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

(11) PI 0408069-6 B1

(22) Data do Depósito: 05/03/2004

(45) Data de Concessão: 30/05/2017

(54) Título: MÉTODOS PARA UMA AUTENTICAÇÃO MÚTUA ENTRE UM USUÁRIO E UMA REDE DE COMUNICAÇÕES E PARA PERMITIR A UM USUÁRIO VERIFICAR A CONFIABILIDADE DE UMA REDE DE COMUNICAÇÕES

(51) Int.Cl.: H04L 9/06; H04W 12/06; H04W 12/12; H04L 29/06; H04L 12/28; H04L 12/70

(30) Prioridade Unionista: 06/03/2003 IT RM2003A000100

(73) Titular(es): TIM ITALIA S.P.A.

(72) Inventor(es): MAURIZIO MARCELLI

"MÉTODOS PARA UMA AUTENTICAÇÃO MÚTUA ENTRE UM USUÁRIO E UMA REDE DE COMUNICAÇÕES E PARA PERMITIR A UM USUÁRIO VERIFICAR A CONFIABILIDADE DE UMA REDE DE COMUNICAÇÕES"

[0001] A presente invenção refere-se a um método para autenticação em uma rede de comunicações, especialmente um pacote, *e.g.* em uma rede IP (Protocolo de Internet).

[0002] O forte crescimento no número de usuários da Internet tem sido um dos fenômenos mais notáveis nas comunicações nos últimos anos. A Internet gerou e desenvolveu uma "rede aberta", adaptada para compartilhar informações entre usuários. Aplicações, tal como e-mail, a navegação em páginas da Web, o baixar arquivos, baseado sobre protocolos de comunicações na Internet tal como o SMTP (Simple Mail Transfer Protocol), o FTP (File Transfer Protocol) ou o HTTP (Hyper Text Transfer Protocol) são agora de conhecimento comum e usados por número continuamente crescente de usuários. A tecnologia da Internet também vem sendo usada em contextos não abertos para o público, tais como redes de área local corporativas, para compartilhar informações entre empregados, em um ambiente denominado Intranet. Recentemente, a tecnologia W-LAN (Redes de Área Local Sem Fio) também nasceu e vem sendo desenvolvida, permitindo aos usuários de Internet ou Intranet a conectarem-se com a rede sem a necessidade de um cabo, explorando adaptadores de terminal de rede sem fio e pontos de acesso.

[0003] Para conectar-se com a rede, uma técnica bem conhecida provê que o usuário forneça suas credenciais na forma de um ID de usuário e uma senha associada a um servidor de autenticação, possivelmente pertencente a um provedor de serviços. Por exemplo, RADIUS (Remote Autentication Dial-In User Service) é um servidor conhecido para autenticação de usuário remoto baseado sobre um esquema de user-D/senha.

[0004] Outro método proposto para autenticação a ser realizado para

acessar uma rede, especialmente uma rede IP, é apresentado no pedido de patente PCT nº00/0206, em nome da Nokia Networks OY. Para permitir a autenticação de usuários de redes IP em uma área geograficamente extensa, o terminal da rede IP utiliza um terminal de identidade de usuário (SIM) conforme usado em um sistema de comunicações móvel separado, com o qual uma resposta pode ser determinada a partir de um pedido de senha fornecido ao módulo de identidade como entrada. A rede IP inclui um servidor de segurança especial ao qual uma mensagem acerca de um novo usuário é transmitida quando um assinante se liga à rede IP. A informação de autenticação contendo pelo menos um pedido de senha e uma resposta é buscada do sistema de comunicações móvel para a rede IP e a autenticação é realizada baseada sobre as informações de autenticação obtida do sistema de comunicações móvel transmitindo o pedido de senha através da rede IP para o terminal, gerando uma resposta do pedido de senha ao módulo de identidade do terminal e comparando a resposta com a resposta recebida do sistema de comunicações móvel. Praticamente, conforme exposto no mesmo pedido de patente PCT, o método de autenticação de uma rede de comunicações móvel existente, especialmente uma rede GSM (Global System for Mobile communications), é usado em uma rede IP.

[0005] Sem entrar em detalhes específicos, um procedimento de autenticação típico usado em uma rede de comunicação móvel, tal como uma rede GSM, assegura que quando um terminal móvel solicita ligar-se à rede móvel, primeiramente transmite o IMSI (Identificador de Assinante Móvel Internacional), armazenado no SIM associado com o terminal móvel, para a rede. Um Centro de Autenticação (AuC) recebe o número IMSI e gera um número aleatório RAND que é introduzido em um algoritmo dedicado à autenticação (o denominado algoritmo A3). O algoritmo é convertido em parâmetro com uma chave de criptografia $\mathbf{k}_i$ singularmente associada com o número IMSI, dá como um resultado uma denominada Resposta Assinada

SRES1. O número aleatório RAND é também transmitido para o terminal móvel, especificamente para o SIM associado com o terminal móvel, para sua confrontação com a geração de uma Resposta Assinada SRES2, que é possibilitada a partir do fato de que a SIM armazena a mesma chave de criptografia k_i e algoritmo A3. SRES2 é então transmitido para o AuC, que verifica a correspondência entre SRES1 e SRES2 de modo a conceder acesso na rede móvel ao terminal móvel. Se a correspondência entre SRES1 e SRES2 não é verificada, o acesso à rede móvel é negado.

[0006] O uso do procedimento de autenticação acima mencionado para conexão com uma rede de comunicação diferente de uma rede móvel, tal como a Internet ou uma Intranet empresarial, aperfeiçoa a segurança com respeito a um procedimento somente requerendo o fornecimento de uma user-ID e de uma senha. Por exemplo, um provedor de serviços pode ser substancialmente assegurado que as credenciais dadas do usuário requerendo a conexão são genuínas, isto é, de que o usuário é efetivamente um de seus assinantes.

