República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 0607359-0 B1

(22) Data do Depósito: 03/02/2006

(45) Data de Concessão: 02/04/2019

(54) Título: AUTO-INICIAÇÃO SEGURA PARA COMUNICAÇÕES SEM FIO

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

(52) CPC: H04L 63/0853; H04L 63/0869; H04W 12/06.

(30) Prioridade Unionista: 04/02/2005 US 60/650,358; 18/02/2005 US 60/654,133.

(73) Titular(es): QUALCOMM INCORPORATED.

(72) Inventor(es): GREGORY GORDON ROSE; JAMES SEMPLE; JOHN WALLACE NASIELSKI.

(86) Pedido PCT: PCT US2006003947 de 03/02/2006

(87) Publicação PCT: WO 2006/084183 de 10/08/2006

(85) Data do Início da Fase Nacional: 06/08/2007

(57) Resumo: AUTO-INICIAÇÃO SEGURA PARA COMUNICAÇÕES SEM FIO. Um método de autenticação mútua é fornecido para acordar de forma segura chaves de aplicação-segurança com terminais móveis suportando Módulos de Identidade de Assinante legados (por exemplo, GSM SIM e CDMA2000 R-UIM, os quais não suportam mecanismos 3G AKA). Uma troca de chaves de desafio-resposta é implementada entre uma função de servidor de auto-iniciação (BSF) e o terminal móvel (MT). A BSF gera um desafio de autenticação e envia este ao MT sob um mecanismo de chave pública autenticada por servidor, O MT recebe o desafio e determina se este origina da BSF com base em um certificado de servidor de auto- iniciação, O MT formula uma resposta para o desafio de autenticação com base nas chaves derivadas do desafio de autenticação e uma chave secreta pré-compartilhada. A BSF recebe a resposta de autenticação e verifica se esta origina do MT. Uma vez verificado, a BSF e o MT calculam independentemente uma chave de segurança de aplicação que a BSF envia para uma função de aplicação de rede solicitante para estabelecer comunicações seguras com o MT.

"AUTOINICIAÇÃO SEGURA PARA COMUNICAÇÕES SEM FIO

Reivindicação de Prioridade conforme 35 USC §119

O presente Pedido de Patente reivindica prioridade para Pedido Provisório US 60/650.358 intitulado "Secure Bootstrapped Keys in GSM" depositado em 4 de fevereiro de 2005, e Pedido Provisório US 60/654.133 intitulado "Secure Bootstrapping with CAVE" depositado em 18 de fevereiro de 2005 ambos os pedidos provisórios atribuídos ao cessionário da presente e aqui incorporado expressamente como referência.

FUNDAMENTOS

CAMPO

A presente invenção se refere geralmente aos sistemas e métodos para proteger as comunicações sem fio. Mais especificamente, uma característica da invenção provê um esquema de autenticação e convenção, fundamental, inovador, para dispositivos suportando mecanismos de autenticação de rede, legados, para prover chaves de segurança de aplicação pelo fato de tirar proveito dos mecanismos de autenticação e de convenção de chave, sem fio, legados.

FUNDAMENTOS

Um tipo de tecnologia celular para comunicações sem fio é definido pelo protocolo Sistema Global para Comunicações Móveis (GSM), que opera em redes de telefonia sem fio de segunda geração (2G). GSM é estendido adicionalmente pelas redes mais recentes, tal como Serviço de Rádio de Pacote Geral (GPRS), também conhecidas como redes 2.5G, que oferece serviços de dados baseados em pacote e conteúdo da Internet para redes GSM. GSM e GPRS são usados para muitos tipos de comunicações sem fio incluindo voz, navegação na Internet, correio eletrônico, e

dados de multimídia. GSM incorpora diversos mecanismos de segurança para proteger o conteúdo comunicado através de tais sistemas. Provedores de serviço e igualmente os usuários se baseiam nesses mecanismos de segurança para a privacidade de suas comunicações e proteção de seus dados, e os provedores de serviço utilizam essas medidas de segurança para autenticar seus assinantes com o propósito de cobrança. Esses mecanismos de segurança, tipicamente, operam mediante autenticação dos terminais móveis de usuário junto à rede, e as transmissões subseqüentes podem ser codificadas. Contudo, medidas de segurança GSM são vulneráveis ao ataque por terceiros, devido às vulnerabilidades nos protocolos de segurança GSM, tal como ataques de estação base falsa que surgem de uma falta de autenticação de rede, a possibilidade de reprodução dos protocolos de segurança, e vulnerabilidades nos algoritmos de codificação GSM.

Essas vulnerabilidades de segurança foram tratadas no desenvolvimento de protocolos de segurança nos padrões de comunicação sem fio de terceira geração (3G). Especificamente, o protocolo Autenticação e Convenção de Chave (AKA) desenvolvido para o Sistema de Telecomunicação Móvel Universal (UMTS) inclui recursos tais como um número de seqüência e Código de Autenticação de Mensagem (MAC) que impedem os ataques de estação base falsa aos quais GSM está sujeito. Desse modo os assinantes móveis utilizando um Módulo de Identidade de Serviço de Usuário UMTS (USIM) para autenticação de rede não estão vulneráveis aos ataques realizados contra os usuários de um Módulo de Identidade de Assinante GSM (SIM).

Entidades de padronização 3G também estão desenvolvendo uma Arquitetura de Autenticação Genérica (GAA), por exemplo, no documento de projeto de parceria de

terceira geração de Arquitetura de Autenticação Genérica 3GPP 33.220 (GAA), para uma arquitetura de autoiniciação genérica. Essa arquitetura se baseia em um protocolo 3G AKA para estabelecer chaves entre um Equipamento de Usuário (UE) do assinante móvel e uma nova entidade de servidor conhecida como uma Função de Servidor de Autoiniciação (BSF). A partir dessas chaves, chaves adicionais podem ser derivadas e providas pelo BSF para diversas Funções de Aplicação de Rede (NAF), como uma forma de estabelecer chaves de segurança compartilhadas entre a NAF e o UE.

As técnicas em desenvolvimento se baseiam nos métodos de convenção de chave e autenticação 3G, tais como aqueles suportados em um Módulo de Identidade de Assinante Universal UMTS (USIM), com aperfeiçoamentos de segurança inerentes em comparação com 2G ou sistemas legados anteriores tais como GSM. Por exemplo, a Arquitetura de Autenticação Genérica (GAA) e a Arquitetura de Autoiniciação Genérica (GBA) são especificadas para redes 3G e desenvolvidas na infra-estrutura de segurança das redes móveis 3G (isto é, segurança baseada em USIM) para proporcionar autenticação mútua segura entre o equipamento de usuário móvel e um servidor de rede que facilita a aplicação e/ou serviços de rede.

Contudo, essas técnicas de autenticação mútua (por exemplo, GAA e GBA) não estão disponíveis para os sistemas de comunicação anteriormente desenvolvidos (por exemplo, 2G); tal como os Protocolos de Convenção de Chave e Autenticação GSM (AKA), por exemplo. Esses protocolos GSM estão sujeitos a ataques de reprodução, de modo que aquele que ataca pode forçar a reutilização de chaves, e possivelmente explorar as vulnerabilidades em alguns contextos para revelar as chaves e desse modo minar a segurança. Desse modo, é necessário um método para

autoiniciação de chaves de segurança de aplicação a partir da convenção de chave e autenticação GSM de tal maneira que não seja possível reproduzir os ataques e as chaves não podem ser facilmente reveladas.

Desse modo, há a necessidade de se estabelecer técnicas mediante as quais a Arquitetura de Autenticação Genérica (GAA), especificada para as redes 3G, pode ser estendida para suportar sistemas legados (por exemplo, 2G ou sistemas anteriores). Isso permitiria que os assinantes com GSM ou outros dispositivos, tendo Módulo de Identidade de Assinante (SIM), sejam aprovisionados com chaves para uso em aplicações de rede móvel e/ou serviços sem necessitar substituição de suas SIMS por uma UMTS USIM. Além disso, tal método não deve introduzir vulnerabilidades na Arquitetura de Autenticação Genérica devido às vulnerabilidades da própria autenticação GSM.

SUMÁRIO

É provido um método de autenticação mútua para combinar de forma segura chaves de aplicação-segurança com terminais móveis suportando Módulos de Identidade de Assinante legados (por exemplo, GSM SIM e CDMA2000 R-UIM, que não suportam mecanismos 3G AKA). Uma troca de chave de pedido de senha-resposta é implementada entre uma função de servidor de autoiniciação (BSF) e o terminal móvel (MT). A BSF recebe de um registro de localização nativa (HLR) parâmetros de autenticação de rede correspondendo a esse terminal móvel (por exemplo, GSM RAND, SRES, Kc) e gera um pedido de senha de autenticação envolvendo RAND e envio o mesmo para o MT sob um mecanismo de chave pública autenticada pelo servidor. Esse pedido de senha de autenticação pode incluir parâmetros adicionais, tais como números aleatórios, informação de identidade, marcações de tempo, números de seqüência e chaves públicas Diffie-

Hellman.

O MT recebe o pedido de senha de autenticação e determina se ele se origina da BSF com base em um certificado de servidor de autoiniciação. O MT formula uma resposta ao pedido de senha de autenticação com base em chaves derivadas do pedido de senha de autenticação (por exemplo, um número aleatório) e uma chave secreta pré-compartilhada (por exemplo, no GSM SIM). Isto é, o SIM no MT pode derivar chaves secretas (por exemplo, SRES e Kc) usadas pela função de servidor de autoiniciação com base no número aleatório RAND recebido no pedido de senha de autenticação e a chave secreta pré-compartilhada armazenada no SIM. A resposta de autenticação pode incluir parâmetros adicionais, tais como números aleatórios codificados, informação de identidade, marcações de tempo, números de seqüência, e chaves públicas Diffie-Hellman. A BSF recebe a resposta de autenticação e determina se ela se origina no MT. O mecanismo de pedido de senha-resposta faz uso de mecanismos de chave pública para verificar a origem do pedido de senha e das chaves secretas pré-compartilhadas para verificar a origem da resposta. Por exemplo, a BSF pode re-calcular independentemente um ou mais parâmetros na resposta de autenticação (por exemplo, utilizando ou com base no RAND, SRES, e/ou Kc que ele obteve a partir do HLR) para verificar se um ou mais parâmetros recebidos na resposta de autenticação são idênticos.

Onde essas mensagens foram autenticadas, a BSF e o MT podem agora computar chaves de segurança de aplicação com base na RAND, SRES, Kc, e/ou parâmetros adicionais os quais podem ter sido transmitidos entre a BSF e o MT. Observar que as chaves SRES e Kc são conhecidas independentemente pela BSF e MT não são transmitidas entre as mesmas. As chaves de segurança de aplicação podem ser

enviadas a partir da função de servidor de autoiniciação para uma função de aplicação de rede solicitante de modo que o terminal móvel e a função de aplicação de rede compartilham as chaves de segurança de aplicação e podem usar as mesmas para comunicações seguras entre eles.

