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

(21) **PI0608531-8 A2**

BRPI0608531A2

(22) Data de Depósito: 10/02/2006
(43) Data da Publicação: 12/01/2010
(RPI 2036)

(51) Int.Cl.:
H04L 29/06 (2010.01)

(54) Título: **MÉTODO E APARELHO PARA PROVER OS PROCEDIMENTOS DE AUTO-CARREGAMENTO NA REDE DE COMUNICAÇÃO**

(30) Prioridade Unionista: 10/02/2006 US 11/352,058, 11/02/2005 US 60/651,620, 11/02/2005 US 60/652,235, 15/04/2005 US 60/671,621

(73) Titular(es): NOKIA CORPORATION

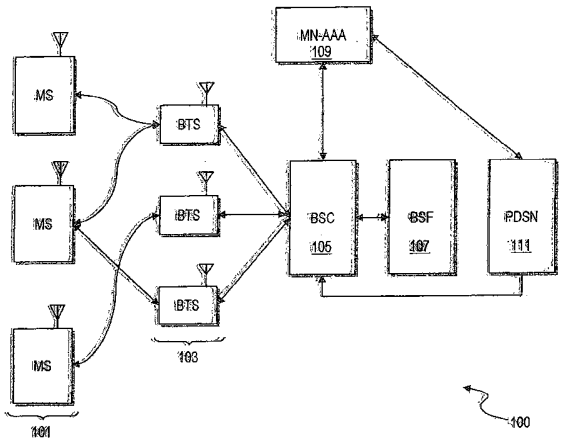
(72) Inventor(es): GABOR BAJKO, NADARAJAH ASOKAN, PEKKA LAITINEN, PHILIP GINZBOORG

(74) Procurador(es): Araripe & Associados

(86) Pedido Internacional: PCT IB2006000272 de 10/02/2006

(87) Publicação Internacional: WO 2006/085207de 17/08/2006

(57) Resumo: MÉTODO E APARELHO PARA PROVER OS PROCEDIMENTOS DE AUTO-CARREGAMENTO NA REDE DE COMUNICAÇÃO. Uma aproximação é fornecida para executar a autenticação no sistema de comunicação. Em uma incorporação, a chave é estabelecida com o terminal na rede de comunicação de acordo com o protocolo de acordo de chave. A chave acordada é fixada para o procedimento de autenticação para prover uma associação de segurança que suporta a reutilização da chave. A chave mestre é gerada baseado na chave acordada. Em outra incorporação, a autenticação de compilação é combinada com os parâmetros de troca de chave (ex., os parâmetros Diffie Hellman) na carga útil da mensagem de compilação, na qual a chave (ex., SMEKEY ou MN-AAA) é utilizada como senha. Em ainda outra incorporação, o aigoritmo de autenticação (ex., Autenticação Celular e Cifragem de Voz (CAVE)) é empregado com o protocolo de acordo de chave com as funções de conversão para suportar o auto-carregamento.



PI0608531-8
Pet. 003972

"MÉTODO E APARELHO PARA PROVER OS PROCEDIMENTOS DE AUTO-CARREGAMENTO NA REDE DE COMUNICAÇÃO".

Este pedido reivindica o benefício da data de depósito sob 35 U.S.C. §119(e) do Pedido Provisório US Nº 60/652,235 depositado em 11 de fevereiro de 2005, intitulado de "Método e Aparelho Para Suportar a Autenticação em um Sistema de Comunicação de Rádio", o Pedido Provisório US Nº 60/671,621 depositado em 15 de abril de 2005, intitulado de "Método e Aparelho Para Autocarregamento em um Sistema de Comunicação de Rádio", e o Pedido Provisório US Nº 60/651,620 11 depositado em 11 de fevereiro de 2005, intitulado de "Usar GAA nas Redes CDMA Legadas"; as totalidades são incorporadas aqui por referência.

Campo da Invenção

A invenção relaciona às comunicações, e mais particularmente, ao provimento dos serviços de autenticação no sistema de comunicação.

Descrição da Técnica Anterior

Os sistemas de comunicação de rádio, tais como os sistemas celulares (por exemplo, os sistemas de espectro de dispersão (tal como as redes de Acesso Múltiplo por Divisão de Código (CDMA)), ou as redes de Acesso Múltiplo por Divisão de Tempo (TDMA)), proporcionam aos usuários a conveniência da mobilidade junto com um grupo rico de serviços e características. Esta conveniência gerou uma adoção significante por um número crescente de consumidores como um modo de comunicação aceito para negócios e usos pessoais. Para promover uma maior adoção, a indústria de telecomunicação, dos fabricantes aos provedores de serviço, tem acordado em uma grande despesa e esforço para desenvolver os padrões para os protocolos de comunicação que disponíveis para os vários serviços e características. Uma área fundamental de esforço envolve a autenticação. A autenticação realiza um papel importante em qualquer sistema de comunicação para assegurar que a comunicação seja estabelecida entre próprios usuários ou aplicações. Infelizmente, a implementação de tais padrões pode requerer a modificação de outros protocolos, que podem ser

de custo proibitivo, mesmo se tecnicamente realizável.

Então, há uma necessidade por uma aproximação para prover os serviços de autenticação sem requerer a alteração dos protocolos padrões existentes ou o desenvolvimento de novos protocolos.

Resumo da Invenção

Estas e outras necessidades são solucionadas pela invenção, na qual uma aproximação é apresentada para executar mais efetivamente a autenticação inicial (bootstrapping) em uma rede de comunicação.

De acordo com o aspecto de uma incorporação da invenção, um método para autenticar compreende estabelecer uma chave com o terminal na rede de comunicação de acordo com o protocolo de acordo de chave, onde o terminal é configurado para operar usando o espectro de dispersão. O método também compreende fixar a chave acordada para o procedimento de autenticação para prover uma associação de segurança que suporta a reutilização da chave. Ainda o método também compreende gerar a chave mestre baseada na chave acordada.

De acordo com outro aspecto de uma incorporação da invenção, o método para autenticar inclui estabelecer uma chave compartilhada com um elemento de rede em uma rede de comunicação de acordo com o protocolo de acordo de chave, em que o elemento de rede é configurado para fixar a chave de acordo com o procedimento de autenticação para prover uma associação de segurança que suporta a reutilização da chave. O método também inclui gerar uma chave mestre baseada na chave de acordo.

De acordo com outro aspecto de uma incorporação da invenção, o aparelho para autenticar inclui um módulo de autenticação configurado para estabelecer uma chave compartilhada com um elemento de rede em uma rede de comunicação de acordo com o protocolo de acordo de chave, em que o elemento de rede é configurado para fixar a chave de acordo com o procedimento de autenticação para prover uma associação de segurança que suporta a reutilização da chave, o módulo de autenticação é configurado para gerar uma chave mestre

baseada na chave acordada.

De acordo com outro aspecto de uma incorporação da invenção, o método para autenticar inclui gerar uma mensagem para autenticar a comunicação com o elemento de rede configurado para executar a autenticação inicial. O método também inclui configurar um campo de senha da mensagem para uma função da chave secreta, em que a chave secreta é codificada; e especificar a informação de estabelecimento de chave dentro da carga útil da mensagem, em que a mensagem é transmitida de acordo com o protocolo de transporte para acessar a informação na rede de dados.

De acordo com outro aspecto de uma incorporação da invenção, o método para autenticar inclui receber uma mensagem do terminal, de acordo com o protocolo de transporte para acessar a informação na rede de dados, solicitar a autenticação, onde a mensagem inclui um campo de senha que é uma função da chave secreta e a carga útil contêm a informação de estabelecimento da chave que especifica os parâmetros para determinar outra chave secreta. O método também inclui gerar uma chave mestre baseada na chave secreta.

De acordo com outro aspecto de uma incorporação da invenção, o aparelho para autenticar inclui um módulo de autenticação configurado para gerar uma mensagem para autenticar a comunicação com o elemento de rede configurado para executar a autenticação inicial, e fixar um campo de senha da mensagem para ser uma função de uma chave secreta, em que a chave secreta é codificada. A mensagem tem uma carga útil que inclui a nova informação de estabelecimento da chave. A mensagem é transmitida de acordo com o protocolo de transporte para acessar a informação na rede de dados.

De acordo com outro aspecto de uma incorporação da invenção, o método para autenticar inclui receber um pedido de autenticação que especifica a identidade do usuário do terminal. O método também inclui direcionar a identidade do usuário para um registro local configurado para gerar, baseado na identidade do usuário, os parâmetros criptográficos incluindo os dados secretos randômicos, e os dados secretos gerados dos dados secretos randômicos de acordo com um

algoritmo criptográfico. Adicionalmente, o método inclui receber os parâmetros criptográficos gerados do registro local. O método também inclui gerar um vetor de autenticação ao converter os parâmetros criptográficos para os parâmetros da chave incluindo um símbolo de autenticação e uma resposta de autenticação; e transmitir o símbolo de autenticação para o terminal configurado para produzir o vetor de autenticação. Em adição, o método inclui validar uma resposta de autenticação do terminal usando a resposta de autenticação do vetor de autenticação; e gerar uma chave mestre baseado nos parâmetros da chave.

De acordo com outro aspecto de uma incorporação da invenção, o método para autenticar inclui gerar um pedido de autenticação que especifica a identidade do usuário. O método também inclui transmitir o pedido de autenticação para um elemento de rede configurado para prover a autenticação inicial, onde o elemento de rede direciona a identidade do usuário para um registro local configurado para gerar, baseado na identidade do usuário, os parâmetros criptográficos incluindo os dados secretos randômicos, e os dados secretos gerados dos dados secretos randômicos de acordo com o algoritmo criptográfico. O elemento de rede gera um vetor de autenticação ao converter os parâmetros criptográficos para os parâmetros de chave incluindo um símbolo de autenticação e uma resposta de autenticação. Adicionalmente, o método inclui receber o símbolo de autenticação do elemento de rede; e produzir a resposta de autenticação baseada no símbolo de autenticação. Em adição, o método inclui determinar uma resposta de compilação usando a resposta de autenticação; transmitir a resposta de compilação para o elemento de rede para validação; e gerar uma chave mestre baseada nos parâmetros da chave.

De acordo com ainda outro aspecto de uma incorporação da invenção, o aparelho inclui um módulo de autenticação configurado para gerar um pedido de autenticação que especifica a identidade de usuário. O aparelho também inclui um transceptor configurado para transmitir o pedido de autenticação para o elemento de rede configurado para prover a autenticação inicial, em que o elemento de rede direciona a identidade do usuário para o registro local

configurado para gerar, baseado na identidade do usuário, os parâmetros criptográficos incluindo os dados secretos randômicos, e os dados secretos gerados ou os dados secretos randômicos de acordo com o algoritmo criptográfico. O elemento de rede gera um vetor de autenticação ao converter os parâmetros criptográficos para os parâmetros de chave incluindo um símbolo de autenticação e uma resposta de autenticação. O transceptor é configurado para receber o símbolo de autenticação do elemento de rede, e o módulo de autenticação é configurado para produzir o vetor de autenticação baseado no símbolo de autenticação, determinar uma resposta de compilação usando a resposta de autenticação, e gerar uma chave mestre baseado nos parâmetros da chave na validação da resposta de compilação pelo elemento de rede.

Outros aspectos, características, e vantagens da invenção são prontamente aparentes da descrição detalhada a seguir, simplesmente ao ilustrar as várias incorporações particulares e a implementação, incluindo o melhor modo contemplado para executar a invenção. A invenção também é capaz de incorporações outras e diferentes, e seus vários detalhes podem ser modificados de vários modos óbvios, sem partir do conceito inventivo e escopo da invenção. Adequadamente, os desenhos e a descrição serão considerados ilustrativos e não como restritivos.

Breve Descrição das Figuras

A invenção é ilustrada por meio de exemplo, e não por meio de limitação, nas figuras dos desenhos apensos, nos quais os mesmos números de referência referem-se a elementos similares e nos quais:

Figura 1 – é um diagrama de um sistema de comunicação de rádio para suportar a Arquitetura de Autenticação Genérica (GAA), de acordo com as várias incorporações da invenção;

Figura 2 – é um diagrama do procedimento de autenticação inicial exemplar utilizado no sistema da Figura 1;

Figura 3 – é um diagrama do procedimento de autenticação inicial que utiliza Segurança de Camada de Transporte anônima (TLS) com o desafio do

Protocolo de Autenticação de Estabelecimento do Desafio (CHAP), de acordo com uma incorporação da invenção;

Figura 4 – é um diagrama de um procedimento de autenticação inicial que utiliza o servidor autenticado TLS com desafio CHAP, de acordo com uma incorporação da invenção;

Figuras 5 e 6 – são diagramas dos procedimentos de autenticação inicial que suportam os parâmetros de troca de chave na carga útil, de acordo com as várias incorporações da invenção;

Figuras 7 e 8 – são diagramas dos procedimentos de autenticação inicial que suportam os parâmetros de troca de chave que são cobertos pelo hash das senhas, de acordo com as várias incorporações da invenção;

Figura 9 - é um diagrama de um procedimento de autenticação inicial que utiliza a Autenticação Celular e a Cifragem de Voz (CAVE) com os dados secretos compartilhados (SSD), de acordo com uma incorporação da invenção;

Figuras 10A e 10B – são diagramas de um procedimento de autenticação inicial que utiliza CAVE com múltiplos SSDs, de acordo com uma incorporação da invenção;

Figura 11 – é um diagrama de um procedimento de autenticação inicial que utiliza CAVE com a Autenticação de Compilação HTTP e o Protocolo de Acordo de Chave (AKA), de acordo com uma incorporação da invenção;

Figura 12 – é um diagrama de hardware que pode ser usado para implementar as várias incorporações da invenção;

Figuras 13A e 13B – são diagramas de diferentes sistemas de telefonia móveis celulares capazes de suportar as várias incorporações da invenção;

Figura 14 – é um diagrama dos componentes exemplares de uma estação móvel capaz de operar nos sistemas das Figuras 13A e 13B, de acordo com uma incorporação da invenção;

Figura 15 – é um diagrama de uma rede da empresa capaz de suportar os processos descritos aqui, de acordo com uma incorporação da

invenção.

Descrição Detalhada da Invenção

Um aparelho, método, e software para prover a autenticação inicial em um sistema de comunicação são descritos. Na descrição a seguir, com a finalidade de explicação, inúmeros detalhes específicos são agrupados para prover uma compreensão completa da invenção. Porém, é aparente ao técnico que a invenção pode ser praticada sem estes detalhes específicos ou com uma disposição equivalente. Em outros exemplos, estruturas bem conhecidas e dispositivos são apresentados na forma de um diagrama em blocos para desnecessariamente evitar obscurecer a invenção.

A Figura 1 é um diagrama de um sistema de comunicação de rádio para suportar uma Arquitetura de Autenticação Genérica (GAA), de acordo com as várias incorporações da invenção. Embora a invenção seja discutida com respeito a um sistema de comunicação de rádio usando a tecnologia de espectro de dispersão, é reconhecido pelo técnico que os vários aspectos da invenção têm aplicabilidade a qualquer tipo de rede de transporte, incluindo os sistemas sem fio e os sistemas cabeados. Também, várias incorporações da invenção são descritas com respeito a Diffie-Hellman e o Protocolo de Transferência de HiperTexto (HTTP); porém, é contemplado que outros protocolos de troca de chave equivalentes e os protocolos de comunicação que suportam a transferência da representação dos recursos podem ser usados para prática da invenção.

A autenticação inicial (i.e., auto-carregamento) da Arquitetura de Autenticação Genérica (GAA) do Projeto de Parceiros da 3ª Geração (3 GPP) é baseado no AKA (Autenticação e Protocolo de Acordo de Chave). Tipicamente, a autenticação nas redes CDMA 2000 (Acesso Múltiplo por Divisão de Código 2000) é baseada no algoritmo CAVE (Autenticação Celular e Cifragem de Voz), enquanto a autenticação no CDMA 1x EvDo (apenas Dados de Evolução) é baseada no CHAP (Protocolo de Autenticação de Estabelecimento de Desafio). Para as redes CDMA (por exemplo, CDMA 2000 1x Revisão C e revisões subseqüentes), AKA foi adotado pelo 2 Projeto de Parceiros da 3ª Geração (3GPP2).

O sistema de comunicação 100 inclui uma ou mais estações móveis (MSs) 101 configuradas para comunicar com um ou mais subsistemas do transceptor da estação base (BTSs) 103. O BTS 103, em troca, é servido por um controlador da estação base (BSC) 105 que opera com o elemento de rede capaz de prover a Função do Servidor de Autenticação Inicial (BSF) 107. O sistema 100 também incluem um Serviço de Autenticação, Autorização e Contabilidade (MN-AAA) do Nó Móvel 109 que comunica com o Nó de Serviço de Dados de Pacote (PDSN) 111.

O sistema 100, de acordo com uma incorporação, provê a funcionalidade de arquitetura de autenticação genérica 3GPP nas redes CDMA Ev-Do. Em particular, um mecanismo de autenticação inicial requer estabelecer uma secreta mestre GAA entre a MS 101 e o BSF 107. Esta secreta mestre, em uma incorporação exemplar, é fixada ao procedimento de autenticação baseado no Protocolo de Autenticação de Estabelecimento de Desafio (CHAP). De acordo com uma incorporação da invenção, tal método de acordo de chave (i.e., a troca de chave) é o Diffie-Hellman. Este método é descrito no Pedido para Comentários (RFC) 2631 da Força Tarefa de Engenharia Internet, que é aqui incorporado por referência em sua totalidade.

Por exemplo, nas redes CDMA 1xEvDo, a MS 101 é autenticada usando CHAP, que é especificado no IETF RFC 1994 (que é aqui incorporado por referência em sua totalidade). No procedimento CHAP definido, o elemento de rede, PDSN 111, envia um desafio à MS 101 que calcula uma resposta baseado no desafio recebido e em uma secreta específica do assinante que é armazenada nas MSs 101. A resposta é mandada de volta à PDSN 111 junto com a identidade do assinante. A PDSN 111 direciona a resposta recebida e a identidade junto com o desafio que a PDSN 111 enviou anteriormente para a MS 101 ao MN-AAA 109.

O MN-AAA 109 localiza a secreta específica do assinante usando a identidade e verifica se a resposta enviada pela MS 101 é igual ao valor da resposta que o MN-AAA 109 calculou. Dependendo do resultado desta verificação, o MN-AAA 109 retorna uma indicação de sucesso ou falha à PDSN 111. Se a

PDSN 111 recebe uma mensagem de sucesso, a MS 101 foi autenticada com sucesso.

É reconhecido que o procedimento de autenticação usado nas redes CDMA 1x EvDo não podem ser usados diretamente para GAA porque a secreta é conhecida apenas pela MS e o MN-AAA (análogo a Sistema do Assinante de Origem (HSS) em GAA). Conseqüentemente, a Função do Servidor de Autenticação Inicial (BSF) (quais atua como PDSN) não pode derivar a chave mestre GAA desta secreta CHAP como o MN-AAA (análogo ao Sistema do Assinante de Origem (HSS) na arquitetura GAA) não provê esta secreta.

De acordo com uma incorporação exemplar, após a chave ter sido acordada entre a MS 101 e o BSF 107, o BSF 107 fixa o procedimento de acordo de chave para a autenticação CHAP ao derivar o desafio CHAP do procedimento de acordo de chave. Várias aproximações podem ser utilizadas, de acordo com as várias incorporações da invenção, para fixar o procedimento de acordo de chave CHAP. Primeiro, o BSF 107 pode derivar o desafio da chave acordada. Segundo, o BSF 107 também deriva o desafio das mensagens de acordo de chave que foram transferidas entre o BSF 107 e a MS 101. Por exemplo, se o acordo de chave Diffie-Hellman foi executado durante o estabelecimento da Segurança da Camada de Transporte (TLS), então a mensagem Terminada pode ser usada para derivar o desafio, uma vez que a mensagem Terminada já contém o Código de Autenticação de Mensagem (MAC) das mensagens de estabelecimento TLS.

Quando a MS 101 recebe o desafio CHAP, a MS 101 valida que o desafio estava em ação derivada do procedimento de acordo de chave para impedir o ataque homem-no-meio. A MS 101 calcula uma resposta CHAP e envia de volta a resposta ao BSF 107, que valida a resposta em troca com o MN-AAA 109. Se o MN-AAA 109 indica que a resposta CHAP está correta, então o BSF 107 autenticou a MS 101, e a secreta mestre GAA tem sido estabelecida. A secreta mestre GAA pode ser a própria chave acordada, ou derivada desta chave.

Alternativamente, para estabelecer a secreta entre a MS 101 e o BSF 107, outra aproximação, de acordo com uma incorporação da invenção, utiliza

uma segurança da camada de transporte (TLS) autenticada pelo servidor, onde o BSF é autenticado usando o certificado do servidor. Neste caso, o desafio CHAP não necessita ser fixado à secreta mestre como acima, uma vez que o BSF 107 já está autenticado. Nestes casos (ambos a autenticação CHAP do protocolo ponto-a-ponto original (PPP) e os procedimentos relacionados GAA descritos), a MS 101 não responde ao desafio CHAP se o servidor (i.e., PDSN 111 ou BSF 107) não foi autenticado; caso contrário, há uma possibilidade para um ataque homem-no-meio.

A invenção, de acordo com uma incorporação, provê um mecanismo para concordar com a secreta mestre entre a MS 101 e o servidor de rede (BSF 107) que é ligado à autenticação da MS 101 para um servidor auxiliar (por exemplo, MN-AAA 109). Esta aproximação vantajosamente pode ser executada, tal que o servidor auxiliar é inalterado, enquanto utiliza os protocolos padronizados.

As aproximações convencionais não suportam a autenticação inicial da autenticação CHAP, de tal modo que a associação de segurança resultante pode ser reutilizada com múltiplos servidores, como executado no GAA. Tal técnica é o Protocolo de Autenticação de Estabelecimento de Desafio - Diffie-Hellman (DH-CHAP), que descreve um mecanismo específico para ligar A autenticação CHAP ao acordo de chave Diffie-Hellman ao adicionar novos elementos de informação às mensagens do protocolo CHAP entre o iniciador CHAP e respondedor (i.e., requerendo a modificação do CHAP).

É assumido, em uma incorporação exemplar que o procedimento de autenticação PPP CHAP original nas redes CDMA 1x EvDo têm um mecanismo para impedir o servidor sem autorização de enviar um desafio CHAP à MS 101 e receber uma resposta. Sem este mecanismo, há uma possibilidade para um ataque homem-no-meio, onde o atacante inicia as comunicações com o BSF 107 que pretende ser a MS 101. No ponto onde o atacante recebe o desafio do BSF 107, o atacante pode direcionar o desafio para a MS real 101, desse modo pretendendo ser a PDSN 111. A MS 101 calcularia a resposta e mandaria esta de volta ao atacante, que em troca enviaria esta ao BSF 107. Se este tiver êxito, o

atacante tem criado uma sessão de autenticação inicial bem sucedida e pode usar as credenciais de GAA com qualquer Função de Aplicação de Rede (NAF).

A Figura 2 – é um diagrama de um procedimento de autenticação inicial exemplar utilizado no sistema da Figura 1. Embora um equipamento do usuário (UE) seja mostrado com a finalidade de explicação, é contemplado que múltiplos UEs sejam empregados tipicamente. Os UEs também podem ser referenciados como dispositivos móveis (por exemplo, telefone móvel), estações móveis, e dispositivos de comunicações móveis. O UE também pode ser os dispositivos, tais como os assistentes digitais pessoais (PDA) com capacidade de transceptor ou os computadores pessoais com capacidade de transceptor.

No passo 201, um UE, tal como a MS 101, envia uma mensagem Compilar HTTP, Autorização GET/HTTP/1.1,: Compilar nome do usuário ="<MPI>," para o BSF 107. Em resposta, o BSF 107, como no passo 203, envia uma mensagem Não Autorizada 401. A seguir, no passo 205, o UE envia uma mensagem que inclui uma parte que é calculada usando a informação compartilhada como uma senha compartilhada (por exemplo, resposta ="<RES usada como pwd>") que retorna para o BSF 107. Depois disso, o BSF 107 submete, como no passo 207, uma mensagem OK 200 que especifica a informação de autenticação inicial.

