República Federativa do Brasil
Ministério da Indústria, Comércio Exterior
e Serviços
Instituto Nacional da Propriedade Industrial

(11) PI 0402910-0 B1

(22) Data do Depósito: 21/07/2004

(45) Data de Concessão: 29/05/2018

(54) Título: MÉTODO DE AUTENTICAR UM DIRETOR EM UM AMBIENTE DE REDE PARA ACESSO AOS RECURSOS DE REDE

(51) Int.Cl.: H04L 12/24; H04L 9/32

(30) Prioridade Unionista: 22/09/2003 US 10/667,582

(73) Titular(es): MICROSOFT TECHNOLOGY LICENSING, LLC

(72) Inventor(es): JEFFREY B. PARHAM; BRENDAN W. DIXON; MURLI D. SATAGOPAN; RICHARD B. WARD

"MÉTODO DE AUTENTICAR UM DIRETOR EM UM AMBIENTE DE REDE PARA ACESSO AOS RECURSOS DE REDE".

CAMPO DA INVENÇÃO

[001] Esta invenção diz respeito em geral ao gerenciamento de rede e, mais particularmente, diz respeito a um sistema e método para autenticar diretores em um ambiente de rede.

ANTECEDENTE

[002] Uma vez que as redes de computadores tornam mais prevalecentes em todas as facetas da indústria e empresa, os usuários mais frequentemente necessitam acessar recursos que ficam localizados em um computador que se encontra remoto de sua própria máquina. Porém, a possibilidade de usuários remotos acessar dados locais levanta muitas preocupações de segurança. Por exemplo, um usuário remoto pode acessar dados que ele não está autorizado a acessar, e ainda pode maliciosamente destruir ou alterar tais dados. Consequentemente, a maioria dos domínios de rede requer que os usuários se registrem e sejam autenticados antes de ganhar acesso aos recursos naquele domínio. A autenticação é intencionada assegurar que a identidade e permissões associadas do usuário sejam conhecidas antes de conceder acesso. O processo de autenticação vincula verificar se acesso é apropriado e depois ou conceder ou negar o acesso com base nos resultados daquela verificação.

[003] Como aqui usado, um diretor é uma entidade (tipicamente um ser humano, computador, aplicação ou serviço) que tenta acessar um recurso ou facilidade protegida (e.g. uma aplicação). A autenticação é o processo de provar ou verificar a identidade. Uma autoridade é uma entidade confiável que é usada para fornecer serviços de autenticação com respeito a algum conjunto de diretores.

[004] Para uma autoridade dada, ela confia nos diretores uma vez os autenticou, mas pode não confiar em outras autoridades para

ter corretamente autenticado seus diretores. Por este motivo, uma convenção de espaço de nome se desenvolveu por meio da qual autoridades particulares autenticam apenas aqueles diretores cujo ID de conta reside em um espaço de nome dado. Em particular, o ID de conta usualmente compreende pelo menos uma porção do identificador de usuário e uma porção da autoridade de autenticação. A porção da autoridade de autenticação do ID de conta identifica o espaço de nome do ID de diretor, e consequentemente a autoridade que deve autenticar o diretor. A porção do identificador de diretor usualmente identifica o usuário particular como distinto de outros usuários dentro do mesmo espaço de nome. Desse modo, por exemplo, o ID de conta bob@dev.microsoft.com deve ser autenticado pela autoridade para o domínio dev.microsoft.com, enquanto que o ID de conta bob@mktg.microsoft.com deve ser autenticado pela autoridade para o domínio mktg.microsoft.com.

[005] Esta solução permitiu certa quantidade de segurança com respeito aos recursos da rede; porém a natureza estática das divisões do espaço de nome cria problemas adicionais. Por exemplo, quando um usuário move de um domínio para outro ou é requerido ter acesso através dos limites de domínio, o presente sistema não é facilmente favorável. No primeiro caso, o usuário é requerido obter um novo ID de conta que identifica o espaço de nome do novo domínio ao invés do domínio velho, enquanto no último caso o usuário tem que obter uma conta adicional no próprio espaço de nome ou tem que existir confidência administrativa forte (e.g. confiança) entre as autoridades.

BREVE SUMÁRIO DA INVENÇÃO

[006] As modalidades da invenção fornecem uma nova arquitetura de rede que permite alteração da convenção de espaço de nome usada na autenticação de diretor de modo que os diretores podem mover através dos limites de segurança sem variar os Ids de

conta, enquanto ao mesmo tempo mantendo substancialmente a proteção de recurso fornecida pelos métodos anteriores. A arquitetura de acordo com certas modalidades da invenção compreende uma Super Autoridade tendo responsabilidade sobre uma pluralidade de autoridades de autenticação. Quando uma autoridade de autenticação recebe uma solicitação de login, ela transmite a solicitação à Super Autoridade para uma decisão com relação qual autoridade de autenticação deve autenticar o diretor associado.

[007] Em resposta, a Super Autoridade avalia um catálogo de identidade para determinar qual autoridade deve autenticar o diretor. O catálogo de identidade compreende, em uma modalidade da invenção, um mapeamento de cada ID de conta para uma autoridade de autenticação. O mapeamento é determinado através de política ou do contrário sendo restringido para respeitar os limites de espaço de nome, de forma que diferente dos sistemas anteriores, duas autoridades de autenticação distintas podem autenticar no mesmo espaço de nome, e qualquer autoridade de autenticação pode autenticar em múltiplos espaços de nome. Por exemplo, o mapeamento pode ser com base na afiliação organizacional dos diretores dentro de uma empresa ou na localização geográfica dos diretores, etc. Uma vez uma autoridade de autenticação foi identificada pela Super Autoridade, a Super Autoridade ou diretamente envia a solicitação de login à autoridade apropriada para autenticação ou do contrário faz com que a solicitação seja enviada à autoridade apropriada para autenticação.

[008] Características e vantagens adicionais da invenção se tornarão evidentes da descrição detalhada a seguir das modalidades ilustrativas que prosseguem com referência às figuras em anexo.