[0007] Todavia, a requerente observa que o uso do procedimento de autenticação acima mencionado não oferece garantias ao usuário da mesma maneira com respeito ao provedor de serviços, isto é, não assegura ao usuário que ele/ela não esteja fornecendo seus dados confidenciais a uma falsa rede, através de um falso ponto de acesso, prestado por uma entidade maliciosa pretendendo ser o provedor de serviços do usuário. Particularmente, a Requerente observa que uma vez que a correspondência entre a Resposta Assinada SRES1 gerada no AUC e a Resposta Assinada SRES2 gerada no SIM do usuário é somente realizada no lado da rede, o usuário não tem como verificar que ele/ela está efetivamente acessando a sua rede confiável;

[0008] A requerente observa ainda que tal problema é de especial importância no acessar redes explorando a tecnologia W-LAN, pelo fato de que pontos falsos de acesso a W-LAN são relativamente fáceis de serem

implementados.

[0009] A requerente enfrentou o problema de implementar um método de autenticação, particularmente adaptado para acessar uma rede de comunicações, mais particularmente uma rede baseada em pacote (*e.g.* IP), em que uma identificação mútua pode ser garantida entre um assinante e um provedor de serviços em ambas as direções.

[00010] A requerente verificou que este problema pode ser resolvido por um método de autenticação em que um número aleatório é gerado no terminal de assinante. O número aleatório é transmitido para o subsistema de autenticação gerenciando a autenticação do assinante para o acesso à rede, *e.g.* juntamente com um identificador de assinante. No subsistema de autenticação, o identificador é usado para verificar as credenciais do assinante. Durante o método de autenticação, parâmetros relacionados com o identificador do assinante são gerados no subsistema de autenticação, e o número aleatório é criptografado usando uma chave de sessão formada usando estes parâmetros. O número aleatório criptografado é então transmitido de volta ao terminal de assinantes, juntamente com informações necessárias para o terminal de modo a reconstruir a chave de sessão. Após ter reconstruído a chave de sessão, o terminal de assinante decodifica o número aleatório e testa a correspondência com o seu número aleatório gerado. A correspondência entre os dois números permite a verificação pelo assinante, de que o ponto de acesso está se conectado não é um falso ponto de acesso

[00011] Sob um primeiro aspecto, a invenção trata de um método de autenticação mútuo entre um usuário e uma rede de comunicações conforme exposto na reivindicação 1. Versões preferenciais do método do primeiro aspecto são expostas nas Reivindicações 2 a 13

[00012] Sob um segundo aspecto, a invenção trata de um método para permitir que um usuário verifique a confiabilidade de uma rede de comunicações conforme exposto na reivindicação 14. Versões preferenciais

do método do segundo aspecto são expostas nas reivindicações 15 a 22.

[00013] Sob um terceiro aspecto, a invenção trata de um método que permite a um usuário verificar a confiabilidade de uma rede de comunicações conforme exposto na reivindicação 27.

[00014] Os aspectos característicos e vantagens da invenção se evidenciarão da descrição detalhada que se segue de algumas modalidades da mesma, apresentadas meramente a título de exemplos não limitativos, a descrição será conduzida reportando-se aos desenhos apensos, em que:

- A figura 1 mostra uma modalidade esquemática de uma arquitetura de rede de comunicações usada na presente invenção;
- A figura 2 mostra uma troca típica de mensagens se processando entre vários elementos de rede durante o procedimento de autenticação da invenção.

[00015] A figura 1 mostra uma modalidade esquemática de uma arquitetura de rede de comunicações, em que um usuário remoto conecta-se com um ponto de acesso 2 de maneira a obter acesso a uma rede IP 7, por exemplo a Internet. Diferentes pontos de acesso 2 podem ser oferecidos por um provedor de serviços para permitir o acesso à rede por diferentes usuários remotos localizados em diferentes pontos geográficos.

[00016] O usuário remoto tem um terminal 1, tal como um computador pessoal, por exemplo um computador portátil, que porta software de cliente apropriado (*e.g.*um programa de software baseado sobre RADIUS) e hardware adaptado para conectar-se com a rede 7 através do ponto de acesso 2. Para esta finalidade, o computador 1 é por exemplo associado com um modem (*e.g.*, um modem ISDN) e explora uma conexão de discar, ou um modem xDSL e explora uma conexão xDSL, ou um modem GPRS e explora uma conexão sem fio, ou um adaptador de terminal LAN Sem fio (WLAN) e explora uma conexão W-LAN (tal como uma conexão WI-FI – Wireless Fidelity, um tipo de acesso a Internet que vem se tornando popular em áreas

tais como hotéis e aeroportos) para o ponto de acesso 2.

[00017] Para obter acesso à rede 7, o usuário é autenticado pelo provedor de serviços. Para fins de autenticação, o usuário remoto é munido de um módulo de identidade de assinante 1', particularmente (embora não limitadamente) um Módulo de Identidade de Assinante (SIM) do tipo usado para fins de autenticação em Sistema de Telefonia Celular (DCSs) ou Public Land Mobile Networks (PLMNs), tais como as redes de telefonia móvel bem difundidas designadas de Sistema Global para comunicações Móveis (GSM) ou suas extensões conhecidas tais como General Packet Radio Service (GPRS) (que efetivamente é uma subrede da rede GSM), redes Universal Móbile Telecommunications System (UMTS) (um sistema de comunicação celular de terceira geração de banda larga), ou uma rede de comunicação móvel baseada em satélite.

[00018] Conforme conhecido da técnica, um SIM normalmente assume a forma de um cartão (da dimensão de um cartão de crédito ou menor, dependendo da escala de miniaturização do terminal de usuário), componentes de circuito integrado embutidos, particularmente armazenando dados personalizados que suportam autenticação do SIM, assim codificação e decodificação. Pelo menos até agora, o uso de um SIM (e do método de autenticação baseado em SIM) para identificar um terminal de comunicação móvel acoplado com o mesmo comprovou ser uma maneira robusta de tornar impossível para outros dispositivos personificar aquele terminal, assim prestando acesso autenticado seguro, *e.g.*, a uma conta correspondente aquele usuário específico.

