Segurança Multilateral e RBAC para Gerência de Contabilidade em Sistemas Distribuídos

Luis Marco Cáceres Alvarez[1], Carlos Becker Westphall[1], Carla Merkle Westphall[1]

[1]Laboratório de Redes e Gerência – Universidade Federal de Santa Catarina
Caixa Postal 476 – Florianópolis – SC – Brasil

{caceres, westphal, carla}@lrg.ufsc.br

Abstract. *This work of research has as objective to consider a model that allows answer the questions of security in a Distributed System environment. This security model is mainly related with the real time accounting management using multiple users and multiple suppliers, where the security aspects are related with the policies and mechanisms considered by Multilateral Security and RBAC (Role-Based Access Control) models. The models was validated through the use of the LOTOS of Formal Description Technique and also for the development of a prototype.*

Resumo. *Este trabalho de pesquisa tem como objetivo propor um modelo que permita responder as questões de segurança em um ambiente de Sistemas Distribuídos. Este modelo de segurança está principalmente relacionado com o gerenciamento de contabilidade em tempo real para múltiplos usuários e múltiplos provedores, onde os aspectos de segurança estão relacionados às políticas e mecanismos propostos pelos modelos de Segurança Multilateral e RBAC (Role-Based Access Control). O modelo foi validado através do uso da técnica de descrição formal LOTOS e também pela implementação de um protótipo.*

1. Introdução

Na atualidade, serviços mais complexos precisam de funcionalidades de gerenciamento que permitam uma rápida, confiável e cuidadosa troca de informações entre os fornecedores e consumidores dos serviços. Nesse sentido, TINA (*Telecommunications Information Networking Architecture*) especifica a Arquitetura de Gerenciamento de Contabilidade que permite oferecer um gerenciamento de contabilidade consistente e que garante uma contabilidade confiável através de um serviço distribuído em um ambiente multi-domínio, onde o aspecto de segurança é parte essencial para a proteção das informações contábeis contra usuários maliciosos ou fornecedores mal intencionados, o que é um fator crítico em TINA e em sistemas distribuídos [Hamada 1996].

Nesse contexto é que surgiu a idéia deste trabalho, o qual tem como objetivo propor um modelo de segurança para o gerenciamento de contabilidade em sistemas distribuídos, que permita solucionar estes fatores críticos através de políticas e mecanismos de segurança propostos pelos modelos da Segurança Multilateral e de Controle de Acesso baseado em Papéis (RBAC). Desse modo, para o estabelecimento de uma sessão de serviço TINA, que define os processos de acesso e de uso [Kristiansen 1997], entre um consumidor e um fornecedor, deve ser permitida uma negociação das características de segurança de ambos processos através dos mecanismos do modelo de

Segurança Multilateral, durante o processo de acesso, e a definição de papéis através do modelo RBAC, durante o processo de uso do serviço.

Observou-se que vários trabalhos correlatos nesta linha de pesquisa estão sendo realizados, como [Hwang 2004], [Le 2004], [Agarwal 2004], [Pilz 2004], [Hamada 2004], [Koutepas 2004], [Kelley 2004] e [Thaler e Ravishankar 2004]. Estes trabalhos abordam aspectos de contabilidade e de segurança em um ambiente distribuído para o fornecimento de serviços em tempo real. A comparação e contribuição do nosso trabalho de pesquisa em relação aos trabalhos correlatos mencionados estão amparadas, diretamente, na arquitetura utilizada para o gerenciamento de contabilidade, através dos princípios e padrões TINA, assim como também nas políticas de segurança definidas em um contexto de gerenciamento de serviço TINA, através dos modelos de segurança multilateral e RBAC. No entanto, deve-se salientar que esta linha de pesquisa desenvolvida no Laboratório de Redes e Gerência (LRG), apresentou vários resultados parciais anteriormente publicados, tais como: [Alvarez 2001], [Sekkaki 2001] e [Westphall 2003].

Este artigo está organizado da seguinte forma: a seção 2 apresenta uma visão geral da arquitetura TINA; a seção 3 apresenta o conceito de segurança no gerenciamento de contabilidade TINA e os modelos de Segurança Multilateral e RBAC; a seção 4 descreve o modelo de segurança proposto; a seção 5 mostra a especificação e validação formal do modelo de segurança. Finalmente, a seção 6 apresenta o protótipo implementado e a seção 7 as conclusões.

2. Visão Geral da Arquitetura TINA

2.1. A Arquitetura de Serviço TINA

TINA define uma estrutura flexível que consiste de vários conceitos e especificações de modelos, tais como: arquitetura de serviço apresentada em [Kristiansen 1997], as principais especificações que envolvem o modelo de negócios [Mulder 1997], o modelo computacional e a especificação de componentes de serviço [Farley 1998] e a arquitetura de gerenciamento de contabilidade [Hamada 1996].

No modelo de negócios os componentes em um serviço são caracterizados dentro de cinco grupos de acordo com as funções que eles realizam no serviço. As funções definidas dentro de TINA são: Consumidor, Provedor, Provedor de Serviço Terceirizado, Provedor de Conectividade e Intermediador. As funções do Intermediador e Provedor de Serviço Terceirizado não são descritos em detalhe em TINA. Entretanto, as funções do Consumidor, Provedor e Provedor de Conectividade foram especificadas com bastante detalhes em TINA, incluindo as interfaces. As interfaces entre os componentes são definidas como Pontos de Referência. O ponto de referência mais importante para o gerenciamento de serviço é o ponto de referência *Ret* [Abarca 1997], definido entre o Consumidor e Provedor.

A arquitetura de serviço também define dois tipos de sessões, uma é a sessão de acesso e outra é a sessão de serviço. A sessão de acesso é responsável pela identificação e autenticação do usuário. Esta também é usada para disponibilizar serviços e executar os serviços criando assim uma sessão de serviço. A sessão de serviço é responsável pelo gerenciamento das condições do serviço e também pela criação e controle da conexão de fluxo, que é uma representação abstrata da conexão fim-a-fim entre as aplicações. O modelo do subsistema de assinatura e o modelo de informação de assinatura definidos

em TINA permitem a um usuário descobrir novos serviços e eventualmente assinar estes serviços [Mampaey e Couturier 2000].