É provido um método para autenticar um terminal móvel legado para comunicação com uma função de aplicação de rede, compreendendo: (a) gerar um pedido e senha de autenticação em uma função de servidor de autoiniciação, (b) enviar o pedido de senha de autenticação para o terminal móvel, em que o terminal móvel pode verificar a origem do pedido de senha de autenticação com base em um certificado de servidor de autoiniciação previamente obtido associado à função de servidor de autoiniciação, (c) receber uma resposta de autenticação na função de servidor de autoiniciação que inclui um primeiro parâmetro computado com uma primeira chave gerada no terminal móvel, (d) verificar se a resposta de autenticação se originou em um terminal móvel mediante nova computação do primeiro parâmetro na função do servidor de autoiniciação com base em uma segunda chave provida à função de servidor de autoiniciação, e (e) comparar o primeiro parâmetro recebido na resposta de autenticação com o primeiro parâmetro outra vez computado pela função de servidor de autoiniciação. A resposta de autenticação é considerada como tendo se originado no terminal móvel se ambos os primeiros parâmetros forem idênticos.

A primeira chave pode ser obtida a partir de um módulo de identificação de assinante, o qual pode ser um módulo de identidade de assinante (SIM) do Sistema Global para Comunicações Móveis (GSM) ou um Módulo de Autenticação CDMA2000, armazenado no terminal móvel. A segunda chave pode ser obtida a partir de um registro de localização

nativa, acoplado comunicativamente com a função de servidor de autoiniciação. A primeira e a segunda chave podem ser geradas com base nos mesmos algoritmos seguros e uma chave secreta pré-compartilhada conhecida do módulo de identificação de assinante no terminal móvel e um banco de dados de rede acoplado comunicativamente com a função de servidor de autoiniciação. O pedido de senha de autenticação pode incluir um número aleatório como um parâmetro, e o número aleatório e a chave secreta pré-compartilhada, armazenados em um módulo de identificação de assinante no terminal móvel, são usados pelo módulo de identificação de assinante para gerar uma primeira chave usada para computar o primeiro parâmetro na resposta de autenticação. A segunda chave provida à função de servidor de autoiniciação pode ser gerada com base em uma cópia da chave secreta pré-compartilhada armazenada fora do terminal móvel e o número aleatório no pedido de senha de autenticação. O primeiro parâmetro da resposta de autenticação pode incluir um código de autenticação de mensagem computado com a primeira chave e usado pela função de servidor de autoiniciação para verificar a origem da resposta de autenticação.

Em algumas implementações, uma terceira chave pode ser gerada na função de servidor de autoiniciação com base na segunda chave; o primeiro parâmetro é outra vez computado na função de servidor de autoiniciação utilizando a terceira chave.

Adicionalmente, o método pode incluir ainda (a) computar uma quarta chave na função de servidor de autoiniciação com base na segunda chave, a qual também é computada independentemente pelo terminal móvel utilizando a primeira chave, e (b) enviar a quarta chave a partir da função de servidor de autoiniciação para uma função de

aplicação de rede solicitante de modo que o terminal móvel e a função de aplicação de rede compartilham a quarta chave para comunicações seguras entre eles.

Outro recurso provê um dispositivo de rede compreendendo: (a) uma interface de comunicação para se comunicar com os terminais móveis sem fio, e (b) um circuito de processamento acoplado à interface de comunicação e configurado para implementar uma função de servidor de autoiniciação para autenticar o terminal móvel. O circuito de processamento pode autenticar o terminal móvel mediante (a) geração de um pedido de senha de autenticação incluindo um número aleatório, (b) envio do pedido de senha de autenticação para o terminal móvel, em que o terminal móvel pode verificar a origem do pedido de senha de autenticação com base em um certificado de servidor de autoiniciação previamente obtido associado à função de servidor de autoiniciação, (c) receber uma resposta de autenticação a partir do terminal móvel, a resposta de autenticação incluindo um primeiro parâmetro computado com uma primeira chave com base no número aleatório, uma chave secreta pré-compartilhada e um algoritmo, em que a chave secreta pré-compartilhada e o algoritmo são conhecidos de um módulo de identificação de assinante no terminal móvel e um banco de dados de rede acoplado comunicativamente à função de servidor de autoiniciação, (d) computar um segundo parâmetro na função de servidor de autoiniciação com base em uma segunda chave provida ao servidor de autoiniciação pelo banco de dados de rede, e (e) comparar o primeiro parâmetro e o segundo parâmetro, em que a resposta de autenticação é considerada como tendo sido originada no terminal móvel se o primeiro e o segundo parâmetros forem idênticos. Em algumas implementações, o módulo de identificação de assinante pode

ser um de: Módulo de Identidade de Assinante (SIM) de Sistema Global para Comunicações Móveis (GSM) ou um Módulo de Autenticação CDMA2000. Adicionalmente, o circuito de processamento pode ser configurado adicionalmente para implementar a função de servidor de autoiniciação para autenticar o terminal móvel mediante (a) computação de uma quarta chave na função de servidor de autoiniciação com base na segunda chave, a qual também é computada no terminal móvel com base na primeira chave, e (b) envio da quarta chave a partir da função de servidor de autoiniciação para uma função de aplicação de rede solicitante de modo que o terminal móvel e a função de aplicação de rede compartilham a quarta chave. O circuito de processamento pode ser configurado adicionalmente para implementar a função de servidor de autoiniciação para autenticar o terminal móvel comparando o primeiro parâmetro recebido na resposta de autenticação com o primeiro parâmetro calculado pela função de servidor de autoiniciação, em que a resposta de autenticação é considerada como tendo sido originada no terminal móvel se ambos os primeiros parâmetros forem idênticos.

Ainda outro aspecto provê um método para autenticar um terminal móvel legado para se comunicar com uma função de aplicação de rede, compreendendo: (a) receber um pedido de senha de autenticação no terminal móvel incluindo um número aleatório, (b) verificar se o pedido de senha de autenticação se origina em uma função de servidor de autoiniciação com base em um certificado de servidor de autoiniciação previamente obtido associado à função de servidor de autoiniciação, (c) gerar uma resposta de autenticação com base em uma primeira chave gerada por um módulo de identificação de assinante legado no terminal móvel, e (d) prover a primeira chave a partir do módulo de

identificação de assinante ao terminal móvel em resposta ao recebimento do número aleatório recebido no pedido de senha de autenticação. O método pode incluir ainda gerar uma primeira chave no módulo de identificação de assinante utilizando o número aleatório, uma chave secreta pré-compartilhada e um algoritmo. A chave secreta pré-compartilhada e o algoritmo são ambos armazenados no módulo de identificação de assinante e um banco de dados de rede acoplado comunicativamente à função de servidor de autoiniciação. Em algumas implementações, a primeira chave pode ser gerada utilizando parâmetros adicionais transmitidos no pedido de senha de autenticação e resposta.

O método pode incluir ainda computar uma terceira chave no terminal móvel com base na primeira chave. A terceira chave também pode ser computada independentemente na função de servidor de autoiniciação com base e uma segunda chave provida à função de servidor de autoiniciação por intermédio de um banco de dados de rede. A terceira chave é enviada a partir da função de servidor de autoiniciação para uma função de aplicação de rede solicitante de modo que o terminal móvel e a função de aplicação de rede compartilham a terceira chave.

Outro recurso provê um terminal móvel compreendendo: (a) uma interface de comunicação sem fio para se comunicar com uma função de servidor de autoiniciação, (b) um módulo de identificação de assinante para armazenar uma chave secreta pré-compartilhada e um algoritmo, e (c) um circuito de processamento configurado para operar um protocolo de comunicação legado e autenticar o terminal móvel em um protocolo de pedido de senha-resposta com uma função de servidor de autoiniciação. O circuito de processamento pode operar mediante (a) recebimento de um pedido de senha de autenticação,

incluindo número aleatório, a partir da função de servidor de autoiniciação, (b) determinar se o pedido de senha de autenticação se origina a partir da função de servidor de autoiniciação com base em um certificado de servidor de autoiniciação previamente obtido associado à função de servidor de autoiniciação, e (c) gerar uma resposta de autenticação incluindo um primeiro parâmetro computado com uma primeira chave, em que a primeira chave é gerada a partir do número aleatório, a chave secreta pré-compartilhada e algoritmo. Adicionalmente, o circuito de processamento pode (a) gerar uma terceira chave derivada com base na primeira chave e outros parâmetros transmitidos no pedido de senha de autenticação e resposta, e (b) gerar um código de autenticação de mensagem computado utilizando a terceira chave. O código de autenticação de mensagem pode ser incluído na resposta de autenticação para o servidor de autoiniciação. O módulo de identificação de assinante pode gerar a primeira chave com base no número aleatório, na chave secreta pré-compartilhada e no algoritmo.

O módulo de identificação de assinante pode ser um módulo de identidade de assinante (SIM) de acordo com o protocolo Sistema Global para Comunicações Móveis (GSM). A chave secreta pré-compartilhada também pode ser empregada para permitir que o terminal móvel estabeleça comunicações através de uma rede sem fio legada.

DESCRIÇÃO RESUMIDA DOS DESENHOS

A Figura 1 é um diagrama de blocos ilustrando um sistema de comunicação no qual um servidor de autoiniciação e um terminal móvel legado podem mutuamente autenticar um ao outro de acordo com uma implementação.

A Figura 2 é um diagrama de blocos ilustrando um terminal móvel configurado para realizar autenticação mútua com função de servidor de autoiniciação operacional na rede

de comunicação de acordo com uma implementação.

A Figura 3 é um diagrama de blocos ilustrando um dispositivo de rede configurado para realizar uma função de servidor de autoiniciação para autenticar uma estação móvel de acordo com uma implementação.

A Figura 4 ilustra um método de realizar um mecanismo de pedido de senha-resposta que autentica mutuamente um terminal móvel legado e uma função de servidor de autoiniciação de acordo com uma implementação.

A Figura 5 ilustra um método de autenticar um terminal móvel utilizando uma função de servidor de autoiniciação e autenticação da função de servidor de acordo com uma implementação.

A Figura 6 ilustra um método de realizar um protocolo de pedido de senha-resposta entre um terminal móvel compatível com GSM e uma função de servidor de autoiniciação para autenticar seguramente um ao outro para funções de aplicação de rede de acordo com a implementação.

A Figura 7 ilustra um método alternativo de realizar um protocolo de pedido de senha-resposta entre um terminal móvel compatível com GSM e uma função de servidor de autoiniciação para autenticar seguramente um ao outro para funções de aplicação de rede para uma implementação.

