Aplicação do Modelo $UCON_{ABC}$ em Sistemas de Comércio Eletrônico B2B

Alexandre Rosa Camy[1], Carla Merkle Westphall[2], Rafael da Rosa Righi[3]

Programa de Pós-Graduação em Ciência da Computação (PPGCC)
Laboratório de Redes e Gerência (LRG) - UFSC
Caixa Postal: 476 - Florianópolis/SC - Brasil - 88040-900
[2]UFSC / UNIVALI - Av. Uruguai, 458 - CEP 88302-202 - Itajaí - SC - Brasil

[1]camy@inf.ufsc.br, [2]{carla}@lrg.ufsc.br, [3]rrighi@lrg.ufsc.br

Abstract. *The systems of Business-to-Business (B2B) Electronic Commerce (EC) are used for business management among different companies. These systems need a differentiate form of treating access control when interact with each other. Researches in this area are being developed in a significant way. Recently the $UCON_{ABC}$ model was proposed embracing new concepts. The application of this model in B2B EC systems is an aspect that is investigated in this article. This article proposes a form of $UCON_{ABC}$ application that assists the specific needs of B2B EC systems that interact with each other, presenting a solution to treat the access control and the permissions management.*

Resumo. *Os sistemas de Comércio Eletrônico (CE) Business-to-Business (B2B) são utilizados para a administração de negócios entre diferentes empresas.Estes sistemas necessitam de uma forma diferenciada de tratar o controle de acesso quando interagem entre si. Pesquisas nesta área vêm evoluindo de maneira significativa. O modelo $UCON_{ABC}$ foi proposto recentemente abrangendo novos conceitos.A aplicação deste modelo em sistemas de CE B2B é um aspecto que é investigado nesse artigo. Este artigo propõe uma forma de aplicação do $UCON_{ABC}$ que atenda as necessidades específicas de sistemas de CE B2B que interagem entre si, apresentando uma solução para tratar o controle de acesso e o gerenciamento de permissões.*

1. Introdução

O controle de acesso é uma área que está em constante evolução. Sua função é mediar o acesso dos sujeitos (usuários ou processos) aos objetos de um sistema computacional, mantendo as propriedades básicas de segurança - integridade, confidencialidade e disponibilidade. Atualmente existem determinados tipos de sistemas que possuem características que exigem soluções específicas para o controle de acesso. [Medjahed et all, 2003], afirma que são necessárias pesquisas na especificação, validação e execução de políticas de controle de acesso para sistemas de Comércio Eletrônico (CE) *Business-to-Business* (B2B).

A interação entre sistemas de CE B2B tem despertado atenção de pesquisadores. Através da interação é possível que sistemas de CE B2B de diferentes tecnologias interajam entre si no intuito de agilizar o processo de negociação entre empresas parceiras. Trabalhos como os de [Medjahed et all, 2003], [Dabous, Rabhi & Ray, 2003] ou [Quix, Schoop & Jeusfeld, 2002] enfatizam o estudo de técnicas, métodos ou tecnologias necessárias para a interação entre sistemas B2B.

[Park & Sandhu, 2002] se juntaram em um esforço no sentido de unir conceitos de *Digital Rights Management* (DRM) [Liu et. All 2003], Gerenciamento de Confiança [Blaze et. All 1996] e Controle de Acesso Tradicional. Além disso, eles propuseram melhorias. Como resultado, foi definido um modelo chamado $UCON_{ABC}$. Devido à sua abrangência, o modelo $UCON_{ABC}$ pode ser utilizado em diferentes sistemas e com arquiteturas variadas. [Park, 2003] afirma que existem ainda muitas melhorias a serem pesquisadas e desenvolvidas relacionadas com o modelo $UCON_{ABC}$. Dentre elas, esta a pesquisa no $UCON_{ABC}$ em arquiteturas de segurança para Sistemas de CE B2B**.**

Este artigo apresenta uma proposta de aplicação do $UCON_{ABC}$ em sistemas de CE B2B que interagem entre si. A proposta utiliza todas as características do $UCON_{ABC}$ que podem ser aplicadas especificamente neste tipo de sistema. Também é apresentado o Agrupamento Implícito Parcial (AIP), uma variação simplificada do Agrupamento Implícito (AI). Seu objetivo é prover meios de gerenciar eficientemente permissões de acesso em um sistema de CE B2B, mas de uma forma mais simplificada que o AI.

Com o objetivo de auxiliar a compreensão da aplicação do modelo $UCON_{ABC}$ em sistemas de CE B2B, este artigo ainda apresenta um estudo de caso entre duas indústrias parceiras que possuem este tipo de sistema para a realização de negócios.

As Seções estão organizadas neste artigo da seguinte forma: A seção 2 faz a comparação deste trabalho com trabalhos relacionados ao controle de acesso em Sistemas de CE B2B. A seção 3 apresenta conceitos fundamentais sobre o modelo $UCON_{ABC}$ e Sistemas de CE B2B como embasamento para a proposta a ser apresentada. Na seção 4 é apresentada a contribuição principal desta pesquisa, que é a proposta de aplicação do modelo $UCON_{ABC}$ em sistemas de CE B2B que interagem entre si. A seção 5 apresenta um estudo de caso que utiliza a proposta deste artigo para desenvolvimento do controle de acesso de um sistema de CE B2B. Por fim, o artigo é finalizado na seção 6 apresentando a conclusão e as contribuições científicas deste trabalho.

2. Trabalhos Relacionados

Os trabalhos relacionados consistem de propostas de esquema, *framework* ou técnica que melhor atendam às necessidades do controle de acesso em sistemas B2B.

[Robison, 2002] sugeriu uma técnica simples denominada: Permissão de Controle de Acesso Baseado em Lista. Esta técnica se baseia no modelo RBAC (Role-Based Access Control), sendo que o conceito da relação dos papéis com as listas de acesso melhora a organização dos dados no controle de acesso em sistemas B2B.

[Goodwin, Goh & Wu, 2002] definiram um esquema para sistemas de *E-marketplace*, também baseado no RBAC, mas que possui algumas melhorias que, segundo eles, tornam o controle de acesso mais conciso e eficiente. Eles definiram um método denominado "Agrupamento Implícito" para gerenciamento de permissões.