2.2. A Arquitetura de Contabilidade TINA

O gerenciamento de contabilidade TINA consiste de quatro ciclos chamados de Medição, Classificação, Tarifa e Cobrança. O gerenciamento de contabilidade TINA apresenta o conceito de Contexto de Gerenciamento de Contabilidade (AcctMgmtCtxt-*Accounting Management Context*) associado com a Transação de Serviço (ST-*Service Transaction*). O propósito do AcctMgmtCtxt é garantir que a contabilidade seja preservada através de um conjunto de atividades de objetos distribuídos, o qual constitui o serviço. É necessário enfatizar que a contabilidade não é uma propriedade ou um atributo de um simples objeto. A contabilidade pode ser vista como um conjunto de quantidades medidas ou calculadas sobre um conjunto de atividades de objetos distribuídos durante todo o serviço. Enquanto que um ST é ativado por um Gerente de Sessão de Serviço (SSM-*Service Session Manager*), seu AcctMgmtCtxt é interpretado de acordo com sua descrição do componente de sessão (unidade de serviço a ser contabilizada) e com a estrutura de tarifa (*Tariffing*) dentro do componente SSM. Então, o SSM passa o controle e parâmetros necessários para os mecanismos de recursos ou mecanismos computacionais tais como: Gerente de Sessão de Comunicação (CSM–*Communication Session Mana*ger), servidor de notificação, gerente de métrica e gerenciamento de serviço [Hamada 1996].

3. Segurança do Gerenciamento de Contabilidade para TINA

Para o gerenciamento de contabilidade a segurança em contabilidade consiste de um serviço garantido, confiável e de informações contábeis integradas. Desse modo:

- **Contabilidade garantida**, refere-se às transações de serviço que devem oferecer mecanismos que garantem a integridade dos serviços. Isto significa que "você não paga se seu serviço contratado não foi fornecido".
- **Contabilidade confiável**, significa que a informação contábil deve ser confiável, adequadamente registrada e segura. Desse modo, o usuário e provedor de serviço devem estar devidamente protegidos.
- **Integridade da informação contábil**, refere-se que a informação deve ser preservada no caso de ocorrência de falhas (falhas de comunicação na rede, interrupção do serviço, etc), considerando que o serviço é transportado sobre diferentes domínios de gerenciamento [Hamada 1996].

Para garantir estes conceitos de segurança em TINA, definidos anteriormente, pretende-se implementar estratégias e políticas de segurança, aplicando os conceitos de Segurança Multilateral e Controle de Acesso Baseado em Papéis (RBAC), de forma a realizar uma abordagem consistente, flexível e segura para o gerenciamento de serviços de telecomunicações TINA.

3.1. O Modelo de Segurança Multilateral

A segurança multilateral tem por objetivo fornecer segurança para todos os participantes envolvidos, requerendo de cada participante um mínimo de confiança na honestidade dos outros participantes envolvidos. Segundo [Pfitzmann 2002]: cada participante tem

seus objetivos de proteção particulares; cada participante pode formular seus objetivos de proteção; conflitos de segurança são reconhecidos e os compromissos negociados; e cada participante pode reforçar seus objetivos de proteção dentro do compromisso negociado.

A segurança multilateral não possibilita necessariamente que todos os participantes possam reforçar seus objetivos de segurança individuais, mas ao menos ela provê a transparência de todas as ações relacionadas à segurança de todos os participantes envolvidos.

3.1.1. Aplicando Segurança Multilateral no Processo de Acesso

Para o processo de acesso será criado o conceito do Contexto de Gerenciamento de Segurança Multilateral (SecMgmtCtxt – *Security Management Context*) que irá permitir a coordenação de todo o comportamento da Transação de Serviço com relação aos interesses de segurança definidos para um determinado SecMgmtCtxt. A Figura 1 mostra a estrutura do SecMgmtCtxt, muito semelhante ao do AcctMgmtCtxt (como definido em [Hamada 1996]), tendo o mesmo domínio e tempo de vida. A estrutura do SecMgmtCtxt é constituída pelos seguintes componentes:

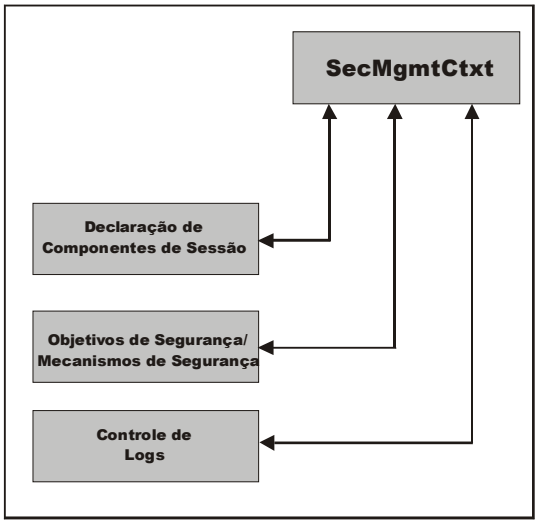

Figura 1. O Modelo do *SecMgmtCtxt*.

- **Declaração dos Componentes de Sessão**: a função desta parte é declarar quais componentes de sessão estão disponíveis ao usuário, quais são os componentes que já possuem uma relação segura e o nível de segurança que foi estabelecido com um determinado componente.
- **Objetivos de Segurança/Mecanismos de Segurança**: discrimina qual objetivo de segurança o participante negociou. Também descreve quais mecanismos de segurança foram adotados para se efetivar os objetivos de segurança desejados.
- **Controle de *Logs***: registra informações de eventos que ocorram durante a existência do *SecMgmtCtxt* para fins de auditoria. Estas informações podem ser o tipo de acesso que foi associado a um determinado objeto, quem acessou o objeto ou quem modificou o objeto.

Estes interesses de segurança serão previamente definidos entre os participantes. Como a segurança multilateral possibilita a negociação dos interesses de segurança, ao

menos os limites mínimos de segurança dos participantes devem estar definidos antes mesmo de qualquer negociação.

