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

(21) PI 0718048-9 A2

* B R P I 0 7 1 8 0 4 8 A 2 *

(22) Data de Depósito: 05/10/2007
(43) Data da Publicação: 29/04/2014
(RPI 2260)

(51) Int.Cl.:
H04L 9/32

(54) Título: MÉTODO E EQUIPAMENTO PARA AUTENTICAÇÃO MÚTUA

(57) Resumo:

(30) Prioridade Unionista: 03/10/2007 US 11/866,946, 10/10/2006 US 60/850,882

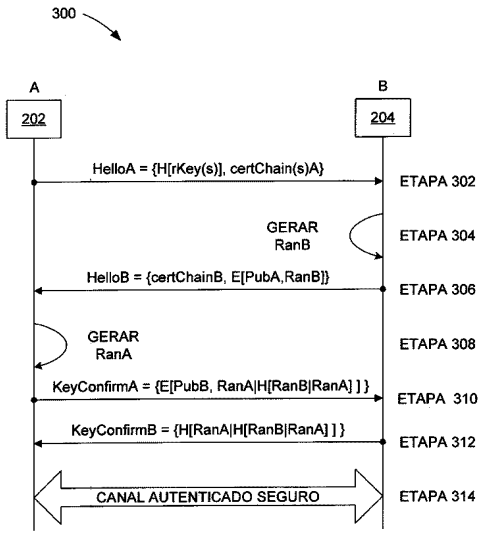
(73) Titular(es): Qualcomm Incorporated

(72) Inventor(es): Aram Perez, Lakshminath Reddy Dondeti

(74) Procurador(es): Montaury Pimenta, Machado & Lioce

(86) Pedido Internacional: PCT US2007080525 de 05/10/2007

(87) Publicação Internacional: WO 2008/045773de 17/04/2008



"MÉTODO E EQUIPAMENTO PARA AUTENTICAÇÃO MÚTUA"

Reivindicação de Prioridade sob 35 U.S.C. seção 119

O presente pedido para patente reivindica prioridade ao Pedido Provisional U.S. No. de série 60/850.882, intitulado "METHOD AND APPARATUS FOR MUTUAL AUTHENTICATION" depositada em 10 de outubro de 2006. Este Pedido Provisional é atribuído ao cessionário deste e incorporado aqui por referência.

FUNDAMENTOS

Campo

A presente invenção se refere geralmente a comunicações sem fio, e mais especificamente, a autenticação mútua.

Fundamentos

Um assinante móvel pode querer acessar o conteúdo protegido por um sistema que exigiria a autenticação com uma outra entidade ou agente. Um protocolo de autenticação popular é o protocolo de Troca de Chave de Internet (IKE), descrito em RFC 4306. Entretanto, o protocolo IKE assume que as entidades no processo de autenticação têm computação suficiente ou potência de processamento tais que a velocidade da autenticação não é um interesse.

Há conseqüentemente uma necessidade na arte para a técnica de autenticação mútua eficiente com um dispositivo possuindo potência de processamento limitada.

SUMÁRIO

Um aspecto da presente invenção pode residir em um método para a autenticação mútua entre uma primeira entidade e uma segunda entidade. No método, a primeira entidade inicia a autenticação mútua enviando uma mensagem à segunda entidade. A segunda entidade verifica uma primeira chave pública associada com a primeira entidade,

gera um primeiro número aleatório, criptografa o primeiro número aleatório usando a primeira chave pública, e envia o primeiro número aleatório criptografado em uma mensagem para a primeira entidade. A primeira entidade verifica uma segunda chave pública associada com a segunda entidade, decriptografa o primeiro número aleatório criptografado usando uma primeira chave privada correspondendo à primeira chave pública, gera um segundo número aleatório, gera um primeiro hash com base pelo menos no primeiro número aleatório, criptografa o segundo número aleatório e o primeiro hash usando a segunda chave pública, e envia o segundo número aleatório criptografado e o primeiro hash em uma mensagem para a segunda entidade. A segunda entidade decriptografa o segundo número aleatório criptografado e o primeiro hash usando uma segunda chave privada correspondendo à segunda chave pública, verifica o primeiro hash para autenticar a primeira entidade, gera um segundo hash com base pelo menos no segundo número aleatório, e envia o segundo hash para a primeira entidade. A primeira entidade verifica o segundo hash para autenticar a segunda entidade.

Em aspectos mais detalhados da invenção, a primeira entidade e a segunda entidade cada uma deriva uma chave de criptografia da sessão e chave de código de autenticação de mensagem (MAC) usando o primeiro número aleatório e o segundo número aleatório com base em uma função de derivação de chave, para uso nas comunicações entre a primeira entidade e a segunda entidade.

Adicionalmente, a mensagem que inicia a autenticação mútua pode incluir um hash de pelo menos uma Chave Raiz confiável e uma corrente de certificado correspondente para a primeira entidade. A corrente de certificado para a primeira entidade pode incluir a chave

pública associada com a primeira entidade. Também, a mensagem a partir da segunda entidade para a primeira entidade possuindo o primeiro número aleatório criptografado ainda pode incluir uma corrente de certificado para a segunda entidade. A corrente de certificado para a segunda entidade pode incluir a chave pública associada com a segunda entidade.

Em outros aspectos mais detalhados da invenção, a primeira entidade pode ser um agente de direitos digitais de uma estação móvel, e a segunda entidade pode ser um dispositivo de mídia removível seguro. A segunda entidade pode ter potência de processamento limitada. Também, o primeiro hash pode ainda ser baseado no segundo número aleatório tal que o primeiro hash é gerado com base no primeiro número aleatório concatenado com o segundo número aleatório. O segundo hash pode ainda ser baseado no primeiro número aleatório, ou ainda ser baseado no primeiro hash tal que o segundo hash pode ser baseado no segundo número aleatório concatenado com o primeiro hash.

Um outro aspecto da invenção pode residir em um equipamento para a autenticação mútua que inclui meios para iniciar a autenticação mútua, meios para verificar uma primeira chave pública, gerar um primeiro número aleatório, e criptografar o primeiro número aleatório usando a primeira chave pública, meios para verificar uma segunda chave pública, decriptografar o primeiro número aleatório criptografado usando uma primeira chave privada que corresponde à primeira chave pública, gerar um segundo número aleatório, gerar um primeiro hash com base pelo menos no primeiro número aleatório, e criptografar o segundo número aleatório e o primeiro hash usando a segunda chave pública, meios para decriptografar o segundo número aleatório criptografado e o primeiro hash usando uma

segunda chave privada que corresponde à segunda chave pública, verificar o primeiro hash para a autenticação, e gerar um segundo hash com base pelo menos no segundo número aleatório, e meios para verificar o segundo hash para a autenticação.