[Essmayr, Probst & Weippl, 2004] propõem um *framework* genérico denominado GAMMA que pode ser aplicado a diferentes tipos de sistemas de CE como: *Bu*siness-*to-Consumer*, *Consumer-to-Consumer* ou até mesmo *Business-to-Business*. GAMMA se baseia no modelo RBAC e é um *framework* independente de plataforma e direcionado para aplicações de multicamadas baseadas em componentes, oferecendo mecanismos de segurança como autenticação, controle de acesso e auditoria.

[Kraft, 2002] desenvolveu um estudo em que define um modelo geral abstrato, específico para componentes de *Web service*, que pode ser utilizado como base no desenvolvimento de um processador de controle de acesso a sistemas de CE.

Os três primeiros trabalhos mencionados fazem referência a sistemas de CE B2B que possuem um sistema central que é acessado diretamente por usuários de empresas parceiras. Nestes casos a solução de controle de acesso não leva em consideração a interação entre os sistemas das empresas envolvidas. A solução proposta por (KRAFT, 2002) vincula um modelo de controle de acesso a uma ferramenta específica: *Web Service*.

Este artigo diferencia-se dos demais por definir uma forma de aplicação do $UCON_{ABC}$ em Sistemas de CE B2B que interagem entre si, independentemente da tecnologia de interação utilizada.

3. Conceitos Fundamentais

Nesta seção são apresentados os seguintes conceitos fundamentais: modelo $UCON_{ABC}$, sistemas de CE B2B e características da interação entre sistemas.

3.1. Modelo de Controle de Acesso $UCON_{ABC}$

O $UCON_{ABC}$ possui oito componentes básicos: sujeitos, atributos dos sujeitos, objetos, atributos dos objetos, direitos, autorizações, obrigações e condições [Park e Sandhu 2004]. Estes componentes podem ser visualizados através da Figura 1.

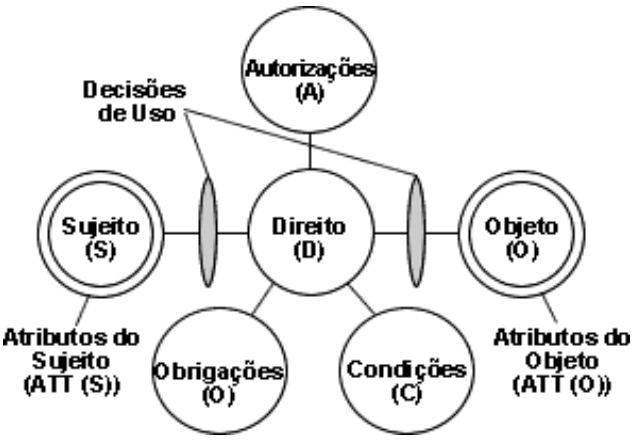

Figura 1: Modelos Básicos do $UCON_{ABC}$ [Park e Sandhu 2004]

Os *Sujeitos* são entidades associadas a atributos que possuem certos direitos sobre os objetos. Um usuário de um sistema computacional pode, por exemplo, ser considerado um sujeito. Os *Objetos* são entidades sobre as quais os sujeitos possuem direitos de acesso. Podem ser ações dentro de um sistema, documentos digitais, arquivos multimídia ou executáveis. *Atributos do Sujeito* e do *Objeto* são propriedades que podem ser utilizadas no processo de decisão de acesso a algum objeto digital.

Em modelos de controle de acesso tradicionais, *direitos* são definidos como privilégios que um sujeito pode ter e exercer sobre um determinado objeto em modos distintos. Entretanto, no modelo $UCON_{ABC}$ são levadas em consideração as atividades do sujeito mesmo após sua autenticação. A existência do direito no $UCON_{ABC}$ é determinada quando o acesso é solicitado pelo sujeito. Assim, as funções de decisão de uso decidem se o acesso pode ou não ser permitido baseando-se nos atributos do sujeito, nos atributos do objeto, nas autorizações, nas obrigações e nas condições.

As *Autorizações* são exigências que devem ser satisfeitas antes de permitir que um sujeito acesse ou use um objeto. Elas avaliam os atributos do sujeito e do objeto para a decisão de uso. As *Obrigações* são funções que verificam as exigências obrigatórias que um sujeito deve executar antes ou enquanto fizer uso de seus direitos. Um exemplo disso é a aceitação dos termos de uso de um sistema antes de se ter acesso ao mesmo. Por fim, as *Condições* são fatores de decisão que se baseiam no estado do sistema ou do ambiente, verificando se exigências relevantes são satisfeitas ou não. Assim, se as condições estiverem de acordo com a política de segurança, o acesso é permitido. As Condições podem ser utilizadas na verificação do horário local para negar acesso em horários indevidos, ou então verificar os *status* do sistema e negar o acesso a todos os usuários caso seja verificado um ataque ao sistema [Park e Sandhu 2004].

Para tornar o processo de decisão de controle de acesso mais eficiente, algumas características inovadoras do $UCON_{ABC}$ que podem ser enumeradas são os conceitos de: oBrigações, Condições, Mutabilidade e Continuidade. As obrigações e condições já foram discutidas.

Em sistemas de controle de acesso tradicionais, os atributos são modificados apenas por ações administrativas. No entanto, em muitas aplicações modernas estes atributos devem ser alterados como efeito das ações dos sujeitos, o que caracteriza a *Mutabilidade* dos atributos de objetos ou sujeitos do $UCON_{ABC}$.

Além disto, em sistemas de controle de acesso tradicionais a autorização é feita antes da permissão do acesso. Entretanto, é possível que se estenda isto para uma execução contínua avaliando as exigências ao longo do uso do sistema, o que caracteriza a *Continuidade* no $UCON_{ABC}$. Esta propriedade pode ser utilizada em sistemas modernos onde seja necessário controlar o tempo de uso relativamente longo ou então para a negação imediata de uso. Para que tal controle seja possível, é necessário que os atributos de sujeito e objeto sejam mutáveis.

Assumindo que exista uma solicitação de uso de um objeto, a tomada de decisão pode ser feita antes (*pre*) ou durante (*ongoing*) a execução do direito solicitado. A tomada de decisão depois (*post*) não possui influência na tomada de decisão atual, apenas na tomada de decisão da próxima vez em que o acesso o objeto for solicitado.

Baseando-se nos oito componentes descritos no início desta seção, [Park e Sandhu 2004] desenvolveram um *framework* para classificar dezesseis modelos distintos do $UCON_{ABC}$. Estes modelos são classificados de acordo com os fatores de decisão: Autorização, oBrigação, Condição, Mutabilidade e Continuidade. Há um padrão numérico para a classificação de acordo com a mutabilidade dos atributos. Caso todos os atributos sejam imutáveis, o modelo adota o número identificador '0'. Para os atributos mutáveis, as pré-atualizações são identificadas pelo número '1', as que ocorrem durante (*ongoing*) por '2' e as pós-atualizações pelo número '3'. A tabela 1 ilustra este *Framework*.