[00019] O SIM 1' de usuário é operativamente, e de preferência amovivelmente acoplado com o comutador de usuário remoto 1; por exemplo,o SIM 1' é embutido em um dispositivo periférico de computador que pode ser operativamente acoplado com, de modo a ser funcionalmente acessível pelo computador 1,por exemplo uma chave de hardware conectável

com uma porta (não explicitamente mostrada na figura 1) do computador 1, *e.g.,* uma porta Universal Serial Bus (USB); alternativamente, o SIM 1 pode ser operativamente acoplado com o computador 1 através de uma porta PCMCIA do mesmo, ou por intermédio de um periférico do tipo de leitora de cartão inteligente adaptada para interagir com um SIM e ser acoplada com, *e.g.,* uma porta serial do computador 1, ou o SIM1 pode ser embutido em um cartão de memória que pode então ser operativamente acoplado com o computador 1 por intermédio de uma leitora de cartão inteligente, é acentuado que a maneira específica pela qual o SIM " é operativamente acoplado com o computador 1 não é limitativa para a presente invenção, sendo em geral suficiente que o SIM " seja operativamente acoplado com o computador 1 (de uma maneira própria para habilitar a comunicação entre o computador 1 e o SIM ") por intermédio de qualquer tipo de dispositivo adaptador/leitor conectado com o computador 1 através de qualquer tipo de porta periférica. O cliente de software adaptado para conectar-se com a rede 7, localizado no computador pessoal 1 é também adaptado para comunicar-se com o SIM 1' acoplado com o computador pessoal 1.

[00020] O ponto de acesso 2 é associado com um nó de acesso 5 que pode compreender um servidor de acesso à rede (NAS) 3 e uma porta (circuito de) 4. O nó de acesso 5 é operativamente conectado com um servidor de autenticação 6, possivelmente, como mostrado na figura 1, da rede móvel 8 de um operador móvel. O nó de acesso 5 é também conectado com a rede 7 à qual o usuário remoto está requerente acesso, possivelmente através de um servidor proxi 9, *e.g.* uma barreira de proteção particularmente se a rede 7 é uma rede privada tal como uma intranet empresarial.

[00021] Com referência ao nó de acesso 5, deve ser entendido que mesmo se a figura 1 mostrar um NAS 3 e uma porta (circuito de) 4 como entidades funcionais separadas dentro do nó de acesso 5, na prática podem corresponder a produtos de software convenientes residentes no mesmo

equipamento de hardware. O NAS 3 pode ser um roteador apropriado para rotear tráfego dirigido para e proveniente dos pontos de acesso 2. A porta (circuito de) 4 pode ser adaptada para selecionar onde o tráfego proveniente dos pontos de acesso 2 tem de ser direcionado, particularmente, durante o procedimento de autenticação solicitado por um usuário remoto conectado com um nó de acesso 2 o tráfego proveniente do nó de acesso 2 é dirigido no sentido do servidor de autenticação 6 (e vice versa), ao passo que uma vez que a autenticação do usuário remoto tenha sido verificada o tráfego proveniente do nó de acesso é dirigido no sentido da rede 7 (e vice versa).

[00022] O servidor de autenticação 6 é adaptado para receber informações de identificação do usuário remoto, de maneira a verificar que o usuário remoto é um usuário de confiança do serviço de acesso de rede. Outrossim, o servidor de autenticação 6 é também adaptado para munir o usuário remoto de informações próprias para permitir a verificação, pelo usuário remoto, do fato de que a rede com a qual ele/ela está se conectando não é uma falsa rede, oferecida por uma entidade pretendendo ser o provedor de serviços dele ou dela. Assim, o inteiro método de autenticação, que será explanado em detalhe a seguir, permite uma autenticação mútua entre o usuário remoto e o provedor de serviço; nas modalidades preferenciais o servidor de autenticação 6 está localizado nas instalações de operador de rede móvel e é adaptado para se comunicar com o Registro de Locação Doméstico (HLR) 6' do operador de rede móvel, de maneira a explorar, para a autenticação do usuário remoto, um procedimento de autenticação baseado sobre o procedimento de autenticação bem conhecido cumprido pelos terminais móveis exigindo acesso à rede móvel. Particularmente, o HLR 6' do operador de rede móvel inclui um banco de dados em que um identificador e uma chave singularmente associada com o usuário remoto estão armazenados. O dito identificador e a chave também são armazenados sobre o SIM 1´ do usuário remoto. Em outras palavras, o servidor de autenticação 6 desempenha

funções similares àquelas de um Registro de Localização de Visitante (VLR) incluído na rede de um operador de rede móvel de maneira a conceder ou negar acesso ao usuário remoto no sentido da rede IP 7: por esta razão, o servidor de autenticação 6 será designado a seguir de I-VLR 6. O I-VLR 6 pode processar software standard tal como RADIUS, para controlar pelo menos algumas etapas do procedimento de autenticação

[00023] Ao solicitar acesso à rede 7, o usuário remoto opera o software cliente dedicado para controlar a conexão com o ponto de acesso 2. A figura 2 mostra uma modalidade preferencial de um fluxo de mensagens trocadas entre os vários equipamentos da arquitetura de rede mostrada na figura 1.

[00024] Com referência à figura 2, o software cliente comunica-se com o SIM (100) de modo a recuperar (101) um identificador de usuário, tal como o International Móbile Subscriber Identity (IMSI) ou o Temporary Mobile Subscriber Identity (TMSI), armazenado no SIM. Outrossim, o software cliente gera um numeral, de preferência um número aleatório Ra que, como será esclarecido adiante, desempenha um papel na forma do procedimento de autenticação requerido de forma a permitir ao usuário autenticar o ponto de acesso 2 e a rede 7 como de "confiança". Aqui e a seguir, o termo "número" pode ser interpretado como qualquer número binário, octal, decimal, ou hexadecimal, ou mesmo como uma cadeia genérica de caracteres alfanuméricos.