Um outro aspecto da invenção pode residir em uma estação móvel possuindo a autenticação mútua com um dispositivo de mídia removível seguro, e incluindo um agente de direitos digitais. O agente de direitos digitais inicia a autenticação mútua enviando uma mensagem a um dispositivo de mídia removível seguro, onde o dispositivo de mídia removível seguro verifica uma primeira chave pública associada com o agente de direitos digitais, gera um primeiro número aleatório, criptografa o primeiro número aleatório usando a primeira chave pública, e envia o primeiro número aleatório criptografado em uma mensagem ao agente de direitos digitais. O agente de direitos digitais verifica uma segunda chave pública associada com o dispositivo de mídia removível seguro, decriptografa o primeiro número aleatório criptografado usando uma primeira chave privada que corresponde à primeira chave pública, gera um segundo número aleatório, gera um primeiro hash com base pelo menos no primeiro número aleatório, criptografa o segundo número aleatório e o primeiro hash usando a segunda chave pública, e envia o segundo número aleatório criptografado e o primeiro hash em uma mensagem ao dispositivo de mídia removível seguro, onde o dispositivo de mídia removível seguro decriptografa o segundo número aleatório criptografado e o primeiro hash usando uma segunda chave privada que corresponde à segunda chave pública, verifica o primeiro hash para autenticar o agente de direitos digitais, gera um segundo hash com base pelo menos no segundo número aleatório, e envia o segundo hash

ao agente de direitos digitais. O agente de direitos digitais verifica o segundo hash para autenticar o dispositivo de mídia removível seguro.

Contudo um outro aspecto da invenção pode residir em um produto de programa de computador compreendendo meio legível por computador compreendendo código para fazer com que um computador de uma estação que tem um agente de direitos digitais inicie a autenticação mútua enviando uma mensagem a um dispositivo de mídia removível seguro, onde o dispositivo de mídia removível seguro verifica uma primeira chave pública associada com o agente de direitos digitais, gera um primeiro número aleatório, criptografa o primeiro número aleatório usando a primeira chave pública, e envia o primeiro número aleatório criptografado em uma mensagem para o agente de direitos digitais, código para fazer com um computador faça com que o agente de direitos digitais verifique uma segunda chave pública associada com o dispositivo de mídia removível seguro, decriptografe o primeiro número aleatório criptografado usando uma primeira chave privada que corresponde à primeira chave pública, gere um segundo número aleatório, gere um primeiro hash com base pelo menos no primeiro número aleatório, criptografe o segundo número aleatório e o primeiro hash usando a segunda chave pública, e envie o segundo número aleatório criptografado e o primeiro hash em uma mensagem ao dispositivo de mídia removível seguro, onde o dispositivo de mídia removível seguro decriptografa o segundo número aleatório criptografado e o primeiro hash usando uma segunda chave privada que corresponde à segunda chave pública, verifica o primeiro hash para autenticar o agente de direitos digitais, gera um segundo hash com base pelo menos no segundo número aleatório, e envia o segundo hash ao agente de direitos digitais, e código para fazer com que

um computador faça com que o agente de direitos digitais verifique o segundo hash para autenticar o dispositivo de mídia removível seguro.

Um outro aspecto da invenção pode residir em um produto de programa de computador, compreendendo meio legível por computador compreendendo código para fazer com um computador faça com que um dispositivo de mídia removível seguro verifique uma primeira chave pública associada com um agente de direitos digitais, gere um primeiro número aleatório, criptografe o primeiro número aleatório usando a primeira chave pública, e envie o primeiro número aleatório criptografado em uma mensagem para o agente de direitos digitais, onde o agente de direitos digitais verifica uma segunda chave pública associada com o dispositivo de mídia removível seguro, decriptografa o primeiro número aleatório criptografado usando uma primeira chave privada que corresponde à primeira chave pública, gera um segundo número aleatório, gera um primeiro hash com base pelo menos no primeiro número aleatório, criptografa o segundo número aleatório e o primeiro hash usando a segunda chave pública, e envia o segundo número aleatório criptografado e o primeiro hash em uma mensagem para o dispositivo de mídia removível seguro, e o código para fazer com que um computador faça com que o dispositivo de mídia removível seguro decriptografe o segundo número aleatório criptografado e o primeiro hash usando uma segunda chave privada que corresponde à segunda chave pública, verifique o primeiro hash para autenticar o agente de direitos digitais, gere um segundo hash com base pelo menos no segundo número aleatório, e envie o segundo hash para o agente de direitos digitais, onde o agente de direitos digitais verifica o segundo hash para autenticar o dispositivo de mídia removível seguro.

BREVE DESCRIÇÃO DOS DESENHOS

Figura 1 é um exemplo de um sistema de comunicação sem fio;

Figura 2 é um diagrama de blocos de uma estação móvel e de um dispositivo de mídia removível seguro possuindo a autenticação mútua;

Figura 3 é um fluxograma de um método para a autenticação mútua entre uma estação móvel e um dispositivo de mídia removível seguro.

DESCRIÇÃO DETALHADA

A palavra "exemplar" é usada aqui para significar "servindo como um exemplo, caso, ou ilustração". Qualquer modalidade descrita aqui como "exemplar" não deve necessariamente ser interpretada como preferida ou vantajosa sobre outras modalidades.

Uma estação remota, também conhecida como uma estação móvel (MS), um terminal de acesso (AT), equipamento de usuário ou unidade de assinante, pode ser móvel ou estacionária, e pode se comunicar com uma ou mais estações base, também conhecidas como estações transceptora base (BTSs) ou nó Bs. Uma estação remota transmite e recebe pacotes de dados através de uma ou mais estações base a um controlador de estação base, também conhecido como controladores de rede rádio (RNCs). As estações base e os controladores de estação base são partes de uma rede chamada uma rede de acesso. Uma rede de acesso transporta pacotes de dados entre múltiplas estações remotas. A rede de acesso pode ainda ser conectada a redes adicionais fora da rede de acesso, tal como uma intranet corporativa ou a Internet, e pode transportar pacotes de dados entre cada estação remota e tais redes externas. Uma estação remota que tenha estabelecido uma conexão de canal de tráfego ativa com uma ou mais estações base é chamada uma estação

remota ativa, e é dita como estando em um estado de tráfego. Uma estação remota que está no processo de estabelecer uma conexão de canal de tráfego ativa com uma ou mais estações base seriam ditas como estando em um estado de configuração de conexão. Uma estação remota pode ser qualquer dispositivo de dados que se comunica através de um canal sem fio. Uma estação remota pode ainda ser qualquer um de um número de tipos de dispositivos que incluem mas não são limitados a cartão PC, flash compacto, modem externo ou interno, ou telefone sem fio. O link de comunicação com o qual a estação remota envia sinais à estação base é chamado uplink, também conhecido como um link reverso. O link de comunicação com que uma estação base envia sinais a uma estação remota é chamado um downlink, também conhecido como um link direto.