Quando for necessário o estabelecimento de uma sessão de comunicação entre dois participantes (entre um consumidor e um provedor, por exemplo) é verificado se ambos os participantes pertencem ao mesmo Domínio de Gerência. Se eles pertencerem ao mesmo domínio, a sessão é estabelecida normalmente, caso contrário, os participantes fazem parte de Domínios de Gerência distintos e, conseqüentemente, de Domínios de Segurança distintos. Neste último caso, a negociação dos objetivos de segurança é necessária. O Agente de Segurança (AS – *Security Agent*) será o responsável por esta negociação que pode terminar com sucesso e a sessão de comunicação estabelecida ou por um erro, caso não seja possível negociar um conjunto mínimo de objetivos de segurança.

3.2. O Modelo de Segurança RBAC

O termo Controle de Acesso Baseado em Papéis (RBAC – *Role-Based Access Control*) é utilizado para descrever mecanismos de segurança que controlam o acesso de usuários a recursos computacionais, baseado na construção de papéis. Esses papéis definem um conjunto de atividades concedidas para usuários autorizados. Pode-se imaginar um papel como se fosse um cargo ou posição dentro de uma organização, que representa a autoridade necessária para conduzir as tarefas associadas [Jansen 1998].

Com RBAC, a segurança é gerenciada em um nível muito próximo à estrutura da organização. Cada usuário está associado a um ou mais papéis, e cada papel está associado a um ou mais privilégios, que são concedidos aos usuários daquele papel. Os papéis podem possuir hierarquia [Ferraiolo 1999].

Em uma abordagem de segurança no gerenciamento de serviço de telecomunicações, um dos problemas mais importantes é o *billing*. Em um ambiente de serviço multimídia, é necessário o *billing on-line*, já que o usuário é capaz de correlacionar sua carga de uso/serviço de recurso de rede com seu preço em tempo real. Para isto ser possível, o provedor do serviço necessita enviar relatórios de *billing* diretamente para a interface do usuário [HAMADA 1998].

3.2.1. Aplicando RBAC no Processo de Uso

Finalizada a primeira fase de negociação que corresponde a uma relação de segurança definida pelo SecMgmtCtxt, será então necessário definir a relação de segurança que deve ser estabelecida para o processo de uso. Neste processo será criado o conceito do Contexto de Gerenciamento de Controle de Acesso Baseado em Papéis – RBACMgmtCtxt, que permitirá definir e coordenar os papéis para um serviço com *billing on-line* no Contexto de Gerenciamento de Contabilidade. A estrutura será definida dinamicamente, similarmente ao AccMgmtCtxt, tendo o mesmo domínio (domínio Provedor) e tempo de vida. A estrutura do RBACMgmtCtxt é constituída pelos seguintes componentes como mostra a Figura 2.

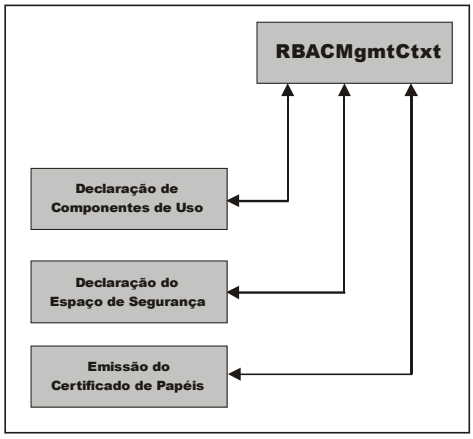

Figura 2. O Modelo do *RBACMgmtCtxt*.

- **Declaração dos Componentes de Uso**: a função desta parte é declarar quais componentes de uso estão disponíveis ao usuário, quais serviços o provedor fornece em um ambiente de serviço multimídia com *billing on-line*, onde os recursos de rede fornecidos pelo serviço relacionado a um usuário devem ser em tempo real. Também se incluem relatórios *billing* para a interface do usuário.
- **Declaração do Espaço de Segurança**: como uma sessão de serviço estende-se por múltiplos domínios, se faz necessário definir um espaço de segurança que permita definir as classes de papéis de forma dinâmica, através de objetos e interfaces. Nesta etapa se definem as chaves do espaço de segurança as quais representam interesses de segurança para cada participante, usuário-provedor. A atribuição destas chaves para definir o espaço de segurança dos participantes dos serviços é estabelecida através da etapa de negociação pelo protocolo SSL (*Socket Service Layer*) usando os certificados X.509.
- **Certificado de Papéis**: o certificado de papel atribuído ao usuário assegura o uso do serviço solicitado ao provedor, cuja definição é estabelecida através da declaração dos componentes de uso.

Desse modo, definido o espaço de segurança através das chaves obtidas e associadas especificamente pelo protocolo SSL, pode-se atribuir os papéis por meio do certificado de papéis que é responsabilidade do componente ACA (*Access Control Agent*) no contexto RBACMgmtCtxt. Este componente interage diretamente com o USM (*User Service Session Manager*) definido para o usuário e gerenciado pelo componente SSM (*Service Session Manager*), para a emissão do certificado pelo provedor para o consumidor via o componente UAP (*User Application*) no domínio do consumidor. Este certificado permitirá definir o papel do usuário no serviço e que relaciona seu objeto *billing on-line* para estabelecer a coleta de dados contáveis que interagem com o contexto AccMgmtCtxt definido no gerenciamento de contabilidade TINA para um ambiente de serviço multi-provedor e multi-usuário em tempo real.

4. Descrição do Modelo de Segurança no Gerenciamento de Contabilidade TINA

O modelo se segurança da arquitetura de contabilidade SSGCT – Sistema de Segurança do Gerenciamento de Contabilidade TINA - é apresentado na Figura 3.