	0 (imutável)	1 (pré-atualização)	2 (atualização-durante)	3 (pós-atualização)
preA	S	S	N	S
onA	S	S	S	S
preB	S	S	N	S
onB	S	S	S	S
preC	S	N	N	N
onC	S	N	N	N

Tabela 1: Modelos $UCON_{ABC}$ (PARK & SANDHU, 2004)

Nos modelos **UCONpreA**, o processo de decisão é tomado antes que o acesso seja permitido. Levando em consideração a mutabilidade de atributos, o UCONpreA divide-se em 3 modelos distintos: $UCONpreA_0$**,** $UCONpreA_1$ e $UCONpreA_3$. No UCONpreA, não existe modelo com identificador '2', pois não há sentido haver atualização durante o acesso se a autorização é feita antes.

Nos modelos **UCONonA**, as solicitações de uso são permitidas sem qualquer tipo de pré-Autorização. As decisões de autorização são feitas de forma contínua, baseadas em tempo ou eventos, enquanto os sujeitos exercem seus direitos sobre os objetos. O UCONonA divide-se em: $UCONonA_0$, $UCONonA_1$, $UCONonA_2$ e $UCONonA_3$.

Nos modelos **UCONpreB,** as obrigações devem ser cumpridas antes que seja permitido o acesso. Os atributos podem não ser utilizados e a classificação relacionada à mutabilidade dos atributos não é obrigatória. Caso se faça necessária utilização de atributos, este modelo divide-se em: $UCONpreB_0$, $UCONpreB_1$ e $UCONpreB_3$.

Os modelos **UCONonB** são semelhantes ao UCONpreB. No entanto, neste caso as obrigações devem ser cumpridas enquanto os direitos estão sendo executados. As obrigações podem ser cumpridas periodicamente, baseadas no tempo ou em eventos. Em necessidade da utilização dos atributos, o UCONonB pode ser dividido em: $UCONonB_0$, $UCONonB_1$, $UCONonB_2$ e $UCONonB_3$.

Nos modelos **UCONpreC** são avaliadas as condições do sistema antes que seja permitido o acesso. Este modelo não utiliza os atributos de sujeitos e objetos. Assim, tais atributos são imutáveis obrigando a existência de apenas um modelo: $UCONpreC_0$. No entanto, tais atributos podem ser utilizados para determinar que tipo de condição deve ser avaliada para possibilitar o acesso do sujeito ao objeto.

Nos modelos **UCONonC** as condições do sistema são verificadas enquanto os direitos estão sendo executados. As condições do ambiente são verificadas constantemente para realizar o controle de acesso. A exemplo do UCONpreC, este modelo também não faz uso dos atributos do sujeito e nem do objeto. Desta forma, o UCONonC é composto apenas pelo modelo $UCONonC_0$.

3.2. Interação em Sistemas de Comércio Eletrônico B2B

CE B2B é o uso de sistemas computadorizados para a administração de negócios entre diferentes empresas parceiras. Segundo [Blodget & McCabe, 2000], o termo "*business-to-business*" teve início na década de 60. Naquela época, empresas parceiras se comunicavam através de linhas telefônicas utilizando um formato de dados proprietário previamente estabelecido entre ambas as partes. Esta tecnologia possuía a desvantagem de os formatos dos dados das empresas variarem muito. Assim, o EDI (*Electronic Data Interchange*) surgiu na década de 70 como forma de transmissão de dados padronizados que agilizaram a execução dos processos entre as empresas. Essa tecnologia era utilizada sobre redes de comunicação privadas, denominadas VANs (*Value Added Networks*), que possuía um custo muito elevado. Já na década de 90, o CE B2B teve um crescimento significativo devido a popularização da Internet.

[Medjahed et All, 2003] afirmam que milhões de empresas já migraram ou estão migrando suas principais operações para a Internet. Com o CE B2B surgiram novas possibilidades de comercialização, possibilitando que empresas de diferentes locais tenham interação e cooperem entre si para realizar transações de forma mais eficiente, encontrem novos parceiros ou compartilhem experiências.

Em um estudo recente, [Radowiisky,2002] afirma que a idéia de junção entre sistemas de CE B2B e Sistemas de Gestão Empresarial (*Enterprise Resource Planning* - ERP) surgiu da grande necessidade de integrar completamente e automatizar todos os fluxos dos processos de uma empresa. Esta integração pode responder perguntas como: "Eu tenho produtos o bastante no estoque para que eu possa entregá-los na hora certa?". Esta junção proporciona um ambiente completo onde, além de ser possível realizar a gestão dos processos da própria empresa, há também a possibilidade de realizar transações comerciais com empresas parceiras. A interação possui um papel importante neste tipo de sistema, pois ela é uma "ponte" de ligação entre o sistema de uma empresa e o sistema de cada empresa parceira, independentemente da tecnologia utilizada. Diversos trabalhos publicados, como os de [Medjahed et All, 2003], [Dabous, Rabhi & Ray, 2002] ou [Quix, Schoop & Jeusfeld, 2002], enfatizam o estudo em métodos ou tecnologias necessárias para a interação entre sistemas B2B.

A partir dessa constatação sobre a prática de interação entre sistemas, observou-se que quando há a interação entre sistemas B2B, usuários externos acessam informações de uma empresa usando sistemas específicos. Portanto, o controle de acesso não pode ser tratado de forma convencional nessas interações. Observou-se, nestes casos, que quem solicita o acesso ao sistema de uma empresa parceira é uma entidade "composta", formada por um usuário de um sistema, com seus atributos individuais, e pelo próprio sistema, com seus atributos. Portanto, é necessária a definição de maneiras eficientes de implementar o controle de acesso especificamente entre sistemas que interagem entre si.

4. $UCON_{ABC}$ em Sistemas de CE B2B

Esta seção apresenta a proposta de aplicação do modelo $UCON_{ABC}$ em sistemas de CE B2B de empresas parceiras que interagem entre si.

A proposta de aplicação é composta por dois sistemas (Figura 3): Sistema da Empresa Provedora (SEP) e Sistema da Empresa Consumidora (SEC).