[00025] O software cliente também controla a conexão com o NAS 3, através do ponto de acesso 2. Em uma etapa designada 102 na figura 2,o software cliente transmite para o NAS 3 o identificador recuperado do SIM e pelo menos uma parte do número aleatório Ra. Por exemplo, com referência específica a uma conexão baseada sobre RADIUS, o identificador IMSI e o número aleatório Ra podem ser conjuntamente concatenados no campo 'nome do usuário' no RADIUS, ao passo que o campo 'senha' do RADIUS pode ser preenchido com qualquer cadeia fixa (*e.g., "SIM_Auth_Subs"*) de modo a

aumentar a privacidade, o identificador e o número aleatório Ra podem ser transmitidos em forma criptografada. Para fins de codificação, o software cliente do usuário pode ser constituído de uma chave pública, *e.g.* uma chave RSA-baseada, fornecida em avanço pelo provedor de serviço, que por sua vez retém a chave privada correlata. Nas modalidades preferenciais, a chave pública tem um comprimento de pelo menos 1024 bits. O protocolo de conexão do computador pessoal1 do usuário remoto 1 e o NAS 3 podem ainda compreender a transmissão de um campo de domínio, por exemplo de maneira a permitir ao NAS 3 identificar diferentes tipos de solicitações de conexão, tal como por exemplo um pedido discado, um pedido xDSL ou um pedido WLAN. Vantajosamente, um único NS 3 pode gerenciar, de tal maneira diferentes tipos de conexões provenientes de vários tipos de pontos de acesso 2, também no caso de um pedido de conexão proveniente de um ponto de acesso de outros provedor de serviço. A título ilustrativo, o campo domínio pode ser preenchido com "@wl" identificando uma conexão W-LAN "@a" identificando uma conexão discada.

[00026] O Servidor de Acesso a Rede (NAS) encaminha (como mostrado em103 na figura 2) o identificador e o número aleatório Ra para o I-VLR 6. A decodificação do identificador e do número aleatório Ra pode ser realizada no NAS 3 ou, de preferência, no I-VLR 6. O I-VLR extrai o identificador de usuário, *e.g.*, o IMSI, e encaminha o mesmo (como mostrado em 104 na figura 2) para o HLR 6'. O HLR 6' (ou um Centro de Autenticação, AuC, conectado com o HLR 6') compreende um banco de dados em que uma chave única $\mathbf{k_i}$ é associada com o IMSI. A chave única $\mathbf{k_i}$ é também armazenada no SIM 1' do usuário remoto. Em outras palavras, a chave única $\mathbf{k_i}$ representa um segredo compartilhado entre o SIM 1' e o subsistema de autenticação da rede, compreendendo o I-VLR 6 e o HLR 6' (ou o AuC). Seguindo um procedimento que é típico para a autenticação de fones celulares em uma rede de telefonia móvel, o HLR 6' (ou o AuC) gera um número aleatório Rand1, ao

qual um primeiro algoritmo, tal como o bem conhecido algoritmo A3, parametrizado com a chave única $\mathbf{k_i}$ é aplicado de maneira a obter uma Resposta Assinada SRES1. Outrossim, um segundo algoritmo, tal como o bem conhecido algoritmo A8, parametrizado com a chave única $\mathbf{k_i}$ é aplicado ao número aleatório Rand1, de forma a obter uma chave de sessão $\mathbf{k_{c1}}$. Em outras palavras, o HLR 6' é adaptado para obter pelo menos um tripleto de parâmetros associado com o identificador de usuário remoto, o tripleto de parâmetros sendo composto por Rand1, k_{c1}, SRES 1. Nas modalidades preferenciais, pelo menos um segundo tripleto é requerido para o HLR 6',o segundo tripleto sendo gerado partindo de um outro número aleatório Rand2 e aplicando o mesmo procedimento conforme explanado acima. O segundo tripleto é composto pelo outro número aleatório Rand2, e pela chave de sessão adicional correlata k_{c2} e Resposta Assinada adicional SRES2. O tripleto ou tripletos é/são então transmitidos (105) do HLR6' para o I-VLR6.

[00027] Após receber o tripleto ou tripletos, o I-VLR6 codifica o número aleatório Ra usando um outro algoritmo, tal como o bem conhecido algoritmo 3DES, parametrizado com uma chave de autenticação de sessão gerada utilizando pelo menos os parâmetros de tripleto, de acordo com uma regra predeterminada. Mais especificamente, a chave autenticadora de sessão pode ser a chave k_{c1} ou k_{c2}, ou uma concatenação das mesmas, ou uma concatenação das chaves k_{c1} e/ou k_{c2} e as respostas assinadas SRES1 e/ou SRES2. Nas modalidades preferenciais pelo menos uma parte do número aleatório Ra recebido do software cliente também pode ser concatenada juntamente com parâmetros tripleto de modo a gerar a chave de sessão de autenticação. A concatenação de diferentes parâmetros obtidos de mais de um tripleto permite obter chaves de sessão de autenticação mais longas, assim permitindo uma conexão mais segura entre o I-VLR 6 e o computador pessoal de usuário 1, que é de importância específica no caso da conexão W-LAN. Por exemplo, o número aleatório Ra pode ser criptografado usando uma chave

de sessão de autenticação formada pela concatenação de k_{c1} SRES2, k_{c2} e Ra8, em que Ra8 sã os 8 primeiros dígitos do número aleatório Ra. Um outro número aleatório TID (ou uma parte do mesmo), gerada pelo I-VLR6, também pode ser criptografada com a chave de sessão de autenticação juntamente com o número aleatório Ra. O dito outro número aleatório TID pode ser um identificador de transação, identificando no I-VLR 6 a sessão de conexão específica iniciada pelo computador pessoal 1 do usuário remoto. Após a codificação do número aleatório Ra, e possivelmente do número aleatório TID, O quadro criptografado, juntamente com os números aleatórios Rand1 e Rand2 (o último no caso de dois tripletos serem obtidos pelo HLR 56'), é transmitido (106) para o computador pessoal 1,isto é, para o software cliente controlando a conexão de rede.