BREVE DESCRIÇÃO DOS DESENHOS

[009] Embora as reivindicações em anexo expõem as

características da presente invenção com particularidade, a invenção, junto com seus objetivos e vantagens, pode ser melhor entendida da descrição detalhada a seguir considerada com os desenhos em anexo, dos quais:

Figura 1 é um diagrama de bloco em geral ilustrando uma arquitetura de dispositivo exemplar em que as modalidades da presente invenção podem ser implementadas;

Figura 2A é um diagrama esquemático de uma arquitetura de rede geral exemplar dentro da qual as autoridades de autenticação associadas aos diretores podem ser implementadas;

Figura 2B é um diagrama lógico exemplar das associações entre os diretores e as autoridades de autenticação;

Figura 3A é um diagrama esquemático de uma arquitetura de rede geral exemplar dentro da qual uma Super Autoridade pode ser implementada dentro de uma modalidade da invenção;

Figura 3B é um diagrama lógico exemplar das associações entre as Super Autoridades, diretores e autoridades de autenticação de acordo com uma modalidade da invenção;

Figura 4A é um diagrama esquemático que ilustra uma Super Autoridade dentro de um ambiente utilizável para implementar uma modalidade da invenção;

Figura 4B é um diagrama esquemático que ilustra um catálogo de identidade de acordo com uma modalidade da invenção para mapear identificadores de conta para autoridades de autenticação;

Figura 5 é um fluxograma que mostra as etapas utilizáveis durante o login para autenticar um ID de conta de diretor de acordo com uma modalidade da invenção.

DESCRIÇÃO DETALHADA

[0010] Voltando aos desenhos, em que tais numerais de referência

se referem a tais elementos, a invenção é ilustrada como sendo implementada em um ambiente de computação adequado. Embora não requerido, a invenção será descrita no contexto geral de instruções executáveis por computador, como módulos de programa, sendo executados por um computador. Em geral, os módulos de programa incluem rotinas, programas, objetos, componentes, estruturas de dados, etc. que executam tarefas particulares ou implementam tipos de dados abstratos particulares. Além disso, aqueles versados na técnica apreciarão que a invenção pode ser praticada com outras configurações de sistema de computador, incluindo dispositivos portáteis, sistemas de multiprocessador, eletrônicos com base em microprocessador ou programáveis pelo consumidor, PCs de rede, minicomputadores, mainframes e outros. A invenção pode ser praticada em ambientes de computação distribuídos onde as tarefas são executadas por dispositivos de processamento remotos que são ligados através de uma rede de comunicação. Em um ambiente de computação distribuído, os módulos de programa podem estar localizados em dispositivos de armazenamento de memória locais e remotos.

[0011] Esta descrição começa com uma descrição de um dispositivo de computação de propósito geral que pode ser usado em um sistema exemplar para implementar a invenção após o qual a invenção será descrita em maior detalhe com referência às Figuras 2-5. Voltando agora para a Figura 1, um dispositivo de computação de propósito geral é mostrado na forma de um computador convencional 20, incluindo uma unidade de processamento 21, uma memória do sistema 22 e um barramento do sistema 23 que acopla vários componentes do sistema incluindo a memória do sistema à unidade de processamento 21. O barramento do sistema 23 pode ser quaisquer de vários tipos de estruturas de barramento incluindo um barramento

de memória ou controlador de memória, um barramento periférico e um barramento local usando qualquer de uma variedade de arquiteturas de barramento. A memória do sistema inclui memória exclusiva de leitura (ROM) 24 e memória de acesso aleatório (RAM) 25. Um sistema básico de entrada/saída (BIOS) 26, contendo as rotinas básicas que ajudam a transferir informação entre os elementos dentro do computador 20, como durante a inicialização, é armazenado na ROM 24. O computador 20 também inclui uma unidade de disco rígido 27 para ler e escrever em um disco rígido 60, uma unidade de disco magnético 28 para ler ou escrever em um disco magnético removível 29 e uma unidade de disco óptico 30 para ler ou escrever em um disco óptico removível 31 como um CD ROM ou outros meios ópticos. Além dos meios legíveis por computador acima mencionados, meios de comunicação tipicamente incorporam instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados em um sinal de dados modulado como uma onda portadora ou outro mecanismo de transporte e incluem quaisquer meios de liberação de informação. O termo "sinal de dados" significa um sinal que tem uma ou mais de suas características determinadas ou alteradas de tal maneira a codificar a informação no sinal. Por via de exemplo, e não de limitação, meios de comunicação incluem meios com fios como uma rede com fios ou conexão com fios, e meios sem fios como acústico, RF, infravermelhos e outros meios sem fios. Combinações de qualquer um dos acima devem também estar incluídas dentro do escopo de meios legíveis por computador.

[0012] A unidade de disco rígido 27, unidade de disco magnético 28 e unidade de disco óptico 30 são conectadas ao barramento do sistema 23 por uma interface da unidade de disco magnético 32, uma interface da unidade de disco magnético 33, e uma interface da unidade de disco óptico 34, respectivamente. As unidades e seus

meios legíveis por computador associados fornecem armazenamento não-volátil das instruções legíveis por computador, estruturas de dados, módulos de programa e outros dados para o computador 20. Embora o ambiente exemplar aqui descrito empregue um disco rígido 60, um disco magnético removível 29 e um disco óptico removível 31, será apreciado por aqueles versados na técnica que outros tipos de meios legíveis por computador que podem armazenar dados que são acessíveis por um computador, como cassetes magnéticos, cartões de memória instantânea, discos de vídeo digital, cartuchos de Bernoulli, memórias de acesso aleatório, memórias exclusivas de leitura, redes de área de armazenamento, e outros, podem também ser usados no ambiente operacional exemplar. Vários módulos de programa podem ser armazenados no disco rígido 60, disco magnético 29, disco óptico 31, ROM 24 ou RAM 25, incluindo um sistema operacional 35, um ou mais programas de aplicação 36, outros módulos de programa 37 e dados de programa 38. Um usuário pode entrar os comandos e a informação no computador 20 através de dispositivos de entrada como um teclado 40 e um dispositivo de apontamento 42. Outros dispositivos de entrada (não mostrados) podem incluir um microfone, joystick, acionador de jogo, disco satélite, escâner ou outros. Estes e outros dispositivos de entrada são frequentemente conectados à unidade de processamento 21 através de uma interface de porta serial 46 que é acoplada ao barramento do sistema, mas podem ser conectados através de outras interfaces, como uma porta paralela, porta de jogo ou um barramento serial universal (USB) ou uma placa de interface de rede. Um monitor 47 ou outro tipo de dispositivo de exibição é também conectado ao barramento do sistema 23 por meio de uma interface, como um adaptador de vídeo 48. Além do monitor, os computadores podem incluir outros dispositivos de saída periféricos, não mostrados, como alto-falantes e impressoras.