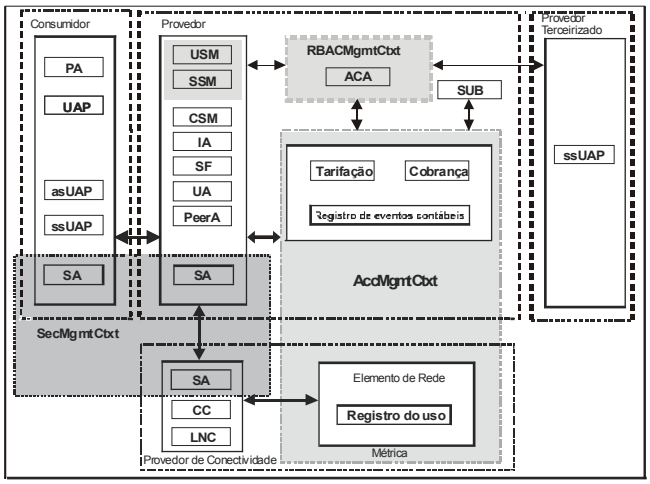

Figura 3. Modelo de Segurança para o SSGCT.

Visualizam-se os domínios que correspondem ao consumidor (quem solicita um tipo de serviço), ao provedor (quem fornece o serviço ao consumidor e gerencia a contabilidade do serviço) e ao provedor terceirizado (que fornece o serviço solicitado pelo provedor), com seus respectivos componentes, interfaces com os componentes de cada domínio e os contextos de contabilidade e de segurança.

Segundo [Le 2002], deve-se verificar e validar corretamente o modelo estrutural e comportamental da arquitetura de contabilidade, para garantir a correta interação entre os componentes do sistema, usando: uma Linguagem de Descrição Formal, como LOTOS; e a implementação de um protótipo de forma a validar o modelo proposto através de uma simulação de serviços oferecidos pelo fornecedor, em um ambiente de gerenciamento de contabilidade em tempo real, que demonstrará como são estabelecidas as políticas de segurança na fase de negociação usando o modelo de segurança multilateral e a fase de uso do serviço usando o modelo RBAC, que definirá um contexto dinâmico para os papéis do serviço disponíveis ao consumidor com *billing on-line*.

5. Especificação e Validação Formal do Modelo de Segurança

Esta seção apresenta a especificação e validação formal do modelo proposto (Figura 3) através da Técnica de Descrição Formal (TDF) padrão ISO 8807-LOTOS - *Language of Temporal Ordering Specification* [Brinksma 1988]. O principal objetivo do emprego desta técnica de alto rigor matemático é fornecer a prova formal de correções do sistema.

O modelo de segurança SSGCT apresentado é especificado formalmente, utilizando-se uma abordagem de refinamentos sucessivos [Vissers 1988], a qual permite validar seu desenvolvimento até sua especificação formal final. A validação do sistema utilizou a última versão beta da ferramenta *Eucaliptus ToolSet* 2.5/CADP 2003-e [Garavel 2004] em ambiente Linux versão RedHad 8.0.

5.1. Especificação dos Serviços SSGCT

A seguir serão descritas, passo a passo, as especificações dos serviços SSGCT, começando de um alto nível de abstração até a definição da especificação formal do modelo de segurança para um gerenciamento de contabilidade TINA.

5.1.1. Especificação Geral

No nível mais alto de abstração, o sistema SSGCT pode ser visto como uma caixa preta, formada pelos domínios Consumidor (*Consumer*) e Provedor (*Retailer*). As duas portas de comunicação entre os domínios são definidas de acordo com o ponto de referência padrão no modelo de negócios TINA, denominado Ret-RP (*Retailer Reference Point*) que estabelece as portas de **acesso** e **uso**, como mostra a Figura 4.

A definição do ponto de referência é uma especificação semi-formal do relacionamento de negócios entre o papel de negócio Consumidor e o papel de negócio Provedor. O Ret-RP é separado em duas partes: de acesso e de uso, as quais definem um alto grau de abstração às portas de comunicação.

Para o Ret-RP, a parte de acesso permite descrever como o papel de negócio Consumidor acessa um papel de negócio Provedor para fazer uso dos serviços por ele fornecido; a parte de uso descreve as interações entre os papéis de negócios envolvidos durante o uso de um serviço. Cada parte é controlada independentemente [Farley 1998] A independência destas partes (para fins do caso de estudo denomina-se portas) permite definir os contextos de segurança e de contabilidade também de forma independente, permitindo que os contextos de segurança sejam criados num ambiente sem possibilidade de incompatibilidade com respeito as políticas de segurança, como definidas nos itens 3.1.1 e 3.2.1.

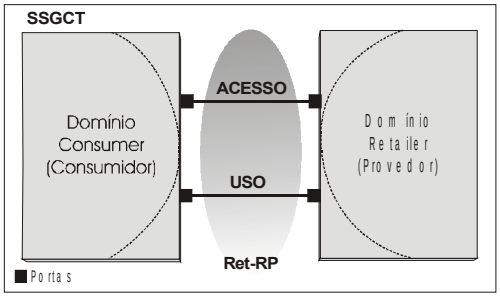

Figura 4. Representação em Alto Nível do SSGCT.

Desse modo a porta de acesso é utilizada para fazer uso de serviços e de negociação dos mecanismos de segurança dos domínios Consumidor e Provedor. A porta de uso que permite usar o serviço selecionado previamente definindo os papéis dentro do contexto RBAC, disponibilizando um contexto de gerenciamento de contabilidade com *billing on-line* confiável e em tempo real. O comportamento do sistema definido através da especificação LOTOS é descrito a seguir:

```
specification SsgctService [acesso, uso] : noexit behaviour
        processo [acesso, uso]
where
    process processo [acesso, uso] : noexit :=
        acesso; uso; processo [acesso, uso]
    endproc

endspec
```

O comportamento do sistema SSGCT é definido pelo processo *SsgctService*, o qual executa uma ação na porta de acesso, para permitir a negociação dos contextos de segurança e de serviço. A segunda ação acontece na porta de uso e é realizada após a ação na porta de acesso. A ação na porta de uso permitirá definir os papéis relacionados ao tipo de serviço que está sendo fornecido para estabelecer um *billing on-line*. A

primeira ação pode ser chamada recursivamente pelo fato de que um Consumidor pode acessar mais de um serviço, podendo estabelecer um outro contexto.

A especificação do nível de abstração do SSGCT corresponde a uma formalização das solicitações de uso de serviço entre o Consumidor e o fornecimento do serviço do Provedor. A partir desta especificação inicial deverão ser realizados sucessivos refinamentos para utilizá-los como prova da correção da especificação final do sistema.