Em referência a figura 2, um sistema de comunicação sem fio 100 inclui uma ou mais estações móveis sem fio (MS) 102, uma ou mais estações base (BS) 104, um ou mais controladores de estação base (BSC) 106, e uma rede núcleo 108. A rede núcleo pode ser conectada a uma Internet 110 e a uma Rede de Telefonia Pública Comutada (PSTN) 112 através dos canais de transporte de retorno apropriados. Uma estação móvel sem fio típica pode incluir um telefone portátil, ou um computador laptop. O sistema de comunicação sem fio 100 pode empregar qualquer um de um número de técnicas de acesso múltiplo tais como o acesso múltiplo por divisão de código (CDMA), acesso múltiplo por divisão de tempo (TDMA), acesso múltiplo por divisão de freqüência (FDMA), acesso múltiplo por divisão de espaço (SDMA), acesso múltiplo por divisão de polarização (PDMA), ou outras técnicas de modulação conhecidas na arte.

Muitos dispositivos de baixo custo com potência de computação limitada estão sendo introduzidos no mercado

tais como smart cards e memória Flash (em muitos fatores de formas diferentes). Tais dispositivos podem exigir autenticação. Por exemplo, há um desejo de ter estes dispositivos mantendo direitos para uso com sistemas de Gerenciamento de Direitos Digitas (DRM). Antes de trocar direitos com estes dispositivos, deveria existir autenticação mútua de ambas as entidades envolvidas na troca para limitar a troca de entidades autorizadas. Estas modalidades fornecem um método eficiente para concretizar a autenticação mútua, e também fornecem uma troca confirmada de um segredo que pode ser usado em comunicações adicionais entre as entidades envolvidas. A eficiência é tanto em termos de potência como de velocidade de computação.

Como aparente a uma pessoa versada na técnica, os esquemas de autenticação mútua podem ser usados sempre que a autenticação mútua entre duas entidades é exigida. Os esquemas de autenticação mútua não são limitados às aplicações específicas (tal Gerenciamento de Direitos Digitas), sistemas, e dispositivos usados aqui para descrever as modalidades.

Uma modalidade da invenção realiza uma autenticação mútua com uma troca de chave confirmada usando a troca de 4 mensagens. Ela exige 2 verificações de assinatura de chave pública (+ 1 para cada certificado intermediário), 2 criptografias de chave pública, 2 decriptografias de chave pública, 2 gerações de hash e 2 verificações de hash. O número específico de trocas de mensagem, verificações de chave pública, decriptografias de chave pública, gerações de hash, e verificações de hash pode ser separado ou alterado para obter quantidades exigidas de segurança e de eficiência.

A eficiência do protocolo é melhorada minimizando o número de operações criptográficas de chave pública e

usando funções de hash para fornecer prova de posse do material de chave trocada.

Uma autenticação mútua eficiente e um protocolo de troca de chave confirmada são descritos para uso com dispositivos dedicados a computar (compute-bound). A eficiência é realizada minimizando o número de operações de chave pública e usando hashes criptográficos para fornecer prova de posse.

O protocolo é ilustrado com respeito a Figuras 2 e 3 que mostram um método 300 (Figura 3) para a autenticação mútua. As etapas abaixo correspondem às setas numeradas na Figura 3.

No método 300, a Entidade A, por exemplo, um agente DRM 202 da MS 102, envia a mensagem HelloA (etapa 302) à entidade B, por exemplo, um dispositivo de mídia removível seguro 204 (SRM) possuindo um agente SRM 206. O agente SRM gerencia acesso ao armazenamento seguro 208 no dispositivo SRM. (Um sistema de operação 210 do MS pode diretamente acessar o armazenamento geral 212 do dispositivo SRM.) HelloA consiste de hashes das Chaves de Raiz confiáveis (ou as próprias Chaves de Raiz) e as correntes de certificado correspondentes. Quando do recebimento desta mensagem, a entidade B encontra uma Chave Raiz que confia a partir da mensagem e encontra uma corrente de certificado sob a Chave Raiz selecionada. Ela verifica a cadeia de certificado da entidade A sob a Chave Raiz selecionada.

A entidade B gera um número aleatório RanB (etapa 304).

A entidade B envia a mensagem HelloB para a entidade A (etapa 306). HelloB consiste da cadeia de certificado da B sob a Chave Raiz selecionada e junto com RanB criptografada com a chave pública da entidade A a

partir da cadeia de certificado selecionada após a etapa 302. Quando do recebimento desta mensagem, a entidade A verifica a cadeia de certificado da entidade B. Se válida, ela decriptografa RanB com sua chave privada (que corresponde à Chave Raiz selecionada).

Observe que uma vez que a seleção de Chave de Raiz e a troca de cadeia de certificado ocorreram, a entidade A e a entidade B terão a cadeia de certificado uma da outra. Assim, estes parâmetros podem não precisar de ser enviados entre a entidade A e a entidade B nas mensagens futuras de HelloA e de HelloB para uma autenticação mútua futura. Nesse caso, a troca de cadeia de certificado nas etapas 302 e 306 pode ser opcional.

A entidade A gera RanA (etapa 308).

A entidade A envia a mensagem KeyConfirmA à entidade B (etapa 310). KeyConfirmA consiste de RanA concatenado com o hash de RanB concatenado com RanA (H[Rana |RanB]) e tudo isto criptografado com a chave pública da B. Quando do recebimento desta mensagem, a entidade B decriptografa-a. Usando o RanA decriptografado, verifica-se o hash de RanB concatenado com RanA. Nota: nesta etapa, a entidade B autenticou a entidade A e é assumido que a entidade A conhece RanB.

A entidade B envia a mensagem do KeyConfirmB para a entidade A (etapa 312). KeyConfirmB consiste do hash da parcela decriptografada da mensagem KeyConfirmA. Quando do recebimento desta mensagem, a entidade A verifica o hash. Nota: nesta etapa, a entidade A autenticou a entidade B e é assegurado que a entidade B conhece RanA.

Neste momento, ambas as entidades autenticaram-se uma a outra e confirmaram que elas cada uma compartilha os mesmos RanA e RanB. RanA e RanB podem agora ser usados para derivar uma chave de criptografia de sessão (SK) e uma

chave MAC (MK) com base em uma Função de Derivação Chave (KDF) para uso com comunicações adicionais entre as partes (etapa 314).