DESCRIÇÃO DETALHADA

Na descrição a seguir, detalhes específicos são fornecidos para prover um entendimento completo das modalidades. Contudo, será entendido por aqueles versados na técnica que as modalidades podem ser praticadas sem esses detalhes específicos. Por exemplo, circuitos podem ser mostrados em diagrama de blocos para não obscurecer as modalidades em detalhe desnecessário. Em outras instâncias, circuitos, estruturas e técnicas, conhecidos, podem não ser mostrados em detalhe para não obscurecer as modalidades.

Além disso, observa-se que as modalidades podem ser descritas como um processo que é ilustrado como um fluxograma, um diagrama de fluxo, um diagrama de estrutura, ou um diagrama de blocos. Além disso, um fluxograma pode descrever as operações como um processo seqüencial, muitas das operações podem ser realizadas em paralelo ou simultaneamente. Além disso, a ordem das operações pode ser rearranjada. Um processo é terminado quando suas operações são concluídas. Um processo pode corresponder a um método, uma função, um procedimento, uma sub-rotina, um subprograma, etc. Quando um processo corresponde a uma função, sua terminação corresponde a um retorno da função a função de solicitação ou à função principal.

Além disso, um meio de armazenamento pode representar um ou mais dispositivos para armazenar dados, incluindo memória de leitura (ROM), memória de acesso aleatório (RAM), meios de armazenamento de disco magnético, meios de armazenamento ótico, dispositivos de memória flash e/ou outros meios legíveis por máquina para armazenar informação. O termo "meio legível por máquina" inclui, mas não é limitado aos dispositivos de armazenamento portáteis ou fixos, dispositivos de armazenamento ótico, canais sem fio e diversos outros meios capazes de armazenar, conter ou transportar instrução (instruções) e/ou dados.

Além disso, as modalidades podem ser implementadas por hardware, software, firmware, middleware, microcódigo, ou uma combinação dos mesmos. Quando implementadas em software, firmware, middleware, microcódigo, o código de programa ou segmentos de código para realizar as tarefas necessárias podem ser armazenados em um meio legível por máquina tal como um meio de armazenamento ou outro armazenador (armazenadores). Um processador pode realizar as tarefas necessárias. Um

segmento de código pode representar um procedimento, uma função, um subprograma, um programa, uma rotina, uma sub-rotina, um módulo, um pacote de software, uma classe, ou uma combinação de instruções, estruturas de dados ou instruções de programa. Um segmento de código pode ser acoplado a outro segmento de código ou a um circuito de hardware mediante passagem e/ou recebimento de informação, dados, argumentos, parâmetros, ou conteúdo de memória. Informação, argumentos, parâmetros, dados, etc. podem ser passados, enviados, ou transmitidos através de um meio adequado incluindo compartilhamento de memória, passagem de mensagem, passagem de ficha, transmissão de rede, etc.

Na descrição a seguir, certa terminologia é usada para descrever certos recursos de uma ou mais modalidades da invenção. Por exemplo, os termos "terminal móvel", "equipamento de usuário", "dispositivo móvel", "dispositivo sem fio" e "dispositivo móvel sem fio" são usados de forma permutável para se referir aos telefones móveis, pagers, modems sem fio, assistentes pessoais digitais, gerenciadores pessoas de informação (PIMs), computadores palmtop, computadores laptop, e/ou outros dispositivos móveis de comunicação/computação os quais se comunicam, pelo menos parcialmente, através de uma rede celular. O termo "legado" é usado para se referir às redes, protocolos, e/ou dispositivos móveis os quais são pré-3G, operam um protocolo pré-3G, ou empregam um SIM compatível com GSM ou um módulo de autenticação compatível com CDMA ou Módulo de Autenticação MN-AAA. Adicionalmente, o termo módulo de identificação de assinante é usado para se referir a um Módulo de Identidade de Assinante compatível com GSM (SIM), um Módulo de Autenticação compatível com CDMA ou Módulo de Autenticação MN-AAA, ou qualquer outro módulo tipicamente incluído em um terminal móvel para

identificar o terminal móvel para uma rede sem fio.

Um recurso provê uma forma de estender a Arquitetura de Autenticação Genérica para suportar sistemas legados, de tal modo que os assinantes de posse de um Módulo de Identidade de Assinante GSM (SIM) podem ser providos com chaves para uso em aplicações móveis sem necessitar substituição do SIM por um Módulo de Identidade de Serviço de Usuário (USIM) de serviço de usuário compatível com UMTS, 3G.

A Figura 1 é um diagrama de blocos ilustrando um sistema de comunicação no qual um servidor de autoiniciação e um terminal móvel legado podem autenticar um ao outro de acordo com uma implementação. Uma arquitetura de rede 100, tal como um sistema de comunicação compatível com CDMA2000 ou compatível com GSM, inclui um terminal móvel (MT) 102, um registro de localização nativa (HLR) 104, uma função de servidor de autoiniciação (BSF) 106, e pelo menos uma função de aplicação de rede (NAF) 108. O HLR 104 e a BSF 106 podem ser hospedados em um ou mais dispositivos e/ou servidores de rede que são parte da infra-estrutura da arquitetura de rede 100. O HLR 104 inclui um banco de dados que contém informação de assinante móvel para uma portadora sem fio, incluindo uma Identidade de Assinante Móvel Internacional (IMSI) para cada MT 102 pertencendo ao assinante. A IMSI é um número singular que é associado a um MT 102 na rede. A IMSI também é armazenada no Módulo de Identidade de Assinante (SIM) de cada MT 102 e é enviada pelo MT para a rede HLR para consultar informação sobre o MT 102.

O MT 102 pode ser um dispositivo de comunicação sem fio legado que se registra ou se conecta com o provedor de serviço utilizando um protocolo predefinido (por exemplo, um protocolo pré-3G) para se comunicar através da

rede 100. Em algumas implementações, esse processo de se conectar com um provedor de serviço pode envolver autenticar o MT 102 mediante uso de uma chave secreta pré-compartilhada (por exemplo, armazenada em uma GSM SIM, módulo de autenticação CDMA, ou outro módulo legado). Por exemplo, o MT 102 pode conter um SIM compatível com GSM ou um módulo de autenticação compatível com CDMA2000 ou habilitar o MT 102 para operar em redes GSM ou CDM2000 e permitir que ele seja autenticado pela rede para comunicação aérea.

Quando o MT 102 é autenticado pelo provedor de serviço para comunicações através da rede, um aspecto da invenção acrescenta outra camada de autenticação para permitir aplicações seguras de rede. Esse mecanismo de autenticação adicional é independente do mecanismo de autenticação ou portador de rede subjacente do portador. A camada adicional de autenticação utiliza as chaves existentes no SIM ou no Módulo de Autenticação, em conjunto com um protocolo inovador para estabelecer chaves que são independentes da rede ou serviços de segurança de portador. Esse novo mecanismo de autenticação provê chaves para autenticação, ou outros propósitos, compartilhadas entre o MT 102 e uma NAF específica 108, distribuídas para a NAF por intermédio da BSF 106. A NSF 108 pode ser uma aplicação que opera em um dispositivo em rede, tal como aplicações de transações comerciais e/ou dispositivos baseados em localização, por exemplo.

Quando o MT 102 está pronto para começar a usar uma aplicação de rede, ele inicia contato com a NAF 108 através de um link de comunicação 110. Se o MT e a NAF já não compartilham chaves apropriadas, então a NAF 108 faz uma solicitação para chaves de autenticação através de uma interface 112 a BFS 106. Se ela já não tiver feito isso, o

MT 102 e a BFS 106 concordam sobre as chaves com o MT 102 através de um link de autenticação 114.

Uma troca de chaves Diffie-Hellman pode ser empregada como parte do processo de convenção de chave entre o MT 102 e a BSF 106. A troca de chaves Diffie-Hellman é um protocolo criptográfico que permite que duas partes que não têm conhecimento uma da outra estabeleçam em conjunto uma chave secreta compartilhada através de um canal de comunicação não seguro. Em uma aplicação essa chave secreta compartilhada pode então ser usada para criptografar comunicações subseqüentes utilizando uma cifragem de chave simétrica.

Contudo, sem mais, os algoritmos de troca de chave Diffie-Hellman convencionais estão sujeitos aos ataques de "intermediários" que minam a segurança desse algoritmo. Isso é de particular preocupação onde informação é permutada através de um meio sem fio para realizar transações comerciais e/ou confidenciais entre um MT 102 e uma NAF 108.

Um recurso da invenção provê um protocolo que habilita a BSF 106 e o MT 102 a concordar sobre uma chave secreta pública ou compartilhada de uma maneira que não é suscetível a vulnerabilidades inerentes do GSM e/ou CDMA2000. Especificamente, o MT 102 é primeiramente aprovisionado com um certificado digital para autenticar a BSF 106. Isso permite que as comunicações a partir da BSF 106 para o MT 102 sejam assinadas digitalmente ou realizadas em um canal autenticado por servidor, desse modo permitindo que o MT 102 verifique se as chaves ou parâmetros recebidos durante o processo de autenticação são provenientes da BSF 106 e não de outra entidade tentando um ataque de reprodução ou de "intermediário". Desse modo, o presente método pode ser aplicado para estender o esquema

de autenticação da Arquitetura de Autoiniciação Genérica 3G para protocolos, diferentes dos UMTS AKA, os quais eles próprios não se beneficiam da autenticação de rede.

A Figura 2 é um diagrama de blocos ilustrando um terminal móvel (MT) 200 configurado para realizar autenticação mútua com a função de servidor de autoiniciação operacional em uma rede de comunicação. O MT 200 inclui um circuito de processamento 202 (por exemplo, processador) acoplado a uma interface de comunicação 202 para se comunicar com uma rede sem fio, e um cartão de Módulo de Identidade de Assinante (SIM) 204. O circuito de processamento 202 pode ser configurado para realizar parte ou todos os métodos ilustrados nas Figuras 4, 5, 6 e 7. O SIM 204 pode conter uma chave secreta Ki, uma implementação da autenticação GSM e algoritmos de convenção de chave (isto é, os algoritmos GSM A3/A8), e é inserido em um MT 102 contendo uma chave pública ou certificado de servidor digital de uma chave pública correspondendo a uma chave privada na BSF 106. Especificamente, o SIM 204 pode ser um cartão inteligente legado padrão configurado para uso em uma rede GSM. A chave pública ou certificado de servidor pode corresponder a uma chave pública RSA, ou outras técnicas de chave pública proporcionando assinaturas digitais também podem ser usadas, por exemplo, DAS (algoritmo de assinatura digital). A BSF 106 e o MT 102 também podem compartilhar um gerador predeterminado P de um grupo cíclico, tal como o subgrupo multiplicativo de um campo finito ou um ponto em uma curva elíptica, permitindo que eles empreguem a troca de chaves Diffie-Hellman. Em modalidades alternativas, o MT 200 pode incluir um módulo de autenticação compatível com CDMA2000 em vez do SIM 204.

