mutabilidade dos atributos do sujeito e do objeto [Zhang et al. 2006, Zhang et al. 2008].

Normalmente, em redes colaborativas o provedor de um serviço tem a última decisão com relação acesso ao recurso compartilhado mas, ao mesmo tempo, como membro da organização virtual deve respeitar as políticas definidas globalmente para a organização. O uso do UCON como modelo de controle de acesso, para o desenvolvimento de um *framework* de controle de acesso para sistemas colaborativos foi justificado em [Zhang et al. 2008] pelo fato de ser um modelo bastante robusto e flexível.

Nas redes colaborativas, os provedores de serviços e, no caso das organizações virtuais, os gerentes das OVs, são os responsáveis por definir ou alterar políticas de segurança [Zhang et al. 2006]. Segundo [Zhang et al. 2008], diferentes tipos de políticas podem ser especificadas, tais como: as políticas de acesso aos recursos, políticas de compartilhamento de recursos, e as políticas para tarefas colaborativas.

Pode-se observar que a solução baseada no UCON é bastante robusta e flexível porém exige que todos os parceiros a implemente o que nem sempre é possível pois organizações contam com sistemas legados e bastante heterogêneos, característica intrínseca de redes colaborativas. Portanto tal solução é bastante pertinente quando existe a possibilidade desta padronização caso contrário, não resolve o problema de casamento semântico de políticas em domínios distintos.

Nas soluções baseadas no mapeamento semântico, como em [Damiani et al. 2004, Patterson e Miller 2006, Patterson et al. 2008, Muthaiyah e Kerschberg 2007], os problemas não são totalmente resolvidos pois a busca por serviços e o casamento das políticas de controle de acesso são feitos sobre inferências realizadas nos domínios de ontologias.Tais inferências, a partir das instâncias de ontologias anotadas nos documentos de descrição

[29]Mais informações em: http://lsdis.cs.uga.edu/projects/meteor-s/downloads/Lumina/

dos serviços, geram um certo grau de incerteza que deve ser tratado para que não seja negado acesso a um recurso que deveria ser liberado ou liberado acesso a recursos que não deveriam ser acessados. Outro problema está relacionado com a forma que as informações semânticas sobre o serviço são publicadas, uma vez que todos podem ter acesso às descrições semânticas de controle de acesso do serviço. Isto gera um problema de privacidade e pode vir a comprometer a segurança do sistema [Patterson et al. 2008].

Estudo de caso

Como forma de abordar os problemas de autorização e controle de acesso, inerentes às redes colaborativas, nessa seção será apresentado um estudo de caso no contexto da *Rede Colaborativa de Ensino e Pesquisa do Brasil (RNP) - Serviço de Acesso a Serviços de Bibliotecas Digitais* descrito na Seção3.2.4.

Supõem-se, neste exemplo, que a própria RNP serve de provedor de serviços e que ofereça um Serviço Web para a busca avançada de artigos, monografias e teses em todas as bibliotecas digitais dos membros federação. O serviço consiste basicamente de uma interface, a qual interage com o usuário, um motor de buscas avançado, responsável por realizar consultas em bases locais, remotas ou ainda invocando outros Serviços Web de membros da rede, e um visualizador de conteúdos.

Cada provedor de serviço da federação CAFe da RNP possui suas políticas de autorização e controle de acesso pois estão sob modelos administrativos distintos. A necessidade da disponibilização deste serviço de busca deve levar em consideração a necessidade de entendimento das políticas de controle de acesso entre todos os participantes. Pode-se imaginar uma situação em que um usuário (Professor), após autenticado no serviço provido pela própria RNP, quer acesso a uma biblioteca digital disponibilizado por outro membro da rede. Como os domínios administrativos (semânticos) são distintos, se a forma de identificar este usuário e os recursos a que se quer verificar o acesso forem diferentes isto pode causar incompatibilidade durante a aplicação das regras de autorização.