Os detalhes das mensagens são dados abaixo. A mensagem de HelloA é enviada para iniciar a autenticação mútua com protocolo de confirmação de chave. A HelloA tem um parâmetro de "versão" e um parâmetro "rootAndChains[]". O parâmetro de versão pode ser um valor de 8 bits que contém a versão de protocolo desta mensagem. Ele é mapeado como os 5 MSBs para a versão principal e os 3 LSBs para a versão secundária. O parâmetro rootAndChains[] pode ser um arranjo dos hashes de raiz e de cadeias de certificado para a entidade A sob todos os modelos de confiança suportados pela A. A estrutura para o parâmetro, RootHashAndCertChain é um parâmetro rootHash, que é o hash de SHA-1 da chave pública de raiz do modelo de confiança, e um parâmetro certChain, a cadeia de certificado da entidade sob a chave pública de raiz. O certificado da entidade vem seguido primeiramente por todos os certificados de CA (em ordem de assinatura) até, mas não incluindo, o certificado de raiz.

A mensagem de HelloB continua a autenticação mútua com protocolo de confirmação chave pela entidade B. A tabela seguinte descreve os parâmetros. O HelloB tem os parâmetros: "versão", "status", "certChain", e "encRanB". O parâmetro de versão pode ser um valor de 8 bits que contém a versão de protocolo desta mensagem. É mapeado como os 5 MSBs para a versão principal e os 3 LSBs para a versão secundária. O parâmetro de status pode ser um valor de 8 bits que contém o status da entidade B processando a mensagem HelloA. Os valores para o parâmetro de status podem ser 0 para o sucesso - nenhum erro foi encontrado com a mensagem precedente, e 1 para o noSharedRootKey - entidade B não encontrou uma chave de raiz que compartilhe

com a entidade A. Os valores de 2 a 255 podem ser reservados para uso futuro. O parâmetro certChain é a cadeia de certificado da entidade B sob uma chave raiz selecionada a partir da mensagem HelloA. Se o valor do parâmetro de status não é bem sucedido, o parâmetro certChain não está presente. O parâmetro encRanB é um ranB criptografado de RSA-OAEP, usando a chave pública da entidade A (a partir da cadeia de certificado selecionada). O ranB pode ser um número aleatório de 20 bytes gerado pela entidade B. Se o valor do status não é bem sucedido, o parâmetro encRanB não está presente.

A mensagem KeyConfirmA continua a autenticação mútua com protocolo de confirmação de chave pela entidade A. A mensagem KeyConfirmA tem um parâmetro de "versão" e um parâmetro "encRanB". O parâmetro de versão pode ser um valor de 8 bits que contém a versão de protocolo desta mensagem. Pode ser mapeado como os 5 MSBs para a versão principal e os 3 LSBs para a versão secundária. O parâmetro encRanB pode ser uma estrutura de KeyConfirmData criptografada de RSA-OAEP possuindo um parâmetro "ranA" e um parâmetro "hashBA". O parâmetro de RanA pode ser um número aleatório de 20 bytes gerado pela entidade A, e o parâmetro hashBA pode ser o hash de SHA-1 de ranB concatenado com RanA.

A mensagem do KeyConfirmB finaliza a autenticação mútua com protocolo de confirmação de chave pela entidade B. A mensagem KeyConfirmB tem um parâmetro "versão", um parâmetro de status, e um parâmetro "hashKeyConfirm". O parâmetro de versão pode ser um valor de 8 bits que contém a versão de protocolo desta mensagem. Pode ser mapeado como os 5 MSBs para a versão principal e os 3 LSBs para a versão secundária. O parâmetro de status pode ser um valor de 8 bits que contém o status da entidade B processando a

mensagem. O parâmetro hashKeyConfirm pode ser o hash de SHA-1 da estrutura de KeyConfirmData que foi decriptografada pela entidade B. Se o valor do parâmetro de status não é bem sucedido, este parâmetro não está presente.

Um outro aspecto da invenção pode residir em uma estação móvel 102 que inclui um processador de controle 216 e o OS 210 para fazer com que o agente DRM 202 execute o método 300. Contudo, um outro aspecto da invenção pode residir em um produto de programa de computador que compreende meio legível por computador (tal como um dispositivo de memória 218) compreendendo código para fazer com que um computador faça com que o agente de DRM execute as etapas do método 300.

Aqueles versados na técnica devem entender que as informações e sinais pode ser representados usando qualquer uma de uma variedade de diferentes tecnologias e técnicas. Por exemplo, dados, instruções, comandos, informações, sinais, bits, símbolos, e chips que podem ser referenciados por toda a descrição acima podem ser representados por tensões, correntes, ondas eletromagnéticas, campos ou partículas magnéticas, campos ou partículas óticas ou qualquer combinação dos mesmos.

Aqueles versados na técnica devem ainda estimar que os vários blocos, módulos, circuitos, e etapas de algoritmo lógicos ilustrativos descritos com relação às modalidades descritas aqui podem ser implementados como hardware eletrônico, software de computador, ou combinações de ambos. Para ilustrar de forma clara esta intercambialidade de hardware e software, vários componentes, blocos, módulos, circuitos, e etapas ilustrativos foram descritos acima geralmente em termos de sua funcionalidade. Se tal funcionalidade é implementada

como hardware ou software depende das restrições específicas de aplicação e projeto impostas no sistema como um todo. Versados na técnica podem implementar a funcionalidade descrita de várias formas para cada aplicação específica, mas tais decisões de implementação não devem ser interpretadas como causando um afastamento do escopo da presente revelação.

Os vários blocos, módulos, e circuitos lógicos ilustrativos descritos em relação à revelação aqui podem ser implementados ou realizados com um processador de propósito geral, um processador de sinal digital (DSP), um circuito integrado de aplicação específica (ASIC), um arranjo de porta programável em campo (FPGA) ou outro dispositivo lógico programável, porta discreta ou lógica de transistor, componentes de hardware discretos, ou uma combinação dos mesmos projetada para realizar as funções descritas aqui. Um processador de propósito geral pode ser um microprocessador, mas na alternativa, o processador pode ser qualquer processador, controlador, microcontrolador, ou máquina de estado convencional. Um processador pode também ser implementado como uma combinação de dispositivos de computação, por exemplo, uma combinação de um DSP e um microprocessador, uma pluralidade de microprocessadores, um ou mais microprocessadores em conjunto com um núcleo DSP, ou qualquer outra tal configuração.