[00028] Os números aleatórios Rand1 e Rand2, que foram obtidos pelo HLR 6' são então transmitidos para o SIM (107) pelo software cliente, de maneira a contestar o SIM para produzir as chaves associadas k_{c1} e k_{c2} e respostas assinadas SRES1, SRES2, usando a chave única armazenada k_1.

[00029] O SIM então fornece (108) os parâmetros obtidos ao software cliente. Usando os parâmetros obtidos pelo SIM, o software cliente pode reconstruir a chave de sessão de autenticação, de uma maneira correspondente àquela usada pelo I-VLR, de maneira a decodificar o quadro criptografado recebido do I-VLR 6. A regra de acordo com a qual a chave de sessão de autenticação é reconstruída pelo software cliente é a mesma usada pelo I-VLR. Após ter reconstruído a chave de sessão de autenticação, o software cliente pode extrair o número Ra recebido do I-VLR 6 e comparar o mesmo com número aleatório Ra autogerado ao início do procedimento. A comparação dos dois números Ra permite a verificação pelo software cliente (isto é, pelo usuário), de que o serviço de conexão através do qual o computador pessoal 1 de que o serviço de conexão através do qual o computador pessoal 1 está se conectando com a rede 7 é confiável. Em outras

palavras, o usuário tem a possibilidade de "autenticar" o serviço de conexão.

[00030] Para completar o procedimento de autenticação, o software cliente encaminha (109) para o I-VLR 6 pelo menos uma das respostas assinadas SRES1 ou SRES2 geradas pelo SIM, possivelmente criptografa com a chave de sessão de autenticação. O TID identificador de transação também pode ser criptografado juntamente com a resposta ou respostas assinadas, e transmitido para o I-VLR 6. O I-VLR 6 então testa a correspondência entre a resposta ou respostas assinadas localmente geradas e a resposta ou respostas assinadas geradas pelo SIM 1'.

[00031] Se a correspondência entre as respostas assinadas é verificada, uma mensagem de pedido aceito é transmitida para o software cliente, permitindo acesso à rede 7. Possivelmente, uma mensagem de registro é transmitida (111) para o servidor proxi 9 de maneira a permitir o uso de serviços de IP (tais como HTTP, FTP, SMTP, e assim por diante) para o usuário remoto. Desta maneira, o provedor de serviço, prestando o serviço de conexão para o usuário, autentica o usuário.

[00032] Por outro lado, se a correspondência entre as respostas assinadas não é verificada, uma rejeição de pedido é transmitida (112) para o software cliente pelo I-VLR 6. Uma mensagem descontinuar conta pode também ser transmitida (113) para o NS 3 pelo I-VLR 67, de modo a instruir o NAS 3 a interromper as comunicações com o computador pessoal 1.

[00033] O procedimento de autenticação de um terminal de usuário remoto para acesso a um serviço de rede assim permite uma autenticação mútua entre o usuário remoto e o serviço de rede. Vantajosamente, a dita autenticação mútua aperfeiçoa a segurança para todas as conexões, inclusive conexões implicando partes usando percursos de radio conexão, tais como conexões W-LAN. A dita autenticação mútua permite ao provedor de serviço identificar o usuário remoto, e também permite ao usuário remoto identificar o provedor de serviço, para que informações confidenciais do usuário remoto

não possam ser recuperadas por um hacker estabelecendo um serviço falso prestado através de um ponto de acesso falso. Além disso, como explanado acima, o procedimento de autenticação pode vantajosamente ser estabelecido de modo a usar o mesmo protocolo para diferentes tipos de conexão, e mesmo para gerenciar pedidos de conexão provenientes de pontos de acesso pertencentes a diferentes provedores de serviço.

[00034] Deve ser entendido que as operações efetivas identificadas no procedimento acima descrito podem ser implementadas como um conjunto de instruções legíveis por computador, e executadas por qualquer computador para fins gerais bem conhecido dotado de faculdades de processamento apropriadas, conforme se evidenciará aqueles versados na técnica. Particularmente, a descrição das etapas de processamento habilita aqueles versados na técnica a desenvolver instruções legíveis apropriadas para contextos e facilidades específicas, tais como máquinas específicas, linguagens de computador, sistemas operacionais e semelhantes.

[00035] Os métodos realizados de acordo com os ensinamentos da presente invenção podem ser por exemplo incorporados em um ou mais arquivos executáveis residentes sobre suporte apropriado acessíveis a partir da memória do computador, tal como um disco rígido, um disquete, um CD ou DVD-ROM, ou um disco externo legível através de uma LAN.

REIVINDICAÇÕES

1. Método para uma autenticação mútua entre um usuário e uma rede de comunicações, o dito usuário sendo munido de um terminal (1) com o qual um módulo de identidade de assinante (1') está operativamente acoplado, o dito módulo de identidade de assinante armazenando pelo menos um identificador e uma primeira cópia de uma chave única associada com o dito usuário, a dita rede incluindo um subsistema de autenticação (6,6') que compreende pelo menos um primeiro aparelho de autenticação (6') armazenando uma segunda cópia da chave única associada com o dito identificador de usuário, o método caracterizado pelo fato de que compreende

- enviar o dito identificador de usuário a partir do dito módulo de identidade de usuário (1') para o dito terminal (1);

- gerar, no dito terminal (1), um primeiro número;

- enviar o dito identificador e pelo menos uma parte do dito primeiro número a partir do dito terminal (1) para o dito subsistema de autenticação (6,6'), através de um ponto de acesso (2) da dita rede;