Como se está em um cenário onde já existem relações de confiança entre os membros da federação, pode-se resolver o problema de controle de acesso distribuído de duas formas:

- todos os membros da rede colaborativa podem definir suas políticas de acordo com o modelo UCON para sistemas colaborativos [Zhang et al. 2008]; ou
- após a definição dos padrões de representação (domínios de ontologia) todos os membros devem fazer o mapeamento entre as políticas de controle de acesso e os domínios de ontologias como em [Patterson et al. 2008, Patterson e Miller 2006, Muthaiyah e Kerschberg 2007]. Como se trata de uma federação de serviços cuja composição é duradoura, impasses no casamento de políticas não devem ocorrem.

3.5. Considerações finais

Os participantes em redes colaborativas desejam poder se comunicar de forma dinâmica e respeitando os requisitos de segurança dos parceiros. As políticas de QoP, principalmente

na linguagem padrão *WS-Policy*, são parte da solução para esse problema. No entanto, ainda há uma carência no suporte das ferramentas atuais às características da especificação que podem oferecer maior dinamismo, como a definição de múltiplas alternativas de política, verificação automática de compatibilidade e configuração dinâmica de segurança.

O estabelecimento dinâmico da confiança em redes colaborativas exige modelos que consigam operar em ambientes de larga escala e compostos por relações que possuem pouco tempo de vida. Modelos de confiança baseados em redes de confiança e aliados a sistemas de reputações se mostram adequados a tal tipo de cenário e apesar da literatura apresentar diversas propostas, não se tem uma implementação completa destinada a criação das redes colaborativas.

Conforme descrito na Seção 3.4.4, é possível concluir que os requisitos necessários para garantir a proteção da privacidade dos participantes de uma rede colaborativas conforme apresentados em [W3C 2004b] ainda não atendem a real necessidade existente no ambiente dos Serviços *Web*, o que exige a criação de novas soluções para a área.

Em se tratando de autorização e controle de acesso, a peça chave para composição e aplicação de políticas de controle de acesso em redes colaborativas está na busca pela representação consistente da semântica das informações da política, já que em domínios administrativos distintos, como já foi citado anteriormente, a busca e tentativa de casamento sintático das políticas não são suficientes. Duas são as abordagens utilizadas para resolver problemas inerentes a ambientes colaborativos: padronização prévia das informações de controle de acesso para todos os parceiros ou mapeamento entre as informações sintáticas e semânticas dos serviços. Mesmo assim alguns problemas ainda precisam ser resolvidos para que se tenha uma solução de controle de acesso, entre estes: o grau de incerteza que é introduzido quando se utiliza inferências sobre os domínios de ontologia para o casamento das políticas de controle de acesso e a necessidade de publicação de informações semânticas das políticas que pode provocar um problema quanto a privacidade.

Referências

[Armbrust et al. 2009] Armbrust, M., Fox, A., Grif?th, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., e Zaharia, M. (2009). Above the clouds: A berkeley view of cloud computing. Technical report, University of California at Berkeley.

[Asokan et al. 2000] Asokan, N., Shoup, V., e Waidner, M. (2000). Optimistic fair exchange of digital signature. *IEEE Journal of Selected Areas in Communication*, 18(4).

[Bartel et al. 2002] Bartel, M., Boyer, J., e Fox, B. (2002). *XML-Signature Syntax and Processing*. W3C. `http://www.w3.org/TR/xmldsig-core`.

[Blaze et al. 1996] Blaze, M., Feigenbaum, J., e Lacy, J. (1996). Decentralized trust management. In *IEEE Symposium on Security and Privacy*, page 164, Washington, DC, USA. IEEE Computer Society.

[Booth e Liu 2007] Booth, D. e Liu, C. K. (2007). *Web Services Description Language (WSDL) Version 2.0 Part 0: Primer*. W3C.

[Buchegger e Boudec 2003] Buchegger, S. e Boudec, J.-Y. L. (2003). A robust reputation system for mobile ad-hoc networks. Technical Report IC/2003/50, EPFL IC.

[Buyya et al. 2008] Buyya, R., Yeo, C. S., e Venugopal, S. (2008). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *HPCC '08: Proceedings of the 2008 10th IEEE International Conference on High Performance Computing and Communications*, pages 5–13. IEEE Computer Society.