A Figura 3 é um diagrama de blocos ilustrando um dispositivo de rede configurado para realizar uma função de

servidor de autoiniciação (BSF) para autenticar uma estação móvel (MT) de acordo comum aspecto da invenção. O dispositivo de rede 300 inclui um circuito de processamento 302 (por exemplo, processador) acoplado a uma interface de comunicação 306 para se comunicar com a rede sem fio, e um dispositivo de memória 304. O circuito de processamento 302 pode ser configurado para executar a função de servidor de autoiniciação enquanto mantendo as chaves e/ou parâmetros para implementa a troca de chaves Diffie-Hellman com um MT. Por exemplo, o circuito de processamento 302 pode ser configurado para realizar parte ou todos os métodos ilustrados nas Figuras 4, 5, 6 e 7.

A Figura 4 ilustra um método para realizar um mecanismo de pedido de senha-resposta que mutuamente autentica um terminal móvel, tendo um SIM legado, e uma função de servidor de autoiniciação de acordo com uma implementação. Esse mecanismo de pedido de senha-resposta faz uso de mecanismos de chave pública para verificar a origem do pedido de senha e chaves secretas pré-compartilhadas para verificar a origem da resposta.

A função de servidor de autoiniciação (BSF) gera um pedido de senha de autenticação e envia o mesmo para o terminal móvel (MT) sob um mecanismo de chave pública autenticada por servidor 402. O pedido de senha de autenticação pode incluir um número aleatório (por exemplo, RAND) e é derivado de uma chave secreta pré-compartilhada (por exemplo, Ki) conhecida de um banco de dados de rede e um módulo de identificação de assinante no MT. Por exemplo, a chave secreta pré-compartilhada Ki e número aleatório (por exemplo, RAND) podem ser usados para gerar chaves secretas (por exemplo, SRES e Kc) que são usadas para gerar parâmetros de pedido de senha de autenticação. O pedido de senha de autenticação pode incluir também parâmetros

adicionais, tal como marcação de tempo, outros números aleatórios, informação de identidade, uma chave pública Diffie-Hellman, etc., e é enviado através de um canal digitalmente assinado e/ou autenticado por servidor.

O MT recebe o pedido de senha de autenticação e verifica se ele tem origem na BSF com base em um certificado de servidor de autoiniciação 404. Tal certificado de servidor de autoiniciação (por exemplo, uma chave pública) pode ter sido aprovisionado ao MT e BSF na configuração, fora de linha, e/ou durante um processo anterior. O MT formula uma resposta ao pedido de senha de autenticação com base nas chaves derivadas e/ou providas pelo módulo de identificação de assinante no MT 406. Essas chaves secretas podem ser geradas pelo módulo de identificação de assinante com base no número aleatório recebido no pedido de senha de autenticação e uma chave secreta pré-compartilhada armazenada no módulo de identificação de assinante. Por exemplo, o número aleatório (por exemplo, RAND) recebido no pedido de senha de autenticação e a chave secreta pré-compartilhada (por exemplo, Ki), armazenados no módulo de identificação de assinante do MT, podem ser usados para gerar chaves (por exemplo, SRES e Kc) que são usadas para gerar parâmetros de resposta de autenticação. Adicionalmente, em algumas implementações, o MT também pode usar parâmetros adicionais (por exemplo, marcação de tempo, outros números aleatórios, informação de identidade, uma chave pública Diffie-Hellman) para calcular as chaves usadas para formular a resposta de autenticação.

A BSF recebe respostas de autenticação e verifica se ela tem origem no MT baseado em chaves secretas (por exemplo, SRES e Kc) obtidas independentemente pela função de servidor de autoiniciação 408. Por exemplo, a BSF pode

usar as chaves secretas (por exemplo, SRES e Kc) geradas pelo banco de dados de rede com base no número aleatório RAND e na chave secreta pré-compartilhada (por exemplo, Ki). Desse modo, um certificado de servidor de autoiniciação é usado pelo MT para verificar a origem do pedido de senha enquanto as chaves (por exemplo, SRES e Kc) são usadas pela BSF para verificar a origem da resposta. Isso garante que nenhum ataque por terceiros esteja ocorrendo.

A partir da verificação e cálculos independentes das chaves (por exemplo, SRES e Kc), o MT e a BSF, uma chave compartilhada pode ser computada. Uma chave de aplicação pode ser gerada no terminal móvel e no servidor de autoiniciação cujo servidor de autoiniciação pode prover uma função de aplicação de rede solicitante para permitir comunicações seguras entre o terminal móvel e a função de aplicação de rede 410. Por exemplo, uma chave compartilhada, ou uma chave de aplicação derivada a partir da chave compartilhada, pode ser enviada pela BSF para uma função de aplicação de rede solicitante (NAF) de modo que a NAF e o MT compartilham uma chave que pode ser usada para garantir as comunicações entre a NAF e o MT.

A Figura 5 ilustra um método de autenticar um terminal móvel utilizando uma função de servidor de autoiniciação e autenticação da função de servidor de acordo com uma modalidade da invenção. Esse método pode ser implementado quando uma função de aplicação de rede pretende concordar sobre chaves com um terminal móvel (MT) antes de iniciar uma transação de aplicação de rede. Por exemplo, convenção de chave e autenticação (AKA) GMS se baseiam em um protocolo de pedido de senha-resposta. Uma chave secreta Ki assim como dois algoritmos A3 e A8 são armazenados em um Módulo de Identidade de Assinante (SIM)

dentro do MT assim como o registro de localização nativa de rede (HLR)/Centro de Autenticação (AuC). O SIM é projetado para ser à prova de violação e contém dados secretos e algoritmos que não podem ser facilmente lidos por um usuário.

Uma solicitação para uma chave é gerada e envida a partir do MT, o qual tem um SIM legado dentro dele, para uma função de servidor de autoiniciação (BSF) 502. A BSF obtém informação de autenticação para o MT a partir de um HLR de rede ou AUC 504. Por exemplo, o HLR/AUC seleciona um pedido de senha aleatório de 128 bits RAND o qual é introduzido, junto com Ki, em dois algoritmos A3 e A8 para produzir saída de 32 bits SRES e saída de 64 bits Kc, respectivamente. O tripleto (RAND, SRES, Kc), correspondendo ao SIM do MT solicitante, é então provido a BSF para autenticar o SIM dentro do MT solicitante. A BSF então realiza pedido de senha ao MT com um número aleatório RAND (gerado pelo HLR) e outros parâmetros 506.

O MT verifica se o pedido de senha de autenticação tem origem na BSF esperada com base em um certificado de servidor de autoiniciação 508. Por exemplo, essa verificação pode ser realizada utilizando uma chave pública ou certificado de servidor digital da BSF que foi aprovisionada no MT. Se o pedido de senha de autenticação não é proveniente da BSF esperada, então o processo termina. Caso contrário, uma resposta de autenticação ao pedido de senha é formulada com base em uma chave secreta provida pelo SIM do MT 510. Por exemplo, o MT passa o número aleatório RAND para o SIM (no MT) que calcula uma ou mais chaves secretas (SRES e Kc) utilizando a chave secreta pré-compartilhada Ki e o número aleatório RAND com os algoritmos A3 e A8. As chaves secretas SRES e Kc são então providas ao MT para formular a resposta de autenticação. Em

uma implementação, as chaves secretas SRS e Kc podem ser usadas para computar um código de autenticação de mensagem, ou derivar ou criptografar um ou mais parâmetros, que são enviados como parte da resposta de autenticação.

A resposta de autenticação é enviada a partir do MT para a BSF 512. A BFS então verifica a origem da resposta de autenticação com base em uma chave secreta independentemente obtida 514. Por exemplo, a SRES e Kc obtidos a partir do HLR (no tripleto correspondendo ao número aleatório RAND e chave secreta pré-compartilhada Ki) podem ser usadas para validar um ou mais parâmetros na resposta de autenticação a partir do MT. Por exemplo, a BSF pode calcular independentemente o código de autenticação de mensagem (ou outro parâmetro na resposta de autenticação) utilizando o número aleatório RAND, SRES, e/ou Kc recebidos a partir do HLR. Se os parâmetros (por exemplo, código de autenticação de mensagem) calculados pelo MT e BSF coincidirem, então a origem da resposta de autenticação é verificada.

Em uma implementação alternativa, o MT pode calcular uma terceira chave utilizando a uma ou mais chaves secretas (SRES e Kc obtidas a partir do SIM) e outros parâmetros (obtidos a partir do pedido de senha de autenticação ou resposta a partir do SIM). Essa terceira chave é então usada para formular a resposta de autenticação (por exemplo, computar o código de autenticação de mensagem). A BSF pode também calcular a mesma chave uma vez que ela conhece as mesmas chaves e/ou parâmetros que o MT. Desse modo, a BSF pode verificar se a resposta de autenticação se originou no MT.

Quando a resposta de autenticação é verificada, a BSF e o MT independentemente computam uma chave compartilhada com base em uma ou mais chaves e/ou

parâmetros (por exemplo, SRES, Kc, e/ou outros parâmetros) conhecidos da BSF e do MT 516. Essa chave compartilhada pode ser então provida a uma NAF solicitante para estabelecer comunicações ou transações seguras entre o MT e a NAF 518.

O MT autentica as transmissões a partir da BSF pode intermédio de um mecanismo de chave pública. A BSF realiza o pedido de senha ao MT com um número aleatório RAND e estabelece que ele está de posse das chaves secretas correspondentes SRES e/ou Kc para autenticar as transmissões a partir do MT. Desse modo, a BSF e o MT são mutuamente autenticados para compartilhar informação a partir da qual as chaves podem ser derivadas com o propósito de autoiniciação.

A Figura 6 ilustra um método de realizar um protocolo de pedido de senha-resposta entre um terminal móvel compatível com GSM 608 e uma função de servidor de autoiniciação 604 para autenticar seguramente um ao outro para funções de aplicação de rede de acordo com uma implementação. A convenção de chave e autenticação (AKA) GSM se baseia em um protocolo de resposta de pedido de senha. Para autoiniciação com base em um SIM legado, o HLR/AUC e o SIM realizam cálculos similares com base na chave secreta existente Ki e algoritmos GSM A3 e A8. No protocolo GSM, a chave secreta Ki e o algoritmo(s) de autenticação A3 e A8 são armazenados em um cartão inteligente de módulo de identidade de assinante (SIM) assim como pelo HLR de rede 602. O SIM 608 é projetado para ser à prova de violação, e contém dados e algoritmos que não podem ser facilmente lidos por um usuário. Tipicamente, a chave secreta Ki e o algoritmo(s) de autenticação A3 e A8 são usados para estabelecer serviço através do ar com a rede.