Após o procedimento de autenticação inicial ambos, a MS 101 (por exemplo, UE) e o BSF 107 concordam no material da chave (Ks), no identificador de transação de autenticação inicial (B-TID), e na vida útil da chave. Depois do procedimento de autenticação inicial, o material da chave (Ks) pode ser usado para derivar outros materiais da chave específicos do servidor de aplicação adicional (Ks_NAFs) que podem ser usados com diferentes servidores. Ks_NAF e B-TID podem ser usados na interface Ua para autenticar mutuamente e opcionalmente o tráfego seguro entre o UE e um servidor de aplicação (i.e., Função de Aplicação de Rede (NAF)). Por meio de exemplo, a Ks é uma secreta compartilhada GAA 256b (no 3GPP GAA Ks=CK||IK). NAF pode ser um servidor de aplicação que usa GAA para autenticação do usuário.

O procedimento de autenticação inicial (i.e., interface Ub) é definida no 3GPP TS 33.220, intitulado de "Detalhes do Protocolo: Arquitetura de Autenticação Genérica (GAA); Arquitetura de Autenticação Inicial Genérica," e TS 24.109, "Interface de Autenticação Inicial (Ub) e Interface da Função de Aplicação de Rede (Ua)"; as totalidades são aqui incorporadas por referência.

A Figura 3 é um diagrama de um procedimento de autenticação inicial que utiliza TLS anônimo com desafio CHAP, de acordo com uma incorporação da invenção. Neste enredo, os pontos de referência, Ub e Zh são envolvidos, desse modo Ub provê uma autenticação mútua entre a MS 101 e o BSF 107, e o Zh suporta a troca de informação de autenticação entre o BSF 107 e o MN-AAA 109. Como discutido, tradicionalmente o BSF 107 não tem conhecimento da secreta CHAP, uma vez que apenas a MS 101 e o MN-AAA 109 possuem tal informação. PDSN 111 envia somente o desafio-CHAP ao MN-AAA 109, e o MN-AAA 109 retorna a identidade e a resposta-CHAP que são computadas usando o desafio-CHAP e a secreta CHAP. MN-AAA 109 pode verificar a resposta-CHAP e determinar o sucesso ou falha. Assim, o acordo da secreta GAA entre a MS 101 e o BSF 107 tem que ser chegado por outros meios. Em uma incorporação da invenção, a secreta GAA é estabelecida por meio de um procedimento de acordo de chave não autenticado, e a autenticação CHAP é fixada à secreta GAA ao derivar o desafio CHAP da secreta GAA, e a MS 101 verifica se a secreta GAA foi usada para derivar o desafio CHAP.

Neste exemplo, a MS 101 inclui um módulo de segurança (SEC) para executar o protocolo CHAP e um módulo GAA para suportar as funcionalidades GAA. No passo 301, a MS 101 empregos TLS anônimo com um algoritmo de troca de chave, tal como o Diffie-Hellman, para estabelecer a secreta GAA (denotada como "chave") com o BSF 107. CHAP pode ser rodada então dentro do túnel TLS. Adequadamente, no passo 303, o BSF 107 gera um desafio CHAP da chave de acordo: Desafio = KDF (chave, "desafio-chap"). A função de derivação de chave (KDF), em uma incorporação exemplar, é provida de acordo com o GAA.

A função de derivação de chave genérica, de acordo com o GAA (TS

33.220), é agora descrito. Primeiro, a cadeia S é gerada ao concatenar os parâmetros de entrada e os comprimentos associados como a seguir. O comprimento de cada parâmetro de entrada (em octetos) é codificado em uma cadeia de dois octetos. O número de octetos é expresso no parâmetro de entrada Pi como o número k na faixa [0, 65535]. Li é uma representação de dois-octetos do número k, com o bit mais significativo do primeiro octeto de Li igual ao bit mais significativo de k, e o bit menos significativo do segundo octeto de Li igual ao bit menos significativo de k.

A cadeia S é construída dos n parâmetros de entrada como a seguir:

S=FC||P0||L0||P1||L1||P2||L2||P3||L3||...||Pn||Ln

onde

FC é um único octeto usado para distinguir entre diferentes exemplos do algoritmo,

P0 é uma cadeia codificada-ASCII estática,

L0 é uma representação do comprimento P0,

P1...Pn são os n parâmetros de entrada, e

L1... Ln são as representações de dois octetos dos parâmetros de entrada correspondentes.

A chave derivada é igual a HMAC-SHA-256 calculada da cadeia S usando a chave : chave derivada = HMAC-SHA-256 (Chave, S).

A mensagem de desafio CHAP é então transmitida pelo BSF 107 dentro do túnel TLS, como no passo 305, para o módulo GAA da MS 101. No passo 307, o módulo GAA verifica o desafio CHAP recebido é gerado da chave acordada. A mensagem de desafio CHAP é então direcionada para o módulo SEC, pelo passo 309. A seguir o módulo SEC calcula a resposta CHAP, como no passo 311, e transmite a resposta para o módulo GAA (passo 313). A MS 101 envia, como no passo 315, a resposta CHAP no túnel TLS para a BSF 107.

A segui, no passo 317, o BSF envia a mensagem Pedido de acordo com o protocolo de autenticação (exemplo: Discagem de Autenticação Remota na Mensagem de Pedido de Acesso ao Serviço do Usuário (RADIUS)) para a MN-

AAA 109. RADIUS é detalhado no Pedido para Comentários (RFC) 2865 da Força Tarefa de Engenharia Internet (IETF) intitulada de "Discagem de Autenticação Remota no Serviço do Usuário (RADIUS)" (Junho de 2000), que é aqui incorporado por referência em sua totalidade. A mensagem Pedido especifica a identidade do usuário (assinante), desafio e resposta. O MN-AAA 109 verifica a resposta, pelo passo 319 e envia uma mensagem de Resposta-Acesso RADIUS (incluindo a identidade) para o BSF 107 (passo 231). Neste ponto, o BSF 107 busca as configurações de segurança do usuário GBA (GUSS), como no passo 323. GUSS são os dados de perfil do usuário especifico do GAA que são relacionados às identidades do usuário específicas NAF e as autorizações armazenadas no registro de localização de origem (HLR). GUSS inclui o elemento de informação específico do BSF 107 e as configurações de segurança do usuário específica da aplicação (USSs). Em uma incorporação exemplar, o USS define uma aplicação e o parâmetro específico do assinante; tal parâmetro inclui uma parte de autenticação e uma parte de autorização. A parte de autenticação especifica as identidades do usuário associadas com a aplicação, enquanto a parte de autorização define as permissões do usuário.

Em adição, o BSF 107 configura a chave mestre GAA (Ks=chave), gera vários parâmetros de autenticação inicial (por exemplo: o identificador de transação de autenticação inicial (B-TID), a vida útil material da chave, etc.), e armazena os dados da MN-AAA 109, pelo passo 325. A seguir, o BSF 107, como no passo 327, envia a mensagem OK no túnel TLS; a mensagem transmitida inclui, por exemplo, o B-TID e a vida útil material da chave. No passo 329, o módulo GAA configura a chave mestre GAA: Ks=chave, e armazena a chave com a B-TID recebida e a vida útil material da chave. A MS 101 então envia a mensagem para a BSF 107 para fechar o túnel TLS, no passo 331.

Com o processo acima, o sistema da Figura 1 provê a autenticação inicial GAA, tal que a MS 101 e o BSF 107 são capazes de acordar na chave, e esta chave é fixada no procedimento de autenticação CHAP. Comparado ao Diffie-Hellman (DH)-CHAP, a aproximação adotada pelo sistema da Figura 1 não requer

quaisquer trocas nas mensagens de protocolo que já são padronizadas, e pode ser implementada pelas funções apropriadas "gancho" na MS 101 e o BSF 107. Também, DH-CHAP descreve uma forma específica de conectar a autenticação CHAP à chave DH: derivar o desafio da chave acordada. A invenção, de acordo com as várias incorporações, provê outros métodos de conectar indiretamente a chave externa à autenticação interna.

A Figura 4 é um diagrama de um procedimento de autenticação inicial que suporta o servidor autenticado TLS com o desafio CHAP, de acordo com uma incorporação da invenção. Nesta incorporação alternativa, o servidor autenticado TLS é usado para estabelecer a secreta GAA entre a MS 101 e o BSF 107, onde a CHAP é empregada dentro do túnel TLS. Especificamente, no passo 401, a MS 101 estabelece o servidor autenticado no túnel TLS com o BSF 107. Como antes, a chave TLS é referenciada por "chave". A seguir, no passo 403, o BSF 107 gera o desafio CHAP -- que não necessita ser gerado do servidor de chave TLS autenticado. A mensagem de desafio CHAP é então transmitida pelo BSF 107 dentro do túnel TLS, como no passo 405, para o módulo GAA da MS 101.

O módulo GAA então direciona o desafio CHAP para o módulo SEC, no passo 407. Subseqüentemente, o módulo SEC calcula a resposta CHAP, como no passo 409, e transmite a resposta para o módulo GAA (passo 411). A MS 101 então envia a resposta CHAP no túnel TLS para o BSF 107, no passo 413.

No passo 415, o BSF 107 envia a mensagem Pedido-Acesso RADIUS para o MN-AAA 109; a mensagem Pedido especifica a identidade, desafio e resposta. O MN-AAA 109 verifica a resposta, no passo 417, e envia mensagem Resposta-Acesso RADIUS (incluindo a identidade) para a BSF 107 (passo 419). Neste ponto, o BSF 107 busca a GUSS do usuário, como no passo 421. Adicionalmente, o BSF 107 configura a chave mestre GAA (Ks=chave), gera vários parâmetros de autenticação inicial (por exemplo, o identificador de transação de autenticação inicial (B-TID), vida útil material da chave, etc.), e armazena os dados do MN-AAA 109, no passo 423.

A seguir, o BSF 107, como no passo 425, envia a mensagem OK no túnel TLS. A mensagem transmitida inclui os parâmetros de autenticação inicial, por exemplo, o B-TID e a vida útil material da chave. No passo 427, o módulo GAA configura a chave mestre GAA: Ks=chave, e armazena a chave com o B-TID recebido e a vida útil material da chave. A MS 101 então envia a mensagem para o BSF 107 para fechar o túnel TLS, no passo 429.

As Figuras 5 e 6 são diagramas dos procedimentos de autenticação inicial que suportam os parâmetros de troca de chave (ou informação de estabelecimento de chave) na carga útil, de acordo com as várias incorporações da invenção. É reconhecido que nenhuma aproximação convencional existe para prover o Diffie-Hellman protegido por senha (i.e., protocolo de troca de chave) dentro do Protocolo de Transferência de Hipertexto (HTTP). Os processos das Figuras 5 e 6 permitem o uso da Compilação HTTP e os parâmetros Diffie-Hellman juntos para prover o Diffie-Hellman protegido por senha para uso na autenticação inicial (por exemplo, como na arquitetura 3GPP2). Quer dizer, as aproximações são fornecidas para uso da Compilação HTTP com senha (i.e., secreta compartilhada), e os parâmetros do protocolo de troca de chave (por exemplo, Diffie-Hellman) na carga útil HTTP e para conectar os dois juntos. O campo de senha é configurado para ser uma função da chave secreta.

De acordo com uma incorporação da invenção, a mensagem Compilação HTTP usa a Chave de Codificação da Mensagem de Sinalização (SMEKEY) ou a chave MN-AAA como senha e a identidade móvel como nome do usuário; os parâmetros Diffie-Hellman são fornecidos na carga útil HTTP. A troca Diffie-Hellman é protegida por senha por causa do campo de qualidade de proteção "qop" na Compilação HTTP ser estabelecida para "aut-int"; conseqüentemente, a carga útil HTTP é incluída no cálculo de compilação. Na carga útil HTTP, os parâmetros Diffie-Hellman podem ser transferidos como é; alternativamente, a carga útil HTTP pode ser fornecida com proteção de senha. Esta aproximação vantajosamente permite que as especificações existentes (por exemplo, Compilação HTTP) sejam reutilizadas. Também, a aproximação remonta

a funcionalidade GAA 3GPP (por exemplo, a Autenticação da Compilação HTTP e o Protocolo de Acordo de Chave (AKA), interface Ub). Também, a aproximação, de acordo com as várias incorporações, podem ser facilmente implementadas sem modificar os protocolos padronizados existentes.

O 3GPP GAA pode ser usado sem modificação para as redes CDMA2000 atuais. É reconhecido, contudo, que a autenticação inicial do 3GPP GAA requer a adaptação para as redes que são baseadas nas edições 3GPP2 anteriores ou nas redes que não suportam AKA e conseqüentemente são adaptados apenas para CAVE. Adequadamente, a arquitetura do sistema e processo são necessários para acomodar CAVE. O sistema 100, de acordo com as várias incorporações, emprega as funções de conversão para mapear a autenticação CAVE 3GPP2 para a Compilação HTTP AKA; esta aproximação é particularmente aplicável para os sistemas CDMA2000 Rev.C.

A autenticação da Compilação HTTP permite ao cliente se autenticar com o servidor sem ter de transmitir a senha. Isto pode ser realizado ao utilizar a função "mono modo" ou calcular irreversivelmente usando a senha e o valor randômico fornecido pelo servidor como valores de entrada. A autenticação Compilação HTTP no contexto de AKA é detalhado no Pedido para Comentários (RFC) 3310 IETF(Força Tarefa de Engenharia Internet), intitulado "Autenticação de Compilação do Protocolo de Transferência de Hipertexto Usando Autenticação e o Acordo de Chave (AKA)", que é aqui incorporado por referência em sua totalidade.

Para os propósitos de ilustração, os procedimentos de autenticação inicial das Figuras 5 e 6 são descritos com relação às redes CDMA 1x e as redes CDMA 1xEvDo, respectivamente. Em uma incorporação exemplar, estes procedimentos de autenticação inicial são baseados no X.P0028, no qual a diferença de chave com X.P0028 é que a variante Compilação HTTP é usada ao invés do Protocolo de Autenticação Extensível (EAP) entre o terminal e BSF 107 (que pode ser considerado Origem (H)-AAA). Adicionalmente, o Diffie-Hellman protegido por senha A senha (i.e., a secreta compartilhada) é a Chave de Codificação da Mensagem de Sinalização (SMEKEY) (CDMA 1x) ou a Chave MN-

AAA (CDMA 1x EvDo). A chave (WKEY) LAN sem fio é gerada (WLAN) da senha (que é detalhada no X.P0028). Adicionalmente, WKEY é a chave mestre da GAA (ks). A Compilação HTTP é usada (como apresentado nas Figuras 5 e 6). A invenção, de acordo com as várias incorporações, descreve como CAVE e CHAP podem ser usados na arquitetura 3GPP GAA para autenticação inicial.

Como apresentado na Figura 5, o terminal (por exemplo, a estação móvel) inclui o módulo CAVE configurado para executar o protocolo CAVE. Adicionalmente, as funcionalidades GAA são suportadas pelo módulo GAA. No passo 501, o módulo GAA gera a mensagem Obter HTTP, que é enviada para o BSF 107; a identidade é enviada na primeira mensagem no campo "nome do usuário". Esta mensagem de pedido de autorização, em uma incorporação exemplar, inclui os campos especificados na Tabela 1, abaixo:

Tabela 1

```
credentials       = "Digest" digest-response
digest-response   = 1#( username | realm | nonce | digest-
uri
                    | response | [ algorithm ] | [cnonce] |
                    [opaque] | [message-qop] |
                    [nonce-count] | [auth-param] )
username          = "username" "=" username-value
username-value    = quoted-string
digest-uri        = "uri" "=" digest-uri-value
digest-uri-value  = request-uri ; As specified by
HTTP/1.1
message-qop       = "qop" "=" qop-value
cnonce            = "cnonce" "=" cnonce-value
cnonce-value      = nonce-value
nonce-count       = "nc" "=" nc-value
nc-value          = 8LHEX
response          = "response" "=" request-digest
request-digest    = <"> 32LHEX <">
LHEX              = "0" | "1" | "2" | "3" |
                    "4" | "5" | "6" | "7" |
                    "8" | "9" | "a" | "b" |
                    "c" | "d" | "e" | "f"
```

Algumas das diretivas na Tabela 1 são definidas na Tabela 2:

Tabela 2

Diretiva	Descrição
resposta	Uma cadeia e 32 hex bits para prover a prova de que o usuário conhece a senha
nomeusuário	O nome do usuário no relm especificado
compilação-uri	O URI do Pedido-URI da Linha-Pedido
qop	Indica o tipo de "proteção de qualidade" aplicado a mensagem.
cnonce	Este é especificado se a diretiva qop for enviada. O valor cnonce é um valor da cadeia cotado opaco fornecido pelo cliente e usado pelo cliente e o servidor para evitar os ataques de texto plano escolhido, para prover uma autenticação mútua, e para prover alguma proteção de integridade da mensagem.
nonce-count	Este é especificado se a diretiva qop for enviada. O valor-nc é uma contagem hexadecimal do número de pedidos (incluindo o pedido atual) que o cliente tem enviado com o valor nonce neste pedido. Por exemplo, o primeiro pedido enviado em resposta a um dado valor nonce, o cliente envia "nc=00000001". O propósito desta diretiva é permitir ao servidor detectar os retardos dos pedidos ao manter a sua própria cópia

	desta conta - se o mesmo valor-nc for visto duas vezes, então o pedido é uma replay.
aut-param	Esta diretiva permite extensões futuras. Qualquer diretiva não reconhecida é ignorada

O BSF 107 então gera o RAND, como no passo 503, e responde com a mensagem Não Autorizado 401 (passo 505). Inicialmente, o cabeçalho sem autorização é enviado para o BSF 107, e então, a mensagem 401 é utilizada como resposta. Como apresentado, o RAND é enviado no campo "nonce" (similar à Compilação HTTP AKA). RAND e Desafio-CHAP podem também ser enviados na carga útil HTTP. Ao receber o RAND, o módulo GAA direciona este para o módulo CAVE, como no passo 507.

Por meio de exemplo, o Cabeçalho Autenticar Resposta é provido na Tabela 3; as diretivas associadas são definidas na Tabela 4.

Tabela 3

```
challenge        = "Digest" digest-challenge
digest-challenge = 1#( realm | [ domain ] | nonce |
                   [ opaque ] |[ stale ] | [ algorithm ] |
                   [ qop-options ] | [auth-param] )
domain           = "domain" "=" <"> URI ( 1*SP URI )
```

```
<">
    URI             = absoluteURI | abs_path
    nonce           = "nonce" "=" nonce-value
    nonce-value     = quoted-string
    opaque          = "opaque" "=" quoted-string
    stale           = "stale" "=" ( "true" | "false" )
    algorithm       = "algorithm" "=" ( "MD5" | "MD5-sess"

                      token )
    qop-options     = "qop" "=" <"> 1#qop-value <">
    qop-value       = "auth" | "auth-int" | token
```

Tabela 4

Diretiva	Descrição
realm	Uma cadeia a ser exibida para os usuários de forma que eles saibam qual o nome do usuário e senha para uso. Esta cadeia pode incluir o nome do servidor que executa a autenticação e os usuários que podem ter acesso.
domain	Uma lista separada em espaço cotada das URIs que definem o espaço de proteção. O cliente pode usar esta lista para determinar o grupo de URIs para o qual a mesma informação de autenticação pode ser enviada: qualquer URI que a URI nesta lista como um prefixo (após ambos terem sido feitos absolutos) podem ser assumidos para estarem no mesmo espaço de proteção. Se esta diretiva for omitida ou o seu valor estiver vazio, o cliente assume que o espaço de proteção inclui todas as URIs no servidor de resposta.
nonce	Cadeia de dados especificada do servidor que pode ser unicamente gerada toda vez que a resposta 401 é feita.

opaque	Uma cadeia de dados, especificada pelo servidor, que pode ser retornada pelo cliente não alterado no cabeçalho Autorização dos pedidos subseqüentes com as URIs no mesmo espaço de proteção.
stale	Um indicador, indicando que o pedido anterior do cliente foi rejeitado porque o valor nonce foi passado. Se stale for VERDADEIRO (caso insensível), o cliente pode re-entrar com o pedido com a nova resposta codificada, sem re-iniciar o usuário para o novo nome do usuário e senha. O servidor deveria apenas configurar stale para VERDADEIRO se este recebe um pedido para que o nonce seja inválido, mas com a compilação válida para este nonce (indicando que o cliente sabe o nome do usuário/senha correto). Se stale for FALSO, ou qualquer outro diferente de VERDADEIRO, ou a diretiva stale não estiver presente, o nome do usuário e/ou senha são inválidos, e novos valores são obtidos.
algoritmo	Uma cadeia indicando um par de algoritmos usado para produzir a compilação e a soma de verificação.

No passo 509, o módulo CAVE envia a Resposta de Autenticação (referenciada como "AUT") e SMEKEY para o módulo GAA. O módulo GAA então, como no passo 511, configura a senha da estação móvel (MS_PW):MS_PW=SMEKEY H1' (MS_PW).gx mod p, onde x é o número secreto randômico gerado pelo UE.

A seguir, o módulo GAA envia no passo 513, uma mensagem HTTP com a carga útil que inclui os parâmetros Diffie-Hellman do cliente para BSF 107. Com CAVE, a carga útil HTTP também contêm o AUT. A carga útil é protegida pela Compilação HTTP porque qop=aut-int; também a carga útil HTTP é incluída no cálculo Compilação HTTP do campo "resposta". Os parâmetros Diffie-Hellman podem ser enviados como estão ou podem ser protegidos. No passo 515, o BSF

107 transmite a mensagem Pedido de Autenticação ("AUTPED") (incluindo AUT e RAND) para o registro de localização de origem/centro de autenticação (HLR/AC), que verifica o RAND/AUT e gera a SMEKEY (passo 517). A SMEKEY é enviada para o BSF 107, no passo 519.

O BSF 107, como no passo 521, configura a senha da estação base BS_PW=SMEKEY H1' (BS_PW).g^y mod p, onde y é o número secreto randômico gerado pelo UE. Subseqüentemente, o BSF 107 gera a chave mestre GAA (Ks) da BS_PW 9 (de maneira similar a esta da WKEY).

A seguir, o BSF 107 então envia a mensagem OK HTTP 200 para o terminal, no passo 525. Os parâmetros Diffie-Hellman do servidor são enviados na carga útil HTTP, protegidos pela Compilação HTTP porque qop=aut-int (i.e., a carga útil HTTP é também incluída no cálculo Compilação HTTP do campo "respauth"). De acordo com uma incorporação, o cabeçalho de informação de autenticação é fornecido na mensagem do passo 525 para indicar uma autenticação bem sucedida, na Tabela 5 abaixo:

Tabela 5

AuthenticationInfo	= "Authentication-Info" ":" auth-info
auth-info	= 1#(nextnonce | [message-qop] | [response-auth] | [cnonce] | [nonce-count])
nextnonce	= "nextnonce" "=" nonce-value
response-auth	= "rspauth" "=" response-digest
response-digest	= <"> *LHEX <">

A diretiva mensagem-qop indica as opções da "qualidade de proteção" aplicada, desse modo o valor "aut" indica autenticação, e o valor "aut-int" indica autenticação com proteção de integridade.

No passo 527, o módulo GAA gera a chave mestre GAA, Ks, da PS_PW (de maneira similar como os procedimentos para WKEY).

No caso de autenticação de inicial no CDMA 1xEvDo, CHAP é utilizado (como apresentado na Figura 6). Neste cenário, o módulo GAA emite a mensagem Obter HTTP, que é enviada para o BSF 107; a identidade é enviada na

primeira mensagem no campo "nome do usuário". O BSF 107 responde, como no passo 603, com a mensagem 401; neste caso CHAP, o desafio-CHAP é enviado no "nonce" (i.e., é apenas randômico, como no padrão Compilação HTTP). A seguir, o desafio CHAP e resposta é trocado entre o módulo GAA e o módulo CHAP (passos 605 e 607). No passo 609, o módulo GAA configura os parâmetros a seguir: chave BS_PW=MN_AAA; H1' (BS_PW).g^x mod p, onde x é o número secreto randômico gerado pelo UE.

Neste ponto, o terminal, usando o módulo GAA, gera e transmite a mensagem Autorização para o BSF 107 (passo 611); a mensagem especifica o seguinte: Compilação nonce='<RAND>", resposta="<MS_PW usado como senha>", qop=aut-int,.....A carga útil HTTP inclui H1' (MS_PWD).g^x mod p. No passo 613, o BSF 107 configura a senha da estação base (BS_PW): BS_PW=MN-AAA chave; H1' (BS_PW).g^y mod p, onde y é o número secreto randômico gerado pelo UE. Também, o BSF 107 gera a chave mestre GAA, Ks, da BS_PW.

Depois disso, o BSF 107 transmite uma mensagem OK 200 que especifica o H1'(MS_PWD) *g^y mod p, B-TID e a vida útil da chave para o módulo GAA (passo 617). No passo 619, o módulo GAA gera a chave mestre GAA, Ks, da MS_PWD. A WKEY é fixada na secreta mestre GAA (Ks).