[Böger et al. 2009] Böger, D., Fraga, J., Mafra, P., e Wangham, M. S. (2009). A model to verify quality of protection policies in composite web services. In *Services, IEEE Congress on*, volume 1, pages 629–636, Los Alamitos, CA, USA. IEEE Computer Society.

[Camargo et al. 2007] Camargo, E., da Silva Fraga, J., Wangham, M. S., e de Mello, E. R. (2007). Autenticação e autorização em arquiteturas orientadas a serviço através de identidades federadas. In *Simpósio Brasileiro de Redes de Computadores e Sistemas DIstribuídos*, pages 75–88.

[Camarinha-Matos 2005] Camarinha-Matos, L. M. (2005). *ICT Infrastructures for VO*, chapter Virtual organisations: Systems and practices, pages 83–104. Springer.

[Camarinha-Matos e Afsarmanesh 2005] Camarinha-Matos, L. M. e Afsarmanesh, H. (2005). Collaborative networks: A new scientific discipline. *Journal of Intelligent Manufacturing*, 16:439–452.

[Camarinha-Matos et al. 2008] Camarinha-Matos, L. M., Afsarmanesh, H., e Ollus, M. (2008). *Methods and Tools for Collaborative Networked Organizations*, chapter Ecolead And Cno Base Concepts, pages 3–32. Springer.

[Cancian 2009] Cancian, M. H. (2009). Uma proposta de guia de referência para provedores de software como um serviço. Master's thesis, Universidade Federal de Santa Catarina.

[Canovas et al. 2004] Canovas, O., Lopez, G., e Gomez-Skarmeta, A. F. (2004). A credential conversion service for saml-based scenarios. In *In Proceedings of 1st European PKI Workshop*, pages 297–305.

[Capkun et al. 2002] Capkun, S., Buttyan, L., e Hubaux, J.-P. (2002). Small worlds in security systems: an analysis of the PGP certificate graph. In *New Security Paradigms Workshop*, pages 28–35.

[Carminati et al. 2005] Carminati, B., Ferrari, E., e Hung, P. C. K. (2005). Web service composition: A security perspective. In *WIRI*, pages 248–253.

[Carmody 2001] Carmody, S. (2001). *Shibboleth Overview and Requirements*. Shibboleth Working Group.

[Cattaneo et al. 2004] Cattaneo, G., Faruolo, P., e Petrillo, U. F. (2004). Providing privacy for web services by anonymous group identification. In *International Conference on Web Services (ICWS'04)*. IEEE.

[Charfi e Mezini 2005] Charfi, A. e Mezini, M. (2005). Using aspects for security engineering of web service compositions. In *Proceedings of the 2005 IEEE International Conference on Web Services, Volume I*, pages 59–66.

[Clement et al. 2004] Clement, L., Hately, A., von Riegen, C., e Rogers, T. (2004). *UDDI Version 3.0.2*. OASIS.

[Damiani et al. 2004] Damiani, E., De Capitani di Vimercati, S., Fugazza, C., e Samarati, P. (2004). Extending policy languages to the semantic web. *Lecture notes in computer science*, pages 330–343.

[Damiani et al. 2003] Damiani, E., di Vimercati, S. D. C., e Samarati, P. (2003). Managing multiple and dependable identities. In *IEEE Internet Computing*, pages 29–37. IEEE.

[de Mello 2009] de Mello, E. R. (2009). *Um modelo para confiança dinâmica em ambientes orientados a serviços*. PhD thesis, Universidade Federal de Santa Catarina.

[de Mello et al. 2009a] de Mello, E. R., da Silva Fraga, J., e Wangham, M. S. (2009a). Um modelo de confiança para composição de serviços web. In *Simpósio Brasileiro de Redes de Computadores*, Recife, PE. Sociedade Brasileira de Computação.

[de Mello et al. 2006] de Mello, E. R., Wangham, M. S., da Silva Fraga, J., e Camargo, E. (2006). *Segurança em Serviços Web*, chapter 1, pages 1–48. Minicursos do SBSeg 2006. Sociedade Brasileira de Computação.