As etapas de um método ou algoritmo descritas em relação às modalidades reveladas aqui podem ser incorporadas diretamente em hardware, em um módulo de software executado por um processador, ou em uma combinação dos dois. Um módulo de software pode residir em memória RAM, memória flash, memória ROM, memória EPROM, memória EEPROM, registradores, disco rígido, disco removível, um CD-ROM, ou qualquer outra forma de meio de armazenamento

conhecida na técnica. Um meio de armazenamento exemplar é acoplado ao processador tal que o processador possa ler informações de, e escrever informações em, o meio de armazenamento. Na alternativa, o meio de armazenamento pode ser integrado ao processador. O processador e o meio de armazenamento podem residir em um ASIC. O ASIC pode residir em um terminal de usuário. Na alternativa, o processador e o meio de armazenamento podem residir como componentes discretos em um terminal de usuário.

Em uma ou mais modalidades exemplares, as funções descritas podem ser executadas em hardware, software, firmware, ou qualquer combinação desses. Se implementado em software, as funções podem ser armazenadas em ou transmitidas sobre uma ou mais instruções ou código em um meio legível por computador. Os meios legíveis por computador incluem tanto os meios de armazenamento de computador como os meios de comunicação que incluem qualquer meio que facilita transferência de um programa de computador a partir de um lugar a outro. Os meios de armazenamento podem ser quaisquer meios disponíveis que podem ser acessados por um computador. Como exemplo, e não limitação, tais meios legíveis por computador podem compreender RAM, ROM, EEPROM, CD-ROM ou outro armazenamento de disco ótico, armazenamento de disco magnético ou outros dispositivos de armazenamento magnético, ou qualquer outro meio que pode ser usado para carregar ou armazenar código de programa desejado sob a forma de instruções ou estruturas de dados e que pode ser acessado por um computador. Também, qualquer conexão é denominada adequadamente um meio legível por computador. Por exemplo, se o software é transmitido a partir de uma página da Web, servidor, ou de outra fonte remota usando um cabo coaxial, cabo de fibra óptica, par trançado, linha de assinante

digital (DSL), ou tecnologias sem fio tais como o infravermelho, rádio, e microondas, a seguir o cabo coaxial, cabo de fibra óptica, par trançado, DSL, ou tecnologias sem fio tais como o infravermelho, rádio, e microondas são incluídas na definição de meio. Disquete e disco, como usados aqui, incluem disco compacto (CD), disco laser, disco ótico, disco digital versátil (DVD), disquete flexível e disco blu-ray onde discos usualmente reproduzem dados magneticamente, enquanto discos reproduzem dados oticamente com lasers. Combinações dos acima deveriam também ser incluídas dentro do escopo dos meios legíveis por computador.

A prévia descrição das modalidades reveladas é fornecida para habilitar qualquer pessoa versada na técnica de fazer ou usar a presente invenção. Várias modificações a estas modalidades estarão prontamente aparentes aqueles versados na técnica, e os princípios gerais definidos aqui podem ser aplicados a outras modalidades sem se afastar do espírito ou escopo da revelação. Dessa forma, a presente revelação não tem intenção de ser limitada às modalidades mostradas aqui, mas deve ser acordado o escopo mais amplo consistente com os princípios e características novas revelados aqui.

REIVINDICAÇÕES

1. Um método para autenticação mútua entre primeira entidade e uma segunda entidade compreendendo:

a primeira entidade iniciar autenticação mútua enviando uma mensagem à segunda entidade;

a segunda entidade verificar uma primeira chave pública associada com a primeira entidade, gerar um primeiro número aleatório, criptografar o primeiro número aleatório usando a primeira chave pública, e enviar o primeiro número aleatório criptografado em uma mensagem para a primeira entidade;

a primeira entidade verificar uma segunda chave pública associada com a segunda entidade, decriptografar o primeiro número aleatório criptografado usando uma primeira chave privada correspondendo à primeira chave pública, gerar um segundo número aleatório, gerar um primeiro hash com base no pelo menos primeiro número aleatório, criptografar o segundo número aleatório e o primeiro hash usando a segunda chave pública, e enviar o segundo número aleatório criptografado e primeiro hash em uma mensagem para a segunda entidade;

a segunda entidade decriptografar o segundo número aleatório criptografado e primeiro hash usando uma segunda chave privada correspondendo à segunda chave pública, verificar o primeiro hash para autenticar a primeira entidade, gerar um segundo hash com base no pelo menos segundo número aleatório, e enviar o segundo hash para a primeira entidade; e

a primeira entidade verificar o segundo hash para autenticar a segunda entidade.

2. Um método para autenticação mútua, de acordo com a reivindicação 1, em que a primeira entidade e a segunda entidade cada uma deriva uma chave de criptografia

de sessão e chave de código de autenticação de mensagem (MAC) usando o primeiro número aleatório e o segundo número aleatório com base em uma função de derivação de chave, para uso em comunicações entre a primeira entidade e a segunda entidade.

3. Um método para autenticação mútua, de acordo com a reivindicação 1, em que a mensagem iniciando autenticação mútua inclui um hash de pelo menos uma Chave Raiz confiável e uma cadeia de certificado correspondente para a primeira entidade.

4. Um método para autenticação mútua, de acordo com a reivindicação 1, em que a mensagem a partir da segunda entidade para a primeira entidade possuindo o primeiro número aleatório criptografado inclui adicionalmente uma cadeia de certificado para a segunda entidade.

5. Um método para autenticação mútua, de acordo com a reivindicação 1, em que a primeira entidade é um agente de direito digitais e a segunda entidade é um dispositivo de mídia removível seguro.

6. Um método para autenticação mútua, de acordo com a reivindicação 1, em que a primeira entidade é uma estação móvel.

7. Um método para autenticação mútua, de acordo com a reivindicação 1, em que a segunda entidade possui potência de processamento limitada.

8. Um método para autenticação mútua, de acordo com a reivindicação 1, em que o primeiro hash é baseado adicionalmente no pelo menos segundo número aleatório tal que o primeiro hash é gerado com base no pelo menos primeiro número aleatório concatenado com o segundo número aleatório.

9. Um método para autenticação mútua, de acordo com a reivindicação 1, em que o segundo hash é baseado adicionalmente no pelo menos primeiro número aleatório.

10. Um método para autenticação mútua, de acordo com a reivindicação 1, em que o segundo hash é baseado adicionalmente com base no pelo menos primeiro hash tal que o segundo hash é gerado com base no pelo menos segundo número aleatório concatenado com o primeiro hash.