As Figuras 7 e 8 são diagramas dos procedimentos de autenticação inicial que suportam os parâmetros de troca de chave que são cobertos pelo hash das senhas, de acordo com as várias incorporações da invenção. O procedimento de autenticação inicial da Figura 7 similar a Figura 5; quer dizer, os passos 701-711 correspondem em grande parte aos passos 501-511. Similarmente, o procedimento da Figura 8 segue o da Figura 6, desse modo os passos 801-809 rastreiam os passos 601-609. Porém, nos cenários das Figuras 7 e 8, os parâmetros de Diffie-Hellman do cliente são cobertos pelo hash da senha (i.e., SMEKEY, ou chave MN-AAA) que é enviado no campo "cnonce". O hash pode ser gerado baseado nos cálculos da Compilação HTTP padrão.

Com respeito ao procedimento da Figura 7, no passo 713 a mensagem que é transmitida do módulo GAA para o BSF 107 inclui cnonce ="

<H1'(MS_PWD) *g^xmod p>". Os passos 715-723 seguem os passos 517-523 da Figura 5. No cenário presente, no passo 725, o BSF 107 transmite uma mensagem 200 OK que especifica nextnonce =" <H1 ' (BS_PWD) g^y mod p>". Quer dizer, os parâmetros Diffie-Hellman do servidor são cobertos pelo hash da senha (i.e., SMEKEY, ou MN-AAA-CHAVE) que é enviado no campo "nextnonce". Depois disso, o módulo GAA gera a chave mestre GAA, Ks, do PS_PW (passo 727).

Como para o procedimento de autenticação inicial da Figura 8, a mensagem HTTP do passo 811 inclui <H1' (MS_PWD)*g^x mod p> no campo cnonce. Os passos 813-819 geralmente rastreiam com os passos 613-619, com a exceção de que a mensagem OK 200 do passo 817 especifica nextnonce =" <H1 ' (BS_PWD)*g^ymod p>."

A Figura 9 é um diagrama do procedimento de autenticação inicial que utiliza CAVE com os dados secretos compartilhados (SSD), de acordo com uma incorporação da invenção. O UE (pelo módulo GAA) provê uma função de geração SSD e uma função de autenticação, desse modo a aplicação GAA requer acesso a SSD_A_NEW e SSD_B_NEW. No passo 901, o procedimento de autenticação inicial é iniciado entre o UE e o BSF 107 com submissão pelo UE do pedido OBTER para o BSF 107. Este pedido OBTER inclui a identidade do usuário que o BSF 107 direciona para o HLR/AC (passo 903). O HLR/AC gera um SSD randômico ("RANDSSD") e deriva SSD_A e SSD_B usando o algoritmo CAVE (passo 905); esta informação é direcionada ao BSF 107, no passo 907. O SSD, em uma incorporação exemplar, é um dado secreto compartilhado de 128-bits e inclui uma chave SSD_A de 64 bits usada para autenticação e uma chave SSD-B de 64 bits usada junto com outros parâmetros para gerar a máscara de cifragem e o código longo privado. RANDSSD é um desafio randômico de 56 bits gerado no HLR/AC. O SSD é uma concatenação da chave SSD_A e a chave SSD_B.

No passo 909, o BSF 107 gera um RAND_CHALLENGE e um vetor autenticação pseudo AKA. Por via de exemplo, o RAND_CHALLENGE é um desafio randômico de 32 bits. Para gerar o vetor de autenticação AKA, funções de conversão são executadas, conforme uma incorporação da invenção, para

converter (ou mapear) os parâmetros CAVE gerados no passo 905 para os parâmetros AKA. As funções de conversão são usadas para gerar um vetor de autenticação pseudo AKA de um ou dois grupos de parâmetros CAVE, incluindo RANDSSD, SSD_A, SSD_B, e AUT_ SIGNATURE.

Como mostrado na Figura 9, as funções de conversão provêem para a geração de uma chave, onde SSD_A e SSD_B são concatenados como a seguir: chave = SSD__A || SSD_B || SSD_A II SSD_B. Logo, a chave, os parâmetros CAVE, e a função de derivação de chave (KDF) 3GPP GAA são usados para formar o vetor de autenticação pseudo AKA (que inclui o RAND, um símbolo de autenticação (AUTN), uma chave de cifragem (CK), uma chave de integridade (IK), e uma resposta de autenticação (RES)). Por via de exemplo, o vetor de autenticação pseudo AKA pode ser gerado como a seguir:

RAND = RANDSSD || RAND_CHALLENGE||ZZRAND

AUTN = KDF (chave, 3gpp2-cave-autn " || RAND), truncado a 128 bits

CK = KDF (chave, 3gpp2-cave-ck " || RAND), truncado a 128 bits

IK = KDF(chave, 3gpp2-cave-ik " || RAND), truncado a 128 bits

RES = KDF(chave, 3gpp2-cave-res " || AUT_ASSINATURA), truncado para 128, onde ZZRAND são os parâmetros avaliados em zero de 40 bits longo (para estender o RAND a 128 bits).

No passo 911, o BSF 107 envia para uma mensagem HTTP 401 para o UE (por exemplo, MS 101); a mensagem especifica o RAND e AUTN. Após a recepção desta mensagem, a MS 101 extrai, como no passo 913, o RANDSSD e RAND_CHALLENGE do RAND recebido. A MS 101 gera então a chave SSD_A_NEW e a chave SSDJBJNEW usando o RANDSSD.

O módulo GAA, como no passo 915, envia o RANDSSD e o ESN ao módulo SEC, que reconhece com a mensagem OK (no passo 917). O ESN é, por exemplo, o Número de Autenticação Celular Eletrônico do terminal (ou estação móvel (MS)) de 32 bits.

No passo 919, o SSD_A_NEW é usado para gerar a

AUT_SIGNATURE e o vetor de autenticação pseudo AKA. O módulo GAA envia a mensagem AUTH_SIGNATURE ao módulo de SEC, como no passo 921. O módulo SEC responde, no passo 923, com uma resposta apropriada (AUTH_SIGNATURE). A seguir, no passo 925, o módulo GAA gera o vetor de autenticação pseudo AKA, determina se o AUTN recebido é igual ao gerado, e calcula a resposta da Compilação usando RES.

No passo 927, o UE envia uma mensagem HTTP, incluindo RES como senha, para o BSF 107. Em troca, o BSF 107 valida, como no passo 929, a resposta da Compilação usando o RES, e gera a chave mestre GAA (Ks=CK||IK), B-TID, vida útil da chave, etc.; tais dados são armazenados. Logo, o BSF 107 busca, como no passo 931, o GUSS; alternativamente, estas informações podem ser entregues no passo 907.

O BSF 107 envia uma mensagem OK 200 que especifica o B-TID e vida útil da chave, para a MS 101, no passo 933. Neste momento, a MS 101 gera a chave mestre GAA, Ks que é armazenada junto com o B-TID recebido e vida útil da chave (passo 935).

As Figuras 10A e 10B são diagramas do procedimento de autenticação inicial que utiliza CAVE com múltiplos SSDs, de acordo com uma incorporação da invenção. Como com o procedimento da Figura 9, o módulo GAA mostrado aqui inclui as funções de geração SSD e de autenticação; também, a aplicação GAA requer acesso a SSD_A_NEW e SSD_B_NEW. Neste exemplo, como mostrado nas Figuras 10A e 10B, para uma sucessão de mensagem, dois SSDs e dois RANDSSDs podem ser usados para obter, por exemplo, uma secreta compartilhada (Ks) da Arquitetura de Autenticação Inicial Genérica (GBA) de 256 bits. No passo 1001, o UE envia um pedido OBTER ao BSF 107 para iniciar o procedimento de autenticação inicial. A identidade do usuário do pedido OBTER é direcionada ao HLR/AC, no passo 1003. Logo, o HLR/AC gera um RANDSSD e deriva o primeiro grupo do SSD_A e SSD_B (referenciado como "SSD_A1 e SSD_B1"), no passo 1005. O RANDSSD (por exemplo, "RANDSSD1") junto com SSD_A1 e SSD_B1 é transmitido ao BSF 107, no passo 1007.

Nos passos 1009 e 1011, a identidade do usuário é direcionada novamente ao HLR/AC, e o HLR/AC gera outro grupo de parâmetros CAVE: RANDSSD2, SSD_A2, e SSD_B2. Estes parâmetros são direcionados subseqüentemente ao BSF 107, como no passo 1013.

No passo 1015, o BSF 107 gera um RAND_CHALLENGE e um vetor de autenticação pseudo AKA. Como com o procedimento da Figura 9, funções de conversão são usadas para gerar o vetor de autenticação pseudo AKA dos parâmetros CAVE (por exemplo, RANDSSD1, SSD_A1, SSD_B1, AUTH_SIGNATURE1, RANDSSD2, SSD_A2, SSD JB2, e AUTH_SIGNATURE2).

Uma chave é gerada como a seguir: chave = SSD_A1 || SSD_B1 || SSD__A2 || SSD_B2. Logo, a chave, os parâmetros CAVE, e a função de derivação de chave (KDF) GAA são usados para formar o vetor de autenticação pseudo AKA. O vetor inclui o RAND, AUTN, CK, IK, e RES, e, por meio de exemplo, é determinado como a seguir:

RAND = RANDSSD1 || RANDSSD2 || ZZRAND.

AUTN = KDF (chave, "3gpp2-cave-autn"||RAND), truncado a 128 bits

CK = KDF (chave, "3gpp2-cave-ck"|| RAND), truncado a 128 bits

IK = KDF(chave, "3gpp2-cave-ik "|| RAND), truncado a 128 bits

RES = KDF(chave, "3gpp2-cave-res" ||AUTH_SIGNATURE1|| AUTH_SIGNATURE2), truncado a 128 bits

dados específicos do servidor = RAND_CHALLENGE1 || RAND_CHALLENGE2,

onde ZZRAND são dados avaliados em zero de 16 bits longos (usado para preencher RAND em 128 bits).

No passo 1017, o BSF 107 envia uma mensagem HTTP 401 que especifica o RAND, AUTN e os dados específicos do servidor para o módulo GAA. Após a recepção desta mensagem, o módulo GAA extrai o RANDSSD1, RANDSSD2, RAND_CHALLENGE1 e RAND_CHALLENGE2 do RAND recebido e os dados específicos do servidor (passo 1019). O módulo GAA gera o SSD_A_NEW1 e SSD_B_NEW1 então como também AUTH_SIGNATURE1, no

passo 1021.

Logo, o módulo GAA direciona uma mensagem de geração SSD (SSD_generation) que inclui o RANDSSD1 e o ESN para o módulo SEC. Em resposta, o módulo SEC reconhece com uma mensagem OK (passos 1023 e 1025).

Adicionalmente, o módulo GAA direciona uma mensagem AUTH_SIGNATURE ao módulo SEC (passo 1027); a mensagem AUTH_SIGNATURE especifica RAND_CHALLENGE1 e o SSD_B_NEW1.

No passo 1029, o módulo SEC proporciona para o módulo GAA AUTH_SIGNATURE1. Neste momento, o módulo GAA armazena, como no passo 1031, o SSD_A_NEW1, o SSD_B_NEW1, e AUTH_SIGNATURE 1.

Os passos 1033 - 1043 correspondem essencialmente aos passos 1021 - 1031, mas para o segundo grupo de parâmetros: SSD_A_NEW2, SSD_B_NEW2, e AUTH_SIGNATURE2.

No passo 1045, o módulo GAA gera o vetor de autenticação pseudo AKA, e determina se o AUTN recebido é igual ao gerado. O módulo GAA também produz uma resposta de Compilação baseado no RES.

Logo, o UE envia, como no passo 1047, uma mensagem HTTP incluindo RES como a senha para o BSF 107. O BSF 107 valida, como no passo 1049, a resposta de Compilação usando o RES, e gera a chave mestre GAA (Ks=CK||IK), B-TID, vida útil da chave, etc.; o BSF 107 também armazena os dados. No passo 1051, o BSF 107 busca o GUSS (que pode ser entregue alternativamente no passo 1007).

O BSF 107 envia então, como no passo 1053, uma mensagem OK 200 que especifica o B-TID e vida útil da chave para o UE. Depois disso, o UE gera a chave mestre GAA, Ks que é armazenada junto com o B-TID recebido e vida útil da chave (passo 1055).

A Figura 11 é um diagrama de um procedimento de autenticação inicial utilizando CAVE com Compilação HTTP AKA, de acordo com uma incorporação da invenção. A sucessão de mensagem, neste procedimento de

autenticação inicial, utiliza dois SSDs e dois RANDSSDs. A identidade do usuário é transmitida, como no passo 1101, para o BSF 107 e para o HLR/AC (passo 1103). No passo 1105, o HLR/AC transmite SSDI, SSD2, RANDSSI, RANDSS2, e as configurações de segurança do usuário GBA (GUSS) para o BSF 107. Em resposta, o BSF 107 gera dois RAND_CHALLENGES (i.e., RAND_CHALLENGE1 e RAND_CHALLENGE2), no passo 1107. No passo 1109, são entregues o RANDSSD1, RANDSSD2, RAND_CHALLENGE1 e RAND_CHALLENGE2 ao UE.

O UE calcula o seguinte então: SSD1, SSD2, AUTH_SIGNATURE1, e AUTH_SIGNATURE2 (passo 1111). SSDI é computado de RANDSSD1, A-Key e ESN; similarmente, SSD2 é determinado de RANDSSD2, A-Key e ESN. AUTH_SIGNATURE1 é calculado de SSD_A1 e RAND_CHALLENGEI; e AUTH_SIGNATURE2 é calculado de SSD_A2 e RAND_CHALLENGE2. No passo 1113, o UE envia a concatenação de AUTH_SIGNATURE1 e AUTH_SIGNATURE2 como senha para o BSF 107.

A chave é então gerada para o BSF 107, como no passo 1115, concatenando CK_UMTSIIIK_UMTS(=SSD_A1||SSD_A2||SSD_B1||SSD_B2). Também, o BSF 107 envia uma mensagem OK 200 que especifica o B-TBD e a vida útil da chave para o UE (passo 1117). No passo 1119, o UE determina a Ks.

O técnico reconheceria que os processos para suportar a autenticação inicial podem ser implementados em software, hardware (por exemplo, processador geral, chip Processador de Sinal Digital (DSP), um Circuito Integrado de Aplicação Específica (ASIC), uma Série de Portas Programáveis de Campo (FPGAs), etc.), firmware, ou uma combinação destes. Tal hardware exemplar para executar as funções descritas é detalhado abaixo com relação à Figura 12.

A Figura 12 ilustra um hardware exemplar no qual podem ser implementadas várias incorporações da invenção. Um sistema de computação 1200 inclui um barramento 1201 ou outro mecanismo de comunicação para comunicar a informação e um processador 1203 acoplado ao barramento 1201 para processar a informação. O sistema de computação 1200 também inclui uma

memória principal 1205, tal como uma memória de acesso randômico (RAM) ou outro dispositivo de armazenamento dinâmico, acoplado ao barramento 1201 para armazenar a informação e as instruções a serem executadas pelo processador 1203. Memória principal 1205 também pode ser usada para armazenar variáveis temporárias ou outras informações intermediárias durante execução das instruções pelo processador 1203. O sistema de computação 1200 pode incluir uma memória de apenas leitura (ROM) 1207 ou outro dispositivo de armazenamento estático acoplado ao barramento 1201 para armazenar as informações estáticas e as instruções para o processador 1203. Um dispositivo de armazenamento 1209, tal como um disco magnético ou disco óptico, é acoplado ao barramento 1201 para persistentemente armazenar as informações e as instruções.

O sistema de computação 1200 pode ser acoplado pelo barramento 1201 ao visor 1211, tal como um visor de cristal líquido, ou um visor de matriz ativa, para exibir a informação para o usuário. Um dispositivo de entrada 1213, tal como um teclado que inclui teclas alfanuméricas e outras, pode ser acoplado ao barramento 1201 para comunicar as informações e as seleções de comando ao processador 1203. O dispositivo de entrada 1213 pode incluir um controle de cursor, tal como um mouse, um trackball, ou a tecla de direção do cursor, para comunicar as informações de direção e as seleções de comando ao processador 1203 e para controlar o movimento do cursor no visor 1211.

De acordo com as várias incorporações da invenção, os processos descritos aqui podem ser providos pelo sistema de computação 1200 em resposta ao processador 1203 que executa um arranjo de instruções contido na memória principal 1205. Tais instruções podem ser lidas da memória principal 1205 de outro médio legível de computador, tal como o dispositivo de armazenagem 1209. A execução do arranjo das instruções contidas na memória principal 1205 ocasiona ao processador 1203 a executar os passos do processo descritos aqui. Também, um ou mais processadores podem ser empregados em um arranjo de multi-processos para executar as instruções contidas na memória principal 1205. Nas

incorporações alternativas, um circuito cabeado pode ser usado no lugar de ou em combinação com as instruções de software para implementar a incorporação da invenção. Em outro exemplo, um hardware de re-configurável tal como Séries de Porta Programáveis de Campo (FPGAs) pode ser usado, no qual a funcionalidade e a topologia de conexão de suas portas lógicas são customizadas no tempo de execução, tipicamente ao programar as tabelas de busca da memória. Assim, as incorporações da invenção não são limitadas a qualquer combinação específica de circuito de hardware e software.

O sistema de computação 1200 também inclui pelo menos uma interface de comunicação 1215 acoplada ao barramento 1201. A interface de comunicação 1215 provê uma comunicação de dados de modo dual acoplando a um enlace de rede (não mostrado). A interface de comunicação 1215 envia e recebe os sinais elétricos, eletromagnéticos, ou ópticos que carregam os fluxos de dados digitais representando os vários tipos de informação. Mais adiante, a interface de comunicação 1215 pode incluir dispositivos de interface periféricos, tal como uma interface Barramento Serial Universal (USB), uma interface PCMCIA (Associação Internacional do Cartão de Memória de Computador Pessoal), etc.

O processador 1203 pode executar o código transmitido enquanto sendo recebidos e/ou armazenar o código no dispositivo de armazenagem 1209, ou em outro dispositivo de armazenagem não-volátil para execução posterior. Desta maneira, o sistema de computação 1200 pode obter o código de aplicação na forma de uma onda portadora.

O termo "meio legível de computador" como usado aqui refere a qualquer meio que participa ao prover as instruções ao processador 1203 para execução. Tal médio pode ter muitas formas, incluindo mas não limitado a uma mídia não-volátil, mídia volátil, e mídia de transmissão. Por exemplo, mídia não-voláteis inclui discos ópticos ou magnéticos, tal como o dispositivo de armazenagem 1209. As mídias voláteis incluem a memória dinâmica, tal como a memória principal 1205. A mídia de transmissão inclui os cabos coaxiais, fio de cobre e fibra ótica, incluindo os cabos que incluem o barramento 1201. A mídia de

transmissão também podem ter a forma de ondas acústicas, ópticas, ou eletromagnéticas, como estas geradas durante as comunicações de dados de rádio freqüência (RF) e infravermelho (IR). Formas comuns de mídia legível de computador incluem, por exemplo, um disquete, um disco flexível, disco rígido, fita magnética, qualquer outro meio magnético, um CD - ROM, CDRW, DVD, qualquer outro meio óptico, cartões punch, fita de papel, folhas de marca óptica, qualquer outro meio físico com padrões de orifícios ou outro índice opticamente reconhecível, a RAM, PROM, e EPROM, um FLASH-EPROM, qualquer outro chip de memória ou cartucho, uma onda portadora, ou qualquer outro meio dos quais um computador pode ler.

Várias formas de mídia legível de computador podem ser envolvidas para prover instruções a um processador para execução. Por exemplo, as instruções podem ser executadas ao menos parte da invenção podem ser afetadas inicialmente em um disco magnético de um computador remoto. Em tal cenário, o computador remoto carrega as instruções na memória principal e envia as instruções na linha de telefone usando modem. O modem de um sistema local recebe os dados na linha de telefone e usa um transmissor infravermelho para converter os dados em um sinal infravermelho e transmitir o sinal infravermelho a um dispositivo de computação portátil, tal como um assistente digital pessoal (PDA) ou um laptop. Um detector infravermelho no dispositivo de computação portátil recebe a informação e as instruções pelo sinal infravermelho e aloca os dados em um barramento. O barramento carrega os dados na memória principal, da qual o processador recupera e executa as instruções. As instruções recebidas pela memória principal podem opcionalmente ser armazenadas em um dispositivo de armazenamento antes ou depois da execução pelo processador.

As Figuras 13A e 13B são diagramas de diferentes sistemas de telefonia móvel celular capazes de suportar as várias incorporações da invenção. As Figuras 13A e 13B apresentam sistemas de telefonia móvel celular exemplares, cada qual com uma estação móvel (por exemplo, aparelho celular) e uma estação base que tem um transceptor instalado (como parte de um Processador de Sinal

Digital (DSP)), hardware, software, um circuito integrado, e/ou um dispositivo semicondutor na estação base e estação móvel). Por meio de exemplo, a rede de rádio suporta os serviços da Segunda e Terceira Geração (2G e 3G) como definido pela União de Telecomunicações Internacional (ITU) para Telecomunicações 2000 Móveis Internacionais (MT-2000). Com a finalidade de explicação, a portadora e a capacidade de seleção de canal da rede de rádio é explicado com respeito a arquitetura cdma2000. Como a versão da terceira-geração do IS-95, cdma2000 está sendo padronizado no Projeto 2 de Parceiros da 3ª Geração (3GPP2).

A rede de rádio 1300 inclui uma estação móvel 1301 (por exemplo, aparelhos celulares, terminais, estações, unidades, dispositivos, ou qualquer tipo de interface para o usuário (como " circuito usável ", etc.)) em comunicação com o Subsistema da Estação Base (BSS) 1303. De acordo com uma incorporação da invenção, a rede de rádio suporta os serviços da Terceira Geração (3G) como definido pela União de Telecomunicações Internacional (ITU) para Telecomunicações 2000 Móveis Internacionais (MT-2000).

Neste exemplo, o BSS 1303 inclui uma Estação Base Transceptora (BTS) 1305 e um Controlador da Estação Base (BSC) 1307. Embora um único BTS seja mostrado, é reconhecido que múltiplos BTSs são tipicamente conectados ao BSC por, por exemplo, enlaces ponto-a-ponto. Cada BSS 1303 é acoplado a um Nó de Serviço de Dados de Pacote (PDSN) 1309 por uma entidade de controle de transmissão, ou uma Função de Controle de Pacote (PCF) 1311. Uma vez que o PDSN 1309 serve como um portal para redes externas, por exemplo, a Internet 1313 ou outra rede privada do consumidor 1315, o PDSN 1309 pode incluir um sistema de Acesso, Autorização e Contabilidade (AAA) 1317 para determinar a identidade e os privilégios do usuário e localizar as atividades de cada usuário. A rede 1315 inclui um Sistema de Gerenciamento de Rede (NMS) 1331 acoplado a uma ou mais bases de dados 1333 por um Agente de Origem (HA) 1335 seguro pelo Origem AAA 1337.

Embora um único BSS 1303 seja mostrado, é reconhecido que múltiplos BSSs 1303 são tipicamente conectados a um Centro de Comutação

Móvel (MSC) 1319. O MSC 1319 provê a conectividade à rede de telefonia comutada por circuito, tal como a Rede de Telefonia Comutada Pública (PSTN) 1321. Semelhantemente, também é reconhecido que o MSC 1319 pode ser conectado a outros MSCs 1319 na mesma rede 1300 e/ou em outras redes de rádio. O MSC 1319 geralmente é disposto em uma base de dados do Registro de Localização Visitante (VLR) 1323 que segura a informação temporária sobre os assinantes ativos para este MSC 1319. Os dados dentro do banco de dados VLR 1323 é a uma extensão grande de uma cópia do banco de dados do Registro de Localização de Origem (HLR) 1325 que armazena a informação de assinatura do assinante detalhada. Em algumas implementações, o HLR 1325 e o VLR 1323 são o mesmo banco de dados físico; porém, o HLR 1325 pode ser localizado em um local remoto acessado, por exemplo, pela rede Número 7 do Sistema de Sinalização (SS7). Um Centro de Autenticação (AuC) 1327 contendo os dados de autenticação específicos do assinante, tal como uma chave de autenticação secreta, é associado com o HLR 1325 para autenticar os usuários. Além disso, o MSC 1319 é conectado a um Centro de Serviço de Mensagem Curta (SMSC) 1329 que armazena e direciona as mensagens curtas para e da rede de rádio 1300.