[0013] O computador 20 opera em um ambiente em rede usando conexões lógicas a um ou mais computadores remotos, como um computador remoto 49. O computador remoto 49 pode ser um servidor, um roteador, um PC de rede, um computador pessoal, um dispositivo semelhante ou outro nó de rede comum, e tipicamente inclui muitos ou todos os elementos acima descritos com relação ao computador 20, embora apenas um dispositivo de armazenamento de memória 50 tenha sido ilustrado na Figura 1. As conexões lógicas descritas na Figura 1 incluem uma rede local (LAN) 51 e uma rede de longa distância (WAN) 52. Tais ambientes de gestão de redes são comuns em escritórios, redes de computadores de grandes empresas, intranets e a Internet.

[0014] Quando usado em um ambiente de gestão de redes LAN, o computador 20 é conectado à rede local 51 através de uma interface ou adaptador de rede 53. Quando usado em um ambiente de gestão de redes WAN, o computador 20 tipicamente inclui um modem 54 ou outros dispositivos para estabelecer comunicações na WAN 52. O modem 54 que pode ser interno ou externo é conectado ao barramento do sistema 23 por meio da interface de porta serial 46. Módulos de programa descritos com relação ao computador 20, ou porções deste, podem ser armazenados no dispositivo de armazenamento de memória remoto se tal estiver presente. Será apreciado que as conexões de rede mostradas são dispositivos exemplares e outras de estabelecer um link de comunicação entre os computadores podem ser usados.

[0015] Aqui, a invenção será em geral descrita com referência às ações e representações simbólicas das operações que são executadas por um ou mais computadores, a menos que do contrário indicado. Como tal, será entendido que tais ações e operações, que são às vezes referidas como sendo executadas por computador,

incluem a manipulação pela unidade de processamento do computador de sinais elétricos que representam dados em uma forma estruturada. Esta manipulação transforma os dados ou os mantém em localizações no sistema de memória do computador que reconfigura ou do contrário altera a operação do computador de uma maneira bem entendida por aqueles versados na técnica. As estruturas de dados, onde são mantidos os dados, são localizações físicas da memória que tem propriedades particulares definidas pelo formato dos dados. Porém, embora a invenção esteja sendo descrita no contexto anterior, não é significado ser limitativa como aqueles de habilidade na técnica apreciarão que várias das ações e operações descritas doravante podem também ser implementadas em hardware. No debate a seguir, dispositivos de computação como dispositivos de autenticação e dispositivos de Super Autoridade podem ser como acima descritos com respeito à Figura 1 relativo ao computador 20 e/ou computador remoto 49, ou podem ser alternativamente outro tipo de dispositivo de computação.

[0016] Figura 2A ilustra esquematicamente um ambiente de rede exemplar 200 dentro do qual as técnicas de administração de recurso da rede anteriores foram usadas. Em particular, diretor A 201, diretor B 203, diretor C 205, diretor D 207, diretor E 209 e diretor F 211 estão cada um associados à Autoridade X 213, Autoridade Y 215 e Autoridade Z 217. Os diretores e pelo menos suas respectivas autoridades de autenticação são comunicativamente ligados por meio da rede 219. Cada diretor pode ser representado na rede 219 por um computador como o computador 20 debatido com respeito à Figura 1, uma estação de trabalho, ou qualquer outro tipo de dispositivo de computação capaz de executar a comunicação de rede necessária e processar tarefas. Rede 219 pode compreender qualquer número e tipo de conexões de rede incluindo conexões com fios e sem fios,

LAN, WAN e conexões de Internet ou qualquer combinação destas como também qualquer outro tipo de conexão de rede.

[0017] Nas técnicas existentes, cada uma da Autoridade X 213, Autoridade Y 215 e Autoridade Z 217 é responsável para autenticar os Ids de conta dentro de um espaço de nome particular, de forma que quando um ID de conta for recebido para autenticação, ele é imediatamente removido do próprio ID de conta cuja autoridade é responsável pela autenticação. Desse modo, quando uma das tentativas dos diretores para entrar em um domínio particular (i.e. os recursos de rede dentro do espaço de nome associado a uma autoridade particular), a autoridade apropriada executa a autenticação por um dos vários protocolos conhecidos adaptados para aquele propósito e concede ou nega acesso ao diretor. Observe que embora um dos diretores 201, 203, 205, 207, 209, 211 pode ser associado a apenas uma de várias autoridades 213, 215, 217, as conexões de rede podem existir dentro do ambiente 200 para o diretor comunicar direta ou indiretamente com as autoridades e máquinas em outros domínios.

[0018] Referindo à Figura 2B, a arquitetura de domínio lógico 202 que corresponde ao diagrama de rede da Figura 2A é esquematicamente mostrada. No exemplo mostrado, diretor A 201 e C 205 do diretor estão associados (e.g. têm contas com) à autoridade X 213, o diretor B 203, diretor D 207 e o diretor F 211 estão associados à autoridade Y 215, e o diretor E 209 está associado à autoridade Z 217. Embora cada diretor pode ou não ter conectividade de rede com respeito às diferentes autoridades e máquinas da respectiva autoridade de autenticação associada, tais conexões não são descritas na estrutura lógica 202 da Figura 2B uma vez que a estrutura 202 da Figura 2B meramente ilustra as relações de autenticação.

[0019] Por causa da convenção de espaço de nome que foi adotada por razões de segurança dos recursos da rede como acima

debatido, não é possível com o sistema atual mover um diretor de um domínio para outro sem alterar o ID de conta do diretor, resultando em um rompimento de serviço potencial. Ou seja, uma vez que os Ids de conta compreendem um identificador de espaço de nome para facilitar a autenticação, e uma vez que as autoridades de autenticação autenticam em espaços de nome de não-sobreposição, um ID de conta utilizável com respeito a uma autoridade particular não é utilizável com respeito a outra autoridade, até mesmo se permissão para acesso no segundo domínio fosse do contrário concedível.

[0020] Há muitas razões que uma empresa particular poderia selecionar manter um sistema de rede compreendido de múltiplos domínios, ou tendo autoridades múltiplas, e que uma empresa particular pode querer mover os diretores entre tais domínios múltiplos. Por exemplo, em uma fusão de empresas, uma companhia ou empresa simples pode ser formada de partes separadas que foram cada uma previamente associada a um ou mais domínios. Se as identidades das empresas de componente são para ser mantidas, a rede de empreendimento resultante frequentemente compreende como partes de componente os domínios associados às companhias fundidas. Em outro exemplo, uma multinacional ou corporação ou interesse multi-regional pode ser requerido por lei para manter domínios separados de controle. Por exemplo, uma companhia bancária multinacional pode ser requerida por lei local para estabelecer um domínio de controle separado para o pessoal de gerenciamento dentro de um país particular, de forma que o controle das atividades locais e do acesso aos dados locais é conferido apenas em pessoal local.