11. Equipamento para autenticação mútua compreendendo:

meios para iniciar autenticação mútua;

meios para verificar uma primeira chave pública, gerar um primeiro número aleatório, e criptografar o primeiro número aleatório usando a primeira chave pública;

meios para verificar uma segunda chave pública, decriptografar o primeiro número aleatório criptografado usando uma primeira chave privada correspondendo à primeira chave pública, gerar um segundo número aleatório, gerar um primeiro hash com base no pelo menos primeiro número aleatório, e criptografar o segundo número aleatório e o primeiro hash usando a segunda chave pública;

meios para decriptografar o segundo número aleatório criptografado e primeiro hash usando uma segunda chave privada correspondendo à segunda chave pública, verificar o primeiro hash para autenticação, e gerar um segundo hash com base no pelo menos segundo número aleatório; e

meios para verificar o segundo hash para autenticação.

12. Equipamento para autenticação mútua, de acordo com a reivindicação 11, compreendendo adicionalmente meios para derivar uma chave de criptografia de sessão e chave de código de autenticação de mensagem (MAC) usando o

primeiro número aleatório e o segundo número aleatório com base em uma função de derivação de chave, para uso em comunicações entre a primeira entidade e a segunda entidade.

13. Equipamento para autenticação mútua, de acordo com a reivindicação 11, em que o primeiro hash é baseado adicionalmente no pelo menos segundo número aleatório tal que o primeiro hash é gerado com base no pelo menos primeiro número aleatório concatenado com o segundo número aleatório.

14. Equipamento para autenticação mútua, de acordo com a reivindicação 11, em que o segundo hash é baseado adicionalmente no pelo menos primeiro número aleatório.

15. Equipamento para autenticação mútua, de acordo com a reivindicação 11, em que o segundo hash é baseado adicionalmente no primeiro hash tal que o segundo hash é gerado com base no segundo número aleatório concatenado com o primeiro hash.

16. Uma estação possuindo autenticação mútua com um dispositivo de mídia removível seguro, compreendendo:

um agente de direitos digitais, em que:

o agente de direitos digitais inicia autenticação mútua enviando uma mensagem ao dispositivo de mídia removível seguro, em que o dispositivo de mídia removível seguro verifica uma primeira chave pública associada com o agente de direitos digitais, gera um primeiro número aleatório, criptografa o primeiro número aleatório usando a primeira chave pública, e envia o primeiro número aleatório em uma mensagem ao agente de direitos digitais;

o agente de direito digitais verifica uma segunda chave pública associada com o dispositivo de mídia removível seguro, decriptografa o primeiro número aleatório

criptografado usando uma primeira chave privada correspondendo à primeira chave pública, gera um segundo número aleatório, gera um primeiro hash com base no pelo menos primeiro número aleatório, criptografa o segundo número aleatório e o primeiro hash usando a segunda chave pública, e envia o segundo número aleatório criptografado e primeiro hash em uma mensagem para o dispositivo de mídia removível seguro, em que o dispositivo de mídia removível decriptografa o segundo número aleatório criptografado e primeiro hash usando uma segunda chave privada correspondendo à segunda chave pública, verifica o primeiro hash para autenticar o agente de direitos digitais, gera um segundo hash com base no pelo menos segundo número aleatório, e envia o segundo hash para o agente de direitos digitais; e

o agente de direito digitais verifica o segundo hash para autenticar o dispositivo de mídia removível seguro.

17. Uma estação possuindo autenticação mútua, de acordo com a reivindicação 16, em que o agente de direitos digitais e o dispositivo de mídia removível seguro cada um deriva uma chave de criptografia de sessão e chave de código de autenticação de mensagem (MAC) usando o primeiro número aleatório e o segundo número aleatório com base em uma função de derivação de chave, para uso em comunicações entre o agente de direitos digitais e o dispositivo de mídia removível seguro.

18. Uma estação possuindo autenticação mútua, de acordo com a reivindicação 16, em que a mensagem enviada pelo agente de direitos digitais para iniciar autenticação mútua inclui um hash de pelo menos uma Chave Raiz confiável e uma cadeia de certificado correspondente para o agente de direitos digitais.

19. Uma estação possuindo autenticação mútua, de acordo com a reivindicação 18, em que a cadeia de certificado para o agente de direitos digitais inclui a chave pública associada com o agente de direitos digitais.

20. Uma estação possuindo autenticação mútua, de acordo com a reivindicação 16, em que a mensagem enviada pelo dispositivo de mídia removível seguro para o agente de direitos digitais possuindo o primeiro número aleatório criptografado inclui adicionalmente uma cadeia de certificado para o dispositivo de mídia removível seguro.

21. Uma estação possuindo autenticação mútua, de acordo com a reivindicação 20, em que a cadeia de certificado para o dispositivo de mídia removível seguro inclui a chave pública associada com o dispositivo de mídia removível seguro.

22. Uma estação possuindo autenticação mútua, de acordo com a reivindicação 16, em que a estação é uma estação móvel.

23. Uma estação possuindo autenticação mútua, de acordo com a reivindicação 16, em que o primeiro hash é baseado adicionalmente no pelo menos segundo número aleatório tal que o agente de direitos digitais gera o primeiro hash com base no pelo menos primeiro número aleatório concatenado com o segundo número aleatório.

24. Um produto de programa de computador, compreendendo:

meio legível por computador compreendendo:

código para fazer com que um computador faça com que um agente de direitos digitais de uma estação inicie autenticação mútua enviando uma mensagem para um dispositivo de mídia removível seguro, em que o dispositivo de mídia removível seguro verifica uma primeira chave pública associada com o agente de direitos digitais, gera

um primeiro número aleatório, criptografa o primeiro número aleatório usando a primeira chave pública, e envia o primeiro número aleatório em uma mensagem ao agente de direitos digitais;

código para fazer com que um computador faça com que o agente de direito digitais verifique uma segunda chave pública associada com o dispositivo de mídia removível seguro, decriptografe o primeiro número aleatório criptografado usando uma primeira chave privada correspondendo à primeira chave pública, gere um segundo número aleatório, gere um primeiro hash com base no pelo menos primeiro número aleatório, criptografe o segundo número aleatório e o primeiro hash usando a segunda chave pública, e envie o segundo número aleatório criptografado e primeiro hash em uma mensagem para o dispositivo de mídia removível seguro, em que o dispositivo de mídia removível decriptografa o segundo número aleatório criptografado e primeiro hash usando uma segunda chave privada correspondendo à segunda chave pública, verifica o primeiro hash para autenticar o agente de direitos digitais, gera um segundo hash com base no pelo menos segundo número aleatório, e envia o segundo hash para o agente de direitos digitais; e

código para fazer com que um computador faça com que o agente de direito digitais verifique o segundo hash para autenticar o dispositivo de mídia removível seguro.