Durante uma operação típica do sistema telefonia celular, as BTSs 1305 recebem e demodula os grupos de sinais de enlace-reverso de grupos de unidades móveis 1301 conduzindo as chamadas telefônicas ou outras comunicações. Cada sinal de enlace-reverso recebido por uma determinada BTS 1305 é processado dentro desta estação. Os dados resultantes são direcionados ao BSC 1307. O BSC 1307 provê a alocação de recurso de chamada e a funcionalidade de gerenciamento de mobilidade incluindo a orquestração de transferências entre as BTSs 1305. O BSC 1307 também direciona os dados recebidos para o MSC 1319, que provê um direcionamento adicional e/ou comutação para a interface com o PSTN 1321. O MSC 1319 também é responsável pela configuração da chamada, terminação da chamada, e o gerenciamento da transferência inter-MSC e serviços adicionais, e colecionar, carregar e tarifar a informação. Similarmente, a rede de rádio 1300 envia as

mensagens de enlace-direto. A PSTN 1321 conecta com o MSC 1319. O MSC 1319 adicionalmente conecta com o BSC 1307, que comunica com as BTSs 1305, que modula e transmite grupo de sinais de enlace-direto das unidades móveis 1301.

Como mostrado na Figura 13B, os dois elementos de chave da infra-estrutura do Serviço de Rádio de Pacote Geral (GPRS) 1350 é o Nó de Suporte de Serviço GPRS (SGSN) 1332 e o Nó de Suporte GPRS de Porta de Comunicação (GGSN) 1334. Além disso, a infra-estrutura GPRS inclui uma Unidade de Controle de Pacote PCU (1336) e uma Função de Portal de Carga (CGF) 1338 acoplada ao Sistema de Faturamento 1339. Uma Estação Móvel (MS) GPRS 1341 emprega um Módulo de Identidade do Assinante (SIM) 1343.

O PCU 1336 é um elemento de rede lógico responsável para as funções relacionadas-GPRS como controle de acesso de interface aérea, programação de pacote na interface aérea, e montagem de pacote e re-montagem. Geralmente o PCU 1336 é fisicamente integrado com o BSC 1345; porém, este pode ser disposto com uma BTS 1347 ou um SGSN 1332. O SGSN 1332 provê as funções equivalentes como o MSC 1349 incluindo o gerenciamento de mobilidade, segurança, e as funções de controle de acesso mas no domínio comutado por pacote. Além disso, o SGSN 1332 tem conectividade com o PCU 1336, por exemplo, uma interface baseada em Frame Relay usando o protocolo BSS GPRS (BSSGP). Embora apenas um SGSN seja mostrado, é reconhecido que múltiplos SGSNs 1331 podem ser empregados e podem dividir a área de serviço em áreas de direcionamento correspondentes (RAs). Uma interface SGSN/SGSN permite a tunelização de pacote dos SGSNs antigos para os SGSNs novos quando uma atualização de RA ocorre durante o contexto de Planejamento de Desenvolvimento Pessoal (PDP) entrante. Enquanto um determinado SGSN pode servir a múltiplos BSCs 1345, qualquer BSC determinado 1345 geralmente conecta com um SGSN 1332. Também, o SGSN 1332 é opcionalmente conectado com o HLR 1351 através de uma interface baseada no SS7 usando uma Parte de Aplicação Móvel (MAP) melhorada GPRS ou com o MSC 1349 através da interface

baseada no SS7 usando a Parte de Controle de Conexão de Sinalização (SCCP). A interface SGSN/HLR permite ao SGSN 1332 prover as atualizações locais ao HLR 1351 e recuperar a informação de assinatura relacionada ao GPRS dentro da área de serviço SGSN. A interface SGSN/MSC permite a coordenação entre os serviços comutados por circuito e os serviços de dados de pacote como chamar o assinante para uma chamada de voz. Finalmente, o SGSN 1332 conecta com o SMSC 1353 para permitir a funcionalidade de mensagem curta na rede 1350.

O GGSN 1334 é o portal para as redes de dados de pacote externas, tal como a Internet 1313 ou outras redes privadas do cliente 1355. A rede 1355 inclui um Sistema de Gerenciamento de Rede (NMS) 1357 acoplado a um ou mais bancos de dados 1359 acessados pelo PDSN 1361. O GGSN 1334 designa os endereços do Protocolo Internet (IP) e também pode autenticar os usuários que atuam como um Servidor de Serviço do Usuário de Autenticação de Discagem Remota. Barreiras de proteção localizadas no GGSN 1334 executam a função de barreira de proteção para restringir o tráfego sem autorização. Embora apenas um GGSN 1334 seja mostrado, é reconhecido que um determinado SGSN 1332 pode conectar com um ou mais GGSNs 1333 para permitir que os dados do usuário sejam tunelizados entre as duas entidades como também para e da rede 1350. Quando as redes de dados externas iniciam as sessões na rede GPRS 1350, o GGSN 1334 consulta o HLR 1351 para o SGSN 1332 que serve atualmente a MS 1341.

O BTS 1347 e o BSC 1345 gerenciam a interface de rádio, incluindo controlar qual Estação Móvel (MS) 1341 têm acesso ao canal de rádio a que horas. Estes elementos retransmitem as mensagens essencialmente entre a MS 1341 e o SGSN 1332. O SGSN 1332 gerencia as comunicações com a MS 1341, enviando e recebendo os dados e mantendo o rastro de seu local. O SGSN 1332 também registra a MS 1341, autentica a MS 1341, e codifica os dados enviados à MS 1341.

A Figura 14 é um diagrama dos componentes exemplares de uma estação móvel (por exemplo, um aparelho celular) capaz de operar nos sistemas

das Figuras 13A e 13B, de acordo com uma incorporação da invenção. Geralmente, um receptor de rádio é freqüentemente definido em termos das características auxiliares e de iniciais. A inicial do receptor cerca todos do circuito de Freqüência de Rádio (RF), considerando que a auxiliar cerca todos do circuito de processamento de banda base. Os componentes internos pertinentes do telefone incluem a Unidade de Controle Principal (MCU) 1403, um Processador de Sinal Digital (DSP) 1405, e uma unidade do receptor/transmissor incluindo uma unidade de controle do microfone e uma unidade de controle de ganho do alto-falante. Uma unidade de exibição principal 1407 provê uma exibição ao usuário no suporte de várias aplicações e funções das estações móveis. Um circuito de função de áudio 1409 inclui um microfone 1411 e amplificador de microfone que amplifica a saída de sinal de fala do microfone 1411. A saída do sinal de fala amplificada do microfone 1411 é alimentada em codificador/decodificador (CODEC) 1413.

Uma seção de rádio 1415 amplifica a potência e converte a freqüência para comunicar com uma estação base que é incluída em um sistema de comunicação móvel (por exemplo, os sistemas das Figuras 13A ou 13B), pela antena 1417. O amplificador de potência (PA) 1419 e o circuito transmissor/modulação são operacionalmente responsivos ao MCU 1403, com a saída do PA 1419 acoplada ao duplexador 1421 ou distribuidor ou comutador de antena, como conhecido na técnica.

Em uso, o usuário da estação móvel 1401 fala no microfone 1411 e a voz dele ou dela junto com qualquer ruído de fundo detectado é convertido em uma voltagem analógica. A voltagem analógica é convertida então em um sinal digital pelo Conversor Analógico para Digital (ADC) 1423. A unidade de controle 1403 direciona o sinal digital no DSP 1405 para processar neste, tal como codificação de fala, codificação de canal, cifragem, e intercalação. Na incorporação exemplar, os sinais de voz processados são codificados, através das unidades não apresentadas separadamente, usando o protocolo de transmissão celular de Acesso Múltiplo por Divisão de Código (CDMA), como descrito no

Padrão de Compatibilidade da Estação Base-Estação Móvel TIA/EIA/IS-95-A da Associação de Indústria de Telecomunicação para Sistema Celular de Espectro de Dispersão de Banda Larga de Modo Dual; que é aqui incorporado por referência em sua totalidade.

Os sinais codificados são direcionados então a um equalizador 1425 para compensação de qualquer prejuízo dependente-freqüência que ocorre durante a transmissão pelo ar, tal como por distorção de fase e de amplitude. Depois de equalizar o fluxo de bit, o modulador 1427 combina o sinal com o sinal RF gerado na interface RF 1429. O modulador 1427 gera uma onda de seno por meio da modulação de freqüência ou de fase. Para preparar o sinal para transmissão, um conversor-p/cima 1431 combina a saída da onda de seno do modulador 1427 com outra onda de seno gerada pelo sintetizador 1433 para alcançar a freqüência desejada de transmissão. O sinal é enviado então por um PA 1419 para aumentar o sinal a um nível de potência apropriado. Nos sistemas práticos, o PA 1419 atua como um amplificador de ganho variável cujo ganho é controlado pelo DSP 1405 da informação recebida de uma estação base da rede. O sinal é filtrado dentro do duplexador 1421 e opcionalmente enviado a um acoplador da antena 1435 para associar as impedâncias para prover a transferência de potência máxima. Finalmente, o sinal é transmitido pela antena 1417 para uma estação base local. Um controle de ganho automático (AGC) pode ser provido para controlar o ganho das fases finais do receptor. Os sinais podem ser direcionados de lá para um telefone remoto, que pode ser outro telefone celular, outro telefone móvel ou uma linha terrestre conectada à Rede de Telefonia Comutada Pública (PSTN), ou outras redes de telefonia.

Os sinais de voz para a estação móvel 1401 são transmitidos pela antena 1417 e imediatamente amplificados por um amplificador de ruído baixo (LNA) 1437. Um conversor-p/baixo 1439 abaixa a freqüência da portadora enquanto o demodulador 1441 tira o RF deixando apenas um fluxo de bit digital. O sinal passa então pelo equalizador 1425 e é processado pelo DSP 1005. Um conversor Digital para Analógico (DAC) 1443 converte o sinal e a produção

resultante é transmitida ao usuário pelo alto-falante 1445, todos sob controle da Unidade de Controle Principal (MCU) 1403 ~ que pode ser implementado como uma Unidade de Processamento Central (CPU) (não mostrada).

O MCU 1403 recebe vários sinais incluindo os sinais de entrada do teclado 1447. O MCU 1403 entrega um comando de exibição e um comando de comutação para o visor 1407 e para o controlador de comutação de saída de fala, respectivamente. Em adição, o MCU 1403 troca a informação com o DSP 1405 e pode acessar o cartão SIM 1449 incorporado opcionalmente e uma memória 1451. Em adição, o MCU 1403 executa as várias funções de controle requeridas da estação. O DSP 1405 pode, dependendo da implementação, executar qualquer de uma variedade de funções de processamento digitais convencionais nos sinais de voz. Adicionalmente, o DSP 1405 determina o nível de ruído de fundo do ambiente local dos sinais detectados pelo microfone 1411 e estabelece o ganho do microfone 1411 para um nível selecionado para compensar a tendência natural do usuário da estação móvel 1401.

O CODEC 1413 inclui o ADC 1423 e o DAC 1443. A memória 1451 armazena os vários dados incluindo os dados de toque da chamada entrante e é capaz de armazenar outros dados incluindo os dados de música recebidos, por exemplo, pela Internet global. O módulo de software poderia residir na memória RAM, memória flash, registros, ou qualquer outra forma de meio de armazenamento que possa ser escrito conhecido na técnica. O dispositivo de memória 1451 pode ser, mas não limitado, a uma única memória, CD, DVD, ROM, RAM, EEPROM, armazenamento óptico, ou qualquer outro meio de armazenamento não-volátil capaz de armazenar dados digitais.

Um cartão SIM opcionalmente incorporado 1449 carrega, por exemplo, uma informação importante, tal como o número do telefone celular, a portadora que fornece o serviço, os detalhes da assinatura, e a informação de segurança. O cartão SIM 1449 serve principalmente para identificar a estação móvel 1401 em uma rede de rádio. O cartão 1449 também contém uma memória para armazenar o registro do número de telefone pessoal, mensagens de texto, e

as configurações da estação móvel específicas do usuário.

A Figura 15 apresenta uma rede da empresa exemplar que pode ser qualquer tipo de rede de comunicação de dados que utiliza as tecnologias baseada em pacote e/ou baseadas em células (por exemplo, Modo de Transferência Assíncrono (ATM), Ethernet, baseado-IP, etc.). A rede da empresa 1501 provê a conectividade para os nós cabeados 1503 como também os nós sem fio 1505-1509 (fixo ou móvel), que são cada qual configurados para executar os processos descritos acima. A rede empresarial 1501 pode comunicar com uma variedade de outras redes, tal como a rede WLAN 1511 (por exemplo, IEEE 802.11), a rede celular cdma2000 1513, uma rede de telefonia 1515 (por exemplo, PSTN), ou a rede de dados pública 1517 (por exemplo, a Internet).

Enquanto a invenção tem sido descrita com relação às várias incorporações e implementações, a invenção não é limitada mas cobre várias modificações óbvias e disposições equivalentes, que são possíveis dentro do escopo das reivindicações apensas. Embora as características da invenção sejam expressadas em certas combinações entre as reivindicações, é contemplado que estas características possam ser dispostas em qualquer combinação e ordem.

REIVINDICAÇÕES

1. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- estabelecer uma chave com o terminal na rede de comunicação de acordo com o protocolo de acordo de chave, onde o terminal é configurado para operar usando o espectro de dispersão;

- fixar a chave acordada para o procedimento de autenticação para prover uma associação de segurança que suporta a reutilização da chave; e

- gerar a chave mestre baseada na chave acordada.

2. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que também compreende gerar uma mensagem de desafio da chave acordada de acordo com o procedimento de autenticação.

3. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que também compreende gerar uma mensagem de desafio da mensagem de acordo de chave trocada com o terminal de acordo com o protocolo de acordo de chave.

4. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o protocolo de acordo de chave inclui o esquema de troca de chave Diffie-Hellman.

5. Método de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que o acordo de chave é executado no túnel de segurança da camada de transporte (TLS).

6. Método de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que o terminal é configurado para comunicar usando o espectro de dispersão e executa o auto-carregador de acordo com a arquitetura de autenticação genérica.

7. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o procedimento de autenticação inclui o protocolo de autenticação do estabelecimento de comunicação de desafio (CHAP).

8. Método de autenticação, **CARACTERIZADO** pelo fato de que

compreende:

- estabelecer uma chave compartilhada com o elemento de rede na rede de comunicação de acordo com o protocolo de acordo de chave, onde o elemento de rede é configurado para fixar a chave acordada para o procedimento de autenticação para prover a associação de segurança que suporta a reutilização da chave; e

- gerar a chave mestre baseado na chave acordada.

9. Método de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o protocolo de acordo de chave inclui o esquema de troca de chave Diffie-Hellman.

10. Método de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o acordo de chave é executado no túnel de segurança da camada de transporte (TLS).

11. Método de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que também compreende:

- comunicar com o elemento de rede usando o Acesso Múltiplo por Divisão de Código (CDMA); e

- executar o auto-carregador de acordo com a arquitetura de autenticação genérica.

12. Método de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o procedimento de autenticação inclui o protocolo de autenticação do estabelecimento de comunicação de desafio (CHAP).

13. Aparelho de autenticação **CARACTERIZADO** pelo fato de que compreende:

- um módulo de autenticação configurado para estabelecer uma chave compartilhada com o elemento de rede na rede de comunicação de acordo com o protocolo de acordo de chave, onde o elemento de rede é configurado para fixar a chave acordada para o procedimento de autenticação para prover a associação de segurança que suporta a reutilização da chave; e

- o módulo de autenticação sendo também configurado para gerar a

chave mestre baseado na chave acordada.

14. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o protocolo de acordo de chave inclui o esquema de troca de chave Diffie-Hellman.

15. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o acordo de chave é executado no túnel de segurança da camada de transporte (TLS).

16. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que também compreende um transceptor configurado para comunicar com o elemento de rede usando o espectro de dispersão, onde o módulo de autenticação é também configurado para executar o auto-carregador de acordo com a arquitetura de autenticação genérica.

17. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o procedimento de autenticação inclui o protocolo de autenticação do estabelecimento de comunicação de desafio (CHAP).

18. Sistema **CARACTERIZADO** pelo fato de que compreende o aparelho e o elemento de rede da reivindicação 13.

19. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- gerar uma mensagem para autenticar a comunicação com o elemento de rede configurado para executar o auto-carregador;

- estabelecer um campo de senha da mensagem para uma função da chave secreta; e

- especificar a informação de estabelecimento de chave dentro da carga útil da mensagem, onde a mensagem é transmitida de acordo com o protocolo de transporte para acessar a informação na rede de dados.

20. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que o protocolo de transporte inclui o protocolo de transferência de hipertexto.

21. Método de acordo com a reivindicação 19, **CARACTERIZADO**

pelo fato de que a informação de estabelecimento da chave inclui os parâmetros Diffie-Hellman.

22. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que também compreende estabelecer o campo do nome do usuário da mensagem para o identificador do terminal.

23. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que a função da chave secreta é a soma de verificação ou compilação.

24. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que a chave secreta é a chave de codificação da mensagem de sinalização (SMEKEY) ou a chave de autenticação, autorização e contabilidade do nó móvel (MN-AAA).

25. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- receber a mensagem do terminal, de acordo com o protocolo de transporte para acessar a informação na rede de dados, solicitar a autenticação, onde a mensagem inclui o campo de senha que é uma função da chave secreta e a carga útil contendo os parâmetros de especificação de informação de estabelecimento da chave para determinar outra chave secreta; e

- gerar uma chave mestre baseada nas chaves secretas.

26. Método de acordo com a reivindicação 25, **CARACTERIZADO** pelo fato de que o protocolo de transporte inclui o protocolo de transferência de hipertexto.

27. Método de acordo com a reivindicação 25, **CARACTERIZADO** pelo fato de que a informação de estabelecimento da chave inclui os parâmetros Diffie-Hellman.

28. Método de acordo com a reivindicação 25, **CARACTERIZADO** pelo fato de que a mensagem inclui o campo do nome do usuário da mensagem para o identificador do terminal.

29. Método de acordo com a reivindicação 25, **CARACTERIZADO**

pelo fato de que a função da chave secreta é a soma de verificação ou compilação.

30. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que a chave secreta é a chave de codificação da mensagem de sinalização (SMEKEY) ou a chave de autenticação, autorização e contabilidade do nó móvel (MN-AAA).

31. Aparelho para autenticação **CARACTERIZADO** pelo fato de que compreende um módulo de autenticação configurado para gerar uma mensagem para autenticar a comunicação com o elemento de rede configurado para executar o auto-carregador, e para estabelecer um campo de senha da mensagem para ser a função da chave secreta, a mensagem tendo uma carga útil que inclui a nova informação de estabelecimento da chave, onde a mensagem é transmitida de acordo com o protocolo de transporte para acessar a informação na rede de dados.

32. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que o protocolo de transporte inclui o protocolo de transferência de hipertexto que suporta as comunicações seguras na rede de dados.

33. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que a informação de estabelecimento da chave inclui os parâmetros Diffie-Hellman.

34. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que o módulo de autenticação é também configurado para estabelecer o campo do nome do usuário da mensagem para o identificador do terminal.

35. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que a função da chave secreta é a soma de verificação ou compilação.

36. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que a chave secreta é a chave de codificação da mensagem de sinalização (SMEKEY) ou a chave de autenticação, autorização e contabilidade do nó móvel (MN-AAA).

37. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que também compreende um transceptor configurado para comunicar com a estação base usando o espectro de dispersão, onde o módulo de autenticação é também configurado para executar o auto-carregador de acordo com a arquitetura de autenticação genérica.

38. Sistema **CARACTERIZADO** pelo fato de que compreende o aparelho e o elemento de rede da reivindicação 31.

39. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- receber um pedido de autenticação especificando a identidade do usuário do terminal;

- direcionar a identidade do usuário para o registro de localização configurado para gerar, baseado na identidade do usuário, os parâmetros criptográficos incluindo os dados secretos randômicos, e os dados secretos gerados dos dados secretos randômicos de acordo com o algoritmo criptográfico;

- receber os parâmetros criptográficos gerados do registro de localização;

- gerar um vetor de autenticação ao converter os parâmetros criptográficos para os parâmetros de chave incluindo o símbolo de autenticação e a resposta de autenticação;

- transmitir o símbolo de autenticação para o terminal configurado para produzir a resposta de autenticação;

- validar a resposta de autenticação do terminal usando a resposta de autenticação do vetor de autenticação; e

- gerar a chave mestre baseada nos parâmetros da chave.

40. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que o pedido de autenticação é gerado de acordo com o protocolo de transferência de hipertexto.

41. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que a conversão dos parâmetros criptográficos para os parâmetros da

chave inclui gerar a chave baseado nos dados secretos.

42. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que o vetor de autenticação inclui um número randômico que é baseado nos dados secretos randômicos, o vetor de autenticação também inclui uma chave de cifragem, e uma chave de integridade.

43. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que o algoritmo criptográfico inclui um algoritmo de autenticação celular e cifragem de voz.

44. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que uma pluralidade de grupos de parâmetros criptográficos são gerados pelo registro de localização para uso na geração do vetor de autenticação.

45. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- gerar um pedido de autenticação especificando a identidade do usuário;

- transmitir o pedido de autenticação para o elemento de rede configurado para prover o auto-carregamento, onde o elemento de rede direciona a identidade do usuário para o registro de localização configurado para gerar, baseado na identidade do usuário, os parâmetros criptográficos incluindo os dados secretos randômicos, e os dados secretos gerados dos dados secretos randômicos de acordo como algoritmo criptográfico, onde o elemento de rede gera o vetor de autenticação ao converter os parâmetros criptográficos para os parâmetros de chave incluindo um símbolo de autenticação e uma resposta de autenticação;

- receber o símbolo de autenticação do elemento de rede;

- produzir a resposta de autenticação baseado no símbolo de autenticação;

- determinar a resposta de compilação usando a resposta de autenticação;

- transmitir a resposta de compilação para o elemento de rede para

validação; e

- gerar a chave mestre baseado nos parâmetros de chave.

46. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que o pedido de autenticação é gerado de acordo com o protocolo de transferência de hipertexto.

47. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que a conversão dos parâmetros criptográficos para os parâmetros da chave inclui gerar a chave baseado nos dados secretos.

48. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que o vetor de autenticação inclui um número randômico que é baseado nos dados secretos randômicos, o vetor de autenticação também inclui uma chave de cifragem, e uma chave de integridade.

49. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que o algoritmo criptográfico inclui um algoritmo de autenticação celular e cifragem de voz.

50. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que uma pluralidade de grupos de parâmetros criptográficos são gerados pelo registro de localização para uso na geração do vetor de autenticação.

51. Aparelho para autenticação **CARACTERIZADO** pelo fato de que compreende:

- um módulo de autenticação configurado para gerar um pedido de autenticação especificando a identidade do usuário;

- um transceptor configurado para transmitir o pedido de autenticação para o elemento de rede configurado para prover o auto-carregamento, onde o elemento de rede direciona a identidade do usuário para o registro de localização configurado para gerar, baseado na identidade do usuário, os parâmetros criptográficos incluindo os dados secretos randômicos, e os dados secretos gerados dos dados secretos randômicos de acordo com o algoritmo criptográfico, onde o elemento de rede gera o vetor de autenticação ao converter os parâmetros criptográficos para os parâmetros de chave incluindo um símbolo de autenticação

e uma resposta de autenticação, onde o transceptor é também configurado para receber o símbolo de autenticação do elemento de rede, e o módulo de autenticação é também configurado para produzir a resposta de autenticação baseado no símbolo de autenticação, para determinar a resposta de compilação usando a resposta de autenticação, e para gerar uma chave mestre baseado nos parâmetros da chave na validação da resposta de compilação pelo elemento de rede.

52. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que o pedido de autenticação é gerado de acordo com o protocolo de transferência de hipertexto.

53. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que a conversão dos parâmetros criptográficos para os parâmetros da chave inclui gerar a chave baseado nos dados secretos.

54. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que o vetor de autenticação inclui um número randômico que é baseado nos dados secretos randômicos, o vetor de autenticação também inclui uma chave de cifragem, e uma chave de integridade.

55. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que o algoritmo criptográfico inclui um algoritmo de autenticação celular e cifragem de voz.

56. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que uma pluralidade de grupos de parâmetros criptográficos são gerados pelo registro de localização para uso na geração do vetor de autenticação.