5.1.2 Especificação Formal da Arquitetura Geral do Modelo SSGCT

O modelo da Figura 5 apresenta a arquitetura geral, na qual estão representado o domínio de negócio do Consumidor e Provedor com seus respectivos componentes e interfaces de acordo com os padrões de TINA. Neste modelo é incorporado o contexto de gerenciamento de segurança multilateral (*SecMgmtCtxt*), para estabelecer a negociação das políticas de segurança entre os domínios através do processo de acesso, o contexto de segurança RBAC (*RBACMgmtCtxt*), para estabelecer o espaço de segurança para a definição dos certificados de papéis para um determinado tipo de serviço com seu respectivo *billing on-line* e o contexto de contabilidade (*AcctMgmtCtxt*), que permite garantir um gerenciamento da contabilidade consistente e confiável durante o fornecimento do serviço em tempo real.

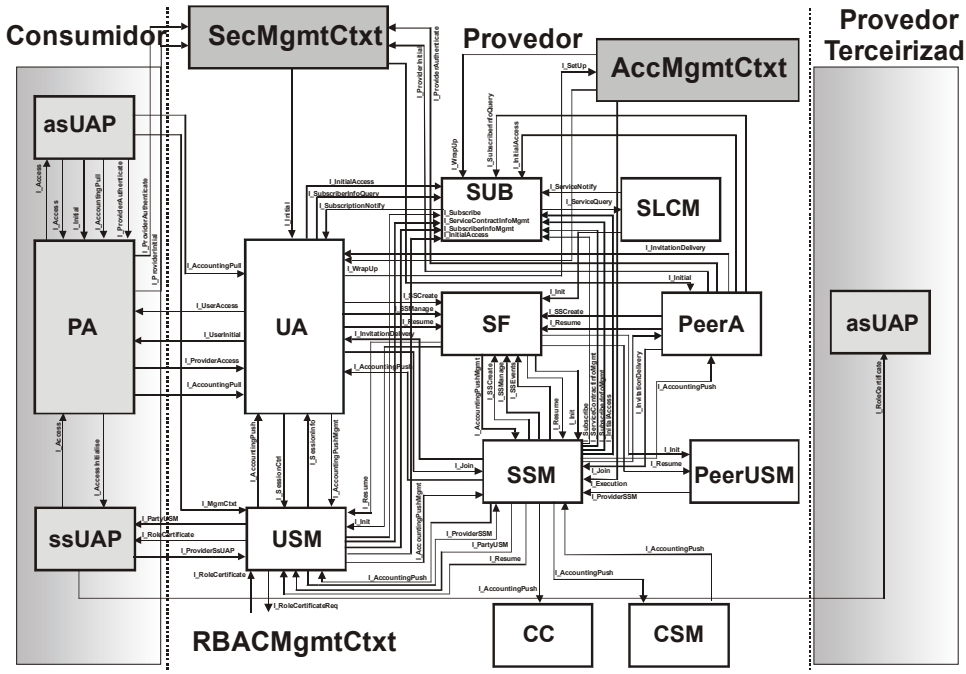

Figura 5. Diagrama Geral do SSGCT.

A arquitetura representada na Figura 5 pode ser definida em LOTOS através da especificação formal descrita a seguir:

```
specification SsgctProtocol [i_Initial1, i_ProviderInitial1, i_ProviderInitial2, i_ProviderAuthenticate1, i_ProviderAuthenticate2,
                i_ProviderAuthenticate3, i_Initial2, i_Access1, i_ProviderAccess, i_SSCreate1, i_Init1, i_Init2, i_ProviderSSM,
                i_ProviderssUAP, i_RoleCertificateReq, i_RoleCertificate1, i_RoleCertificate2,i_RoleCertificate3, i_UserInitial, i_UserAccess,
                i_Access2, i_AccountingPull1, i_AccountingPull2, i_MgmtCtxt, i_AccountingPull3, i_Execution, i_AccountingPush1,
                i_AccountingPush2, i_AccountingPush3, i_AccountingPush4, i_AccountingPush5, i_AccountingPush6, i_AccountingPush7,
                i_AccountingPushMgmt1, i_AccountingPushMgmt2, i_AccountingPushMgmt3, i_SessionCtrl, i_PartyUSM_1, i_SessionInfo,
                i_SSManage1, i_SSManage2, i_Resume1, i_Resume2, i_Resume3, i_Resume4, i_Resume5, i_Resume6, i_PartyUSM2,
                i_InvitationDelivery1, i_InvitationDelivery2, i_InvitationDelivery3, i_Join1, i_Join2, i_SSCreate2, i_SSEvents,
i_InitialAccess1,
                i_InitialAccess2, i_InitialAccess3, i_InitialAccess4, i_SubscriberInfoQuery1, i_SubscriberInfoQuery2, i_Subscribe1,
                i_Subscribe2, i_ServiceContractInfoMgmt1, i_SubscriberInfoMgmt1, i_ServiceContractInfoMgmt2, i_SubscriberInfoMgmt2,
                i_SubscriptionNotify, i_ServiceQuery, i_ServiceNotify, i_WrapUp1, i_WrapUp2] : noexit
behaviour
          hide i_RoleCertificateReq, i_RoleCertificate1, i_RoleCertificate2, i_RoleCertificate3 in modeloSsgct […]
where
     process modeloSsgct […] : noexit :=
          SecMgmtCtxt [i_Initial1, i_ProviderInitial1, i_ProviderInitial2, i_ProviderAuthenticate1,
            i_ProviderAuthenticate2, i_ProviderAuthenticate3, i_Initial2, i_ProviderAccess]
            >>
          RBACMgmtCtxt [i_Access1, i_ProviderAccess, i_SSCreate1, i_Init1, i_Init2, i_ProviderSSM, i_ProviderssUAP,
            i_RoleCertificateReq, i_RoleCertificate1, i_RoleCertificate2, i_RoleCertificate3]
            >>
          AccMgmtCtxt [i_UserInitial, i_UserAccess, i_Access2, i_AccountingPull1, i_AccountingPull2, i_MgmtCtxt,
            i_AccountingPull3, i_Execution, i_AccountingPush1, i_AccountingPush2, i_AccountingPush3, i_AccountingPush4,
            i_AccountingPush5, i_AccountingPush6, i_AccountingPush7, i_AccountingPushMgmt1,i_AccountingPushMgmt2,
            i_AccountingPushMgmt3, i_SessionCtrl, i_PartyUSM_1, i_SessionInfo, i_SSManage1, i_SSManage2, i_Resume1,
            i_Resume2, i_Resume3, i_Resume4, i_Resume5, i_Resume6, i_PartyUSM2, i_InvitationDelivery1, i_InvitationDelivery2,
            i_InvitationDelivery3, i_Join1, i_Join2, i_SSCreate2, i_SSEvents, i_InitialAccess1, i_InitialAccess2, i_InitialAccess3,
            i_InitialAccess4, i_SubscriberInfoQuery1, i_SubscriberInfoQuery2, i_Subscribe1, i_Subscribe2, i_ServiceContractInfoMgmt1,
            i_SubscriberInfoMgmt1, i_ServiceContractInfoMgmt2, i_SubscriberInfoMgmt2, i_SubscriptionNotify, i_ServiceQuery,
            i_ServiceNotify, i_WrapUp1, i_WrapUp2]
        where
            process SecMgmtCtxt […]      endproc
            process RBACMgmtCtxt […]     endproc
            process AccMgmtCtxt […]      endproc
        endproc
endspec
```