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

[de Mello et al. 2005] de Mello, E. R., Wangham, M. S., da Silva Fraga, J., e Rabelo, R. J. (2005). A secure model to establish trust relationships in web services for virtual organizations. In Camarinha-Matos, L. M., Afsarmanesh, H., e Ortiz, A., editors, *Collaborative Networks in Their Breeding Environment*, pages 183–190. Springer.

[Demchenko et al. 2005] Demchenko, Y., Gommans, L., e de Laat an Bas Oudenaarde, C. (2005). Web services and grid security vulnerabilities and threats analysis and model. In *SC'05: Proc. The 6th IEEE/ACM International Workshop on Grid Computing CD*, pages 262–267, Seattle, Washington, USA. IEEE/ACM.

[Erl 2006] Erl, T. (2006). *Service-Oriented Architecture, Concepts, Technology, and Design*. Prentice Hall.

[Gambetta 1988] Gambetta, D. (1988). *Trust: Making and Breaking Cooperative Relations*. Basil Blackwell.

[Godfrey et al. 2006] Godfrey, P. B., Shenker, S., e Stoica, I. (2006). Minimizing churn in distributed systems. In *Proceedings of ACM SIGCOMM*, pages 147–158, Pisa, Italy.

[Gray et al. 2003] Gray, E., Seigneur, J.-M., Chen, Y., e Jensen, C. D. (2003). Trust propagation in small worlds. In *First International Conference on Trust Management*, pages 239–254.

[Hayes 2008] Hayes, B. (2008). Cloud computing. *Communications of the ACM*, 51(7):9–11.

[Hung et al. 2004] Hung, P. C. K., Ferrari, E., e Carminati, B. (2004). Towards standardized web services privacy technologies. In *International Conference on Web Services (ICWS'04)*. IEEE.

[Imamura et al. 2002] Imamura, T., Dillaway, B., e Simon, E. (2002). *XML Encryption Syntax and Processing*. W3C. `http://www.w3.org/TR/xmlenc-core`.

[Jain 1991] Jain, R. (1991). *The art of computer systems performance analysis*. Wiley.

[Jones e Pickles 2007] Jones, M. e Pickles, S. (2007). Shebangs final report. Technical report, University of Manchester.

[Jøsang et al. 2005] Jøsang, A., Fabre, J., Hay, B., Dalziel, J., e Pope, S. (2005). Trust requirements in identity management. In *Australasian workshop on Grid computing and e-research (CRPIT'44)*, pages 99–108, Darlinghurst, Australia. Australian Computer Society, Inc.

[Jøsang e Pope 2005] Jøsang, A. e Pope, S. (2005). User centric identity management. In *Asia Pacific Information Technology Security Conference (AusCERT'05)*.

[Kürümlüoglu et al. 2005] Kürümlüoglu, M., Nostdal, R., e Karvonen, I. (2005). *Base concepts*, chapter Virtual organisations: Systems and practices, pages 11–28. Springer.

[Liberty 2003a] Liberty (2003a). *Introduction to the Liberty Alliance Identity Architecture*. Liberty Alliance.

[Liberty 2003b] Liberty (2003b). *Privacy and Security Best Practices*. Liberty Alliance.

[Lopez et al. 2005] Lopez, G., Canovas, O., Gomez-Skarmeta, A. F., Otenko, S., e Chadwick, D. (2005). A Heterogeneous Network Access Service based on PERMIS and SAML. In *In Proceedings of 2nd EuroPKI Workshop*.

[Lorch et al. 2003a] Lorch, M., Kafura, D., e Shah, S. (2003a). An xacml-based policy management and authorization service for globus resources. In *GRID '03: Proceedings of the 4th International Workshop on Grid Computing*, page 208, Washington, DC, USA. IEEE Computer Society.

[Lorch et al. 2003b] Lorch, M., Proctor, S., Lepro, R., Kafura, D., e Shah, S. (2003b). First experiences using xacml for access control in distributed systems. In *ACM Workshop on XML Security*.

[Ma 2007] Ma, D. (2007). Business model of software-as-a-service. In *Proc. of IEEE International Conference on Services Computing (SCC 2007)*.

[Mcafee 2006] Mcafee, A. P. (2006). Enterprise 2.0: The dawn of emergent collaboration. *MIT Sloan Management Review*, 47(3):21–28.