No **SEP** estão todas as funcionalidades necessárias para o controle de acesso, interação e execução de processos de negócios. Este sistema é constituído de três módulos distintos: i) O *Módulo de Interação* possibilita a interação das diferentes tecnologias utilizadas pelo SEP e SECs. Esta insteração poder ser realizada através da utilização de *Webservices* ou então de vários *frameworks* baseados em XML como: eCO**,** BizTalk**,** cXML**,** RosettaNet e ebXML. ii) O Módulo de Controle de Acesso é responsável por estabelecer o controle de acesso obedecendo aos conceitos básicos do modelo $UCON_{ABC}$. iii) O Módulo de Processos compreende os processos de negócios que são funções, rotinas ou métodos implementados e configurados para serem acessados remotamente. Estes processos atendem pelo nome de "Objetos", como analogia ao modelo $UCON_{ABC}$.

O **SEC** representa os parceiros comerciais que desejam interagir com seu parceiro fornecedor de produtos através de seu próprio sistema. Assim, apesar desta proposta apresentar apenas um SEC, na realidade o SEP pode interagir com muitos outros SECs. Em se tratando de um sistema de CE B2B, este sistema possui um *Módulo Cliente de Interação* que realiza a conversação com o SEP. Da mesma forma que no sistema servidor, este módulo pode utilizar uma das opções de ferramentas de interação existentes para poder se comunicar. A figura 2 apresenta esta proposta de aplicação.

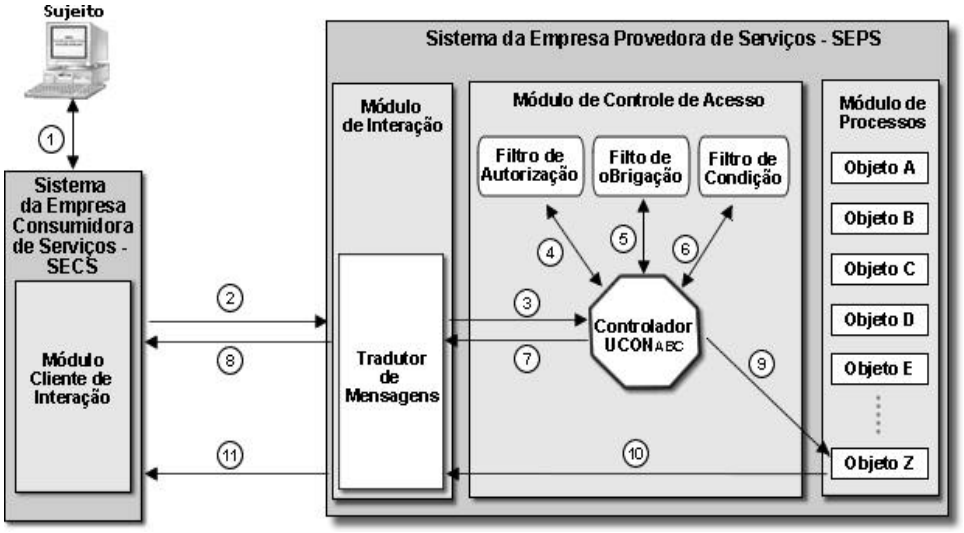

Figura 2: Modelo de Implementação Proposto

4.1. Funcionamento do Modelo

Para explicar a forma de funcionamento da proposta, é apresentado um caso onde uma Empresa Montadora de Computadores (EMC) possui um SEC que interage com um SEP de uma Empresa Fabricante de Processadores (EFP).

Um usuário da EMC que deseja trocar informações com a EFP deve, primeiramente, autenticar-se no SEC da EMC. Posteriormente é necessário autenticar-se no SEP da EFP para que, a partir de então, seja possível a interação entre os sistemas.

No processo de autenticação primeiramente é verificado se o SEC de origem do pedido de autenticação é realmente quem diz ser. Esta verificação pode ser feita simplesmente através da verificação do IP de origem do SEC ou então de maneira mais sofisticada, como por exemplo, através de certificados digitais. Sem o processo de autenticação de um sistema seria possível copiar um SEC e instalá-lo em outro local. Com isto, este sistema "clonado" poderia acessar os serviços de um SEP como se fosse o sistema original. Tal situação poderia causar sérios danos para as empresas parceiras.

Caso o resultado do processo de autenticação do SEC no SEP seja positivo, é liberado então o processo de autenticação do usuário. Quando este processo é finalizado sem erros, o sistema de controle de acesso do SEP inicia a busca pelas permissões as quais este usuário tem acesso. Estas permissões devem ser alocadas na memória do sistema para serem utilizadas pelo sistema de controle de acesso posteriormente.

Observando a figura 2, quando um usuário da EMC deseja fazer uma consulta de preços dos produtos da EFP ele deve, após autenticar-se no SEP, executar o comando de pedido da lista de produtos (passo 1). O Módulo Cliente de Interação recebe esta solicitação e se encarrega de encaminhá-la para o SEP (passo 2).

O Módulo de Interação do SEP recebe esta solicitação e a traduz para a tecnologia utilizada no sistema. Esta solicitação é enviada para o Controlador $UCON_{ABC}$ (passo 3). Qualquer solicitação recebida pelo Módulo de Interação é, obrigatoriamente, direcionada para este Controlador. Sua implementação deve seguir as especificações do modelo $UCON_{ABC}$ na qual, através dos atributos do sujeito e do objeto a ser acessado, são verificadas as regras de condição, autorização e obrigação do SEP através de seus respectivos filtros (passos 4, 5 e 6). Estas verificações são coordenadas seqüencialmente de forma que, em caso de negação de acesso por algum dos filtros, o Controlador pára de executar as tarefas subseqüentes. O primeiro filtro verificado é o de Condição. Isto

porque caso haja alguma irregularidade, por exemplo, no horário de acesso, no endereço IP do SEC do usuário ou no estado do sistema, os demais filtros nem precisam ser verificados. O Filtro de Autorização é verificado em seguida porque se não houver autorização de acesso, não há razão para se verificar o Filtro de Obrigação. É no Filtro de Autorização que são verificadas as permissões do usuário que foram coletadas em seu processo de autenticação. O Filtro de Obrigação se encarrega de verificar se o usuário deve executar alguma ação prévia antes de ter acesso a um determinado objeto.

O conceito de Continuidade desta proposta está no fato de todas as solicitações de acesso a um objeto serem controladas por estes três filtros. Assim, mesmo após autenticar-se o usuário é constantemente monitorado pelo SEP.