Em uma modalidade, uma solicitação para chaves de autenticação pode ser iniciada pelo MT 606 recuperando sua Identidade de Assinante Móvel Internacional (IMSI) associada 600 a partir de seu SIM 608 e enviando o mesmo para uma função de servidor de autoiniciação (BSF) 604. A BSF 604 envia o IMSI 600 para o HLR 602 onde ele pode verificar se o IMSI 600 pertence a um MT que subscreve para a rede. O HLR 602 pode ser operado pelo provedor de serviço para o assinante cujo SIM está contido no MT 606. O HLR 602 seleciona, por exemplo, um pedido de senha aleatório de 128 bits RAND e junto com a chave secreta pré-compartilhada Ki, utiliza os mesmos como entradas para dois algoritmos A3 e A8 para produzir resposta assinada de saída de 32 bits SRES e chave de confidencialidade secreta de saída de 64 bits Kc, respectivamente. O HLR 602 então provê o tripleto (RAND, SRES, Kc) ao BSF 604, correspondendo ao IMSI de identidade do SIM 608. A BSF 604 gera um expoente secreto aleatório x e computa uma chave pública Diffie-Hellman P^x onde P é um gerador de um grupo cíclico previamente aprovisionado a ambos: BSF 604 e MT 606, tal como o grupo multiplicativo de um campo finito ou o grupo aditivo de uma curva elíptica. A BSF 602 então envia um tripleto (RAND, P^x, SIG) 610 ao MT 606, onde SIG é uma assinatura digital computada utilizando a chave privada RSA da BSF 604. A mensagem 610 pode ser adicionalmente aperfeiçoada para incluir outros parâmetros autenticados por servidor tal como um identificador de transação.

O MT 606 recebe o tripleto (RAND, P^x, SIG) 610 e utiliza o certificado digital da BSF 604 para verificar o SIG. O MT 606 supostamente é aprovisionado com o certificado digital para permitir que ele autentique os dados transmitidos a partir da BSF 604. Se os dados forem considerados como tendo sido originados na BSF, o MT 606

gera um número aleatório Y e computa P^Y. O MT 606 também passa o RAND 612 para o SIM 608 o qual retorna um par (SRES, Kc) 614, gerado com base no RAND e Ki, ao MT 606. Se o SIM 608 for autêntico, então ele deve gerar o mesmo SRES e Kc com foram gerados pelo HLR 602. O MT 606 então computa um código de autenticação de mensagem MAC de P^Y, chaveado com SRES e Kc, e envia uma resposta (P^Y, MAC) 616 para a BSF 604. Essa resposta 616 pode ser melhorada adicionalmente para incluir outros parâmetros através dos quais o MAC é computado, tal como um identificador de transação.

A BSF 604 recebe P^Y e verifica o MAC utilizando o SRES e Kc que ele recebe no tripleto de autenticação a partir do HLR 602. Se esse MAC estiver correto, isso verifica que o MT 606 está de posse do SIM correto 608, e uma mensagem de confirmação 618 pode ser enviada para o MT 606.

Nessa modalidade o MT 606 e a BSF 604 desse modo realizaram uma troca de chave Diffie-Hellman mutuamente autenticada e concordam com uma chave P^{XY} que eles computam respectivamente. Uma chave para comunicação adicional pode então ser computada, por exemplo, como um hash de P^{XY}, incluindo possivelmente informação adicional conhecida tanto do MT como da BSF tal como informação de identidade, RAND, SRES e Kc. No caso onde os cálculos Diffie-Hellman ocorrem, ou a chave resultante é armazenada, no MT 606 mais propriamente do que no SIM 608, essa chave P^{XY} e a chave concordada resultante devem ser deletadas se o SIM 608 for removido do MT, ou se o MT for acionado utilizando um SIM diferente 608.

Observar que esse protocolo protege contra vulnerabilidades padrão surgindo a partir do GSM desde que o MT 606 não suporte o algoritmo A5/2. O algoritmo A5/2

permite uma quebra quase instantânea no protocolo GSM que pode minar o protocolo acima. Contudo, o algoritmo A5/2 está sendo colocado fora de fase nas especificações do 3GPP Release 6.

Observar ainda que uma tentativa de terceiros em atacar o protocolo não podem mudar o pedido de senha inicial (RAND, P^X, SIG), devido ao SIG, de modo que aquele que ataca não pode inserir seu próprio P^Z ou utilizar um RAND diferente. Ele poderia na melhor das hipóteses reproduzir essas mensagens, mas não pode personificar a BSF uma vez que qualquer reprodução é equivalente a usar Diffie-Hellman efêmero. Inversamente, se a BSF garantir que o RAND usado é novo, a partir de um uso desse protocolo para o próximo, e garantir que a resposta (P^Y, MAC) seja recebido em um curto período de tempo, então aquele que ataca não tem a chance de derivar o SRES e Kc através de outros meios tais como pedido de senha com RAND no cenário GSM típico e atacar o algoritmo A5/1 para derivar as chaves.

A Figura 7 ilustra um método alternativo de realizar um protocolo de pedido de senha-resposta entre um terminal móvel legado (MT) 706 suportando um Módulo de Identidade de Assinante consoante com GSM 708 (SIM) e uma função de servidor de autoiniciação (BSF) 704 para autenticar seguramente um ao outro e concordar com uma chave para funções de aplicação de rede (NSF) de acordo com uma implementação. Similar ao método na Figura 6, uma solicitação para chaves de autenticação pode ser iniciada pelo MT 706 enviando seu IMSI associado 700 a partir de seu SIM 708 para a BSF 704. A BSF 704 envia o IMSI 700 para o HLR 702 onde ele pode verificar se o IMSI pertence a um MT que subscreve para a rede. O HLR 702 então seleciona a provê o tripleto (RAND, SRES, Kc) a BSF 704, correspondendo

ao IMSI de identidade 700 do SIM 708. Por exemplo, RAND pode ser um número aleatório de 128 bits e Ki é uma chave de integridade secreta pré-compartilhada Ki, e eles são usados como entradas para dois algoritmos A3 e A8 que produzem uma resposta assinada SRES (por exemplo, número de 32 bits) e chave de confidencialidade secreta Kc (por exemplo, número de 64 bits), respectivamente. O MT 706 supostamente é provisionado com uma chave pública ou certificado digital permitindo que ele autentique os dados transmitidos a partir da BSF 704.

A BSF 704 recebe o tripleto (RAND, SRES, Kc) a partir do HLR 702. A BSF 704 então computa uma assinatura digital SIG do RAND (e possivelmente outros parâmetros, tal como uma marcação de tempo, número de seqüência, semente aleatória ou informação de identidade) utilizando um mecanismo baseado em chave pública que permite que o MT 706 autentique a fonte de dados recebidos a partir da BSF 704. A BSF 704 envia RAND e SIG 710 para o MT 706. Mediante recebimento do (RAND, SIG) 710, o MT 706 verifica o SIG utilizando o certificado digital da BSF 704. Se os dados forem considerados como sendo provenientes da BSF 704, o MT 706 envia RAND 712 para o SIM 708 para recuperar os parâmetros correspondentes SRES e Kc. Isto é, o SIM 708 gera um par de SRES e Kc mediante uso da chave secreta pré-compartilhada Ki e RAND como entradas para os algoritmos A3 e A8 com os quais ele foi aprovisionado. O MT 706 pode então gerar uma chave PSK, codificando PSK sob um mecanismo baseado em chave pública, e aplica um código de autenticação de mensagem MAC ao resultado. Parâmetros adicionais tais como uma marcação de tempo, número de seqüência, semente aleatória ou informação de identidade podem ser incluídos na resposta. O MAC pode ser baseado em uma função ou algoritmo (conhecido tanto do MT 706 como da

BSF 704) que pode incluir Kc e SRES como parâmetros de entrada, e é usado para provar à BSF 704 que o MT 706 possui o SIM correto 708. Observar que as operações de codificação baseada em chave pública dos dados e o MAC chaveado com SRES e Kc podem ser realizados em qualquer ordem. O MT 706 então envia (PSK, MAC codificado) 716 para a BSF 704, a qual verifica que o MT 706 está de posse do SRES e Kc corretos mediante verificação do MAC. Essa verificação do MAC é feita mediante uso do SRES e Kc recebidos pela BSF 704 a partir do HLR 702 para re-calcular um MAC e comparar o mesmo com o MAC recebido a partir do MT 706. Se o MAC for considerado correto, o PSK é considerado como tendo sido originado a partir do MT 706 e SIM 708, e uma confirmação 718 é enviada para o MT 706. Desse modo, esse PAK é concordado entre o MT 706 e a BSF 704, ou derivações de chave adicionais podem ser feitas utilizando PSK, Kc, SRES, informação de identidade e possivelmente outros parâmetros.

O mecanismo de pedido de senha-resposta ilustrado nas Figuras 6 e 7 para terminais móveis baseados em GSM também pode ser implementado em outros tipos de terminais móveis. Por exemplo, a invenção pode ser operacional em uma rede consoante com CDMA2000 e terminal móvel (MT). Em tal implementação, um terminal móvel consoante com CDMA2000 contém um Módulo de Autenticação CDMA2000, UIM ou RUIM para concordar sobre uma chave secreta pré-compartilhada que pode ser usada para segurança de aplicações de rede. Em uma implementação, a chave pré-compartilhada pode ser gerada utilizando-se um algoritmo Diffie-Hellman autenticado, onde o parâmetro público P^X, provido pela BSF, é autenticado por intermédio de um mecanismo de assinatura digital de chave pública (isto é, um certificado de servidor de autoiniciação conhecido do MT), ao passo que o parâmetro

P^Y, provido pelo MT, é autenticado mediante adição de um Código de Autenticação de Mensagem chaveado com tal material como a SMEKEY (chave de criptografia de mensagem de sinalização) a partir do CAVE (Algoritmo de Criptografia de Voz e Autenticação Celular) ou do autenticador MN-AAA (Autenticação, Autorização, e Contabilidade de Nó Móvel). Supõe-se que o MT é aprovisionado com a chave pública ou certificado digital que permite que ele autentique mensagens digitalmente assinadas a partir da BSF e uma chave secreta pré-compartilhada Ki e identificador de Código de Autenticação IMSI é conhecido tanto do Módulo de Código de Autenticação e do HLR.

Aqueles versados na técnica considerarão que essa abordagem se aplique igualmente na circunstância em que autenticação do portador se baseia em CAVE, e outra vez oferece a vantagem de que essas operações de autoiniciação podem ser realizadas utilizando operações simétricas e RSA do princípio ao fim e desse modo podem oferecer vantagens de implementação em relação aos protocolos exigindo suporte tanto de Diffie-Hellman como de RSA.

Um ou mais dos componentes e funções ilustrados nas Figuras 1, 2 e/ou 3 podem ser rearranjados e/ou combinados em um único componente ou incorporados em vários componentes sem se afastar da invenção. Elementos ou componentes adicionais também podem ser adicionados sem se afastar da invenção. O equipamento, dispositivos, e/ou componentes ilustrados nas Figuras 1, 2 e/ou 3 podem ser configurados para realizar os métodos, características, ou etapas ilustrados nas Figuras 4, 5, 6 e/ou 7.