A especificação formal após os refinamentos para os diferentes contextos (*SecMgmtCtxt*, *RBACMgmtCtxt* e *AccMgmtCtxt*) que formam os processos do sistema SSGCT através da especificação *SsgctProtocol*, definem-se os operadores **hide** *i_RoleCertificateReq, i_RoleCertificate1*, *i_RoleCertificate2*, *i_RoleCertificate3* ..**in** *modeloSsgct*[...] com o objetivo de ocultar as portas aos usuários de um serviço contra o uso desonesto ou violações dos certificados definidos pelo provedor e o operador de habilitação de processos >> que vai permitir executar um processo com sucesso através do processo predefinido **exit**. Neste caso, o processo *SecMgmtCtxt* deve terminar com sucesso para que o processo *RBACMgmtCtxt* possa ser executado, e este por sua vez deve terminar com sucesso para executar o processo *AccMgmtCtxt*. Para melhor observação pelo leitor, as definições dos componentes e interfaces relacionadas com a Figura 5, encontram-se especificadas detalhadamente em [ALVAREZ 2004].

Na seqüência, o sistema pode ser validado através do emprego de ferramentas apropriadas como **EUCALYTUS toolset** [Garavel 2004]. A seguir descreve-se os passos para a verificação de correção do sistema, isto é, a obtenção da prova formal de correção do sistema.

Passos 1 - 2: Geração e Visualização do LTS

Para gerar o LTS (*Labelled Transition System*) correspondente à especificação do protocolo do arquivo *ModeloSsgct.lotos*, é gerado um arquivo com extensão ***.aut*** - *ModeloSsgct.aut* – LTS no formato ALDEBARAN onde o primeiro estado é "0", o número de transições é "80" e o número de estados é "79". O seguinte grafo é visualizado através de um arquivo criado com extensão ***.bcg*** - *ModeloSsgct.bcg* - como mostra a Figura 6.

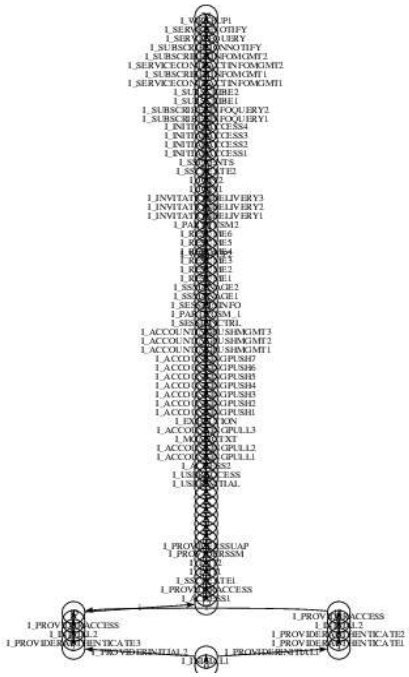

Figura 6. LTS com Transições.

Como pode ser observado, o LTS tem um número de estados e transições, segundo o grafo não muito denso, devido as transições que ocorrem quase de forma seqüencial. Se este fosse muito complexo, poder-se-ia utilizar a opção de redução. Neste caso isto não é necessário já que o resultado é o mesmo.

Passo 3: Geração do LTS

Da mesma maneira como apresentado no Passo 1, neste passo é gerado o LTS associado a especificação *SsgctService.lotos*. Este LTS é pequeno e desta forma não é necessário reduzi-lo. Como pode ser observado a seguir, o LTS inicia no estado "0", inclui 2 estados e 2 transições.

```
des (0, 2, 2)
(0, ACESSO, 1)
(1, USO, 0)
```

Passo 4: Comparação de LTS

Neste passo estamos em condições de comparar o LTS que representa o protocolo com o LTS e o serviço esperado. Para conseguir a comparação, posiciona-se no arquivo *ModeloSsgct_bmin.bcg* e escolhe-se a ferramenta para comparar os LTSs (*ALDEBARAN* ou *Fc2tools*), bem como a relação de comparação (*Strong equivalence bisimulation*, *Observationnal equivalence bissimulation*, ...). Neste caso se selecionou: *ModeloSsgcService.bcg* para o LTS a ser comparado; *ALDEBARAN* para a ferramenta a ser utilizada; *Observational Equivalence* para a relação de comparação; e *Standard* para o método de decisão. Depois de confirmado, o resultado da comparação aparece na Figura 7.

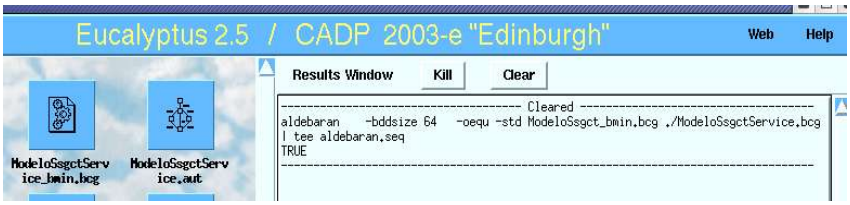

Figura 7. Resultado da Equivalência de Observação.