[0021] Outras razões para manter múltiplas autoridades incluem isolamento administrativo e isolamento de dados. O diretor de isolamento administrativo é útil quando conglomerados acoplados

livremente descentralizados quererem compartilhar os recursos até certo ponto mas não quererem compartilhar o gerenciamento dos recursos ou dos diretores a ele associados. O diretor de isolamento de dados é útil quando os recursos de rede incluírem dados ou recursos preciosos, confidenciais ou do contrário sensíveis e a criação de autoridades múltiplas minimiza o número de indivíduos que podem acessar o conjunto particular de recursos.

[0022] Como acima observado, é também frequentemente útil ou conveniente mover um diretor através dos limites de segurança. Por exemplo, isto é frequentemente desejado quando um usuário individual, associado a uma conta do usuário particular, alterar as posições dentro de uma empresa, movendo de uma divisão para a outra. Se cada divisão for associada a sua própria autoridade, o empregado transferido necessitará sua conta transferida de uma autoridade para a outra. Nas técnicas anteriores, isto requereu uma alteração de ID de conta e uma interrupção concomitante de serviço ou acesso. Outra situação exemplar em que pode ser desejável mover uma conta do usuário ocorre após uma fusão ou aquisição quando uma parte para a transação quiser migrar seus diretores para uma autoridade preexistente associada à outra parte para a transação.

[0023] O sistema da modalidade exemplar aqui descrito mantém isolamento administrativo e isolamento de dados ao mesmo tempo permitindo mover os diretores e fusões de autoridade sem interrupção de serviço. Em geral, este nível de desempenho é alcançado por meio do uso de uma Super Autoridade junto com um catálogo de identidade. Como será descrito doravante em maior detalhe, a Super Autoridade não é uma autoridade de autenticação, mas do contrário direciona uma tentativa de acesso a uma autoridade usual apropriada para autenticação. A Super Autoridade emprega um catálogo de identidade para facilitar esta tarefa. O catálogo de identidade eficazmente mapeia

os Ids de conta para autenticar as autoridades, onde cada ID de conta está associado a uma autoridade de autenticação simples.

[0024] O diagrama esquemático da Figura 3A ilustra uma arquitetura de rede 300 dentro da qual uma Super Autoridade de acordo com uma modalidade da invenção é implementada. A Super Autoridade pode também ser referida como uma autoridade de controle uma vez que controla a autenticação dos diretores, mas não conduz de fato tal autenticação com respeito a aqueles diretores. Além dos diretores e autoridades de autenticação análogos a aqueles mostrados na Figura 2A, a arquitetura 300 também inclui uma ou mais Super Autoridades ilustradas por meio da Super Autoridade I exemplar (321) e Super Autoridade II exemplar (323). Cada Super Autoridade 321, 323 pode ser conectada por meio da(s) rede(s) 319 a algumas ou todas as outras entidades da rede mostradas na figura. Porém, a única conexão requerida é entre cada Super Autoridade 321, 323 e qualquer autoridade ou autoridades de autenticação associados àquela Super Autoridade. A inter-relação entre as autoridades de autenticação e as Super Autoridades será explicada em maior detalhe abaixo.

[0025] Referindo à Figura 3B, uma relação lógica exemplar entre as autoridades de autenticação e as Super Autoridades é esquematicamente ilustrada por meio da estrutura lógica 302. Como mostrado, cada Super Autoridade 321, 323 está associada a uma ou mais autoridades de autenticação, enquanto cada autoridade de autenticação está no máximo associada a uma Super Autoridade. Observe que embora uma autoridade possa estar associada a um diretor simples e/ou uma Super Autoridade possa estar associada a uma autoridade simples, tais situações são tipicamente, embora não necessariamente, transientes.

[0026] Embora a invenção não requeira que cada autoridade de autenticação esteja associada a apenas uma Super Autoridade, tal é

preferível em que tende a simplificar a administração e tarefas de autenticação. No exemplo ilustrado, a Super Autoridade I (321) está associada à Autoridade X (313) e à Autoridade Y (315), enquanto a Super Autoridade II (323) está associada à Autoridade Z (317).

[0027] Por sua vez, cada uma da Autoridade X (313), Autoridade Y (315) e Autoridade Z (317) está associada aos usuários particulares ou diretores, e.g. contas particulares. Porém, diferente das técnicas de autenticação, a ligação entre as autoridades de autenticação e os diretores não são com base em espaço de nome de não-sobreposição, mas são do contrário com base nas escolhas de política incorporadas em um catálogo de identidade mantido pela Super Autoridade pertinente. O catálogo de identidade que será debatido doravante em maior detalhe essencialmente mapeia o identificador de conta de cada diretor para uma autoridade de autenticação, e o mapeamento do catálogo pode ser alterado sem alterar os identificadores de conta.

[0028] Uma vez que o mapeamento é determinado pela política ou do contrário é restringido para respeitar os limites de espaço de nome, duas autoridades de autenticação distintas podem autenticar no mesmo espaço de nome, e qualquer autoridade de autenticação pode autenticar em múltiplos nomes de espaço. O mapeamento pode ser com base na afiliação organizacional dos diretores dentro de uma empresa, na localização geográfica dos diretores, tempo de serviço, posição, etc.

[0029] Figura 4A mostra uma representação esquemática de uma Super Autoridade como Super Autoridade I (321) e Super Autoridade II (323). O diagrama da Figura 4A é dado para propósitos de ilustração e simplificação, e representa uma possível implementação da Super Autoridade 401. A invenção inclui outras implementações como será apreciado por aqueles de habilidade na técnica dado os ensinamentos aqui. A Super Autoridade 401 exemplar é compreendida de uma

interface de rede 403, lógica de resolução de autoridade 405 e um catálogo de identidade 407. Os componentes estão comunicativamente inter-relacionados de modo que a interface de rede 403 e o catálogo de identidade 407 estejam disponíveis à lógica de resolução de autoridade 405.