Deve ser observado que as modalidades anteriores são apenas exemplos e não devem ser consideradas como limitando a invenção. Pretende-se que a descrição das modalidades seja ilustrativa, e não limite o escopo das

reivindicações. Como tal, os presentes ensinamentos podem ser aplicados prontamente a outros tipos de equipamentos e muitas alternativas, modificações e variações serão evidentes para aqueles versados na técnica.

REIVINDICAÇÕES

1. Método para autenticar uma função de servidor de auto-iniciação (106, 604, 704) para um terminal móvel (102, 200, 606, 706) suportando um módulo de identidade de assinante legado, **caracterizado** por compreender:

- aprovisionar o terminal móvel com um certificado digital associado com a função de servidor de auto-iniciação;

- receber (404) um desafio de autenticação no terminal móvel incluindo um número aleatório;

- autenticar, no terminal móvel, a função de servidor de auto-iniciação com base no certificado digital associado com a função de servidor de auto-inicição;

- sendo aprovisionado com uma primeira chave privada pelo módulo de identidade de assinante legado em resposta a passar o número aleatório recebido no desafio de autenticação para o módulo de identidade de assinante legado;

- formular (510) uma resposta de autenticação com base na primeira chave privada aprovisionada pelo módulo de identidade de assinante legado ao terminal móvel.

2. Método, de acordo com a reivindicação 1, **caracterizado** por compreender ainda enviar uma resposta de autenticação para a função de servidor de auto-iniciação para permitir a função de servidor de auto-iniciação a autenticar o terminal móvel.

3. Método, de acordo com a reivindicação 1 ou 2, **caracterizado** pelo aprovisionamento permitir comunicações com a função de servidor de auto-iniciação para o terminal móvel para ser realizada em um canal autenticado por servidor.

4. Método, de acordo com qualquer uma das reivindicações 1 a 3, **caracterizado** por compreender ainda:

calcular a primeira chave privada no módulo de identidade de assinante legado utilizando o número aleatório, uma chave privada pré-compartilhada e um algoritmo em que a chave privada pré-compartilhada e o algoritmo são ambos armazenados no módulo de identidade de assinante legado.

5. Método, de acordo com qualquer uma das reivindicações 1 a 4, **caracterizado** pelo desafio de autenticação recebido compreender ainda parâmetros adicionais.

6. Método, de acordo com a reivindicação 5, **caracterizado** pela primeira chave privada ser calculada utilizando parâmetros adicionais recebidos no desafio de autenticação.

7. Método, de acordo com a reivindicação 2, **caracterizado** por compreender:

computar uma chave adicional no terminal móvel com base na primeira chave privada, onde a segunda chave é também computada independentemente na função de servidor de auto-iniciação (106, 604, 704) com base em uma segunda chave privada aprovisionada na função de servidor de auto-iniciação por uma base de dados de rede (104, 602, 702),

em que a chave adicional é enviada a partir da função de servidor de auto-iniciação para uma função de aplicação de rede solicitante (108) de modo que o terminal móvel (102, 200, 606, 706) e a função de aplicação de rede compartilhem a chave adicional.

8. Método, de acordo com a reivindicação 7, **caracterizado** pela chave adicional ser uma chave de aplicação, a chave de aplicação sendo derivada a partir de uma chave compartilhada que é computada com base na primeira chave privada.

9. Método, de acordo com qualquer uma das

reivindicações 1 a 8, **caracterizado** pelo módulo de identificação de assinante (204, 608, 708) ser um dentre um Módulo de Identidade de Assinante, SIM, de Sistema Global para Comunicações Móveis, GSM, ou um Módulo de Autenticação CDMA2000.

10. Método, de acordo com qualquer uma das reivindicações 1 a 9, **caracterizado** pelo desafio de autenticação para o terminal móvel ser enviado através de um canal autenticado por servidor.

11. Método, de acordo com qualquer uma das reivindicações 1 a 10, **caracterizado** pelo desafio de autenticação para o terminal móvel incluir informação de identidade.

12. Terminal móvel (102, 200, 606, 706) suportando um módulo de identidade de assinante legado (204, 608, 708), **caracterizado** por compreender:

meios para receber e armazenar um certificado digital associado com uma função de servidor de auto-iniciação (106, 604, 704);

meios para receber a partir de uma função de servidor de auto-iniciação um desafio de autenticação incluindo um número aleatório;

meios para autenticar a função de servidor de auto-iniciação com base no certificado digital associado com a função de servidor de auto-inicição;

meios para receber uma primeira chave privada pelo módulo de identidade de assinante legado em resposta a passar o número aleatório recebido no desafio de autenticação para o módulo de identidade de assinante legado;

meios para formular uma resposta de autenticação para o desafio de autenticação com base na primeira chave privada aprovisionada pelo módulo de identidade de

assinante legado ao terminal móvel.

13. Terminal móvel, de acordo com a reivindicação 12, **caracterizado** por compreender ainda meios para enviar uma resposta de autenticação para a função de servidor de auto-iniciação.

14. Terminal móvel, de acordo com a reivindicação 12 ou 13, **caracterizado** por compreender ainda:

meios para calcular a primeira chave privada com base em uma chave privada pré-compartilhada e um algoritmo armazenados no módulo de identidade de assinante legado, e o número aleatório recebido no desafio de autenticação.

15. Terminal móvel, de acordo com a reivindicação 14, **caracterizado** pela primeira chave privada ser com base em parâmetros adicionais transmitidos no desafio de autenticação.

16. Terminal móvel, de acordo com a reivindicação 14 ou 15, **caracterizado** por compreender ainda:

meios para computar um código de autenticação de mensagem utilizando a primeira chave privada e para incluir o código de autenticação de mensagem na resposta de autenticação.

17. Terminal móvel, de acordo com qualquer uma das reivindicações 12 a 16, **caracterizado** por compreender ainda:

uma interface de comunicação sem fio para comunicar com a função de servidor de auto-iniciação; e

um circuito de processamento (202, 204) configurado para operar um protocolo de comunicação legado e autenticar o terminal móvel em um protocolo de resposta de desafio com a função de servidor de auto-iniciação.

18. Terminal móvel, de acordo com a reivindicação 17, **caracterizado** pelo circuito de processamento ser configurado para gerar uma chave adicional com base na

primeira chave privada.

19. Terminal móvel, de acordo com a reivindicação 18, **caracterizado** pela chave adicional ser com base ainda em parâmetros adicionais transmitidos no desafio de autenticação.

20. Terminal móvel, de acordo com a reivindicação 18 ou 19, **caracterizado** pela chave adicional ser uma chave de aplicação com base em uma chave compartilhada, a chave compartilhada sendo calculada utilizando a primeira chave privada.

21. Terminal móvel, de acordo com qualquer uma das reivindicações 18 a 20, **caracterizado** pelo circuito de processamento ser ainda configurado para gerar um código de autenticação de mensagem.

22. Terminal móvel, de acordo com a reivindicação 21, **caracterizado** pela resposta de autenticação incluir um código de autenticação de mensagem computado utilizando a chave adicional.

23. Terminal móvel, de acordo com qualquer uma das reivindicações 17 a 22, **caracterizado** pelo módulo de identificação de assinante ser acoplado ao circuito de processamento e o módulo de identificação de assinante ser para armazenar uma chave privada pré-compartilhada e um algoritmo.

24. Terminal móvel, de acordo com a reivindicação 23, **caracterizado** pelo módulo de identificação de assinante gerar a primeira chave privada com base no número aleatório, a chave privada pré-compartilhada e o algoritmo.

25. Terminal móvel, de acordo com a reivindicação 23 ou 24, **caracterizado** pelo módulo de identificação de assinante ser um Módulo de Identidade de Assinante, SIM, de acordo com o protocolo de Sistema Global para Comunicações Móveis, GSM.

26. Terminal móvel, de acordo com a reivindicação 14, **caracterizado** pela chave secreta pré-compartilhada é também empregada para permitir que o terminal móvel estabeleça comunicações através de uma rede sem fio legada.

27. Terminal móvel, de acordo com qualquer uma das reivindicações 12 a 26, **caracterizado** pelo desafio de autenticação para o terminal móvel ser enviado através de um canal autenticado por servidor.

28. Terminal móvel, de acordo com qualquer uma das reivindicações 12 a 18, **caracterizado** pelo desafio de autenticação para o terminal móvel incluir informação de identidade.

29. Memória legível por computador **caracterizada** por compreender instruções que, quando realizadas por um processador, realizam o método conforme definido em qualquer uma das reivindicações 1 a 11.

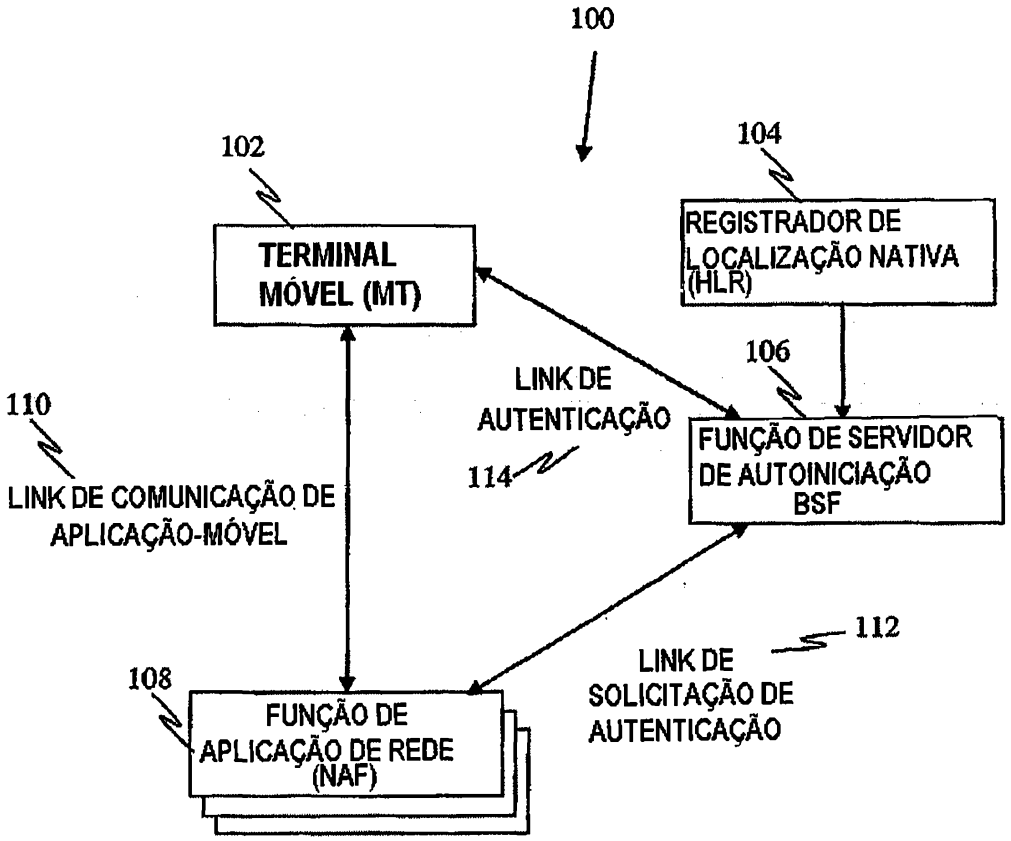

100
102
TERMINAL MÓVEL (MT)
104
REGISTRADOR DE LOCALIZAÇÃO NATIVA (HLR)
106
FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO BSF
LINK DE AUTENTICAÇÃO
114
110
LINK DE COMUNICAÇÃO DE APLICAÇÃO-MÓVEL
112
LINK DE SOLICITAÇÃO DE AUTENTICAÇÃO
108
FUNÇÃO DE APLICAÇÃO DE REDE (NAF)