O resultado "***TRUE***", significa que o protocolo executa o serviço esperado. Isto representa a prova formal de equivalência entre as especificações de observação do *ModeloSsgc*t e o *ModeloSsgctService*, com resultado "*TRUE*" que indica a equivalência entre a especificação inicial do sistema e as especificações finais refinadas.

6. Descrição e Visualização das especificações

Devido a alta complexidade necessária para a implementação de todo o conceito da segurança multilateral na arquitetura de contabilidade TINA, decidiu-se limitar a implementação do protótipo na negociação dos objetivos de segurança e na simulação da vídeo conferência com toda a estrutura de contabilidade. Esta implementação fornece a base para a simulação de uma vídeo-conferência entre diversos usuários. Ela é composta por um módulo servidor e um módulo cliente. O módulo servidor é responsável pelo controle dos usuários e por prover o serviço de vídeo-conferência para estes usuários, que por sua vez, utilizam o módulo cliente para interagir na vídeo-conferência. Diversos usuários podem se conectar ao servidor simultaneamente.

Ao iniciar uma sessão, o usuário deve configurar as suas preferências de segurança que serão utilizadas na negociação para o estabelecimento da sessão. A Figura 8 mostra a interface onde o usuário pode escolher quais objetivos de segurança ele irá usar e quais mecanismos existentes ele poderá usar para alcançar o objetivo de segurança desejado.

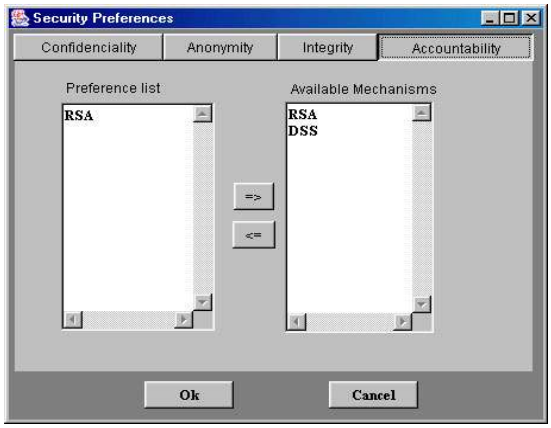

Figura 8. Caixa de Diálogo para Seleção de Preferências de Segurança.

Neste exemplo ilustrado, para alcançar uma contabilidade eficiente, o usuário selecionou o algoritmo RSA. Após a negociação ser concluída com sucesso, uma segunda interface é visualizada, como mostra a Figura 9, sub-dividida nos seguintes módulos:

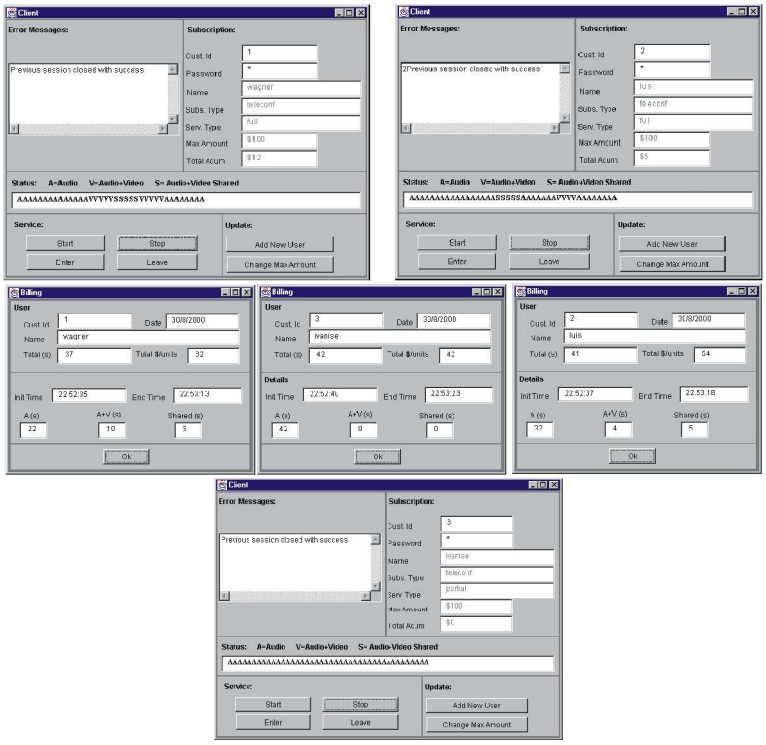

Figura 9. Exemplo de Execução do Protótipo.

- ***Subscription*:** login do usuário e visualização dos dados do usuário;
- ***Update*** : atualização do usuário (*Insert, Modify, Delete, etc*);
- ***Monitoring service***: monitorização do serviço de vídeo conferência para cada usuário; e
- ***Error messages***: visualização de erros que podem ocorrer durante a sessão de serviço.

Na Figura 9 foram considerados na execução do protótipo três usuários que compartilham a mesma sessão de um "*serviço de vídeo conferência múltiplo*" fornecido pelo *Retailer*, mostrando um exemplo da interface gráfica "*Client*" com sua respectiva interface gráfica "*Billing*" que representa a cobrança *on-line* de um usuário pelo uso do serviço fornecido pelo *Retailer*.

Os usuários tem três opções de acesso ao serviço de acordo com o contrato estabelecido entre as partes: V (Vídeo+Áudio); A (Áudio); e S (Vídeo+Áudio Compartilhado). O uso da opção "V" custa 3$/unit, da opção "A" custa 1$/unit e da opção "S" custa 2$/unit.