Em caso de negação de acesso, o Controlador $UCON_{ABC}$ retorna ao Módulo de Interação uma resposta de negação de acesso ou de necessidade de cumprimento de alguma obrigação (passo 7). No Módulo de Interação esta resposta é traduzida em uma mensagem que é retornada ao SEC (passo 8). Caso a solicitação passe pela verificação de todos os filtros, então o acesso ao objeto desejado é liberado (passo 9). Após serem acessados e executados, os Objetos podem retornar ao Módulo de Interação diferentes tipos de dados, como por exemplo: uma lista de produtos, um arquivo de contrato ou então valores lógicos do tipo verdadeiro/falso (passo 10). Após converter os valores de retorno em uma mensagem, o Módulo de Interação a envia para o SEC (passo 11) que, por sua vez traduz novamente o conteúdo para o formato utilizado e exibe a resposta para o usuário. Assim, o ciclo de funcionamento é finalizado.

4.2. Gerenciamento de Permissões

Além de processos de autenticação e controle de acesso, também é necessário definir como deve ser feito o gerenciamento de permissões dos sistemas das empresas e de seus usuários em um sistema B2B.

Apesar de [Sandhu, 2001] ter mencionado a utilização do RBAC para sistemas de CE B2B, [Robison, 2002] e [Goodwin, Goh & Wu, 2002] afirmam que o RBAC possui limitações quanto a sua utilização neste tipo de sistema e propõem melhorias. [Goodwin, Goh & Wu, 2002] propõem uma técnica específica para sistemas B2B e que estende o RBAC, denominada Agrupamento Implícito (AI). Eles possuem argumentações convincentes quanto à limitação do RBAC e das vantagens existentes em sua proposta. Sendo assim, foi feito um estudo sobre esta técnica para que ela pudesse ser incorporada à proposta de aplicação do $UCON_{ABC}$ em sistemas B2B.

Apesar de descrever o funcionamento do AI, [Goodwin, Goh & Wu, 2002] não apresentam uma representação gráfica clara de sua técnica, o que dificulta a sua visualização e compreensão. Sendo assim, outra contribuição deste artigo é a apresentação de uma representação gráfica desta técnica (figura 3).

O AI tem por objetivo agrupar sujeitos e objetos em grupos distintos de acordo com seus atributos. Diferentemente do RBAC, a permissão entre um sujeito e um objeto não é feita por intermédio de um papel, mas sim por intermédio da permissão entre o grupo que o sujeito pertence e o grupo que o objeto pertence.

Para pertencer a um grupo é necessário que o sujeito, ou objeto, satisfaçam algumas restrições obrigatórias pré-estabelecidas. As restrições para um Agrupamento Implícito de Sujeitos (AIS) podem ser a empresa a que o sujeito pertence, o país de localização da empresa, o papel que desempenha na empresa, dentre outros. As restrições para um Agrupamento Implícito de Objetos (AIO) podem ser: tipo de objeto, tipo de execução, dentre outros.

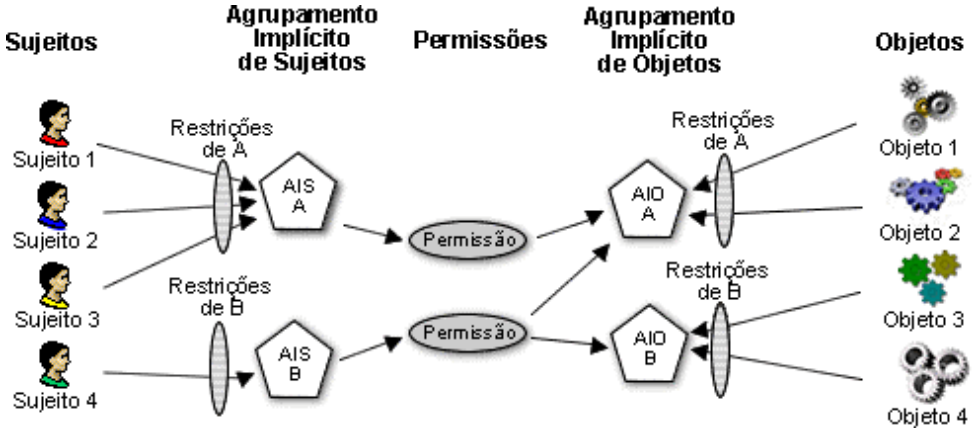

Figura 3: Agrupamento Implícito no Gerenciamento de Permissões

O AI possui duas grandes vantagens sobre o RBAC no que diz respeito à administração de permissões. A primeira delas é o fato de que se um atributo do sujeito é alterado, como por exemplo, o país em que trabalha, a sua mudança de grupo será automática, sem que haja a intervenção do administrador do sistema. A segunda vantagem refere-se ao caso em que haja alguma outra restrição que deva ser levada em consideração para que um sujeito ou objeto faça parte de um grupo. Utilizando o AI, basta definir um novo grupo e atribuí-lo às permissões necessárias. Utilizando o RBAC, seria necessário definir novos papéis e então reatribuí-los a todos os sujeitos que estejam com os papéis antigos, o que acarretaria em um maior custo de administração.

Estas vantagens se devem ao fato de no AI não haver a necessidade de relacionar diretamente os usuários com os seus grupos[1]. O próprio sistema de controle de acesso se encarrega de fazer isso sem a intervenção de um administrador.

Apesar das vantagens mencionadas, [Goodwin, Goh & Wu, 2002] afirmam que além de agrupar os sujeitos, é necessário agrupar os objetos a serem acessados. Apesar deles afirmarem que esta característica é uma vantagem, ela possui uma maior complexidade na gestão sobre estes grupos de objetos. A figura 4 ilustra um exemplo propositalmente gerado de forma que houvesse uma grande variação entre os objetos que podem ser acessados por cada AIO.