FIGURA 1

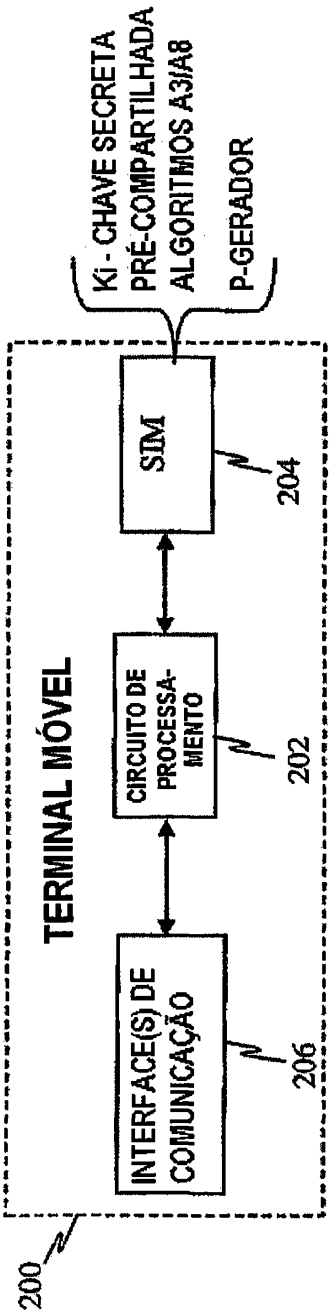


FIGURA 2

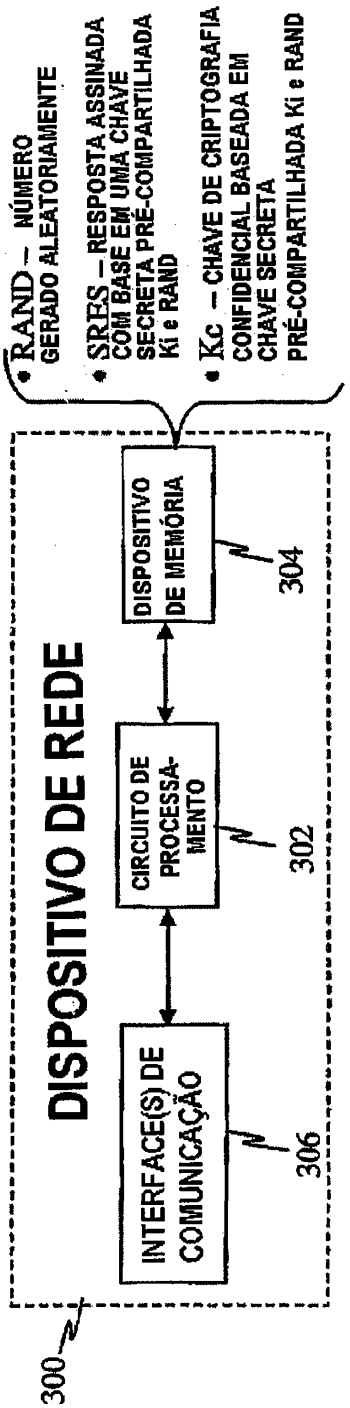


FIGURA 3

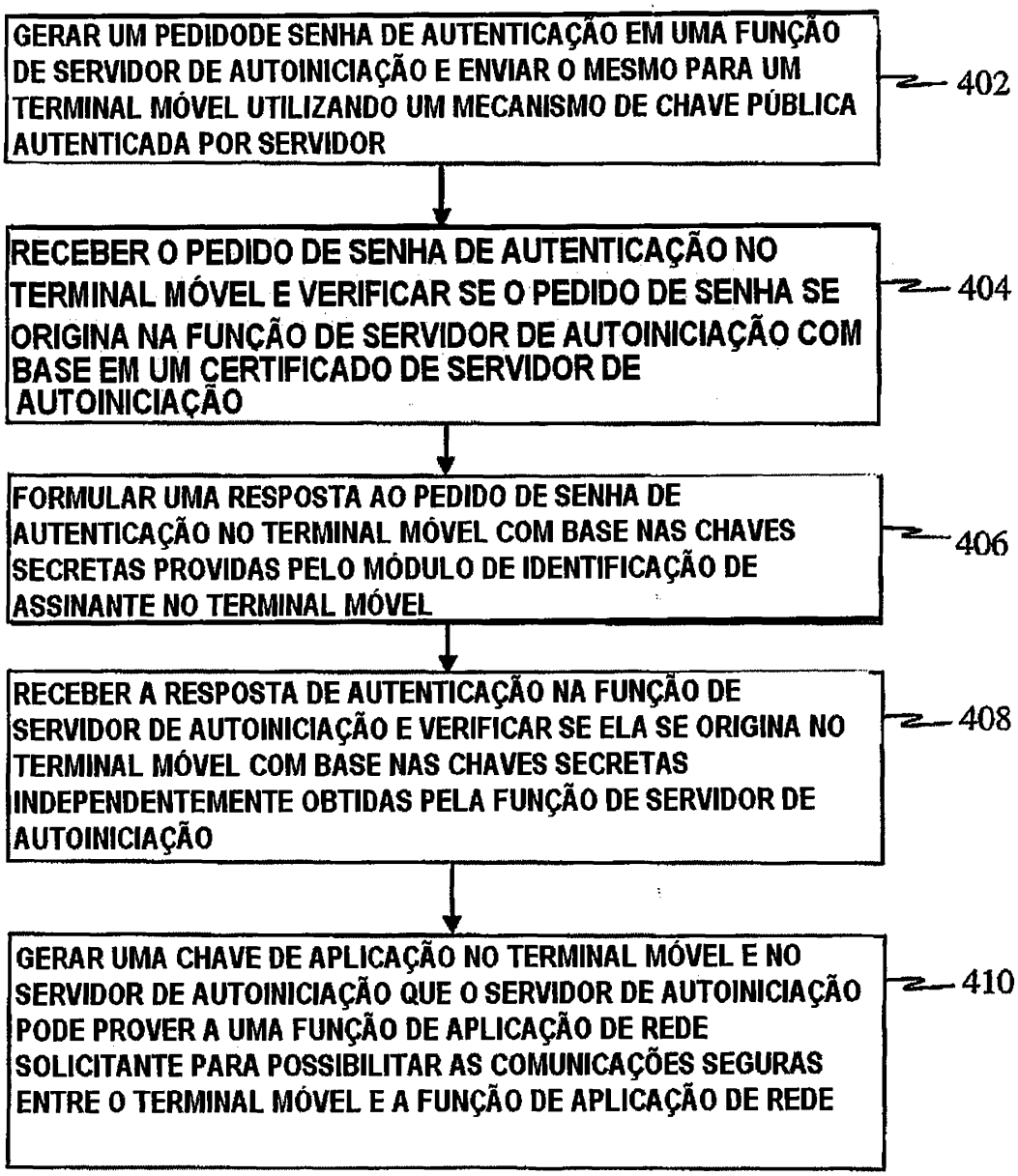

GERAR UM PEDIDODE SENHA DE AUTENTICAÇÃO EM UMA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO E ENVIAR O MESMO PARA UM TERMINAL MÓVEL UTILIZANDO UM MECANISMO DE CHAVE PÚBLICA AUTENTICADA POR SERVIDOR
402
RECEBER O PEDIDO DE SENHA DE AUTENTICAÇÃO NO TERMINAL MÓVEL E VERIFICAR SE O PEDIDO DE SENHA SE ORIGINA NA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO COM BASE EM UM CERTIFICADO DE SERVIDOR DE AUTOINICIAÇÃO
404
FORMULAR UMA RESPOSTA AO PEDIDO DE SENHA DE AUTENTICAÇÃO NO TERMINAL MÓVEL COM BASE NAS CHAVES SECRETAS PROVIDAS PELO MÓDULO DE IDENTIFICAÇÃO DE ASSINANTE NO TERMINAL MÓVEL
406
RECEBER A RESPOSTA DE AUTENTICAÇÃO NA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO E VERIFICAR SE ELA SE ORIGINA NO TERMINAL MÓVEL COM BASE NAS CHAVES SECRETAS INDEPENDENTEMENTE OBTIDAS PELA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO
408
GERAR UMA CHAVE DE APLICAÇÃO NO TERMINAL MÓVEL E NO SERVIDOR DE AUTOINICIAÇÃO QUE O SERVIDOR DE AUTOINICIAÇÃO PODE PROVER A UMA FUNÇÃO DE APLICAÇÃO DE REDE SOLICITANTE PARA POSSIBILITAR AS COMUNICAÇÕES SEGURAS ENTRE O TERMINAL MÓVEL E A FUNÇÃO DE APLICAÇÃO DE REDE
410