[0030] A Super Autoridade 401 pode ser implementada em quaisquer de vários tipos de dispositivos de computação. Em uma modalidade da invenção, a Super Autoridade 401 é implementada em um servidor, e os componentes da Super Autoridade 401 são módulos e elementos de software como descrito em geral acima com respeito à Figura 1. Em uma modalidade da invenção, as trajetórias de comunicações entre os componentes compreendem o barramento ou trajetórias de comunicações internas do computador servidor.

[0031] Detalhes do catálogo de identidade 407 de acordo com uma modalidade da invenção são esquematicamente mostrados na Figura 4B. Em particular, o catálogo de identidade 407 fornece um mapeamento dos Ids de conta dos diretores (e.g. bobsmith@msn.com) para as autoridades de autenticação. O mapeamento é ilustrado na Figura 4B como um mapeamento em um formato tabelar, em que cada entrada 453 em uma coluna de identidade 455 é mapeada por meio da tabela para uma entrada 457 correspondente em uma coluna de autoridade de autenticação 459.

[0032] Como ilustrado pelo exemplo mostrado, o mapeamento dos Ids de conta dos diretores para autoridades de autenticação não necessita respeitar os limites de espaço de nome. Por exemplo, clientes no domínio "msn.com" é autenticado tanto através da autoridade de autenticação A quanto da autoridade de autenticação B. O mesmo é verdade dos clientes no domínio "microsoft.com". Alterando um mapeamento simplesmente no catálogo de identidade resulta em um re-mapeamento do diretor pertinente para uma

autoridade de autenticação diferente sob a mesma Super Autoridade. Como debatido acima, isto é benéfico em que a responsabilidade de autenticação pode ser alterada sem requerer alteração do próprio ID de conta.

[0033] No geral, a operação da Super Autoridade 401 é como segue de acordo com uma modalidade da invenção. Uma máquina que pertence a um usuário ou diretor como máquina rotulada Principal A (413) contata uma autoridade como residindo na máquina rotulada Autoridade 411 requerendo acesso aos recursos. Esta solicitação pode estar na forma de uma solicitação ou tentativa de login. A Autoridade 411 contatada depois envia a solicitação à Super Autoridade 401 por meio da rede 409 e da interface de rede 403 para identificação pela lógica de resolução de autoridade 405 de uma autoridade apropriada, usando o catálogo de identidade 407, para autenticar o diretor identificado na solicitação. A Super Autoridade 401 depois ou transmite uma solicitação de autenticação diretamente à autoridade de autenticação selecionada ou faz com que tal seja transmitida, como pela autoridade inicialmente receptora. A autoridade de autenticação selecionada pode ser, mas pode não necessitar ser, a autoridade de autenticação que inicialmente recebeu a tentativa de login do diretor.

[0034] Observe que o processo de alterar os conteúdos do catálogo de identidade 407, por exemplo para re-mapear um ID de conta dado para outra autoridade de autenticação, ele é também preferivelmente realizado quando necessário pela lógica de resolução de autoridade 405 de acordo com uma modalidade da invenção. Tipicamente um administrador emite comandos que levam a lógica de resolução de autoridade 405 fazer alterações apropriadas ao catálogo de identidade 407. Tais comandos podem ser recebidos por meio da interface do usuário do computador hospedando a super autoridade

401, ou pode chegar por meio da interface de rede 403 ou outra conexão de rede, de uma localização remota.

[0035] O fluxograma 500 da Figura 5 transmite em mais detalhe a operação da nova arquitetura aqui descrita enquanto processa uma solicitação para acesso para os recursos de rede. Em particular, na etapa 501, um diretor tenta se registrar para acessar os recursos particulares da rede enviando uma solicitação de login a uma autoridade. A solicitação inclui a o ID de conta do diretor que é tipicamente compreendido de um identificador individual e um identificador de domínio como mostrado na Figura 4B. Na etapa 503, a autoridade que recebe a solicitação não decide imediatamente se ou não autentica a solicitação do diretor, mas do contrário envia a solicitação para a Super Autoridade responsável para a autoridade receptora particular.

[0036] Subsequentemente na etapa 505, a Super Autoridade extrai a informação do ID de conta da transmissão e usa a informação do ID de conta, na etapa 507, como uma chave na tabela de identidade para identificar uma autoridade de autenticação associada ao diretor particular. Observe que a Super Autoridade pode primeiro verificar para determinar se a autoridade de envio particular é a pessoa pela qual a Super Autoridade é responsável. Um identificador de autoridade pode ser usado para este propósito. Observe também que a autoridade de autenticação associado à identidade de diretor particular pode ou pode não ser igual à autoridade que recebeu e passou a solicitação de login dependendo dos conteúdos do catálogo de identidade. Na etapa 509, a Super Autoridade faz com que a solicitação de login seja transmitida para a autoridade apropriada identificada por meio do catálogo de identidade.

[0037] Nesta etapa, a super autoridade ou pode enviar diretamente a solicitação ou pode fazer um terceiro enviar a

solicitação. O processo de remeter a solicitação diretamente pode ser referido como "encadeamento". Porém, o encadeamento não é requerido e a solicitação pode ser cumprida por meio de quaisquer de vários outros mecanismos também. Por exemplo, a Super Autoridade, tendo solucionado a autoridade de autenticação apropriada na etapa 507, pode "encaminhar" a solicitação em vez de encadeá-la. O encaminhamento acarreta na Super Autoridade responder à autoridade que remeteu a solicitação e transmitir à autoridade a identidade da autoridade de autenticação apropriada. A solicitação é depois passada para a autoridade de autenticação apropriada da autoridade que inicialmente remeteu a solicitação à Super Autoridade. Embora encadeamento ou encaminhamento, ou de fato outros métodos, possa ser usado, o uso de encaminhamento é preferido se as autoridades pertinentes estiverem comunicativamente ligadas. Isto é devido ao fato que o encaminhamento em geral permite maior escalamento do sistema uma vez que uma Super Autoridade simples pode ser uma parte em um maior número de solicitações de autenticação durante um período particular de tempo.

[0038] Por fim, na etapa 511, a autoridade selecionada autentica a solicitação conforme apropriado. Como resultado da autenticação, se com sucesso, a autoridade de autenticação pode transmitir uma notificação de permissão ao diretor.