57. Sistema **CARACTERIZADO** pelo fato de que compreende o aparelho da reivindicação 51 e o elemento de rede.

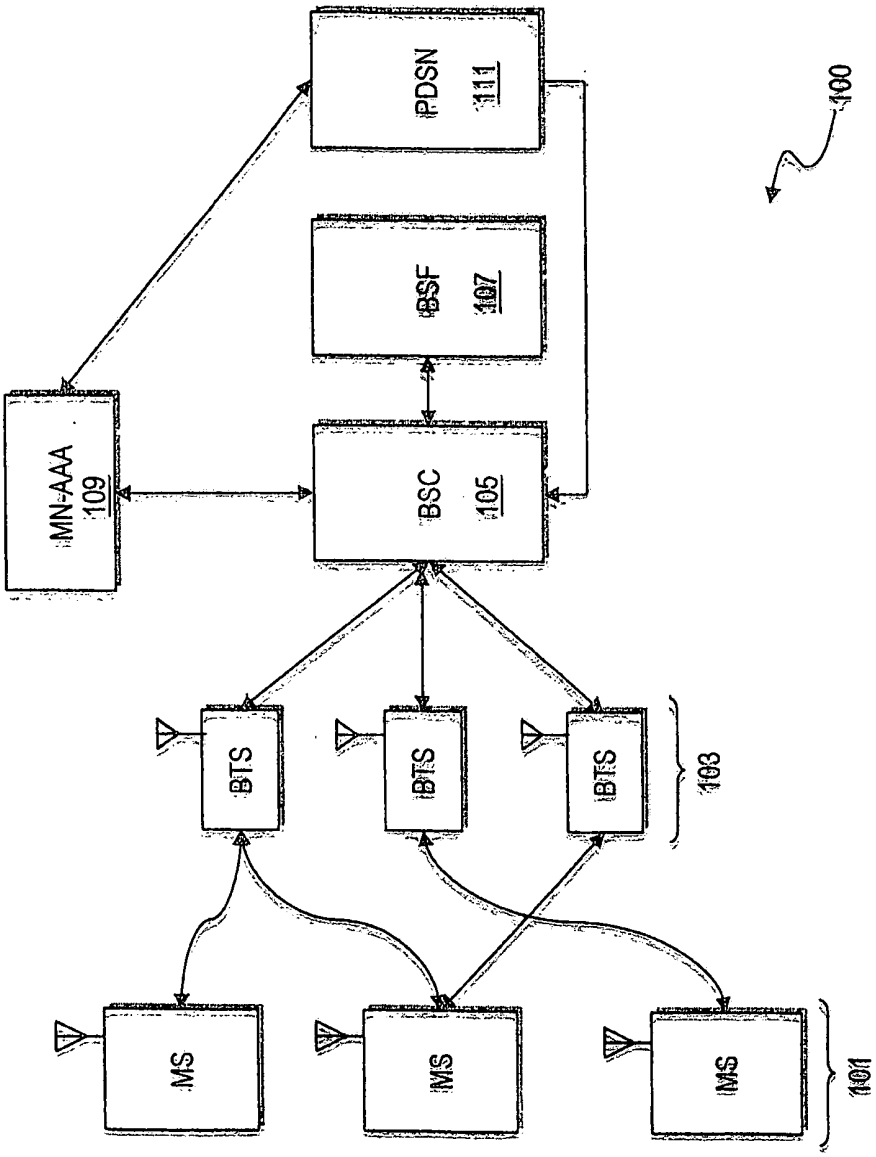

PDSN
111
100
BSF
107
MN-AAA
109
BSC
105
BTS
BTS
BTS
103
MS
MS
MS
101

FIG. 1

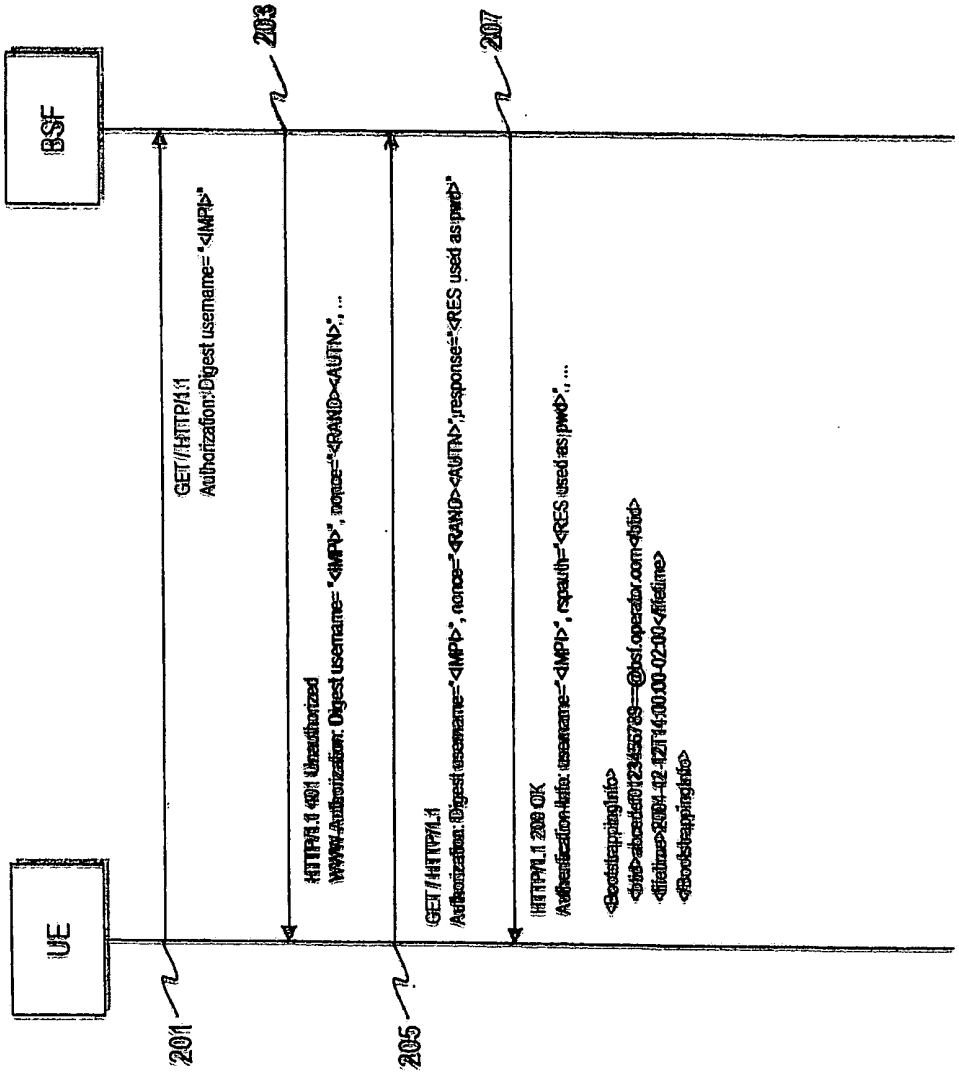
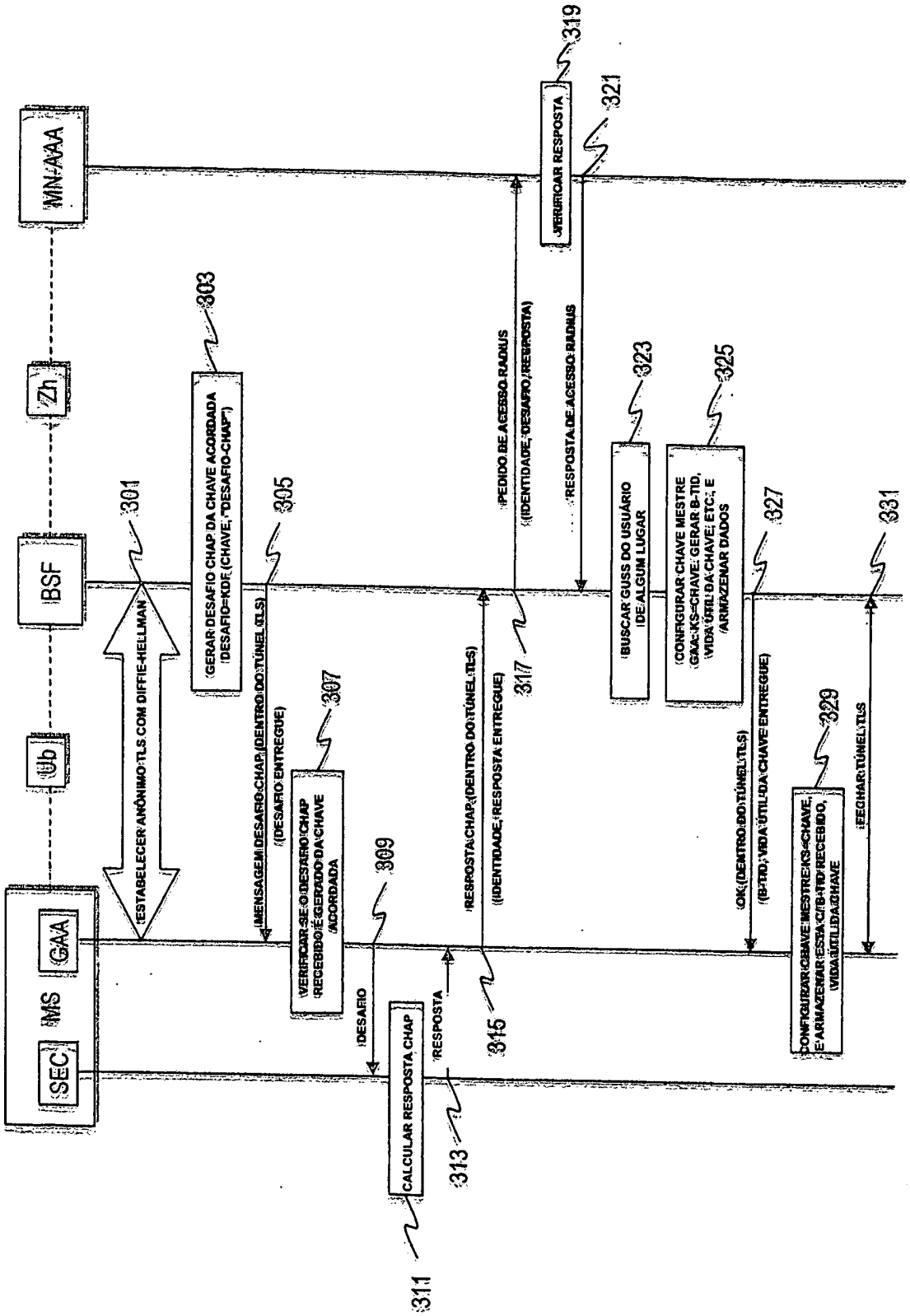

UE
BSF
201
GET /HTTP/1.1
Authorization::Digest username="<IMPI>"
203
HTTP/1.1 401 Unauthorized
WWW-Authorization: Digest username="<IMPI>", nonce="<RAND><AUTN>", ...
205
GET /HTTP/1.1
Authorization: Digest username="<IMPI>", nonce="<RAND><AUTN>",response="<RES used as pwd>"
207
HTTP/1.1 200 OK
Authentication-Info: username="<IMPI>", rspauth="<RES used as pwd>", ...
<BootstrappingInfo>
<btid>aliceid@12345678@bsf.operator.com</btid>
<lifetime>2004-12-12T14:00:00-02:00</lifetime>
<BootstrappingInfo>

FIG. 2

FIG. 3


SEC
MS
GAA
Ub
BSF
Zh
MN-AAA
301
303
305
307
309
311
313
315
317
319
321
323
325
327
329
331
ESTABELECER ANÔNIMO TLS COM DIFFIE-HELLMAN
GERAR DESAFIO CHAP DA CHAVE ACORDADA
DESAFIO=KDF (CHAVE, "DESAFIO-CHAP")
MENSAGEM DESAFIO-CHAP (DENTRO DO TÚNEL TLS)
(DESAFIO ENTREGUE)
VERIFICAR SE O DESAFIO CHAP RECEBIDO É GERADO DA CHAVE ACORDADA
DESAFIO
RESPOSTA
CALCULAR RESPOSTA CHAP
RESPOSTA CHAP (DENTRO DO TÚNEL TLS)
(IDENTIDADE, RESPOSTA ENTREGUE)
PEDIDO DE ACESSO RADIUS
((IDENTIDADE, DESAFIO, RESPOSTA)
VERIFICAR RESPOSTA
RESPOSTA DE ACESSO RADIUS
BUSCAR GUSS DO USUÁRIO
DE ALGUM LUGAR
CONFIGURAR CHAVE MESTRE
(GAA: KS=CHAVE; GERAR B-TID,
VIDA ÚTIL DA CHAVE; ETC.; E
ARMAZENAR DADOS
OK ((DENTRO DO TÚNEL TLS)
(B-TID, VIDA ÚTIL DA CHAVE ENTREGUE)
CONFIGURAR CHAVE MESTRE KS=CHAVE,
E ARMAZENAR ESTA C/ B-TID RECEBIDO,
VIDA ÚTIL DA CHAVE
FECHAR TÚNEL TLS

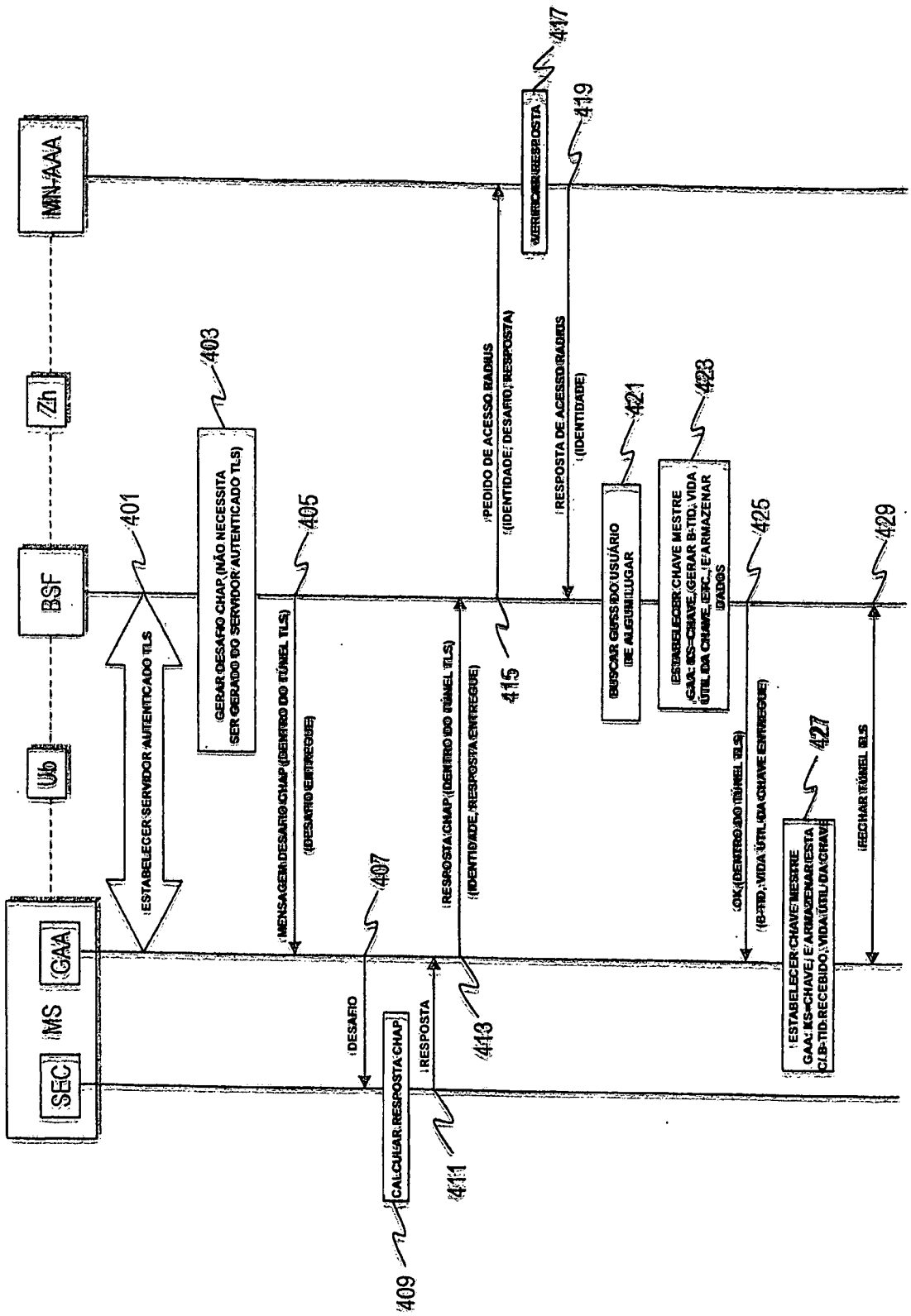
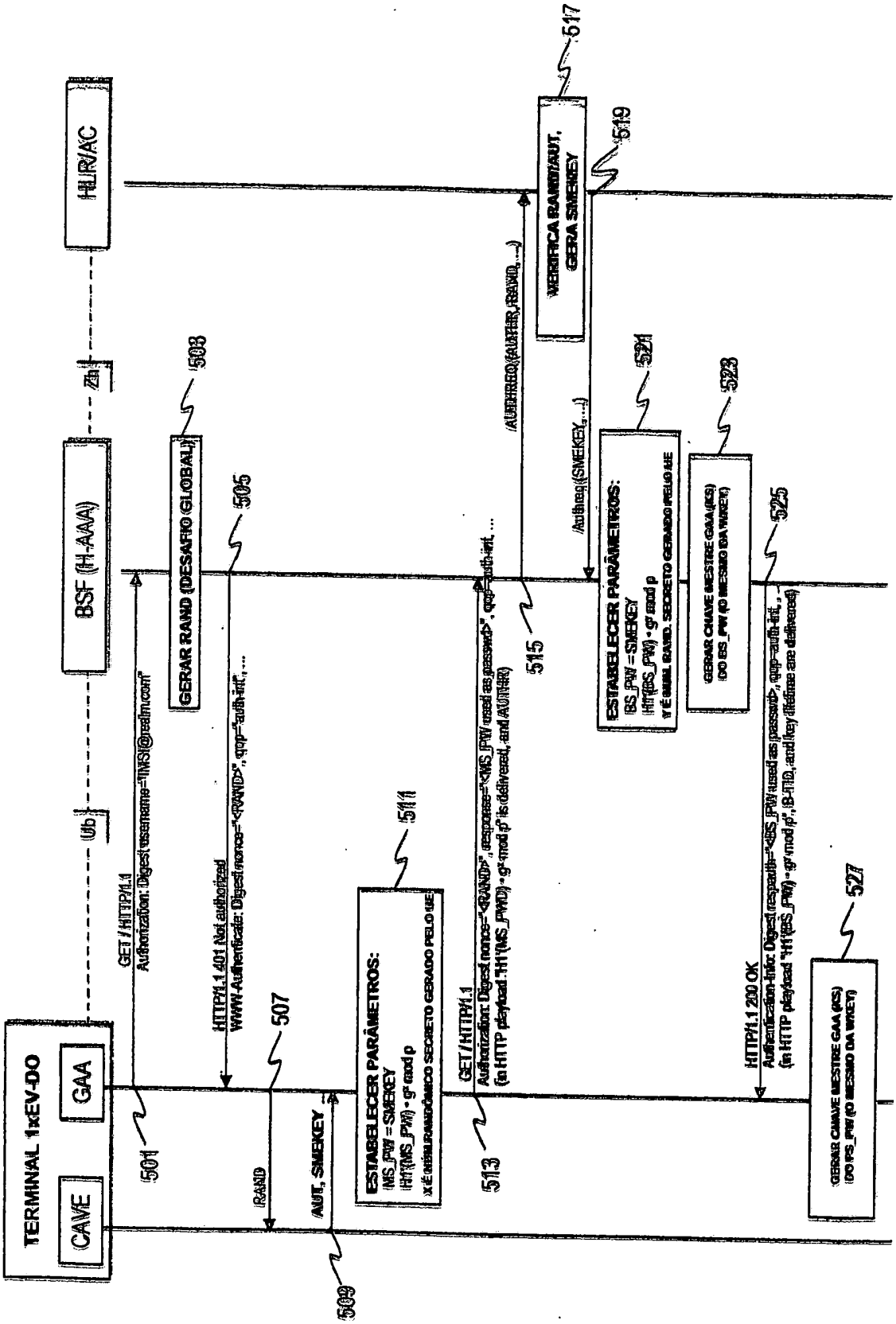

SEC
MS
GAA
Ub
BSF
Zh
MN-AAA
ESTABELECER SERVIDOR AUTENTICADO TLS
401
GERAR DESAFIO CHAP (NÃO NECESSITA SER GERADO DO SERVIDOR AUTENTICADO TLS)
403
MENSAGEM DESAFIO CHAP (DENTRO DO TÚNEL TLS)
(DESAFIO ENTREGUE)
405
DESAFIO
407
CALCULAR RESPOSTA CHAP
409
RESPOSTA
411
RESPOSTA CHAP (DENTRO DO TÚNEL TLS)
(IDENTIDADE, RESPOSTA ENTREGUE)
413
PEDIDO DE ACESSO RADIUS
(IDENTIDADE, DESAFIO, RESPOSTA)
415
VERIFICAR RESPOSTA
417
RESPOSTA DE ACESSO RADIUS
(IDENTIDADE)
419
BUSCAR GMSS DO USUÁRIO DE ALGUM LUGAR
421
ESTABELECER CHAVE MESTRE GAA: KS=CHAVE, GERAR B-TID, VIDA ÚTIL DA CHAVE, IERC, E ARMAZENAR DADOS
423
OK (DENTRO DO TÚNEL TLS)
(B-TID, VIDA ÚTIL DA CHAVE ENTREGUE)
425
ESTABELECER CHAVE MESTRE GAA: KS=CHAVE, E ARMAZENAR ESTA C.I.B-TID RECEBIDO, VIDA ÚTIL DA CHAVE
427
FECHAR TÚNEL TLS
429

FIG. 4

FIG. 5


TERMINAL 1xEV-DO
CAVE
GAA
BSF (H-AAA)
HLR/AC
Ub
Zh
501
503
505
507
509
511
513
515
517
519
521
523
525
527
GET / HTTP/1.1
Authorization: Digest username="IMSI@realm.com"
HTTP/1.1 401 Not authorized
WWW-Authenticate: Digest nonce="<RAND>", qop="auth-int",...
GERAR RAND (DESAFIO GLOBAL)
RAND
AUT, SMEKEY
ESTABELECER PARÂMETROS:
IMS_PW = SMEKEY
H1'(IMS_PW) = g^ mod p
x É UM NÚMERO ALEATÓRIO SECRETO GERADO PELO UE
GET / HTTP/1.1
Authorization: Digest nonce="<RAND>", response="<IMS_PW used as password>", qop="auth-int", ...
(o HTTP payload "H1'(IMS_PW) = g^ mod p" is delivered, and AUTHR)
AUTHREQ(AUTHR, RAND, ...)
VERIFICA RAND/AUT, GERA SMEKEY
Authreq((SMEKEY, ...)
ESTABELECER PARÂMETROS:
BS_PW = SMEKEY
H1'(BS_PW) = g^ mod p
(Y É UMA NOVA RAND, SEGREDO GERADO PELO HE
GERAR CHAVE MESTRE GAA (KS)
(DO BS_PW (O SEGREDO DA SMEKEY)
HTTP/1.1 200 OK
Authentication-Info: Digest rspauth="<BS_PW used as password>", qop="auth-int", ...
(o HTTP payload "H1'(BS_PW) = g^ mod p", IB-TID, and Key lifetime are delivered)
GERAR CHAVE MESTRE GAA (KS)
(DO PS_PW (O SEGREDO DA SMEKEY)