[Merrill 2006] Merrill, D. (2006). Mashups: The new breed of web app. Technical report, IBM. http://www.ibm.com/developerworks/web/library/x-mashups.html.

[Milgram 1967] Milgram, S. (1967). The small world problem. *Psychology Today*, 1:61.

[Mitra e Lafon 2003] Mitra, N. e Lafon, Y. (2003). *SOAP Version 1.2 Part 0: Primer*. W3C. = http://www.w3.org/TR/soap12-part0.

[Muthaiyah e Kerschberg 2007] Muthaiyah, S. e Kerschberg, L. (2007). Virtual organization security policies: An ontology-based integration approach. *Information Systems Frontiers*, 9(5):505–514.

[OASIS 2004] OASIS (2004). *Web Services Security: SOAP Message Security 1.0*. OASIS. http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.

[OASIS 2005a] OASIS (2005a). *eXtensible Access Control Markup Language (XACML) version 2.0*. Organization for the Advancement of Structured Information Standards (OASIS). http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

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

[O'Reilly 2005] O'Reilly, T. (2005). What is web 2.0: Design patterns and business models for the next generation of software.

[Papastergiou et al. 2008] Papastergiou, S., Valvis, G., e Polemi, D. (2008). A holistic anonymity framework for web services. In *PETRA '08: Proceedings of the 1st international conference on PErvasive Technologies Related to Assistive Environments*, pages 1–8, New York, NY, USA. ACM.

[Patterson e Miller 2006] Patterson, R. e Miller, J. (2006). Expressing authorization in semantic web services. In *2006 IEEE International Conference on Granular Computing*, pages 792–795.

[Patterson et al. 2008] Patterson, R., Miller, J., Cardoso, J., e Davis, M. (2008). Bringing semantic security to semantic web services. *The Semantic Web Real-world Applications from Industry*, page 273.

[Penning 2006] Penning, H. P. (2006). Analysis of the strong set in the pgp web of trust. http://www.cs.uu.nl/people/henkp/henkp/pgp/pathfinder/plot/.

[Pfitzmann e Hansen 2007] Pfitzmann, A. e Hansen, M. (2007). Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology. Version 0.29. `http://dud.inf.tu-dresden.de/Anon_Terminology.shtml`.

[Rabelo 2008] Rabelo, R. J. (2008). *Methods and Tools for Collaborative Networked Organizations*, chapter Advanced Collaborative Business ICT Infrastructures, pages 337–365. Springer.

[Rabelo et al. 2008] Rabelo, R. J., del Mar Castro Rodriguez, M., Conconi, A., e Sesana, M. (2008). *Methods and Tools for Collaborative Networked Organizations*, chapter The ECOLEAD Plug and Play Collaborative Business Infrastructure, pages 371–395. Springer.

[Rannenberg 2000] Rannenberg, K. (2000). Multilateral security a concept and examples for balanced security. In *Workshop on New security paradigms (NSPW'00)*, pages 151–162, New York, NY, USA. ACM Press.

[Rao e Sadeh 2005] Rao, J. e Sadeh, N. (2005). A semantic web framework for interleaving policy reasoning and external service discovery. *Lecture notes in computer science*, 3791:56.

[Sabater e Sierra 2001] Sabater, J. e Sierra, C. (2001). Regret: A reputation model for gregarious societies. *4th Workshop on Deception, Fraud and Trust in Agent Societies*, pages 61–69.

[Sabater e Sierra 2005] Sabater, J. e Sierra, C. (2005). Review on Computational Trust and Reputation Models. *Artificial Intelligence Review*, 24(1):33–60.

[Sandhu e Samarati 1994] Sandhu, R. S. e Samarati, P. (1994). Access control: Principles and practice. *IEEE Communications Magazine*, 32(9):40–48.

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

[Spence et al. 2006] Spence, D., Geddes, N., Jensen, J., Richards, A., Viljoen, M., Martin, A., Dovey, M., Norman, M., Tang, K., Trefethen, A., Wallom, D., Allan, R., e Meredith, D. (2006). Shibgrid: Shibboleth access for the uk national grid service. In *Proceedings of the Second IEEE International Conference on e-Science and Grid Computing (e-Science'06)*, page 75. IEEE Computer Society.