[0039] Será apreciado que a nova arquitetura e sistema da modalidade exemplar aqui descrita permitem flexibilidade aumentada de autenticação sem um aumento concomitante na vulnerabilidade do sistema ao mascaramento e outra infração. Por exemplo, em um sistema tradicional onde duas autoridades distintas A e B são confiáveis para autenticar os diretores de "@msn.com" e "@microsoft.com", as autoridades A e B tem que ter confiança administrativa alta uma na outra, uma vez que seria possível a um

administrador para autoridade A autenticar um diretor que deve apenas ser autenticado pela autoridade B, e vice-versa. Em outras palavras, autoridade A precisaria dos administradores de B de autoridade de confiança tanto quanto confiar em seus próprios administradores, e em alguns casos isto simplesmente não é possível. Porém o sistema exemplar aqui descrito permite as autoridades compartilhar espaço de nomes sem necessariamente ter confiança administrativa mútua. Cada autoridade apenas necessita ter confiança administrativa no administrador da Super Autoridade que pode ser muito mais agradável uma vez que o número, localização e a afiliação dos administradores da Super Autoridade tipicamente serão restringidos mais que aqueles das autoridades padrões. Outro resultado benéfico atingível em muitas modalidades da invenção é que os diretores podem ser movidos através dos limites de espaço de nome sem alterar sua identidade; uma alteração simples no catálogo de identidade da Super Autoridade é tudo que é requerido para registrar um novo mapeamento de uma identidade de diretor para uma autoridade de autenticação.

[0040] Será apreciado que um sistema e método melhorado para autenticação de conta de diretor foi descrito. Devido às muitas possíveis modalidades nas quais os diretores desta invenção podem ser aplicados, deve ser reconhecido que as modalidades aqui descritas com respeito às figuras dos desenhos são intencionadas ser ilustrativas apenas e não devem ser consideradas como limitativas do escopo de invenção. Por exemplo, aqueles de habilidade na técnica reconhecerão que alguns elementos das modalidades ilustradas mostradas em software podem ser implementadas em hardware e vice-versa ou que as modalidades ilustradas podem ser modificadas em arranjo e detalhe sem divergir do espírito da invenção. Além disso, será apreciado que a invenção pode ser implementada em qualquer

ambiente de rede adequado de qualquer tamanho e tipo. Além disso, embora as ilustrações aqui mostrem um número pequeno de diretores, autoridades e Super Autoridades, a invenção envolve sistemas com um maior ou menor de quaisquer destas entidades. Portanto, a invenção como aqui descrita contempla todas tais modalidades que podem encaixar dentro do escopo das reivindicações a seguir e equivalentes destas.

REIVINDICAÇÕES

1. Método de autenticar um diretor em um ambiente de rede para acesso aos recursos de rede, o dito ambiente de rede compreendendo uma primeira autoridade (313), uma segunda autoridade atribuída (315) e um diretor (301), o método **caracterizado** pelo fato de que compreende as etapas de:

receber na primeira autoridade uma solicitação de login do diretor, em que a solicitação de login compreende um identificador de conta, ID, para o qual a dita segunda autoridade atribuída (315) é responsável para autenticar o diretor, sem autenticar a primeira autoridade;

transmitir (503) o identificador de conta da primeira autoridade para uma super autoridade (321) para identificação (507) de uma autoridade que é autorizada para autenticar o diretor,

em que a dita identificação compreende:

acessar um mapeamento de atribuição de uma pluralidade de IDs de contas para uma correspondente pluralidade de autoridades de autenticação e localizar no mapeamento a conta ID recebida para ser autenticada, e

localizar no mapeamento uma identidade da segunda autoridade atribuída que é mapeada para a conta ID a ser autenticada;

transmitir (509) uma solicitação de autenticação da super autoridade para a segunda autoridade atribuída, em que a solicitação pede à segunda autoridade atribuída para autenticar o diretor a ser autenticado; e

autenticar (511) o diretor na primeira autoridade se uma transmissão for recebida na primeira autoridade a partir da super autoridade indicando que a primeira autoridade está autorizada a autenticar o diretor;

alterar o mapeamento de atribuição em que uma ID de

conta previamente mapeada para uma primeira autoridade é remapeada para uma segunda autoridade; e

receber na primeira autoridade a partir da super autoridade uma solicitação para autenticar um segundo diretor baseado em uma solicitação de login feita pelo segundo diretor, em que a solicitação de login feita pelo segundo diretor foi feita pelo segundo diretor para outra autoridade diferente da primeira autoridade.

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o identificador de conta compreende um identificador de diretor e um identificador de espaço de nome.