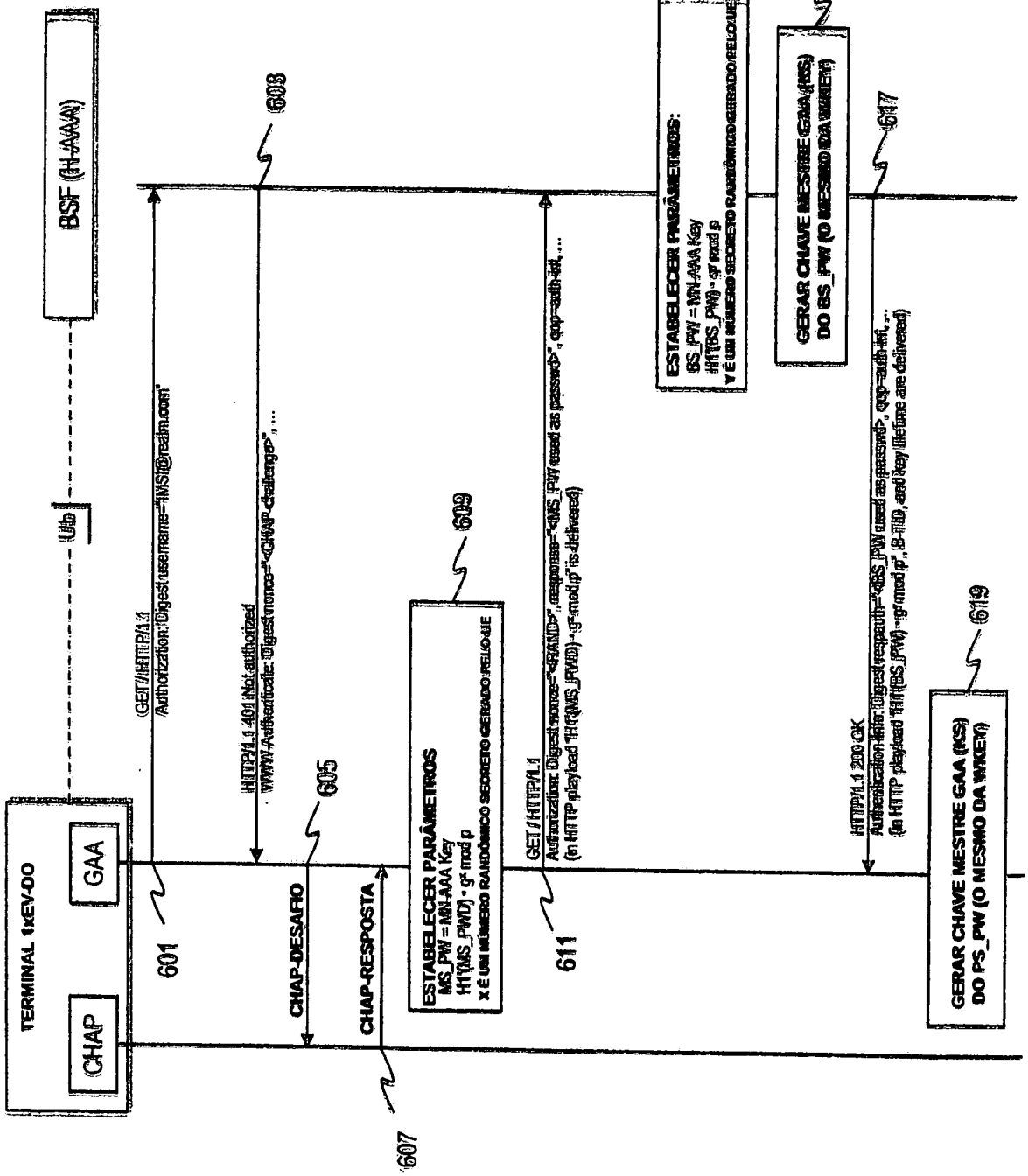
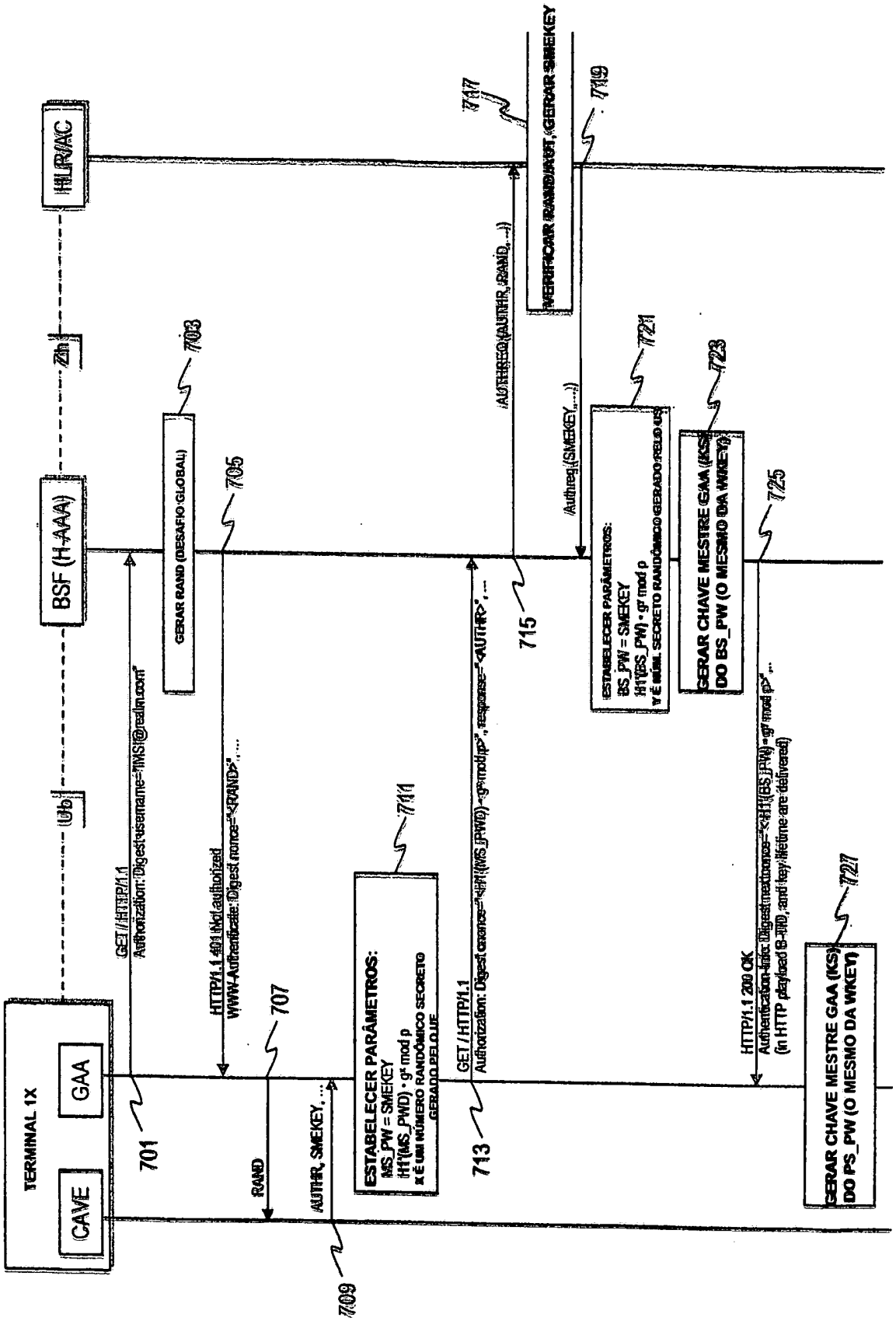

TERMINAL 1xEV-DO
CHAP
GAA
BSF (H-AAA)
Ub
601
603
605
607
611
613
615
617
619
619
GET /HTTP/1.1
Authorization: Digest username="IMSI@realm.com"
HTTP/1.1 401 Not authorized
WWW-Authenticate: Digest nonce="<CHAP challenge>", ...
CHAP-DESAFIO
CHAP-RESPOSTA
ESTABELECER PARÂMETROS
MS_PW = MN-AAA Key
HTTP(MS_PWD) - g^ mod p
x É UM NÚMERO RANDÔMICO SECRETO GERADO PELO MS
GET /HTTP/1.1
Authorization: Digest nonce="<RAND>", response="<MS_PW used as password>", qop=auth-int, ...
(in HTTP payload "HTTP(MS_PWD) - g^ mod p" is delivered)
ESTABELECER PARÂMETROS:
BS_PW = MN-AAA Key
HTTP(BS_PW) - g^ mod p
Y É UM NÚMERO SECRETO RANDÔMICO GERADO PELO AE
GERAR CHAVE MESTRE GAA (MS)
DO BS_PW (O MESMO DA MKEY)
HTTP/1.1 200 OK
Authentication-Info: Digest rspauth="<BS_PW used as passwd>", qop=auth-int, ...
(in HTTP payload "HTTP(BS_PW) - g^ mod p", B-TID, and key lifetime are delivered)
GERAR CHAVE MESTRE GAA (KS)
DO PS_PW (O MESMO DA MKEY)

FIG. 6

FIG. 7


TERMINAL 1X
CAVE
GAA
BSF (H-AAA)
HLR/AC
Ub
Zh
701
GET /HTTP/1.1
Authorization: Digest username="IMSI@realm.com"
703
GERAR RAND (DESAFIO GLOBAL)
705
HTTP/1.1 401 Not authorized
WWW-Authenticate: Digest nonce="<RAND>",...
707
RAND
AUTHR, SMEKEY, ...
709
711
ESTABELECER PARÂMETROS:
MS_PW = SMEKEY
H1'(MS_PWD) · g^ mod p
x É UM NÚMERO RANDÔMICO SECRETO GERADO PELO UE
713
GET / HTTP/1.1
Authorization: Digest cnonce="<H1'(MS_PWD)·g^ mod p>", response="<AUTHR>",...
715
AUTHREQ (AUTHR, RAND, ...)
717
VERIFICAR (RAND,AUTHR) E GERAR SMEKEY
719
Authreq (SMEKEY,...)
721
ESTABELECER PARÂMETROS:
BS_PW = SMEKEY
H1'(BS_PW) · g^ mod p
y É UM SEGUNDO SECRETO RANDÔMICO GERADO PELO US
723
GERAR CHAVE MESTRE GAA (KS) DO BS_PW (O MESMO DA WKEY)
725
HTTP/1.1 200 OK
Authentication-Info: Digest nextnonce="<H1'(BS_PW) · g^y mod p>",...
(in HTTP payload B-TID, and key lifetime are delivered)
727
GERAR CHAVE MESTRE GAA (KS) DO PS_PW (O MESMO DA WKEY)

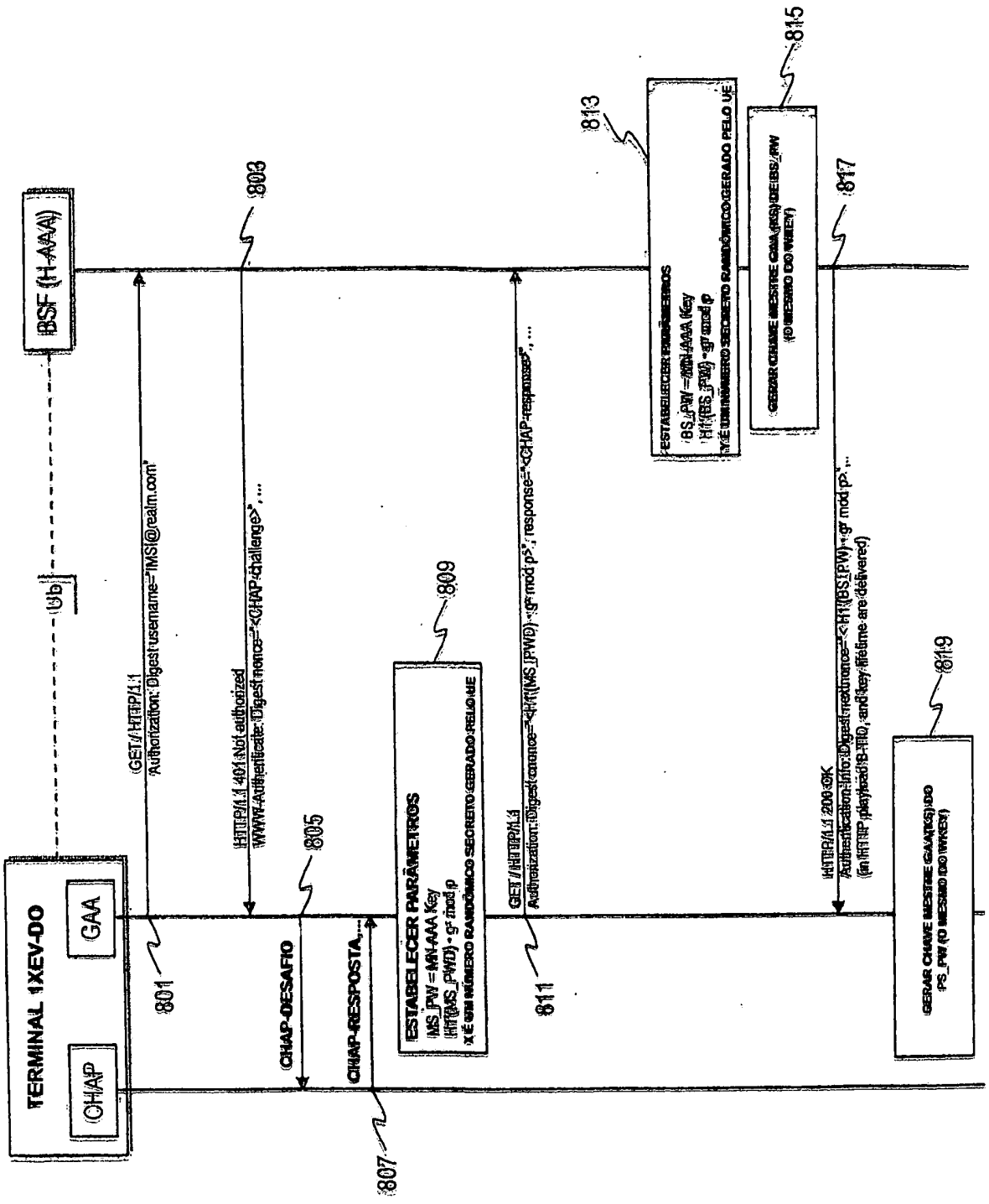

TERMINAL 1XEV-DO
CHAP
GAA
BSF (H-AAA)
Ub
801
803
805
807
809
811
813
815
817
819
GET / HTTP/1.1
Authorization: Digest username="IMSI@realm.com"
HTTP/1.1 401 Not authorized
WWW-Authenticate: Digest nonce="<CHAP-challenge>", ...
CHAP-DESAFIO
CHAP-RESPOSTA,...
ESTABELECER PARÂMETROS
MS_PW = MN-AAA Key
HTTP(MS_PW) - gr mod p
X É UM NÚMERO RANDÔMICO SECRETO GERADO PELO UE
GET / HTTP/1.1
Authorization: Digest cnonce="<H'(MS_PW) - gr mod p>", response="<CHAP-response>", ...
ESTABELECER PARÂMETROS
BS_PW = MN-AAA Key
HTTP(BS_PW) - gr mod p
Y É UM NÚMERO SECRETO RANDÔMICO GERADO PELO UE
GERAR CHAVE MESTRE GAA (MK) DE BS_PW
(O MESMO DO WIKEY)
HTTP/1.1 200 OK
Authentication-Info: Digest rsltnonce="<H'(BS_PW) - gr mod p>", ...
(an HTTP playback of S-HTID, and key lifetime are delivered)
GERAR CHAVE MESTRE GAA (MK) DO
PS_PW (O MESMO DO WIKEY)

FIG. 8

FIG. 9

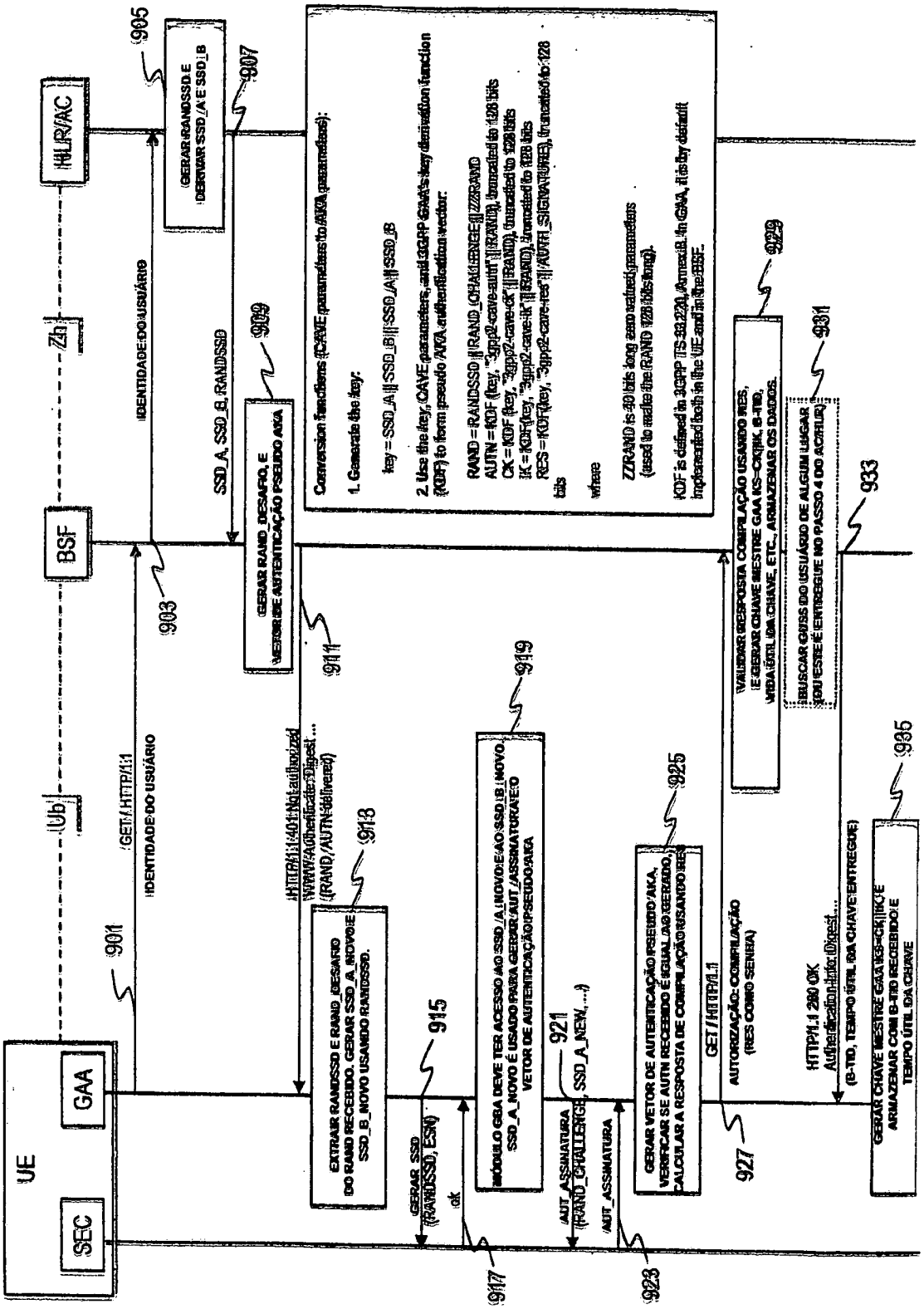

UE
SEC
GAA
BSF
HLR/AC
Ub
Zh
/GET/HTTP/1.1
IDENTIDADE DO USUÁRIO
901
903
905
907
909
911
913
915
917
919
921
923
925
927
929
931
933
935
GERAR RAND_DESAFIO, E VETOR DE AUTENTICAÇÃO PSEUDO AKA
SSD_A, SSD_B, RANDSSD
Conversion functions (CAVE parameters to AKA parameters):
1. Generate the key:
key = SSD_A || SSD_B || SSD_A || SSD_B
2. Use the key, CAVE parameters, and 3GPP SAA's key derivation function (KDF) to form pseudo AKA authentication vector:
RAND = RANDSSD || RAND_CHALLENGE || ZZRAND
AUTN = KDF (key, "3gpp2-cave-autn" || RAND), truncated to 128 bits
CK = KDF (key, "3gpp2-cave-ck" || RAND), truncated to 128 bits
IK = KDF (key, "3gpp2-cave-ik" || RAND), truncated to 128 bits
RES = KDF (key, "3gpp2-cave-res" || AUTH_SIGNATURE), truncated to 128 bits
where
ZZRAND is 40 bits long zero padded parameters (used to make the RAND 128 bits long).
KDF is defined in 3GPP TS 33.220, Annex B. In GAA, it is by default implemented both in the UE and in the BSF.
HTTP/1.1 401 Not authorized WWW-Authenticate: Digest ... (RAND, AUTN, ME Identity)
EXTRAIR RANDSSD E RAND_DESAFIO RAND RECEBIDO. GERAR SSD_A_NOVO E SSD_B_NOVO USANDO RANDSSD.
GERAR_SSD (RANDSSD, ESN)
ok
MÓDULO GBA DEVE TER ACESSO AO SSD_A_NOVO E AO SSD_B_NOVO. SSD_A_NOVO É USADO PARA GERAR AUT_ASSINATURA E O VETOR DE AUTENTICAÇÃO PSEUDO AKA
AUT_ASSINATURA (RAND_CHALLENGE, SSD_A_NEW, ...)
AUT_ASSINATURA
GERAR VETOR DE AUTENTICAÇÃO PSEUDO AKA, VERIFICAR SE AUTN RECEBIDO É IGUAL AO GERADO, CALCULAR A RESPOSTA DE COMPILAÇÃO USANDO RES
GET / HTTP/1.1
AUTORIZAÇÃO: COMPILAÇÃO (RES COMO SENHA)
VALIDAR RESPOSTA COMPILAÇÃO USANDO RES, E GERAR CHAVE MESTRE GAA (S-CK||K-CK, B-TID, VIDA ÚTIL DA CHAVE, ETC., ARMAZENAR OS DADOS.
BUSCAR CHAVES DO USUÁRIO DE ALGUM LUGAR (OU ESTE É ENTREGUE NO PASSO 4 DO ACIMA)
HTTP/1.1 200 OK Authentication-Info: (Digest ... (B-TID, TEMPO ÚTIL DA CHAVE ENTREGUE)
GERAR CHAVE MESTRE GAA (KS=CK||KCK) E ARMAZENAR COM B-TID RECEBIDO E TEMPO ÚTIL DA CHAVE

FIG. 10A

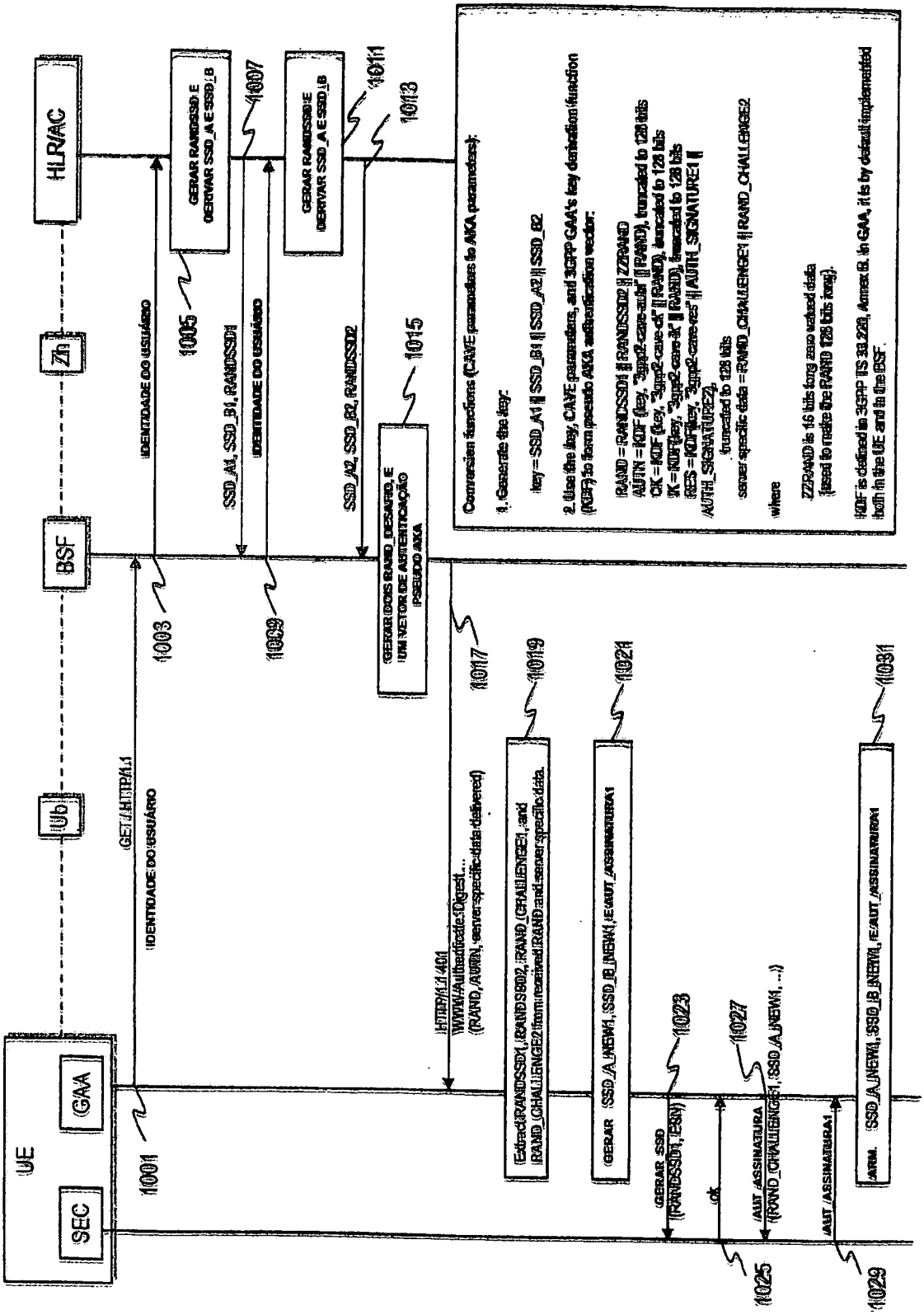

UE
SEC
GAA
Ub
BSF
Zh
HLR/AC
1001
1003
1005
1007
1009
1011
1013
1015
1017
1019
1021
1023
1025
1027
1029
1031
GET /.HTTP/1.1
IDENTIDADE DO USUÁRIO
IDENTIDADE DO USUÁRIO
GERAR RAND'S E DERIVAR SSD_A E SSD_B
SSD_A1, SSD_B1, RANDSSD1
IDENTIDADE DO USUÁRIO
GERAR RAND'S E DERIVAR SSD_A E SSD_B
SSD_A2, SSD_B2, RANDSSD2
GERAR DOIS RAND, DESAFIO, E UM VETOR DE AUTENTICAÇÃO PSEUDO AKA
HTTP/1.1 401
WWW-Authenticate:Digest...
(RAND, AUTN), server-specific-data delivered)
Extract RANDSSD1, RANDSSD2, RAND_CHALLENGE1, and RAND_CHALLENGE2 from received RAND and server-specific data.
GERAR SSD (RANDSSD1, ESN)
GERAR SSD_A_NEW1, SSD_B_NEW1, IEAUT_ASSINATURA1
ck
AUT_ASSINATURA (ROUND_CHALLENGE1, SSD_A_NEW1, ...)
AUT_ASSINATURA1
ATRIB. SSD_A_NEW1, SSD_B_NEW1, IEAUT_ASSINATURA1
Conversion functions (CAVE parameters to AKA parameters):
1. Generate the key:
key = SSD_A1 || SSD_B1 || SSD_A2 || SSD_B2
2. Use the key, CAVE parameters, and 3GPP GAA's key derivation function (KDF) to form pseudo AKA authentication vector:
RAND = RANDSSD1 || RANDSSD2 || ZZRAND
AUTN = KDF (key, "3gpp2-cave-autn" || RAND), truncated to 128 bits
CK = KDF (key, "3gpp2-cave-ck" || RAND), truncated to 128 bits
IK = KDF (key, "3gpp2-cave-ik" || RAND), truncated to 128 bits
RES = KDF (key, "3gpp2-cave-res" || AUTH_SIGNATURE1 || AUTH_SIGNATURE2),
truncated to 128 bits
server-specific data = RAND_CHALLENGE1 || RAND_CHALLENGE2
where
ZZRAND is 16 bits long zero valued data
(used to make the RAND 128 bits long).
KDF is defined in 3GPP TS 33.220, Annex B. In GAA, it is by default implemented both in the UE and in the BSF.