[Sutton e Barto 1998] Sutton, R. S. e Barto, A. G. (1998). *Reinforcement Learning: An Introduction*. MIT Press.

[Teacy et al. 2006] Teacy, W. T., Patel, J., Jennings, N. R., e Luck, M. (2006). Travos: Trust and reputation in the context of inaccurate information sources. *Autonomous Agents and Multi-Agent Systems*, 12(2):183–198.

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

[Vecchio et al. 2005] Vecchio, D. D., Basney, J., e Nagaratnam, N. (2005). Credex: User-centric credential management for grid and web services. In *International Conference on Web Services*, pages 149–156, Orlando, Florida - EUA.

[W3C 2002] W3C (2002). *The Platform for Privacy Preferences 1.0 (P3P1) Specification*. W3C Recommendation. `http://www.w3c.org/TR/P3P`.

[W3C 2004a] W3C (2004a). *Web Services Architecture*. W3C Working Group. `http://www.w3.org/TR/2004/NOTE-ws-arch-20040211`.

[W3C 2004b] W3C (2004b). *Web Services Architecture Requirements*. W3C Working Group. `http://www.w3.org/TR/2004/NOTE-wsa-reqs-20040211`.

[Wang e Vassileva 2003] Wang, Y. e Vassileva, J. (2003). Bayesian Network Trust Model in Peer-to-Peer Networks. *Workshop on Deception, Fraud and Trust in Agent Societies*, 7.

[Wangham et al. 2005] Wangham, M. S., de Mello, E. R., Rabello, R., e da Silva Fraga, J. (2005). Provendo garantias de segurança para formação de organizações virtuais. *Gestão Avançada de Manufatura*, 22:75–84.

[Weerawarana et al. 2005] Weerawarana, S., Curbera, F., Leymann, F., Storey, T., e Ferguson, D. F. (2005). *Web Services Plataform Architecture*. Prentice Hall, Indiana.

[Whitby et al. 2005] Whitby, A., Jøsang, A., e Indulska, J. (2005). Filtering out unfair ratings in bayesian reputation systems. *The Icfain Journal of Management Research*, 4(2):48–64.

[Winslett et al. 2002] Winslett, M., Yu, T., Seamons, K. E., Hess, A., Jacobson, J., Jarvis, R., Smith, B., e Yu, L. (2002). Negotiating trust on the web. *IEEE Internet Computing*, 06(6):30–37.

[WS-FEDERATION 2006] WS-FEDERATION (2006). Web services federation language (ws-federation) version 1.1. http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/WS-Federation-V1-1B.pdf.

[WS-METADATAEXCHANGE 2009] WS-METADATAEXCHANGE (2009). Web services metadata exchange (ws-metadataexchange). W3C Working Draft. http://www.w3.org/TR/2006/REC-ws-addr-core-20060509.

[WS-POLICY 2007] WS-POLICY (2007). Web services policy 1.5 - framework. W3C Recommendation. http://www.w3.org/TR/2007/REC-ws-policy-20070904/.

[WS-SECURITY 2006] WS-SECURITY (2006). Web services security: Soap message security 1.1. OASIS Standard Specification. http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf.

[WS-SECURITYPOLICY 2007] WS-SECURITYPOLICY (2007). Ws-securitypolicy 1.2. OASIS Standard. http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf.

[Zhang e Zhou 2009] Zhang, L.-J. e Zhou, Q. (2009). Ccoa: Cloud computing open architecture. In *2009 IEEE International Conference on Web Services*, pages 607–616.

[Zhang et al. 2006] Zhang, X., Nakae, M., Covington, M., e Sandhu, R. (2006). A usage-based authorization framework for collaborative computing systems. In *Proceedings of the eleventh ACM symposium on Access control models and technologies*, pages 180–189. ACM New York, NY, USA.

[Zhang et al. 2008] Zhang, X., Nakae, M., Covington, M. J., e Sandhu, R. (2008). Toward a usage-based security framework for collaborative computing systems. *ACM Trans. Inf. Syst. Secur.*, 11(1):1–36.