100

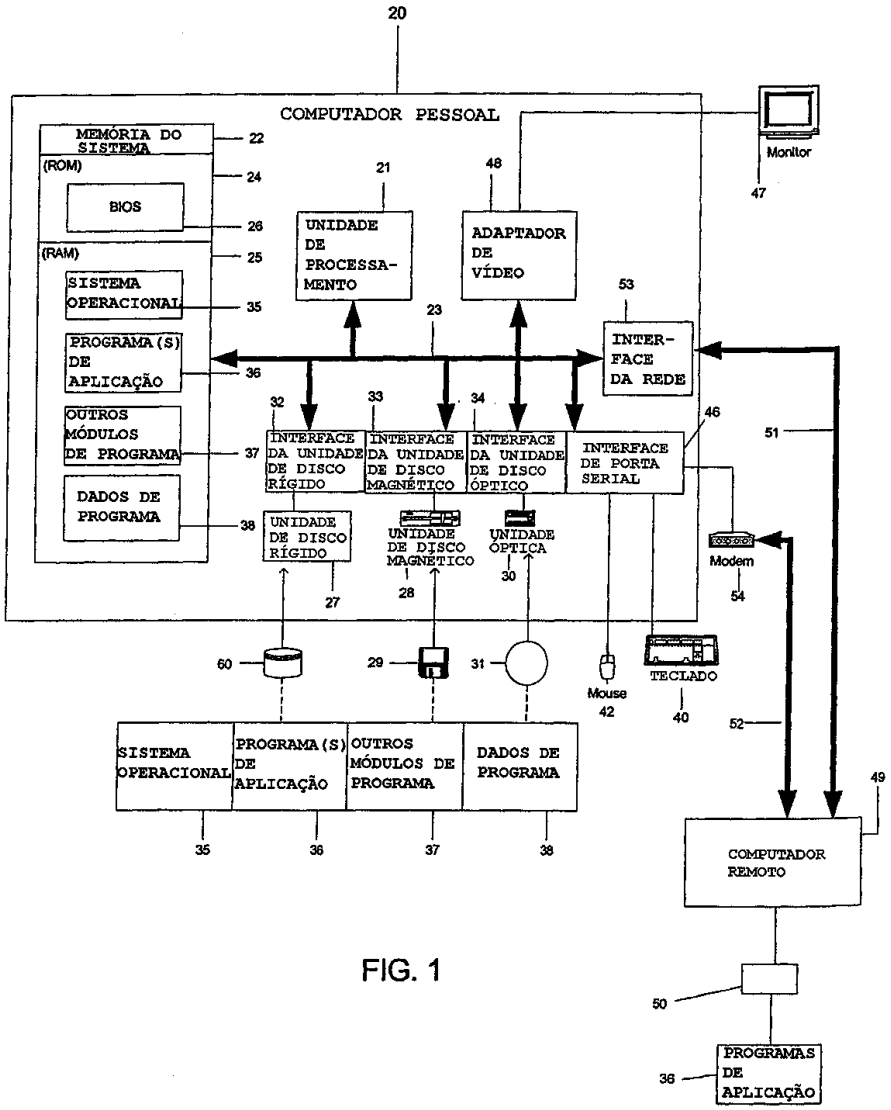

FIG. 1

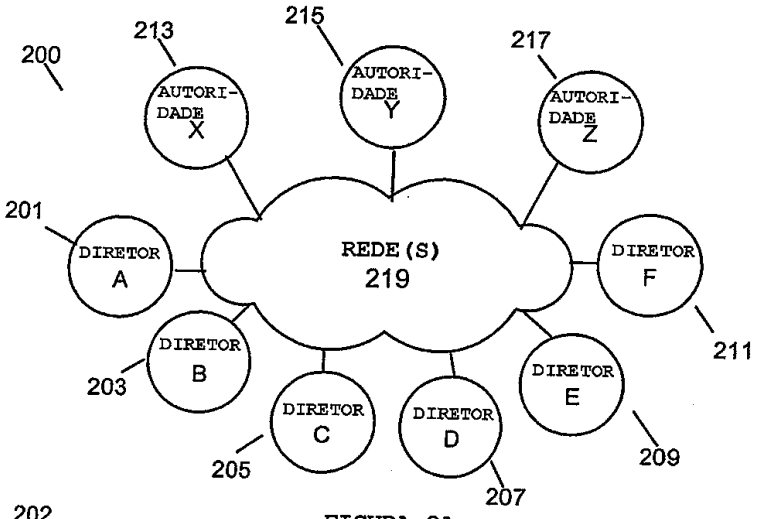

FIGURA 2A

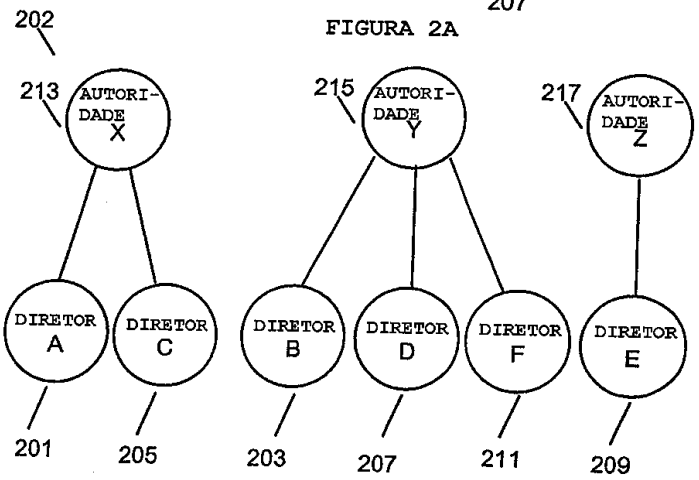

FIGURA 2B

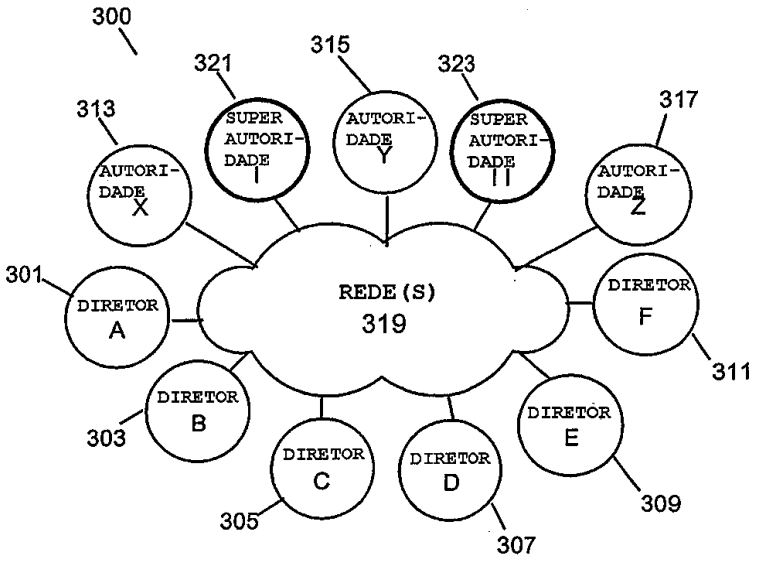

FIGURA 3A