- identificar, no dito sistema de autenticação (6,6'), a dita segunda cópia da chave única usando o dito identificador, gerar pelo menos um segundo número e confrontar o dito segundo número com a dita segunda cópia da chave única, de modo a gerar pelo menos uma primeira chave de sessão e pelo menos uma primeira resposta assinada;

- formar, no dito subsistema de autenticação (6,6'), de acordo com uma primeira regra, uma segunda chave de sessão usando pelo menos a dita primeira chave de sessão, e criptografar pelo menos a dita parte de primeiro número usando a dita segunda chave de sessão;

- enviar pelo menos a dita parte de primeiro número criptografada e o dito segundo número a partir do dito subsistema de autenticação (6,6') para o dito terminal (1);

- encaminhar o dito segundo número do terminal (1) para o

dito módulo de identidade de assinante (1'), e confrontar, no dito módulo de identidade de assinante (1'), o dito segundo número com a dita primeira cópia da dita chave única, de modo a gerar pelo menos uma terceira chave de sessão e pelo menos uma segunda resposta assinada;

- enviar a dita terceira chave de sessão e a dita segunda resposta assinada a partir do dito módulo de identidade de assinante (1') para o dito terminal (1);

- formar, no dito terminal (1), uma quarta chave de sessão, de acordo com uma segunda regra correspondente à dita primeira regra, usando pelo menos a dita terceira chave de sessão, e descriptografar a dita parte de primeiro número recebida a partir do dito subsistema de autenticação (6,6') usando a dita quarta chave de sessão;

- verificar, no dito terminal (1), uma correspondência entre a dita parte de primeiro número descriptografada com uma parte correspondente do dito primeiro número gerado, de modo a permitir comunicações a partir da dita rede para o dito terminal (1);

- enviar pelo menos a dita segunda resposta assinada a partir do dito terminal (1) para o dito subsistema de autenticação (6,6');

- verificar, no dito subsistema de autenticação (6,6'), uma correspondência entre a dita primeira resposta assinada e a dita segunda resposta assinada, de modo a permitir comunicações a partir do dito terminal (1) para a dita rede.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que compreende ainda criptografar o dito identificador e a dita parte de primeiro número no dito terminal (1), antes da dita etapa de enviar a partir do dito terminal (1) para o dito subsistema de autenticação (6,6'), a criptografação sendo realizada com uma chave pública predeterminada, armazenada no dito terminal (1).

3. Método de acordo com a reivindicação 2, caracterizado pelo

fato de que compreende ainda descriptografar o dito identificador e a dita parte de primeiro número no subsistema de autenticação (6,6'), a dita descriptografação sendo realizada com uma chave privada, relacionada com a dita chave pública predeterminada.

4. Método de acordo com qualquer uma das reivindicações 1 a 3, caracterizado pelo fato de que a primeira regra para formar a dita segunda chave de sessão compreende concatenar a dita primeira chave de sessão e a dita primeira resposta assinada.

5. Método de acordo com a reivindicação 4, caracterizado pelo fato de que a dita segunda regra para formar a quarta chave de sessão compreende concatenar a dita terceira chave de sessão e a dita segunda resposta assinada.

6. Método de acordo com qualquer uma das reivindicações 1 a 5, caracterizado pelo fato de que a dita etapa de criptografar, no dito subsistema de autenticação (6,6'), pelo menos a dita parte do primeiro número usando a dita segunda chave de sessão compreende criptografar também um identificador de transação gerado no dito subsistema de autenticação (6,6").

7. Método de acordo com a reivindicação 6, caracterizado pelo fato de que a etapa de descriptografar, no dito terminal (1) a parte de primeiro número recebida do dito subsistema de autenticação (6,6') usando a dita quarta chave de sessão também compreende descriptografar o dito identificador de transação.

8. Método de acordo com a reivindicação 7, caracterizado pelo fato de que compreende ainda enviar o dito identificador de transação descriptografado a partir do dito terminal (1) para o dito subsistema de autenticação (6,6').

9. Método de acordo com qualquer uma das reivindicações 1 a 8, caracterizado pelo fato de que compreende ainda gerar, no dito subsistema de autenticação (6,6'), pelo menos um terceiro número e confrontar o dito

terceiro número com a dita segunda cópia da dita chave única, de modo a gerar pelo menos uma quinta chave de sessão e pelo menos uma terceira resposta assinada.

10. Método de acordo com a reivindicação 9, caracterizado pelo fato de que a dita primeira regra para formar a segunda chave de sessão compreende concatenar pelo menos uma entre a dita primeira chave de sessão e a dita primeira resposta assinada com pelo menos uma entre a dita quinta chave de sessão e a dita terceira resposta assinada.

11. Método de acordo com a reivindicação 9 ou 10, caracterizado pelo fato de que a dita etapa de enviar pelo menos a dita parte de primeiro número criptografada e o dito segundo número do subsistema de autenticação (6,6') para o dito terminal (1) compreende ainda enviar o dito terceiro número para o dito terminal (1).

12. Método de acordo com a reivindicação 11, caracterizado pelo fato de que compreende ainda confrontar, no dito módulo de identidade de assinante (1'), o dito terceiro número com a dita primeira cópia da chave única, de modo a gerar pelo menos uma sexta chave de sessão e pelo menos uma quarta resposta assinada.

13. Método de acordo com a reivindicação 12, caracterizado pelo fato de que a dita segunda regra para formar a dita quarta chave de sessão compreende concatenar pelo menos uma entre a dita terceira chave de sessão e a dita segunda resposta assinada com pelo menos uma entre a dita sexta chave de sessão e a dita quarta resposta assinada.