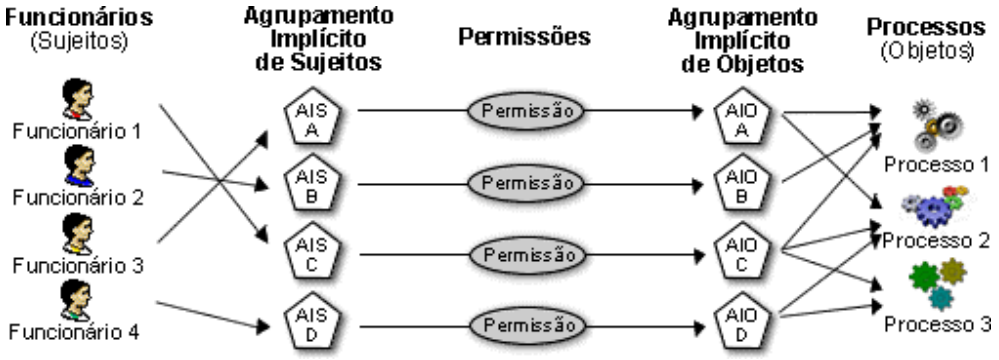

Figura 4: Relação de permissões entre Sujeitos e Objetos através do AI

Em piores casos como este não há outra escolha a não ser formar um AIO que atenda especificamente a um AIS. Assim, o gerenciamento de um AI pode ser uma tarefa muito complexa, pois [Goodwin, Goh & Wu, 2002] afirmam que os objetos devem ser agrupados de acordo com os seus atributos. Isto ocasionaria um custo

[1] Muitos sistemas implementam esta relação através de tabelas de Banco de Dados ou arquivos XML

desnecessário e complexo de gestão, pois da mesma forma que pode haver vários AISs, também podem haver vários AIOs. Com a necessidade de um AIO para cada AIS, a existência de um AIO torna-se desnecessária, pois é perfeitamente possível relacionar os AISs diretamente aos processos de que tem direito. Apesar de ser considerado um "pior caso", exemplos como este não são difíceis de acontecer devido a diversos fatores de variação entre diferentes funções que funcionários de diferentes empresas e países podem executar.

4.2.1. Agrupamento Implícito Parcial - AIP

Para solucionar o problema relacionado com a figura 4, este artigo propõe o Agrupamento Implícito Parcial (AIP), em que apenas os sujeitos devam ser agrupados. Assim, as permissões seriam atribuídas diretamente aos AISs, como mostra a figura 5.

Ao se observar a figura 5 da proposta feita pode surgir um questionamento: Esta proposta não equivale exatamente ao modelo RBAC? A resposta é: aparentemente sim. No entanto, é importante lembrar que na prática este modelo ainda possui as vantagens de facilidade de gestão de usuários e grupos, com a única diferença da exclusão dos AIOs. Com isto, o AIP torna-se mais simples que o AI na gestão de permissões.

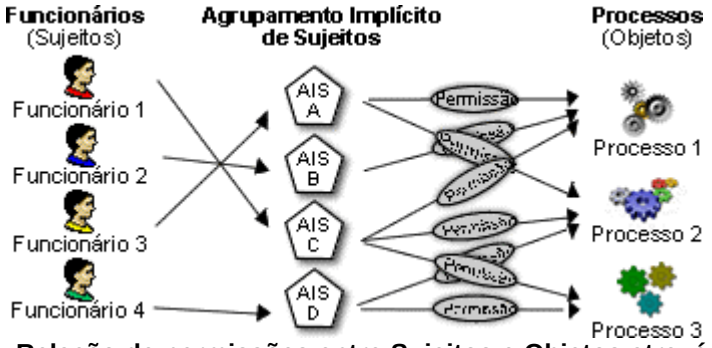

Figura 5: Relação de permissões entre Sujeitos e Objetos através do AIP

5. Estudo de Caso: Indústria Automobilística

Esta seção apresenta um estudo de caso para exemplificar a aplicação da proposta deste artigo em um ambiente de CE B2B. Os nomes das empresas e sistemas abordados neste estudo de caso são ilustrativos e não possuem qualquer relação com o mundo real.

Rodas Forte é uma indústria brasileira fabricante de rodas esportivas para automóveis. Seus clientes são as indústrias de automóvel, onde os veículos fabricados já saem de fábrica com seus produtos. Para reduzir os custos e aumentar a eficiência nas transações entre a *Rodas Forte* e suas empresas parceiras, foi desenvolvido um sistema de CE B2B, denominado RF-B2B (*Rodas Forte Business-to-Business*). O RF-B2B não tem por objetivo substituir o sistema de gestão empresarial (ERP) já existente na *Rodas Forte*, mas sim agregar funcionalidades através de um trabalho em conjunto.

A *Rodas Forte* possui como principal parceira a *Puma Motors*, uma indústria Inglesa fabricante de carros que possui filiais em diversos países do mundo. Ela foi a primeira empresa parceira da *Rodas Forte* a desenvolver um módulo adicional ao seu sistema ERP para interagir com o RF-B2B.

A *Rodas Forte* está situada no Brasil e o sistema RF-B2B atende pelo IP 200.135.71.74. Assim, os sistemas das empresas parceiras podem interagir com o RF-B2B através deste IP. A *Puma Motors*, com sede na Inglaterra, possui seu sistema central que atende pelo IP 213.161.77.151.

Cada uma das filiais da *Puma Motors* tem acesso ao sistema RF-B2B através do sistema central da *Puma Motors*. O sistema central da *Puma Motors* possui uma *extranet* onde todas as filiais podem trocar informações com a matriz. Desta forma, qualquer uma das filiais tem autonomia para realizar negociações com a Rodas Forte. Este cenário caracteriza um ambiente de CE B2B de sistemas que interagem entre si.

Estes sistemas foram implementados, para esta pesquisa, utilizando a tecnologia Java. O RF-B2B foi implementado em EJB (Enterprise Java Bean) e executado no *container* JBoss. O sistema da *Puma Motors* foi implementado em JSP (Java Server Pages) e Java Servlets. Para a realização da interação entre os dois sistemas foi escolhido o *Web service* Apache Axis.

5.1. Gerenciamento de Permissões

O gerenciamento de permissões do RF-B2B leva em consideração a empresa parceira, filial da empresa parceira e a função do usuário na empresa. Desta forma, o sistema de controle de acesso do RF-B2B pode atribuir diferentes permissões entre: i) diferentes empresas; ii) diferentes filais de uma mesma empresa e iii) diferentes funções dentro de uma mesma filial. Nestes itens são considerados os atributos do usuário e sua combinação pode determinar a participação de um usuário em um determinado grupo de acesso do sistema. A tabela 2 ilustra alguns dos grupos existentes e suas respectivas restrições configuradas no sistema de controle de acesso do RF-B2B.