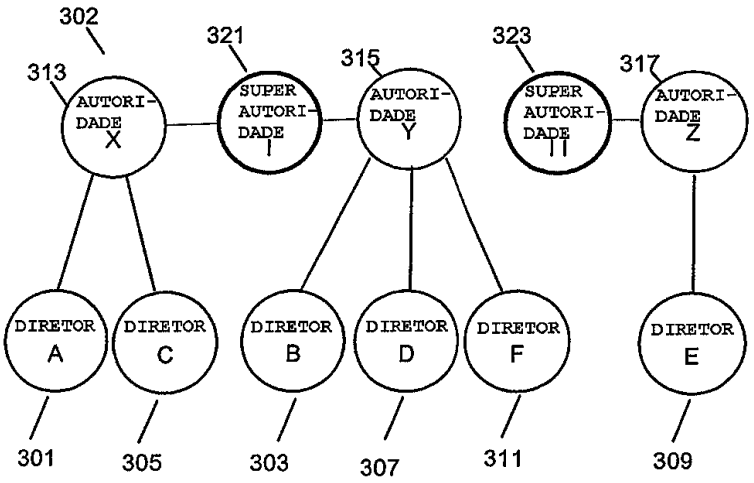

FIGURA 3B

103

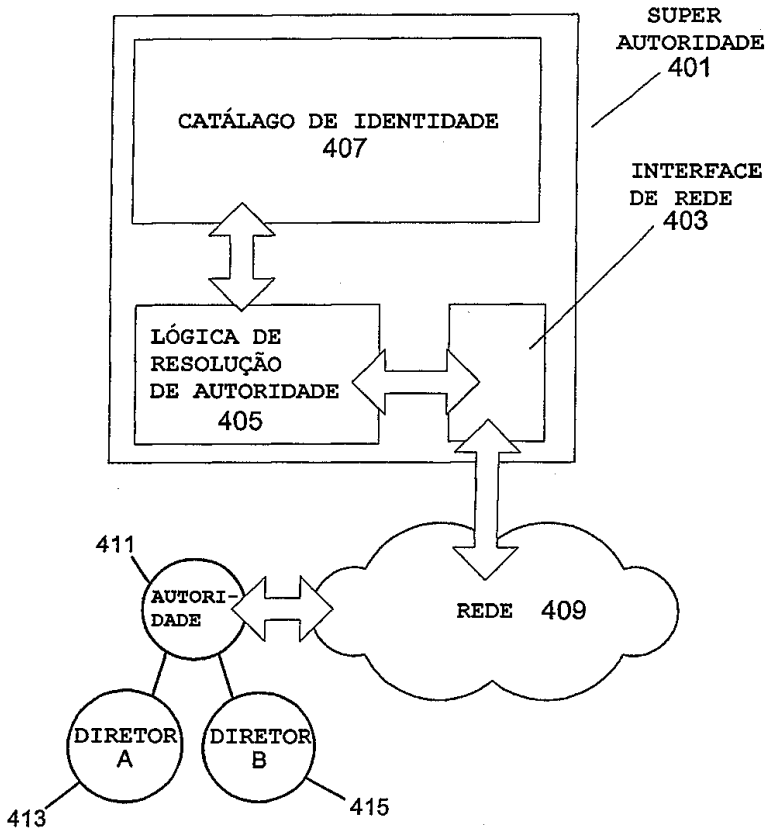

FIGURA 4A

104

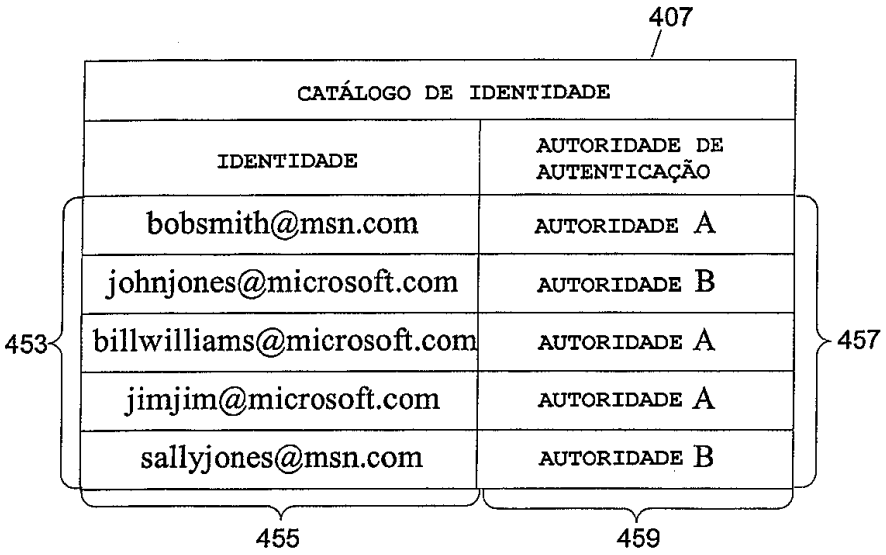

FIGURA 4B

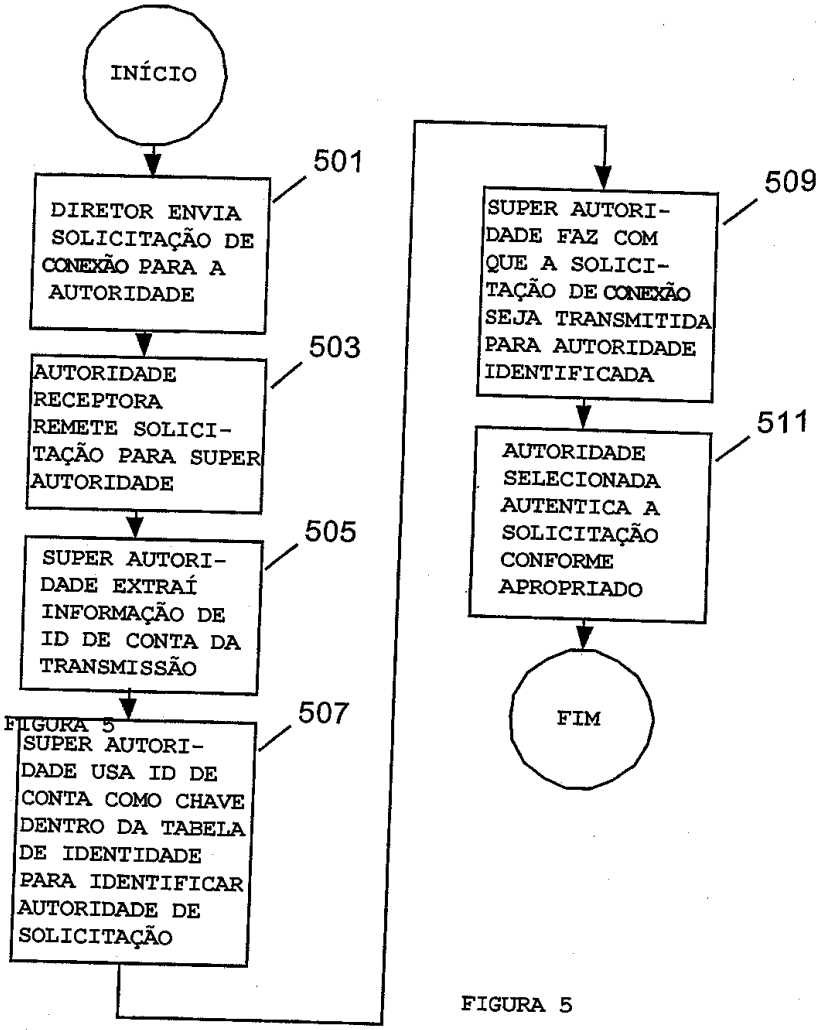

FIGURA 5

FIGURA 5