14. Método para permitir a um usuário verificar a confiabilidade de uma rede de comunicações, o usuário sendo munido de um terminal (1) com o qual um módulo de identidade de assinante (1') é operativamente acoplado, o dito módulo de identidade de assinante armazenando pelo menos um identificador e pelo menos uma chave única associada com o dito usuário, a dita rede incluindo um subsistema de

autenticação (6,6'), o método caracterizado pelo fato de compreende, no dito terminal (1):

- receber o dito identificador de usuário a partir do dito módulo de identidade de assinante (1');

- gerar um primeiro número;

- enviar o dito identificador e pelo menos uma parte do dito primeiro número para o dito subsistema de autenticação (66'), através de um ponto de acesso (2) da dita rede;

- receber a partir do dito subsistema de autenticação (6,6') através do dito ponto de acesso (2), um número criptografado e pelo menos um segundo número gerado no dito subsistema de autenticação (6,6');

- encaminhar o dito segundo número para o dito módulo de identidade de assinante (1');

- receber, a partir do dito módulo de identidade de assinante (1'), pelo menos uma primeira chave de sessão e uma primeira resposta assinada, obtida no dito módulo de identidade de assinante (1') a partir de uma confrontação do dito segundo número com a dita chave única;

- gerar uma segunda chave de sessão usando pelo menos uma entre a dita primeira chave de sessão e a dita primeira resposta assinada, de acordo com uma regra predeterminada;

- descriptografar o dito número criptografado recebido a partir do dito subsistema de autenticação (6,6') usando a dita segunda chave de sessão;

- verificar uma correspondência entre a dita parte do primeiro número com uma primeira parte correspondente do dito número descriptografado, de modo a permitir a verificação da confiabilidade da dita rede.

15. Método de acordo com a reivindicação 14, caracterizado pelo fato de que compreende ainda criptografar o dito identificador e a dita

parte do primeiro número no terminal (1), antes da dita etapa de enviar o dito terminal (1) para o dito subsistema de autenticação (6,6'), a dita criptografação sendo efetuada com uma chave pública predeterminada, armazenada no dito terminal (1).

16. Método de acordo com a reivindicação 14 ou 15, caracterizado pelo fato de que a dita regra predeterminada para formar a dita segunda chave de sessão compreende concatenar a dita primeira chave de sessão e a dita primeira resposta assinada.

17. Método de acordo com qualquer uma das reivindicações 14 a 16, caracterizado pelo fato de que compreende ainda enviar a dita primeira resposta assinada para o dito subsistema de autenticação (6,6').

18. Método de acordo com a reivindicação 17, caracterizado pelo fato de que compreende ainda enviar uma segunda parte do dito número descriptografado para o dito subsistema de autenticação (6,6').

19. Método de acordo com qualquer uma das reivindicações 14 a 19, caracterizado pelo fato de que compreende ainda receber a partir do dito subsistema de autenticação (6,6'), pelo menos um terceiro número gerado no dito subsistema de autenticação (6,6').

20. Método de acordo com a reivindicação 19, caracterizado pelo fato de que compreende ainda encaminhar o dito terceiro número para o dito módulo de identidade de assinante (1').

21. Método de acordo com a reivindicação 20, caracterizado pelo fato de que compreende ainda receber, a partir do dito módulo de identidade de assinante (1') pelo menos uma terceira chave de sessão e uma segunda resposta assinada obtida, no dito módulo de identidade de assinante (1'), a partir de uma confrontação do dito terceiro número com a dita chave única.

22. Método de acordo com a reivindicação 21, caracterizado pelo fato de que a dita regra predeterminada para formar a dita segunda chave

de sessão compreende concatenar pelo menos uma entre a dita primeira chave de sessão e a dita primeira resposta assinada com pelo menos uma entre a dita terceira chave de sessão e a dita segunda resposta assinada.

23. Método para permitir a um usuário verificar a confiabilidade de uma rede de comunicações, o usuário sendo munido de um terminal (1), com um identificador e com um segredo compartilhado, a dita rede incluindo um subsistema de autenticação (6,6') que armazena o dito identificador de usuário associado com uma cópia do dito segredo compartilhado, o método caracterizado pelo fato de que compreende, sob controle do dito terminal (1):

- gerar um primeiro número;

- enviar o dito identificador de usuário e pelo menos uma parte do dito primeiro número para o dito subsistema de autenticação (6,6'), através de um ponto de acesso (2) da dita rede;

- receber, a partir do dito subsistema de autenticação (6, 6'), através do dito ponto de acesso (2), um número criptografado, o dito número criptografado sendo criptografado com uma chave de sessão gerada no dito subsistema de autenticação (6,6') com base na dita cópia do dito segredo compartilhado e em um segundo número gerado no dito subsistema de autenticação (6,6');

- receber, a partir do dito subsistema de autenticação (6,6'), através do dito ponto de acesso (2), o dito segundo número;

- processar o dito segundo número e o dito segredo compartilhado de modo a obter uma copia da dita chave de sessão;

- descriptografar o dito número criptografado recebido do dito subsistema de autenticação (6,6') usando a dita cópia da chave de sessão;

- verificar uma correspondência entre a dita parte do primeiro número com uma parte correspondente do dito número criptografado, de modo a permitir a verificação da confiabilidade da dita rede.