25. Um produto de programa de computador, compreendendo:

meio legível por computador compreendendo:

código para fazer com que um computador faça com que um dispositivo de mídia removível seguro verifique uma primeira chave pública associada com um

agente de direitos digitais, gere um primeiro número aleatório, criptografe o primeiro número aleatório usando a primeira chave pública, e envie o primeiro número aleatório em uma mensagem ao agente de direitos digitais, em que o agente de direito digitais verifique uma segunda chave pública associada com o dispositivo de mídia removível seguro, decriptografe o primeiro número aleatório criptografado usando uma primeira chave privada correspondendo à primeira chave pública, gere um segundo número aleatório, gere um primeiro hash com base no pelo menos primeiro número aleatório, criptografe o segundo número aleatório e o primeiro hash usando a segunda chave pública, e envie o segundo número aleatório criptografado e primeiro hash em uma mensagem para o dispositivo de mídia removível seguro;

código para fazer com que um computador faça com que o dispositivo de mídia removível decriptografe o segundo número aleatório criptografado e primeiro hash usando uma segunda chave privada correspondendo à segunda chave pública, verifique o primeiro hash para autenticar o agente de direitos digitais, gere um segundo hash com base no pelo menos segundo número aleatório, e envie o segundo hash para o agente de direitos digitais, em que o agente de direito digitais verifica o segundo hash para autenticar o dispositivo de mídia removível seguro.

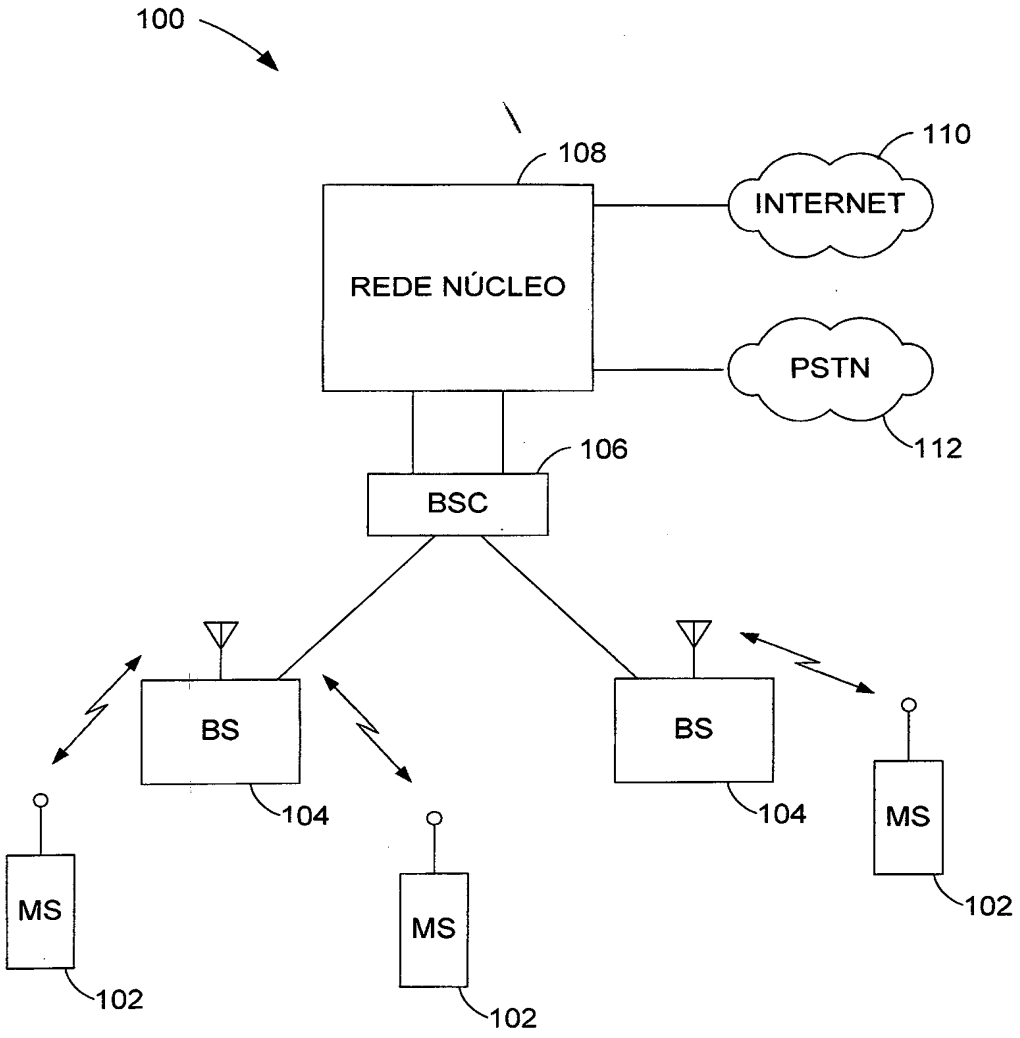
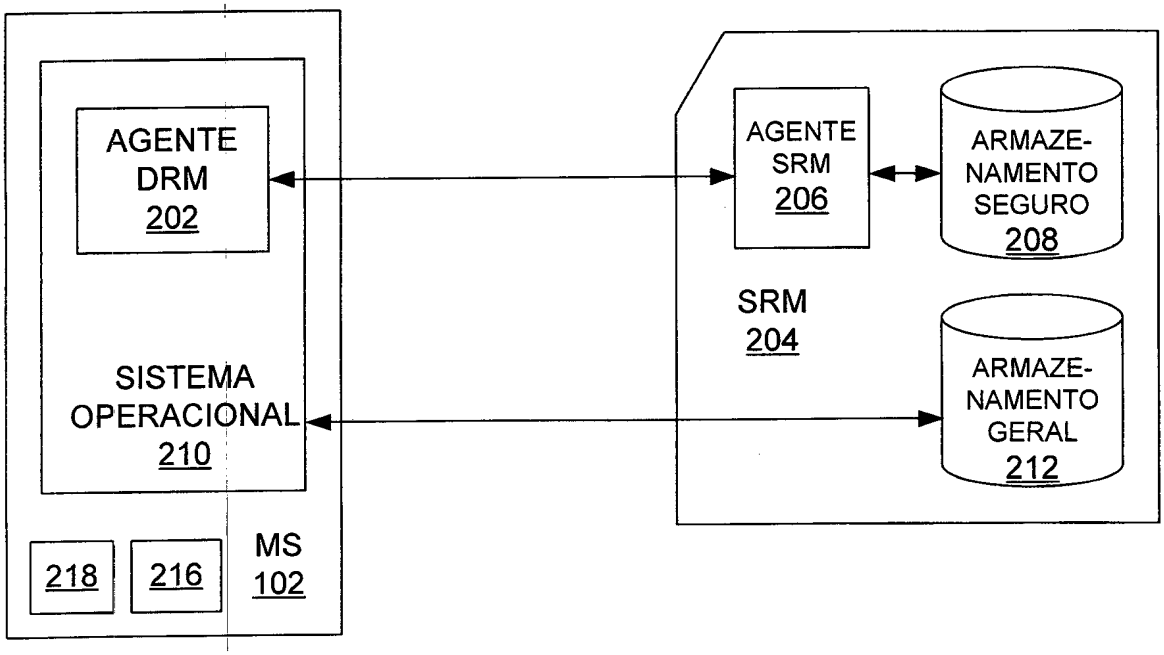