FIGURA 4

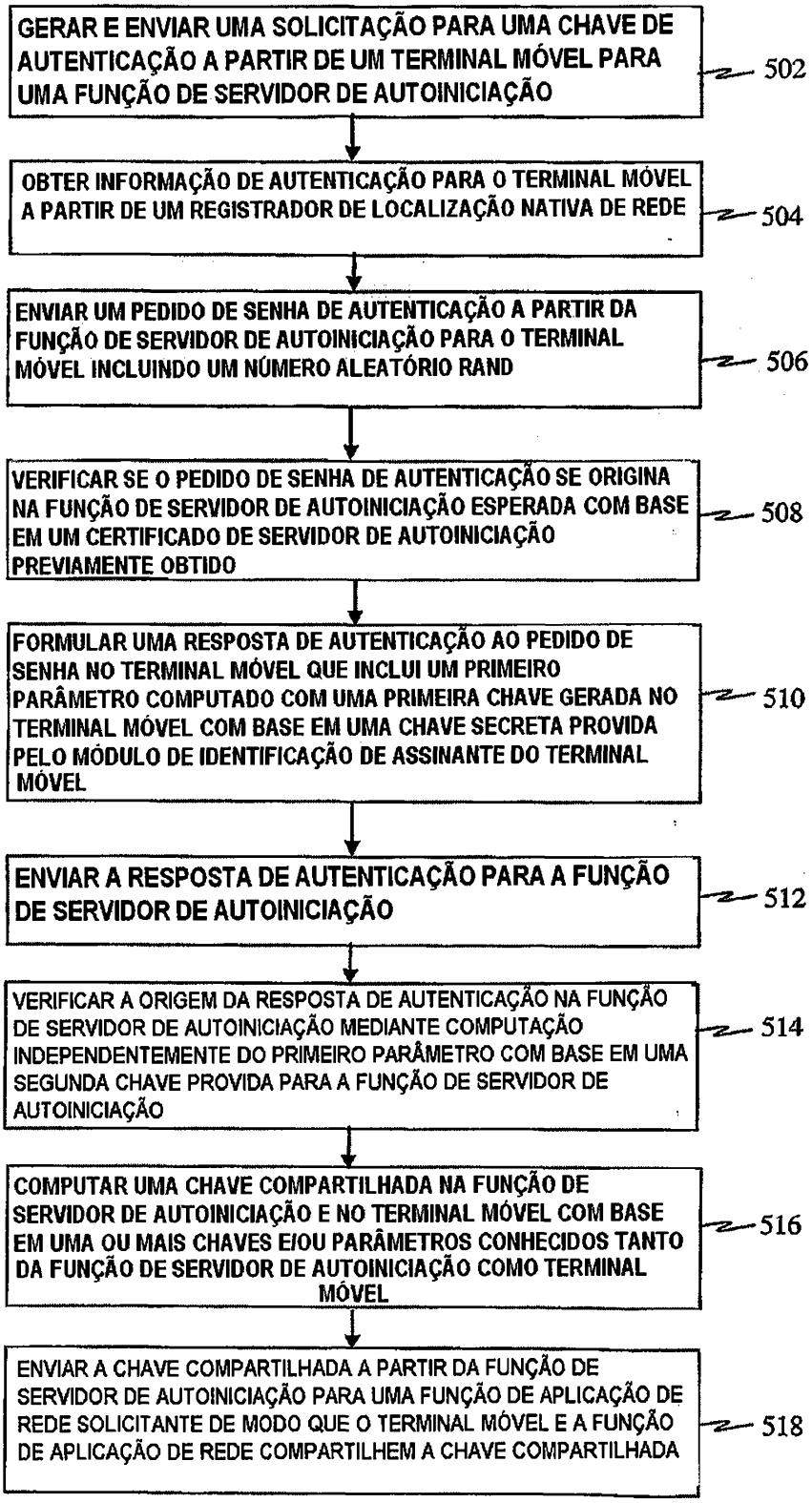

GERAR E ENVIAR UMA SOLICITAÇÃO PARA UMA CHAVE DE AUTENTICAÇÃO A PARTIR DE UM TERMINAL MÓVEL PARA UMA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO
502
OBTER INFORMAÇÃO DE AUTENTICAÇÃO PARA O TERMINAL MÓVEL A PARTIR DE UM REGISTRADOR DE LOCALIZAÇÃO NATIVA DE REDE
504
ENVIAR UM PEDIDO DE SENHA DE AUTENTICAÇÃO A PARTIR DA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO PARA O TERMINAL MÓVEL INCLUINDO UM NÚMERO ALEATÓRIO RAND
506
VERIFICAR SE O PEDIDO DE SENHA DE AUTENTICAÇÃO SE ORIGINA NA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO ESPERADA COM BASE EM UM CERTIFICADO DE SERVIDOR DE AUTOINICIAÇÃO PREVIAMENTE OBTIDO
508
FORMULAR UMA RESPOSTA DE AUTENTICAÇÃO AO PEDIDO DE SENHA NO TERMINAL MÓVEL QUE INCLUI UM PRIMEIRO PARÂMETRO COMPUTADO COM UMA PRIMEIRA CHAVE GERADA NO TERMINAL MÓVEL COM BASE EM UMA CHAVE SECRETA PROVIDA PELO MÓDULO DE IDENTIFICAÇÃO DE ASSINANTE DO TERMINAL MÓVEL
510
ENVIAR A RESPOSTA DE AUTENTICAÇÃO PARA A FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO
512
VERIFICAR A ORIGEM DA RESPOSTA DE AUTENTICAÇÃO NA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO MEDIANTE COMPUTAÇÃO INDEPENDENTEMENTE DO PRIMEIRO PARÂMETRO COM BASE EM UMA SEGUNDA CHAVE PROVIDA PARA A FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO
514
COMPUTAR UMA CHAVE COMPARTILHADA NA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO E NO TERMINAL MÓVEL COM BASE EM UMA OU MAIS CHAVES E/OU PARÂMETROS CONHECIDOS TANTO DA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO COMO TERMINAL MÓVEL
516
ENVIAR A CHAVE COMPARTILHADA A PARTIR DA FUNÇÃO DE SERVIDOR DE AUTOINICIAÇÃO PARA UMA FUNÇÃO DE APLICAÇÃO DE REDE SOLICITANTE DE MODO QUE O TERMINAL MÓVEL E A FUNÇÃO DE APLICAÇÃO DE REDE COMPARTILHEM A CHAVE COMPARTILHADA
518

FIGURA 5

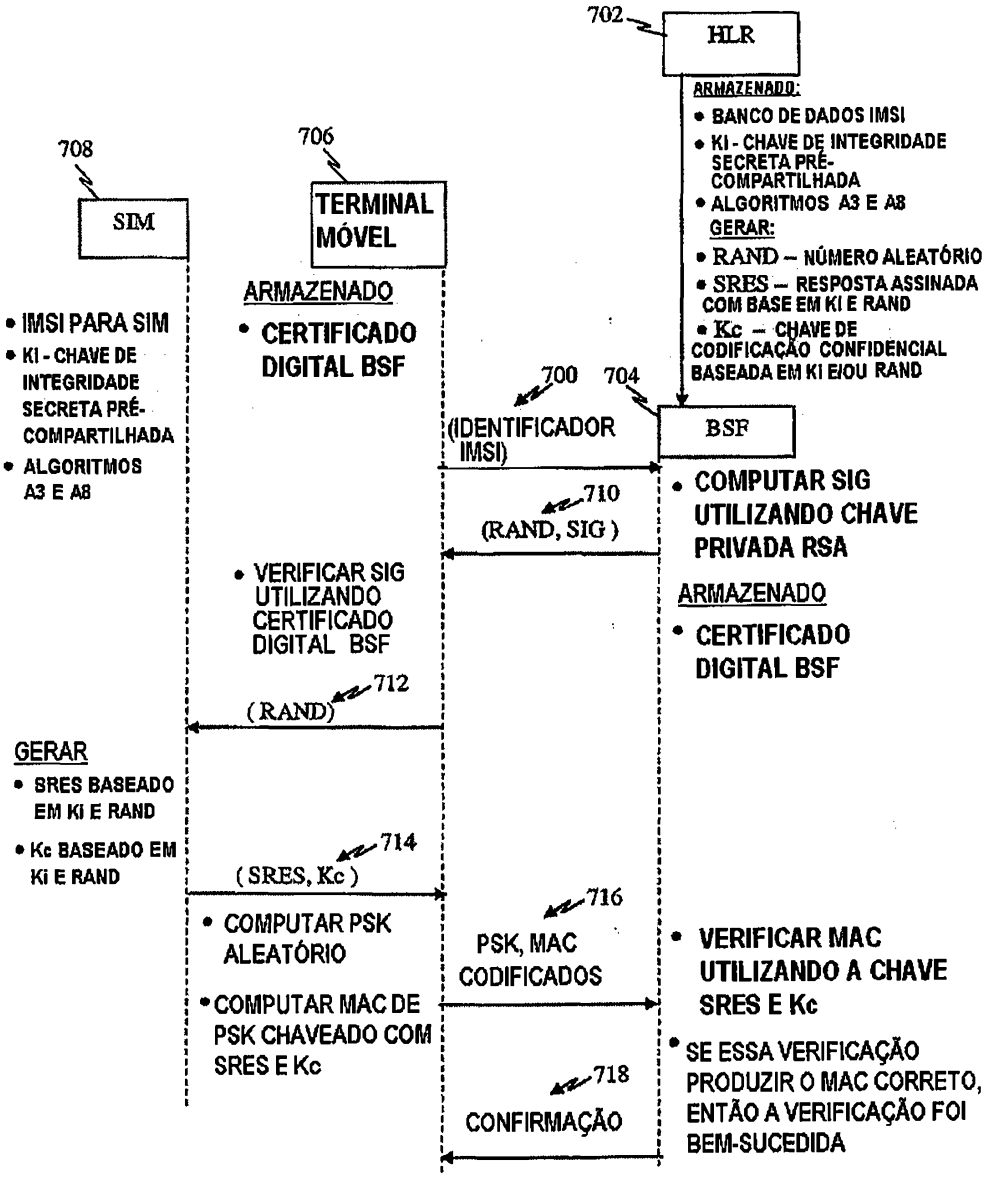

702
HLR
ARMAZENADO:
• BANCO DE DADOS IMSI
• KI - CHAVE DE INTEGRIDADE SECRETA PRÉ-COMPARTILHADA
• ALGORITMOS A3 E A8
GERAR:
• RAND – NÚMERO ALEATÓRIO
• SRES – RESPOSTA ASSINADA COM BASE EM KI E RAND
• Kc – CHAVE DE CODIFICAÇÃO CONFIDENCIAL BASEADA EM KI E/OU RAND
708
SIM
706
TERMINAL MÓVEL
704
BSF
700
(IDENTIFICADOR IMSI)
• IMSI PARA SIM
• KI - CHAVE DE INTEGRIDADE SECRETA PRÉ-COMPARTILHADA
• ALGORITMOS A3 E A8
ARMAZENADO
• CERTIFICADO DIGITAL BSF
• COMPUTAR SIG UTILIZANDO CHAVE PRIVADA RSA
710
(RAND, SIG)
• VERIFICAR SIG UTILIZANDO CERTIFICADO DIGITAL BSF
ARMAZENADO
• CERTIFICADO DIGITAL BSF
712
(RAND)
GERAR
• SRES BASEADO EM KI E RAND
• Kc BASEADO EM Ki E RAND
714
(SRES, Kc)
716
PSK, MAC CODIFICADOS
• COMPUTAR PSK ALEATÓRIO
• COMPUTAR MAC DE PSK CHAVEADO COM SRES E Kc
• VERIFICAR MAC UTILIZANDO A CHAVE SRES E Kc
• SE ESSA VERIFICAÇÃO PRODUZIR O MAC CORRETO, ENTÃO A VERIFICAÇÃO FOI BEM-SUCEDIDA
718
CONFIRMAÇÃO

FIGURA 7