FIG. 10B

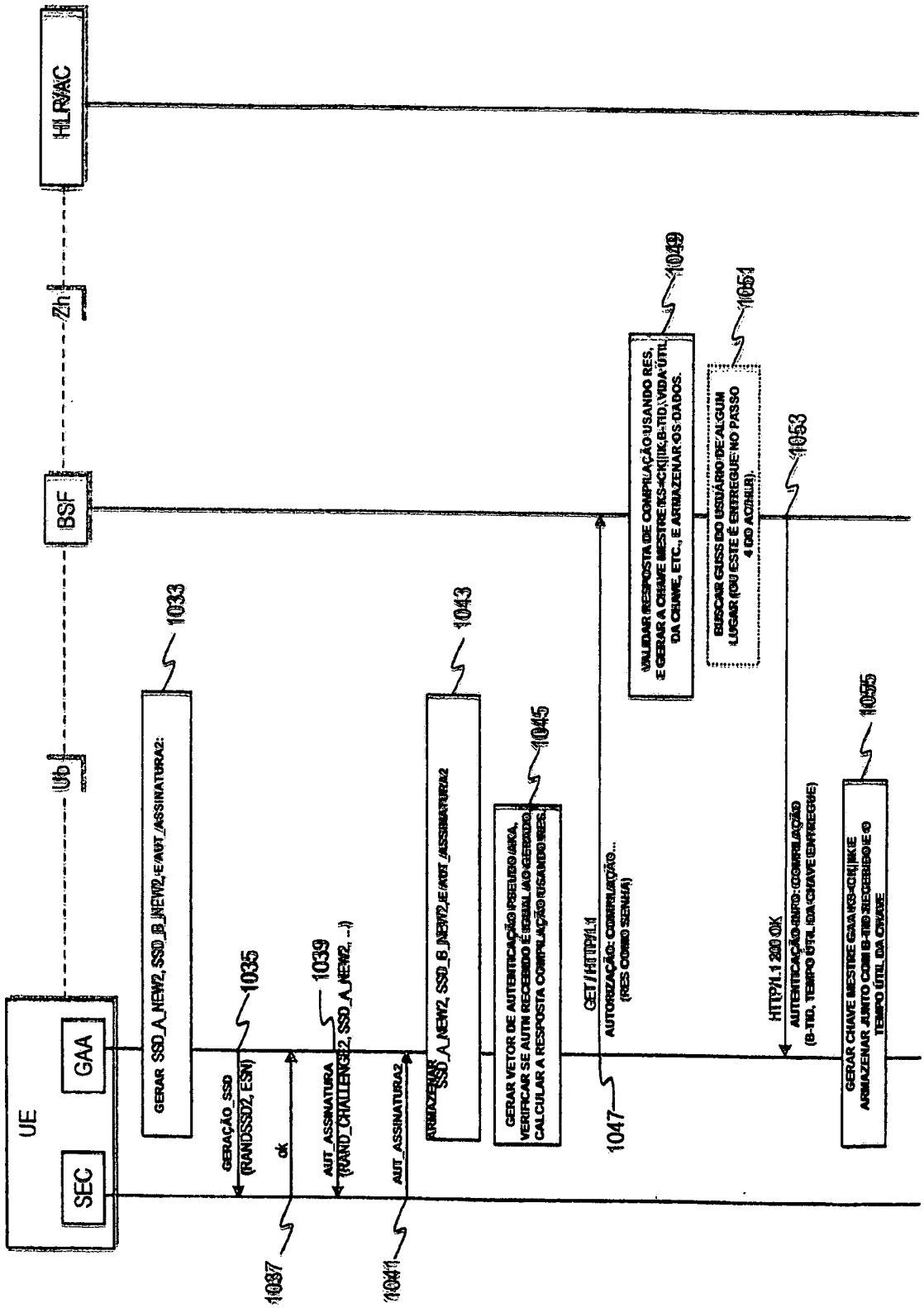
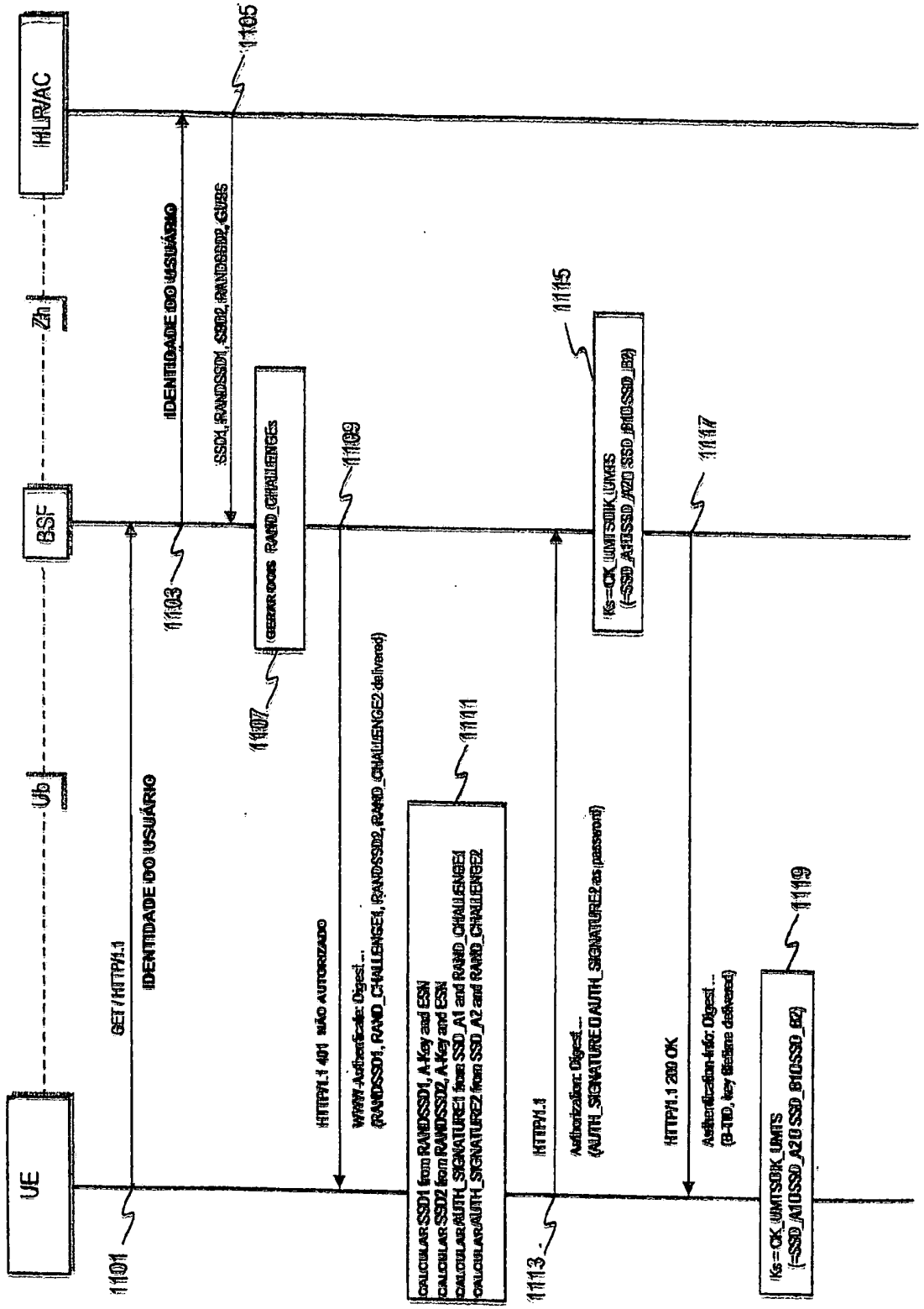

UE
SEC
GAA
Ub
BSF
Zh
HLR/AC
GERAR SSD_A_NEW2, SSD_B_NEW2, E AUT_ASSINATURA2:
1033
GERAÇÃO_SSD (RANDSSD2, ESN)
1035
ok
AUT_ASSINATURA (RAND_CHALLENGE2, SSD_A_NEW2, ...)
1039
AUT_ASSINATURA2
1041
1037
ARMAZENAR SSD_A_NEW2, SSD_B_NEW2, E AUT_ASSINATURA2
1043
GERAR VETOR DE AUTENTICAÇÃO (RESPOSTA ESPERADA, VERIFICAR SE AUTN RECEBIDO É IGUAL AO GERADO, CALCULAR A RESPOSTA COMPILAÇÃO USANDO RES)
1045
GET / HTTP/1.1
AUTORIZAÇÃO: COMPILAÇÃO... (RES COMO SENHA)
1047
VALIDAR RESPOSTA DE COMPILAÇÃO USANDO RES, E GERAR A CHAVE MESTRE (KS-ICK||IK,B-TID,VIDA ÚTIL DA CHAVE, ETC., E ARMAZENAR OS DADOS.
1049
BUSCAR GUSS DO USUÁRIO DE ALGUM LUGAR (OU ESTE É ENTREGUE NO PASSO 4 DO ACIMA).
1051
HTTP/1.1 200 OK
AUTENTICAÇÃO-INFO: (COMPILAÇÃO (B-TID, TEMPO ÚTIL DA CHAVE ENTREGUE)
1053
GERAR CHAVE MESTRE GAA KS-ICK||IK E ARMAZENAR JUNTO COM B-TID RECEBIDO E O TEMPO ÚTIL DA CHAVE
1055

FIG. 11


UE
BSF
HLR/AC
Ub
Zh
GET / HTTP/1.1
IDENTIDADE DO USUÁRIO
1101
IDENTIDADE DO USUÁRIO
1103
SSD1, RANDSSD1, SSD2, RANDSSD2, CUBS
1105
GERAR CUBS, RAND_CHALLENGE1
1107
HTTP/1.1 401 NÃO AUTORIZADO
WWW-Authenticate: Digest ...
(RANDSSD1, RAND_CHALLENGE1, RANDSSD2, RAND_CHALLENGE2 delivered)
1109
CALCULAR SSD1 from RANDSSD1, A-Key and ESN
CALCULAR SSD2 from RANDSSD2, A-Key and ESN
CALCULAR AUTH_SIGNATURE1 from SSD_A1 and RAND_CHALLENGE1
CALCULAR AUTH_SIGNATURE2 from SSD_A2 and RAND_CHALLENGE2
1111
HTTP/1.1
Authorization: Digest ...
(AUTH_SIGNATURE1 AUTH_SIGNATURE2 as (password))
1113
Ks=CK_UMTSDIK_UMTS
(=SSD_A1 SSD_A2 SSD_B1 SSD_B2)
1115
HTTP/1.1 200 OK
Authentication-Info: Digest ...
(B-TID, key lifetime delivered)
1117
Ks=CK_UMTSDIK_UMTS
(=SSD_A1 SSD_A2 SSD_B1 SSD_B2)
1119

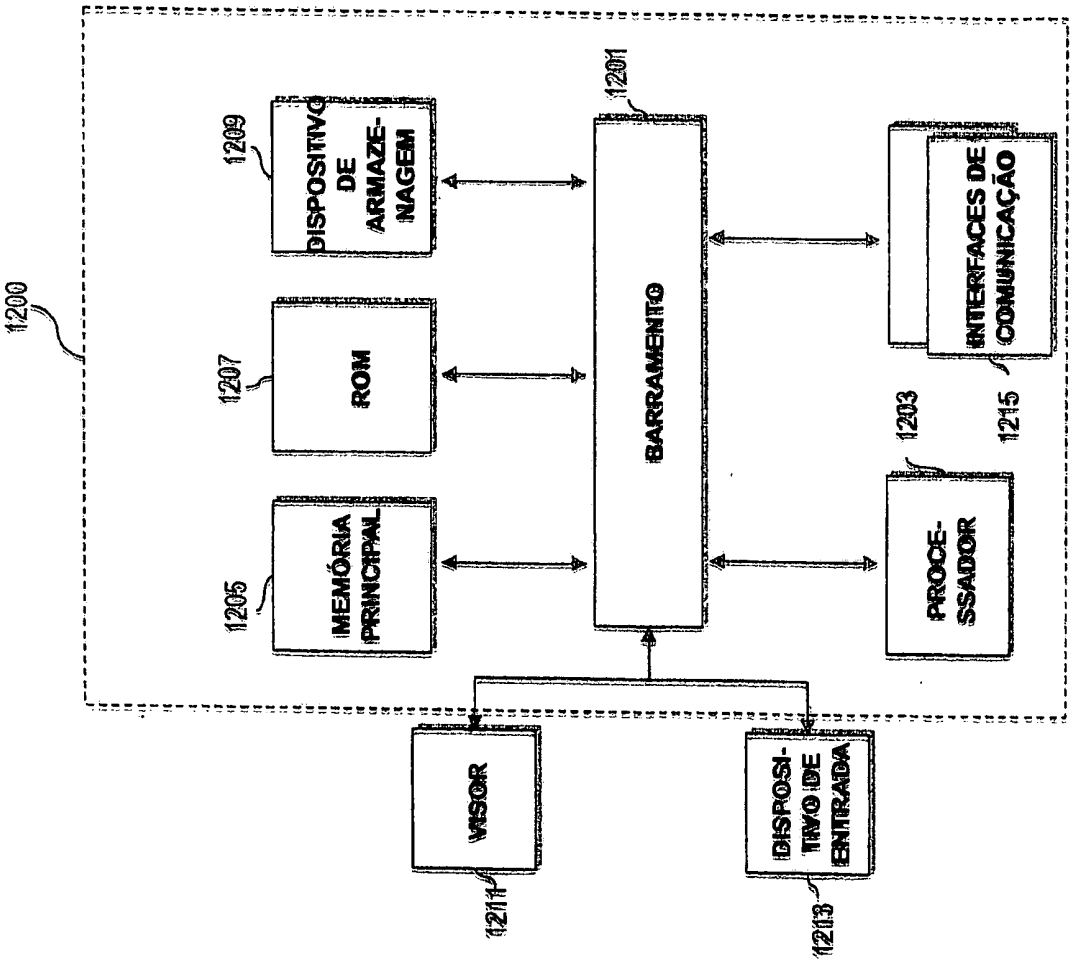

1200
1209
DISPOSITIVO DE ARMAZENAGEM
1207
ROM
1205
MEMÓRIA PRINCIPAL
1201
BARRAMENTO
INTERFACES DE COMUNICAÇÃO
1215
1203
PROCESSADOR
VISOR
1211
DISPOSITIVO DE ENTRADA
1213

FIG. 12

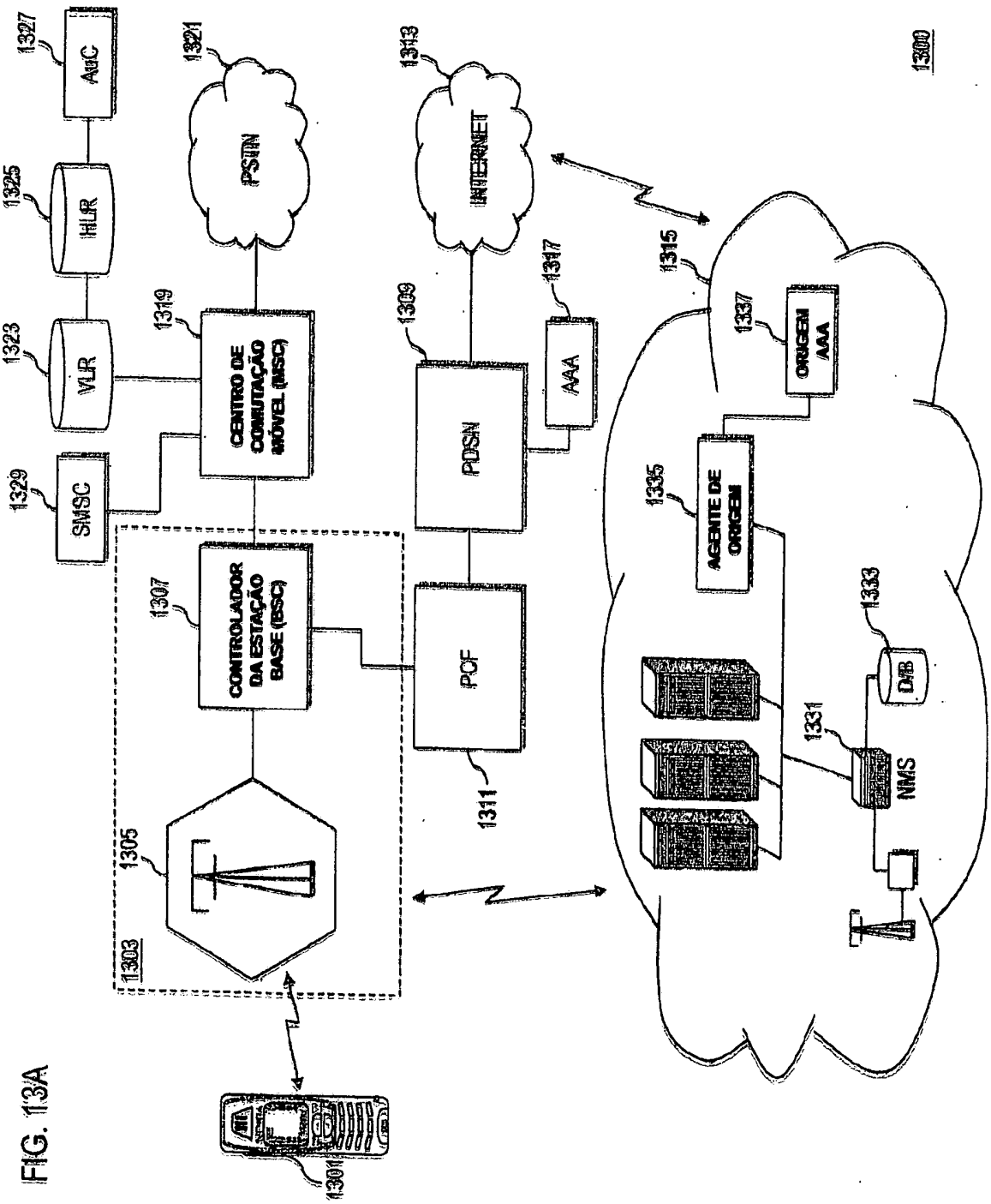

1327
AuC
1325
HLR
1323
VLR
1329
SMSC
1321
PSTN
1319
CENTRO DE COMUTAÇÃO MÓVEL (MSC)
1307
CONTROLADOR DA ESTAÇÃO BASE (BSC)
1305
1303
1301
1313
INTERNET
1309
PDSN
1317
AAA
1311
PCF
1315
1337
ORIGEM AAA
1335
AGENTE DE ORIGEM
1333
DMB
1331
NMS
1300

FIG. 13A

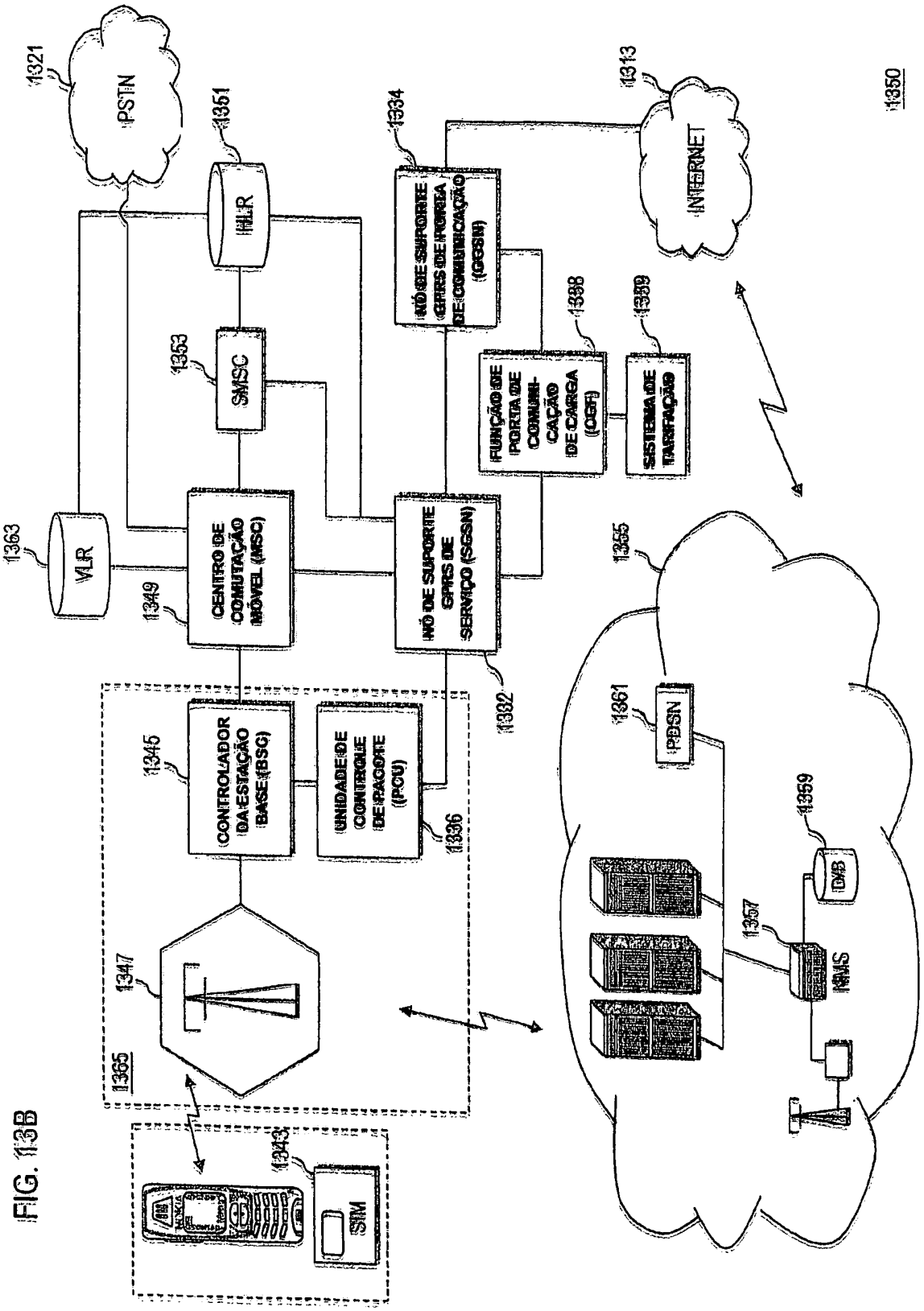

1321
PSTN
1351
HLR
1353
SMSC
1334
NÓ DE SUPORTE GPRS DE PASSAGEM DE COMUNICAÇÃO (GGSN)
1313
INTERNET
1350
1338
FUNÇÃO DE PORTA DE COMUNICAÇÃO DE CARGA (OCF)
1339
SISTEMA DE TARIFAÇÃO
1363
VLR
1349
CENTRO DE COMUTAÇÃO MÓVEL (MSC)
NÓ DE SUPORTE GPRS DE SERVIÇO (SGSN)
1332
1355
1345
CONTROLADOR DA ESTAÇÃO BASE (BSC)
UNIDADE DE CONTROLE DE PACOTE (PCU)
1336
1361
PDSN
1359
DMB
1357
NMS
1347
1365
1343
SIM