Grupo	Restrições			Serviços
	Empresa	Filial	Função	
RF1				Gestão de dados pessoais
RF2			Gestor de Permissões	Gestão de permissões em seu ambiente
RF3	Puma Motors		Comprador	Gestão de pedidos de compra da Puma Motors
RF4	Puma Motors		Gerente de Compras	Gestão de histórico de compras da Puma Motors
RF5	Puma Motors	Puma - USA	Gestor de Contratos	Gestão de Contratos da Puma – USA
RF6	Puma Motors	Puma - México	Gestor de Contratos	Gestão de Contratos da Puma - México
RF7	Puma Motors	Puma - Rússia	Gestor de Contratos	Gestão de Contratos da Puma - Rússia
RF8	Alfa Motors		Comprador	Gestão de pedidos de compra da Alfa Motors
...	...	...	...	...

Tabela 2: Relação de acesso entre Grupos e Serviços

A tabela 2 mostra que não há qualquer restrição para que o usuário pertença ao grupo RF1. Todos os usuários que acessam o RF-B2B têm acesso às funcionalidades que este grupo tem permissão, independentemente da empresa, filial ou função. O grupo RF2 possui apenas a restrição de que o usuário possua a função especificada. Com isto, todos os usuários que possuam esta função têm acesso às funcionalidades que estes grupos têm permissão, independentemente da empresa ou filial. Os grupos RF3 e RF4 não possuem restrição com relação à filial que um usuário pertence. Para o usuário pertencer a um destes grupos é necessário que ele possua uma das respectivas funções e que seja funcionário da *Puma Motors.*

Na *Puma Motors* houve a necessidade de os usuários com função de "Gestor de Contratos" tivessem diferentes permissões que variavam de acordo com as filiais a que pertenciam. Isto porque as leis de contratos variam em cada país. Por isto a necessidade de se criar os grupos cujas restrições levassem em consideração estes três fatores.

Caso um usuário da *Puma Motors* seja transferido, por exemplo, da filial do México para a filial da Rússia, seu grupo será automaticamente modificado do RF6 para

o RF7. Os grupos posteriores já pertencem a outras empresas parceiras da *Rodas Forte.* Esta tabela na realidade possui um tamanho muito superior ao apresentado. Seus dados foram resumidos de forma a apenas ilustrar seu funcionamento.

5.2. Funcionamento

O usuário José Silva trabalha na filial do México da *Puma Motors*. Para poder trocar informações com a *Rodas Forte* ele deve, primeiramente, estar autenticado na *extranet* do sistema central da *Puma Motors*. Posteriormente José Silva deve autenticar-se novamente, mas agora no RF-B2B, para então ser possível a troca de informações.

No processo de autenticação, é verificado primeiramente se o IP de origem do pedido de autenticação é o mesmo que está relacionado à *Puma Motors*, cadastrado no RF-B2B. Este é o processo de autenticação do sistema cliente adotado pelo RF-B2B. Em caso positivo é liberado o processo de autenticação de José Silva. Quando o processo de autenticação do sistema central da *Puma Motors* é finalizado sem erros, o sistema de controle de acesso do RF-B2B inicia então o processo de busca das permissões as quais José Silva tem acesso.

Primeiramente é verificado, baseando-se nos atributos de José Silva, a quais grupos do AIP ele pertence. Definido os grupos, é então feita uma busca pelas permissões de acesso as quais estes grupos têm acesso. Estas permissões são alocadas na memória do sistema, para posteriormente serem acessadas pelo Filtro de Autorização e Obrigação enquanto José Silva estiver utilizando o sistema.

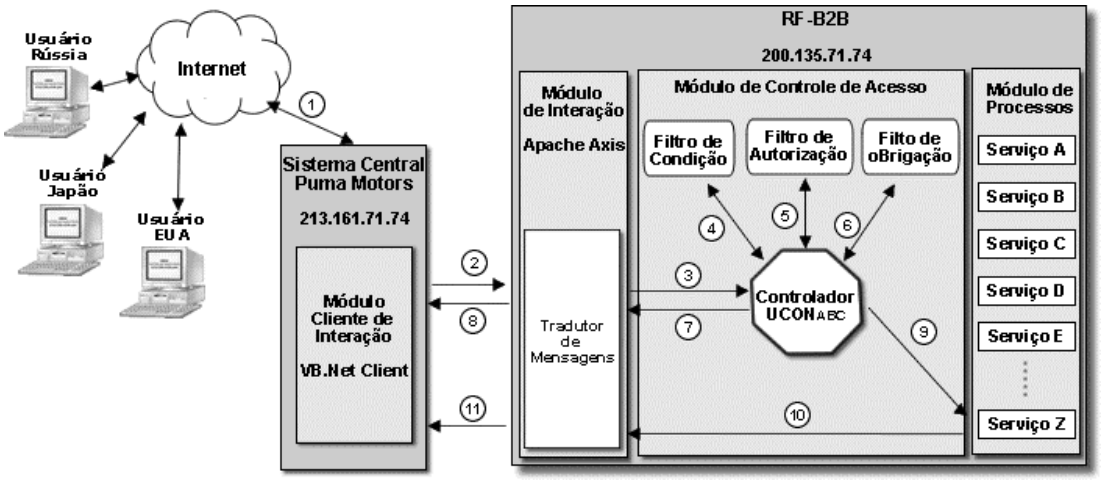

Figura 6: Controle de Aceso entre Puma Motors e Rodas Forte

De acordo com a figura 6, quando José Silva deseja realizar um pedido de produtos, ele envia uma solicitação via HTTP para a *extranet* da *Puma Motors* (passo 1). O Módulo Cliente de Interação recebe esta solicitação e se encarrega de encaminhá-la para o RF-B2B (passo 2). O Módulo de Interação do RF-B2B recebe esta solicitação pelo *Webservice* e a traduz para a tecnologia do RF-B2B. Em seguida, a solicitação é enviada para o Controlador $UCON_{ABC}$ (passo 3), que verifica as regras de condição, autorização e obrigação do RF-B2B através de seus respectivos filtros (passos 4, 5 e 6). O filtro de condição analisa o endereço IP 213.161.77.151, que é proveniente do sistema da *Puma Motors*. Além disto, este filtro analisa os horários a que José Silva têm direito de acesso no RF-B2B. O filtro de autorização analisa as permissões que correspondem

ao grupo a que o José Silva pertence. O filtro de obrigação analisa a necessidade do fornecimento de uma senha crítica para a execução de um determinado serviço.

Caso a solicitação passe pela verificação de todos os filtros o acesso ao serviço de pedidos é liberado (passo 9). Após ser acessado e executado, o serviço de pedidos de produtos retorna ao Módulo de Interação um valor lógico do tipo verdadeiro/falso informando do sucesso ou fracasso da operação (passo 10). Após converter o valor de retorno em uma mensagem, o Módulo de Interação do RF-B2B a envia para o sistema da *Puma Motors* (passo 11) que, por sua vez traduz novamente o conteúdo para a tecnologia ASP/.Net e exibe a resposta para José Silva através de sua *extranet*.