7. Conclusões

Os resultados obtidos nesta linha de pesquisa permitem concluir que o sistema proposto a partir do modelo de segurança definido para o gerenciamento de contabilidade de TINA, demonstrou que modelos de segurança diferentes, os quais proporcionam políticas e mecanismos que podem ser incorporados no sistema, podem ser implementados num nível de negociação e de definição de papéis respectivamente, sem ter a desvantagem de incompatibilidades entre eles. Isto permite garantir a segurança num ambiente de serviço TINA através do gerenciamento de contabilidade em tempo real e cujo *billing on-line* é definido especificamente para o cliente que está usando um serviço determinado através do certificado de papel, visando garantir que não se

produzam fraudes ou manipulações das informações produzidas pelos eventos contábeis. Isto fica demonstrado através da aplicação de técnicas de especificação formal que permitiram validar o correto comportamento funcional e estrutural do sistema e a implementação de um protótipo no ambiente de serviço baseado em TINA considerando o uso de cobrança *on-line* (*billing*).

8. Referências

Abarca, C.; et al. (1997) Network Resource Architecture. V. 3.0, TINA-C, [http://www.tinac.com], 1997.

Agarwal, V.; et al. (2004) An Information Model for Metering and Accounting. 2004 IEEE/IFIP Network Operations&Management Symposium. NOMS 2004. COEX Convention Center Seoul, Korea. 19 – 23 April 2004.

Alvarez, L. M. C.; et. al.(2001) Development of a prototype based on TINA Accounting and Security Management Architecture. XXI International Conference of the Chilean Society of Computer Science. SCCC 2001, IEEE CS Press. Punta Arenas - Chile, Novembro, 2001. Págs. 50-57.

Alvarez, L. M. C. (2004) Modelo de Segurança Multilateral e RBAC em um Ambiente de Serviço no Contexto de Gerenciamento de Contabilidade TINA. Tese de Doutorado em Ciências da Computação-UFSC. Florianópolis, Agosto 2004.

Brinksma, E. (1988) A Tutorial on LOTOS. ISO 8807 Information Processing Systems – Open System Interconnection – LOTOS. A formal description technique on the temporal ordering of observational behaviour, 1988.

Farley, P.; et al. (1998) Ret Reference Point Specification. V.1.0, TINA-C, [http://www.tinac.com], 1998.

Ferraiolo, D. F.; et al. (1999) A Role-Based Access Control Model and Reference Implementation within a Corporate Intranet. NIST - National Institute of Standards and Technology. 1999.

Garavel, H. (2004) CADP(CAESAR/ALDEBARAN DEVELOPMENT PACKAGE): A Software Engineering Toolbox for Protocol and Distributed Systems – Version 2003-e. INRIA/VASY. Grenoble, França, 2004. http://www.inrialpes.fr/vasy/cadp.

Hamada, T.; et al. (1996) Accounting Management Architecture. TINA-C, [http://www.tinac.com], 1996.

Hamada, T. (1998) Role-Based Access Control in Telecommunication Service Management – Dynamic Role Creation and Management in TINA Service Environment. In: Proceeding of the Third ACM Workshop on Role-Based Access Control, Outubro 1998, USA. Págs. 105 – 113.

Hamada, T.; et al. (2004) Peer-to-Perr Traffic in Metro Networks: Analysis, Modeling, and Policies. 2004 IEEE/IFIP Network Operations&Management Symposium. NOMS 2004. COEX Convention Center Seoul, Korea. 19 – 23 April 2004.

Hwang, J., et al. (2004) Transaction Management for Sender/Receiver – Payment Schemes in Charging and Accounting Systems for Interconnected Networks. 2004 IEEE/IFIP Network Operations&Management Symposium. NOMS 2004. COEX Convention Center Seoul, Korea. 19 – 23 April 2004.

Jansen, W. A. (1998) A Revised Model for Role-Based Access Control. NIST 6192, 1998.

Kelley, D. (2004) Security Management Convergence via SIM (Security Information Management) – A Requirements Perspective. Journal of Network and Systems Management, Vol. 12 - Report, No. 1, Março 2004. págs. 137 – 144.

Koutepas, G.; et al. (2004) Distributed Management Architecture for Cooperative Detection and Reaction to DdoS Attacks. Journal of Network and Systems Management, Vol. 12, No. 1, Março 2004. págs. 73 – 94.

Kristiansen, L.; et al. (1997) TINA Service Architecture 5.0. TINA-C, [http://www.tinac.com], 1997.

Le, M. Van, et al. (2002) Formal Modeling of Service Session Management. IFIP/IEEE International Conference on Management of Multimedia Networks and Services, MMNS 2002. Santa Bárbara – USA, 2002. Págs. 36 – 48.

Le, M. Van, et al. (2004) A Service Component – Based Accounting and Charging Architecture to Support Interim Mechanism across Múltiple Domains. 2004 IEEE/IFIP Network Operations&Management Symposium. NOMS 2004. COEX Convention Center Seoul, Korea. 19 – 23 April 2004.

Manpaey, M. and Couturier, A. (2000) Using TINA Concepts for IN Evolution. In: IEEE Communications Magazine, Junho 2000. págs 94 – 99.

Mulder, H.; et al. (1997) TINA Business Model and Reference Points. TINA-C, [http://www.tinac.com], 1997

Pfitzmann, A.; et al. (2002) Striking a Balance between Cyber-Crime Prevention and Privacy. IPTS – Institute for Prospective Technological Studies. Report vol. 57, 2002.

Pilz A. (2004) "Policy-Maker": a Toolkit for Policy-Based Security Management. 2004 IEEE/IFIP Network Operations&Management Symposium. NOMS 2004. COEX Convention Center Seoul, Korea. 19 – 23 April 2004.

Sekkaki, A.; et al. (2001) Development of a Prototype Based on TINA Accounting Management Architecture. In: IFIP/IEEE International Simposium on Integrated Network Management, 2001. V.1. Págs. 100-120.

Thaler, D. G. e Ravishankar, Ch. V. (2004) An Architecture for Inter – Domain Troubleshooting. Journal of Network and Systems Management, Vol. 12, No. 1, Março 2004. págs. 155 – 189.

Vissers, C. A.; Scollo, G.; Sinderen, M. V. (1988) Architecture and Specification Style in Formal Descriptions of Distributed Systems. University of Twente. The Netherlands, 1988.

Westphall, C. B.; et. al. (2003) Extending TINA with Secure On-Line Accounting Services. Journal of Network and Systems Management. Plenum Publishing Corporation. Meddletown, USA (2003, Vol.11 , No. 4), 2003. Págs. 379 – 397.