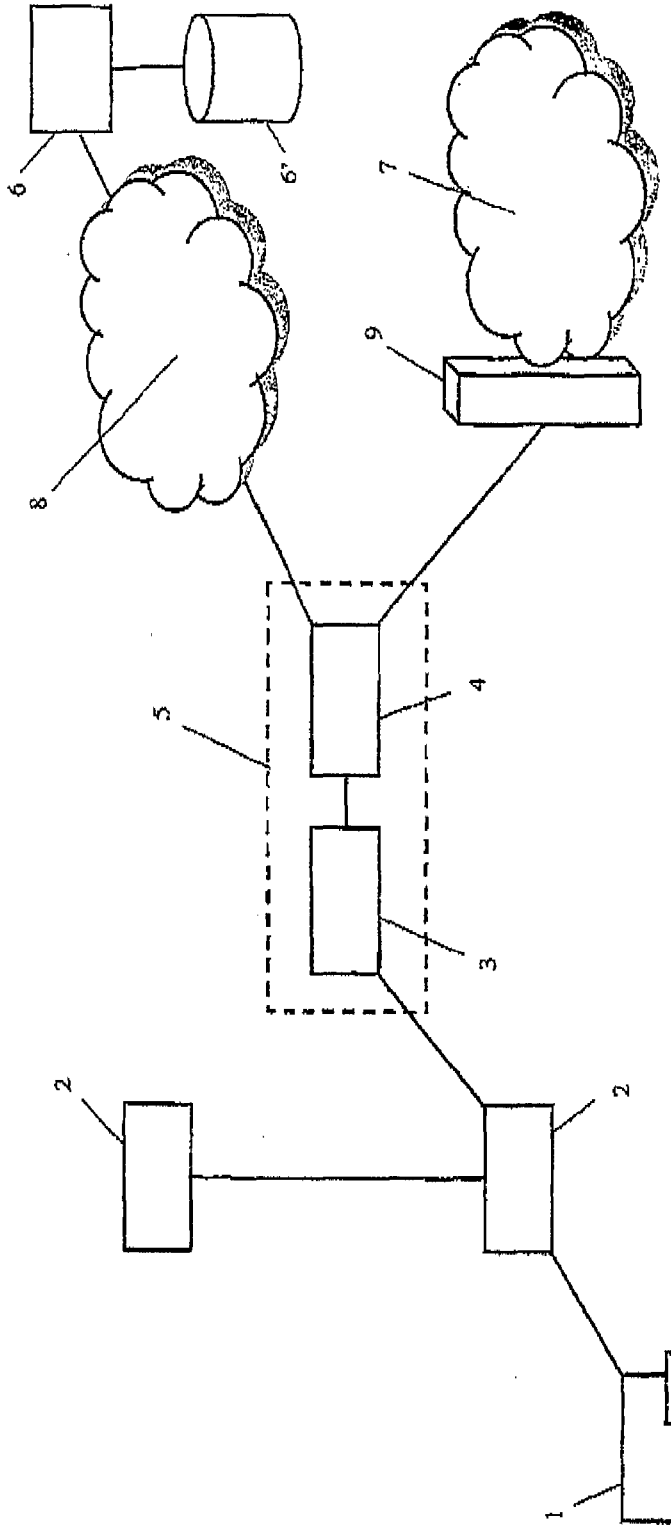

Fig.1

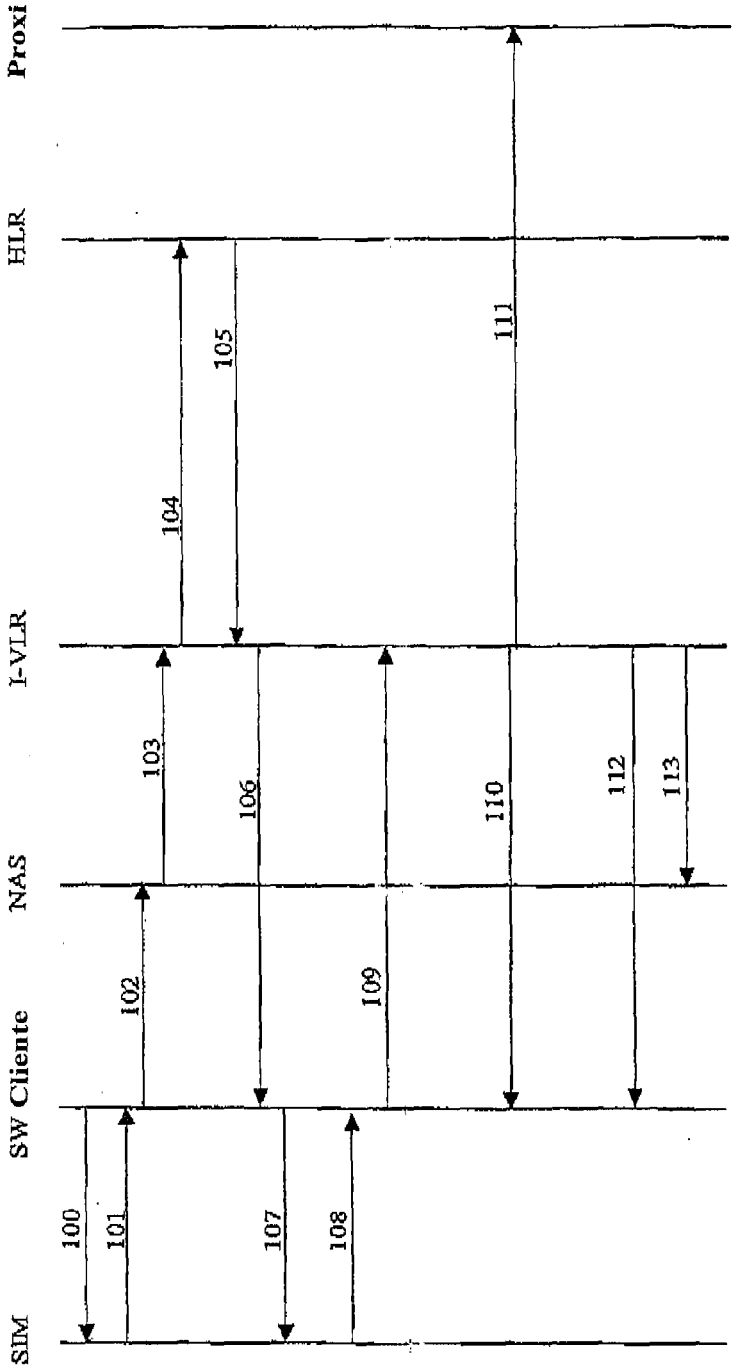
Proxi
HLR
I-VLR
NAS
SW Cliente
SIM
100
101
102
103
104
105
106
107
108
109
110
111
112
113

Fig.2