6. Conclusão

Diversas estratégias para controle de acesso têm sido propostas há algumas décadas e vêm crescendo e melhorando de acordo com as necessidades exigidas pelas inovações tecnológicas. O $UCON_{ABC}$ é um modelo promissor por lidar com aspectos do controle de acesso até então ignorados pelos modelos tradicionais. No entanto, pelo fato de sua apresentação para a comunidade científica ser recente, não existem estudos práticos sobre a aplicabilidade de seus conceitos em sistemas do mundo real.

Os trabalhos relacionados se restringem a definir um esquema, *framework* ou técnica de controle de acesso para sistemas de CE B2B, ou então vincular um modelo de controle de acesso a uma ferramenta específica. Este trabalho diferencia-se dos demais por definir, como principal contribuição científica, uma forma de aplicação do modelo $UCON_{ABC}$ em sistemas de CE B2B que interagem entre si. Com isso, tornou-se mais fácil a visualização de como é possível aplicar o $UCON_{ABC}$ em sistemas onde é necessária uma interação, independentemente da tecnologia de interação utilizada.

A necessidade de se definir maneiras eficientes de implementar o controle de acesso neste tipo de sistema é justificada pelo fato da interação possibilitar que usuários externos acessem informações de uma empresa pelo intermédio de outros sistemas.

O AI proposto por [Goodwin, Goh & Wu, 2002] é uma forma de gerenciamento de permissão definida para as necessidades específicas de sistemas de CE B2B. No entanto, observou-se que o agrupamento de objetos desta técnica gera uma sobrecarga administrativa desnecessária. Sendo assim, foi sugerida a criação do AIP como gerenciamento de permissões na proposta de aplicação do $UCON_{ABC}$ em sistemas B2B. A pesquisa e análise de modelos, a explicação do AI utilizando exemplos e formas diferentes de ilustração, o levantamento de desvantagens do AI e a sugestão do AIP são também contribuições científicas deste artigo.

O estudo de caso entre empresas parceiras da indústria automobilística contribuiu para o melhor entendimento da aplicabilidade da proposta deste artigo.

A proposta da forma de aplicação do $UCON_{ABC}$ em sistemas de CE B2B foi a principal contribuição científica deste artigo. Foi feita uma pesquisa para encontrar qual a melhor forma de se gerenciar as autorizações. O Agrupamento Implícito Parcial foi escolhido como forma de gerenciar as autorizações.

Para trabalhos futuros é sugerida uma análise comparativa da forma de aplicação do $UCON_{ABC}$ em sistema B2B, proposta por este artigo, com a pesquisa que utilize o Gerenciamento de Confiança.

Referências

Blaze, M.; Feigenbaum, J. e Lacy, J. (1996) "Decentralized Trust Management", em Proceedings of the 1996 IEEE Symposium on Security and Privacy. p. 164. ISBN:0-8186-7417-2 Publisher: IEEE Computer Society Press. Washington, DC, USA.

Blodget, H.; McCabe, E. (2000) "The B2B Market Maker Book: Indepth Report", Acessado em 20 de Novembro de 2004, http://www.visi.com/~keefner/pdfs/ml020700.pdf, Merrill Lynch and Company.

Dabous, F.; Rabhi, F.; Ray, P. (2003) "Middleware Technologies for B2B Integration", em Annual Review of Communications. ISBN:1-931695-22-9. Vol. 56, International Engineering Consortium.

Essmayr, W.; Probst, S. & Weippl, E. (2004) "Role-Based Access Controls: Status, Dissemination, and Prospects from Generic Security Mechanisms". Electronic Commerce Research. ISSN: 1389-5753. Vol 4, nº 1-2, P. 127-156. Áustria.

Goodwin, R; Goh, S.; Wu, F. (2002) "Instance-level access control for business-to-business electronic commerce". IBM Systems Journal, Vol. 41, Nº 2, p. 303 - 317.

Kraft, R. (2002) "Designing a distributed access control processor for network services on the Web", em: ACM workshop on XML security. p. 36-52, ISBN: 1-58113-632-3. ACM Press, New York, NY, USA.

Liu, Q. et. All (2003) "Digital Rights Management for Content Distribution", em: Australasian Information Security Workshop Conference, ACM. Vol. 21, p. 49-58, ISBN ~ ISSN:1445-1336 , 1-920682-00-7. Adelaide, Austrália.

Medjahed, B. et. All (2003) "Business-to-Business interactions: issues and enabling technologies**",** em The VLDB Journal — The International Journal on Very Large Data Bases. ISSN:1066-8888. Vol. 12, p. 59-85. Springer-Verlag, New York.

Park, J. e Sandhu R. (2002) "Towards Usage Control Models: Beyond Traditional Access Control", em SACMAT - Proceedings of the Seventh {ACM} Symposium on Access Control Models and Technologies. p. 57 – 64, New York – USA.

Park, J (2003) "*Usage Control: A Unified Framework for Next Generation Access Control*". 155 f. Tese de Doutorado em Tecnologia da Informação - Universidade George Mason. Virginia – USA.

Park, J. e Sandhu R. (2004) "The UCONABC Usage Control Model", To appear in Proceedings of 9th ACM Symposium on Access Control Models and Technologies.

Quix, C.; Schoop, M. e Jeusfeld, M. (2002) em "Business Data Management for Business-to-Business Electronic Commerce.", SIGMOD. Vol 31, Nº 1, p. 49 – 54.

Radowiisky, Z. (2002) "Business-to-Business E-Commerce And Enterprise Resource Planning: Increasing Value in Supply Chain Management". Em Proceeding of the 87th Annual International Supply Management Conference, Institute of Supply Management. São Francisco – USA.

Robison, L. (2002) "Implementing Security in B2B Applications". Implementing B2B Commerce with .NET: A Guide for Programmers and Technical Managers. Capítulo 7, ISBN: 0201719320, Edição 1, Ed.: Addison Wesley Professional. Obtido em: http://www.awprofessional.com/articles/article.asp?p=27143.

Sandhu, R. (2001). "Future Directions in Role-Based Access Control Models". International Workshop on Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security. ISBN:3-540-42103-3. Vol. 2052, p. 22 – 26, London – UK.