100
108
110
INTERNET
REDE NÚCLEO
PSTN
112
106
BSC
BS
BS
104
104
MS
MS
MS
102
102
102

FIG. 1

FIG. 2


AGENTE
DRM
202
SISTEMA
OPERACIONAL
210
218
216
MS
102
AGENTE
SRM
206
ARMAZE-
NAMENTO
SEGURO
208
SRM
204
ARMAZE-
NAMENTO
GERAL
212

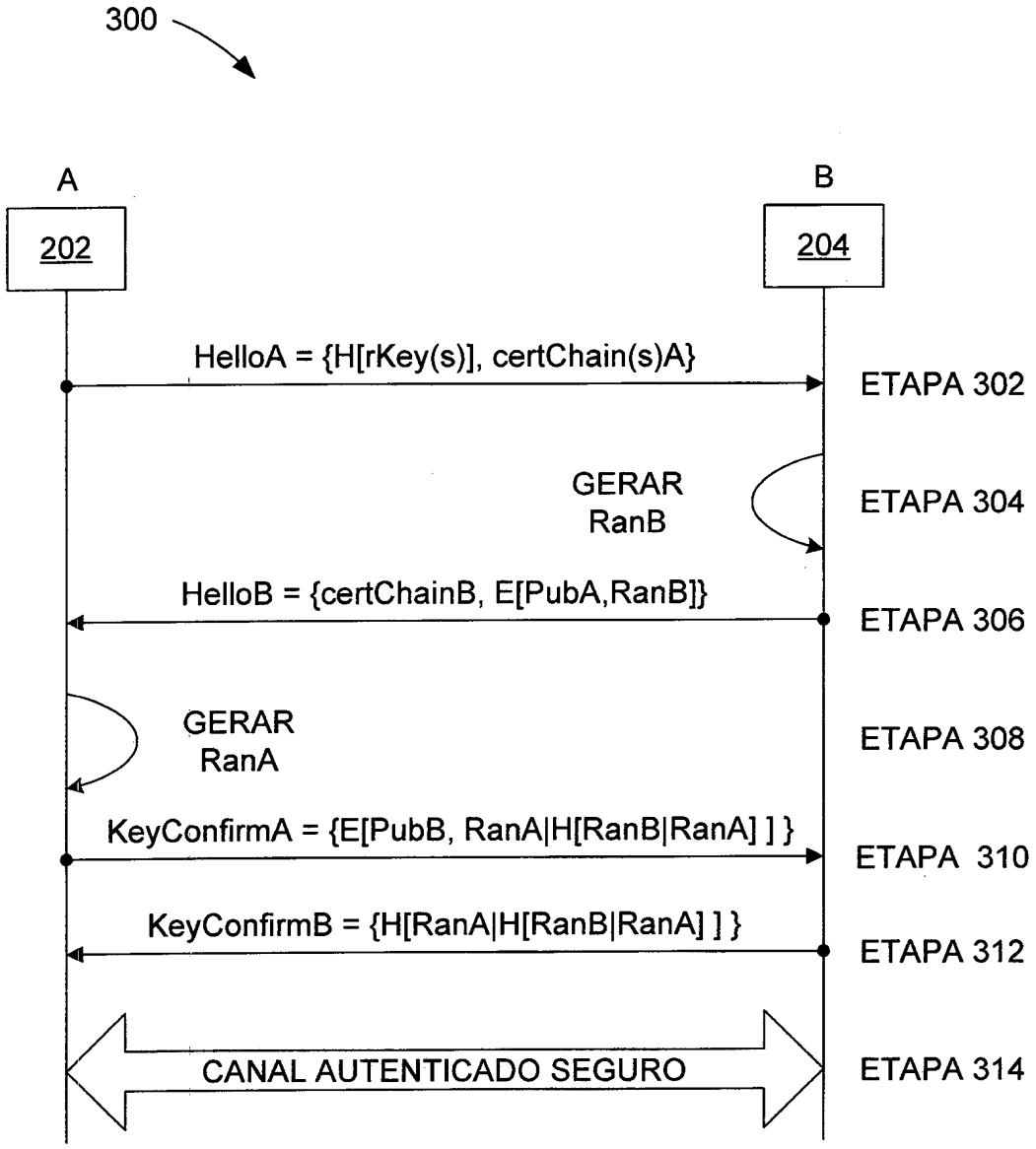

300
A
202
B
204
HelloA = {H[rKey(s)], certChain(s)A}
ETAPA 302
GERAR
RanB
ETAPA 304
HelloB = {certChainB, E[PubA,RanB]}
ETAPA 306
GERAR
RanA
ETAPA 308
KeyConfirmA = {E[PubB, RanA|H[RanB|RanA]] }
ETAPA 310
KeyConfirmB = {H[RanA|H[RanB|RanA]] }
ETAPA 312
CANAL AUTENTICADO SEGURO
ETAPA 314

FIG. 3

RESUMO

"MÉTODO E EQUIPAMENTO PARA AUTENTICAÇÃO MÚTUA"

É revelado um método para autenticação mútua entre uma estação, possuindo um agente de direitos digitais, e um dispositivo de mídia removível seguro. O agente de direitos digitais inicia autenticação mútua enviando uma mensagem ao dispositivo de mídia removível seguro. O dispositivo de mídia removível seguro criptografa um primeiro número aleatório usando uma chave pública associada com o agente de direitos digitais. O agente de direitos digitais decriptografa o primeiro número aleatório criptografado, e criptografa um segundo número aleatório e um primeiro hash com base no pelo menos primeiro número aleatório. O dispositivo de mídia removível seguro descriptografa o segundo número aleatório criptografado e o primeiro hash, verifica o primeiro hash para autenticar o agente de direitos digitais, e gera um segundo hash com base no pelo menos segundo número aleatório. O agente de direitos digitais verifica o segundo hash para autenticar o dispositivo de mídia removível seguro.