FIG. 13B

FIG. 14

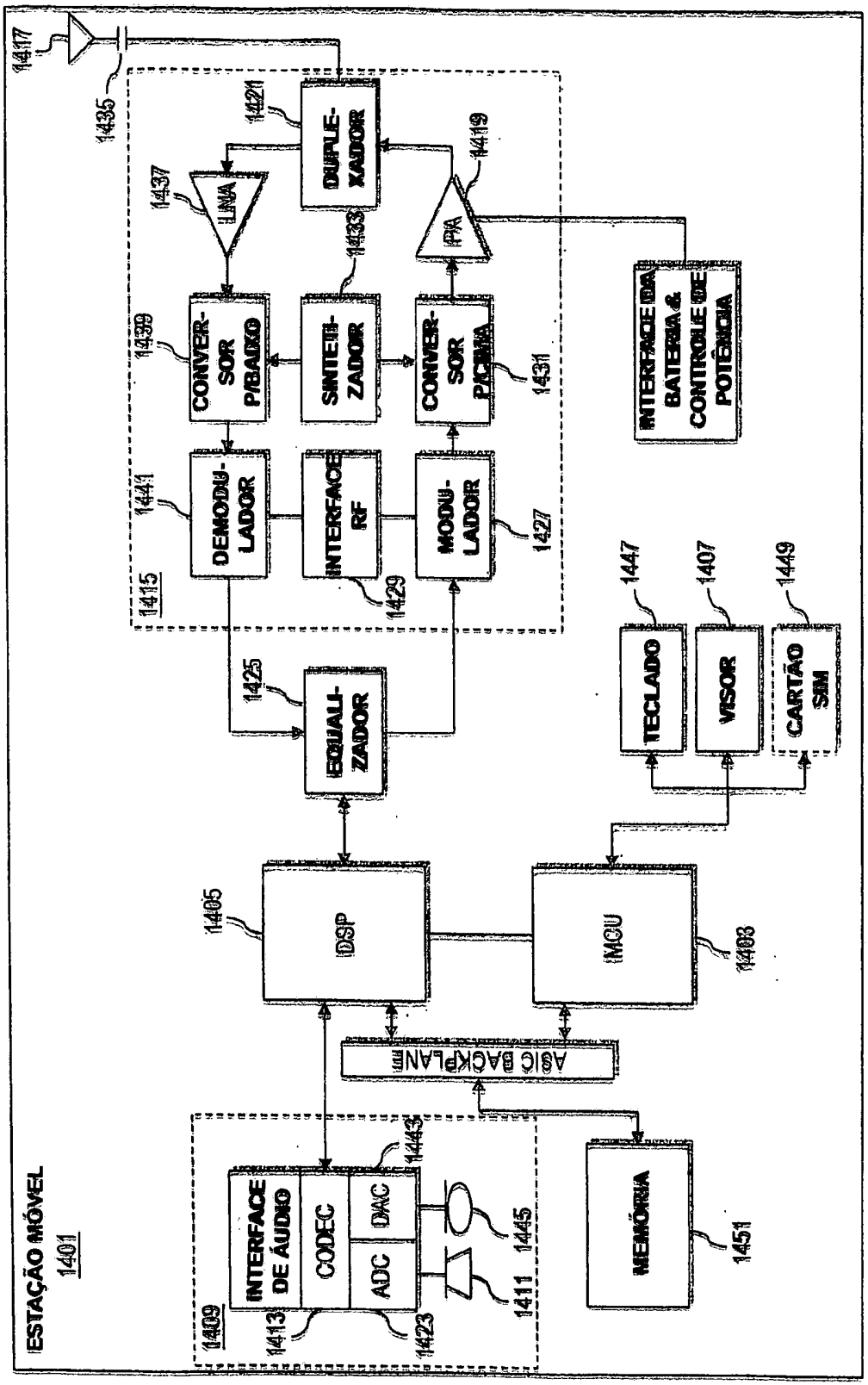
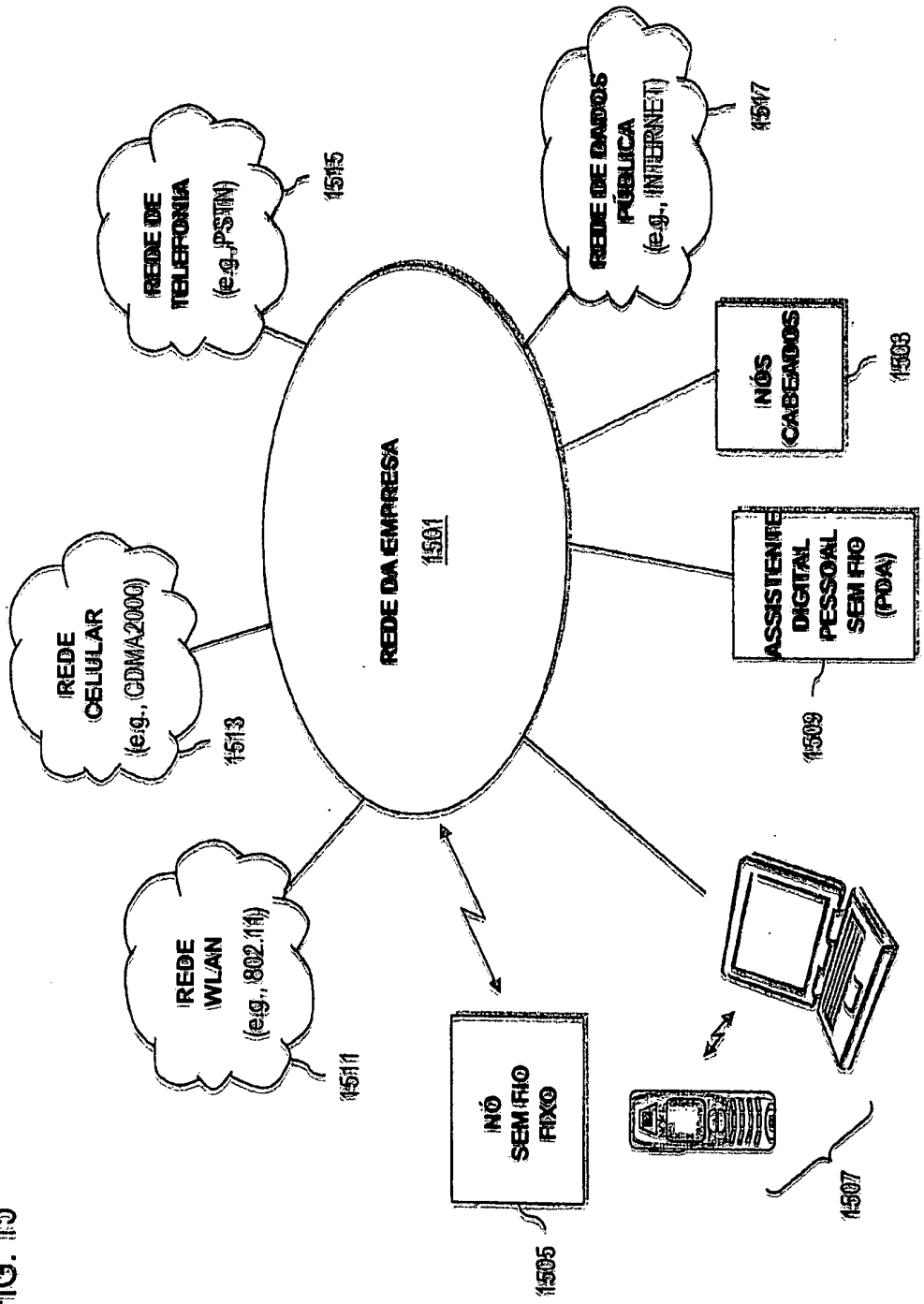

ESTAÇÃO MÓVEL
1401
1417
1435
1421
DUPLE-XADOR
1437
LNA
1419
PA
1433
1439
CONVER-SOR P/BAIXO
SINTETI-ZADOR
CONVER-SOR P/ALTA
1431
INTERFACE DA BATERIA & CONTROLE DE POTÊNCIA
1441
DEMODU-LADOR
INTERFACE RF
MODU-LADOR
1427
1415
1429
1425
EQUALI-ZADOR
1447
TECLADO
1407
VISOR
1449
CARTÃO SIM
1405
DSP
MCU
1403
ASIC BACKPLANE
1443
INTERFACE DE ÁUDIO
CODEC
DAC
ADC
1445
1411
1409
1413
1423
MEMÓRIA
1451

FIG. 15


REDE DA EMPRESA
1501
REDE DE TELEFONIA (e.g., PSTN)
1515
REDE DE DADOS PÚBLICA (e.g., INTERNET)
1517
NÓS CABEADOS
1503
ASSISTENTE DIGITAL PESSOAL SEM FIO (PDA)
1509
REDE CELULAR (e.g., CDMA2000)
1513
REDE WLAN (e.g., 802.11)
1511
NÓ SEM FIO FIXO
1505
1507

RESUMO

"MÉTODO E APARELHO PARA PROVER OS PROCEDIMENTOS DE AUTO-CARREGAMENTO NA REDE DE COMUNICAÇÃO".

Uma aproximação é fornecida para executar a autenticação no sistema de comunicação. Em uma incorporação, a chave é estabelecida com o terminal na rede de comunicação de acordo com o protocolo de acordo de chave. A chave acordada é fixada para o procedimento de autenticação para prover uma associação de segurança que suporta a reutilização da chave. A chave mestre é gerada baseado na chave acordada. Em outra incorporação, a autenticação de compilação é combinada com os parâmetros de troca de chave (ex., os parâmetros Diffie Hellman) na carga útil da mensagem de compilação, na qual a chave (ex., SMEKEY ou MN-AAA) é utilizada como senha. Em ainda outra incorporação, o algoritmo de autenticação (ex., Autenticação Celular e Cifragem de Voz (CAVE)) é empregado com o protocolo de acordo de chave com as funções de conversão para suportar o auto-carregamento.

REIVINDICAÇÕES

1. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- estabelecer uma chave com o terminal na rede de comunicação de acordo com o protocolo de acordo de chave, onde o terminal é configurado para operar usando o espectro de dispersão;

- fixar a chave acordada para o procedimento de autenticação para prover uma associação de segurança que suporta a reutilização da chave; e

- gerar a chave mestre baseada na chave acordada.

2. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que também compreende gerar uma mensagem de desafio da chave acordada de acordo com o procedimento de autenticação.

3. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que também compreende gerar uma mensagem de desafio da mensagem de acordo de chave trocada com o terminal de acordo com o protocolo de acordo de chave.

4. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o protocolo de acordo de chave inclui o esquema de troca de chave Diffie-Hellman.

5. Método de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que o acordo de chave é executado no túnel de segurança da camada de transporte (TLS).

6. Método de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que o terminal é configurado para comunicar usando o espectro de dispersão e executa o auto-carregador de acordo com a arquitetura de autenticação genérica.

7. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o procedimento de autenticação inclui o protocolo de autenticação do estabelecimento de comunicação de desafio (CHAP).

8. Método de autenticação, **CARACTERIZADO** pelo fato de que

compreende:

- estabelecer uma chave compartilhada com o elemento de rede na rede de comunicação de acordo com o protocolo de acordo de chave, onde o elemento de rede é configurado para fixar a chave acordada para o procedimento de autenticação para prover a associação de segurança que suporta a reutilização da chave; e

- gerar a chave mestre baseado na chave acordada.

9. Método de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o protocolo de acordo de chave inclui o esquema de troca de chave Diffie-Hellman.

10. Método de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o acordo de chave é executado no túnel de segurança da camada de transporte (TLS).

11. Método de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que também compreende:

- comunicar com o elemento de rede usando o Acesso Múltiplo por Divisão de Código (CDMA); e

- executar o auto-carregador de acordo com a arquitetura de autenticação genérica.

12. Método de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o procedimento de autenticação inclui o protocolo de autenticação do estabelecimento de comunicação de desafio (CHAP).

13. Aparelho de autenticação **CARACTERIZADO** pelo fato de que compreende:

- um módulo de autenticação configurado para estabelecer uma chave compartilhada com o elemento de rede na rede de comunicação de acordo com o protocolo de acordo de chave, onde o elemento de rede é configurado para fixar a chave acordada para o procedimento de autenticação para prover a associação de segurança que suporta a reutilização da chave; e

- o módulo de autenticação sendo também configurado para gerar a

chave mestre baseado na chave acordada.

14. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o protocolo de acordo de chave inclui o esquema de troca de chave Diffie-Hellman.

15. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o acordo de chave é executado no túnel de segurança da camada de transporte (TLS).

16. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que também compreende um transceptor configurado para comunicar com o elemento de rede usando o espectro de dispersão, onde o módulo de autenticação é também configurado para executar o auto-carregador de acordo com a arquitetura de autenticação genérica.

17. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o procedimento de autenticação inclui o protocolo de autenticação do estabelecimento de comunicação de desafio (CHAP).

18. Sistema **CARACTERIZADO** pelo fato de que compreende o aparelho e o elemento de rede da reivindicação 13.

19. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- gerar uma mensagem para autenticar a comunicação com o elemento de rede configurado para executar o auto-carregador;

- estabelecer um campo de senha da mensagem para uma função da chave secreta; e

- especificar a informação de estabelecimento de chave dentro da carga útil da mensagem, onde a mensagem é transmitida de acordo com o protocolo de transporte para acessar a informação na rede de dados.

20. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que o protocolo de transporte inclui o protocolo de transferência de hipertexto.

21. Método de acordo com a reivindicação 19, **CARACTERIZADO**

pelo fato de que a informação de estabelecimento da chave inclui os parâmetros Diffie-Hellman.

22. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que também compreende estabelecer o campo do nome do usuário da mensagem para o identificador do terminal.

23. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que a função da chave secreta é a soma de verificação ou compilação.

24. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que a chave secreta é a chave de codificação da mensagem de sinalização (SMEKEY) ou a chave de autenticação, autorização e contabilidade do nó móvel (MN-AAA).

25. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- receber a mensagem do terminal, de acordo com o protocolo de transporte para acessar a informação na rede de dados, solicitar a autenticação, onde a mensagem inclui o campo de senha que é uma função da chave secreta e a carga útil contendo os parâmetros de especificação de informação de estabelecimento da chave para determinar outra chave secreta; e

- gerar uma chave mestre baseada nas chaves secretas.

26. Método de acordo com a reivindicação 25, **CARACTERIZADO** pelo fato de que o protocolo de transporte inclui o protocolo de transferência de hipertexto.

27. Método de acordo com a reivindicação 25, **CARACTERIZADO** pelo fato de que a informação de estabelecimento da chave inclui os parâmetros Diffie-Hellman.

28. Método de acordo com a reivindicação 25, **CARACTERIZADO** pelo fato de que a mensagem inclui o campo do nome do usuário da mensagem para o identificador do terminal.

29. Método de acordo com a reivindicação 25, **CARACTERIZADO** pelo fato de que a função da chave secreta é a soma de verificação ou compilação.

30. Método de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que a chave secreta é a chave de codificação da mensagem de sinalização (SMEKEY) ou a chave de autenticação, autorização e contabilidade do nó móvel (MN-AAA).

31. Aparelho para autenticação **CARACTERIZADO** pelo fato de que compreende um módulo de autenticação configurado para gerar uma mensagem para autenticar a comunicação com o elemento de rede configurado para executar o auto-carregador, e para estabelecer um campo de senha da mensagem para ser a função da chave secreta, a mensagem tendo uma carga útil que inclui a nova informação de estabelecimento da chave, onde a mensagem é transmitida de acordo com o protocolo de transporte para acessar a informação na rede de dados.

32. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que o protocolo de transporte inclui o protocolo de transferência de hipertexto que suporta as comunicações seguras na rede de dados.

33. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que a informação de estabelecimento da chave inclui os parâmetros Diffie-Hellman.

34. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que o módulo de autenticação é também configurado para estabelecer o campo do nome do usuário da mensagem para o identificador do terminal.

35. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que a função da chave secreta é a soma de verificação ou compilação.

36. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que a chave secreta é a chave de codificação da mensagem de sinalização (SMEKEY) ou a chave de autenticação, autorização e contabilidade do nó móvel (MN-AAA).

37. Aparelho de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que também compreende um transceptor configurado para comunicar com a estação base usando o espectro de dispersão, onde o módulo de autenticação é também configurado para executar o auto-carregador de acordo

com a arquitetura de autenticação genérica.

38. Sistema **CARACTERIZADO** pelo fato de que compreende o aparelho e o elemento de rede da reivindicação 31.

39. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- receber um pedido de autenticação especificando a identidade do usuário do terminal;

- direcionar a identidade do usuário para o registro de localização configurado para gerar, baseado na identidade do usuário, os parâmetros criptográficos incluindo os dados secretos randômicos, e os dados secretos gerados dos dados secretos randômicos de acordo com o algoritmo criptográfico;

- receber os parâmetros criptográficos gerados do registro de localização;

- gerar um vetor de autenticação ao converter os parâmetros criptográficos para os parâmetros de chave incluindo o símbolo de autenticação e a resposta de autenticação;

- transmitir o símbolo de autenticação para o terminal configurado para produzir a resposta de autenticação;

- validar a resposta de autenticação do terminal usando a resposta de autenticação do vetor de autenticação; e

- gerar a chave mestre baseada nos parâmetros da chave.

40. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que o pedido de autenticação é gerado de acordo com o protocolo de transferência de hipertexto.

41. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que a conversão dos parâmetros criptográficos para os parâmetros da chave inclui gerar a chave baseado nos dados secretos.

42. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que o vetor de autenticação inclui um número randômico que é baseado nos dados secretos randômicos, o vetor de autenticação também inclui

uma chave de cifragem, e uma chave de integridade.

43. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que o algoritmo criptográfico inclui um algoritmo de autenticação celular e cifragem de voz.

44. Método de acordo com a reivindicação 39, **CARACTERIZADO** pelo fato de que uma pluralidade de grupos de parâmetros criptográficos são gerados pelo registro de localização para uso na geração do vetor de autenticação.

45. Método de autenticação **CARACTERIZADO** pelo fato de que compreende:

- gerar um pedido de autenticação especificando a identidade do usuário;

- transmitir o pedido de autenticação para o elemento de rede configurado para prover o auto-carregamento, onde o elemento de rede direciona a identidade do usuário para o registro de localização configurado para gerar, baseado na identidade do usuário, os parâmetros criptográficos incluindo os dados secretos randômicos, e os dados secretos gerados dos dados secretos randômicos de acordo como algoritmo criptográfico, onde o elemento de rede gera o vetor de autenticação ao converter os parâmetros criptográficos para os parâmetros de chave incluindo um símbolo de autenticação e uma resposta de autenticação;

- receber o símbolo de autenticação do elemento de rede;

- produzir a resposta de autenticação baseado no símbolo de autenticação;

- determinar a resposta de compilação usando a resposta de autenticação;

- transmitir a resposta de compilação para o elemento de rede para validação; e

- gerar a chave mestre baseado nos parâmetros de chave.

46. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que o pedido de autenticação é gerado de acordo com o protocolo de transferência de hipertexto.

47. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que a conversão dos parâmetros criptográficos para os parâmetros da chave inclui gerar a chave baseado nos dados secretos.

48. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que o vetor de autenticação inclui um número randômico que é baseado nos dados secretos randômicos, o vetor de autenticação também inclui uma chave de cifragem, e uma chave de integridade.

49. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que o algoritmo criptográfico inclui um algoritmo de autenticação celular e cifragem de voz.

50. Método de acordo com a reivindicação 45, **CARACTERIZADO** pelo fato de que uma pluralidade de grupos de parâmetros criptográficos são gerados pelo registro de localização para uso na geração do vetor de autenticação.

51. Aparelho para autenticação **CARACTERIZADO** pelo fato de que compreende:

- um módulo de autenticação configurado para gerar um pedido de autenticação especificando a identidade do usuário;

- um transceptor configurado para transmitir o pedido de autenticação para o elemento de rede configurado para prover o auto-carregamento, onde o elemento de rede direciona a identidade do usuário para o registro de localização configurado para gerar, baseado na identidade do usuário, os parâmetros criptográficos incluindo os dados secretos randômicos, e os dados secretos gerados dos dados secretos randômicos de acordo com o algoritmo criptográfico, onde o elemento de rede gera o vetor de autenticação ao converter os parâmetros criptográficos para os parâmetros de chave incluindo um símbolo de autenticação e uma resposta de autenticação, onde o transceptor é também configurado para receber o símbolo de autenticação do elemento de rede, e o módulo de autenticação é também configurado para produzir a resposta de autenticação baseado no símbolo de autenticação, para determinar a resposta de compilação usando a resposta de autenticação, e para gerar uma chave mestre baseado nos

parâmetros da chave na validação da resposta de compilação pelo elemento de rede.

52. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que o pedido de autenticação é gerado de acordo com o protocolo de transferência de hipertexto.

53. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que a conversão dos parâmetros criptográficos para os parâmetros da chave inclui gerar a chave baseado nos dados secretos.

54. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que o vetor de autenticação inclui um número randômico que é baseado nos dados secretos randômicos, o vetor de autenticação também inclui uma chave de cifragem, e uma chave de integridade.

55. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que o algoritmo criptográfico inclui um algoritmo de autenticação celular e cifragem de voz.

56. Aparelho de acordo com a reivindicação 51, **CARACTERIZADO** pelo fato de que uma pluralidade de grupos de parâmetros criptográficos são gerados pelo registro de localização para uso na geração do vetor de autenticação.

57. Sistema **CARACTERIZADO** pelo fato de que compreende o aparelho da reivindicação 51 e o elemento de rede.

RESUMO

"MÉTODO E APARELHO PARA PROVER OS PROCEDIMENTOS DE AUTO-CARREGAMENTO NA REDE DE COMUNICAÇÃO".

Uma aproximação é fornecida para executar a autenticação no sistema de comunicação. Em uma incorporação, a chave é estabelecida com o terminal na rede de comunicação de acordo com o protocolo de acordo de chave. A chave acordada é fixada para o procedimento de autenticação para prover uma associação de segurança que suporta a reutilização da chave. A chave mestre é gerada baseado na chave acordada. Em outra incorporação, a autenticação de compilação é combinada com os parâmetros de troca de chave (ex., os parâmetros Diffie Hellman) na carga útil da mensagem de compilação, na qual a chave (ex., SMEKEY ou MN-AAA) é utilizada como senha. Em ainda outra incorporação, o algoritmo de autenticação (ex., Autenticação Celular e Cifragem de Voz (CAVE)) é empregado com o protocolo de acordo de chave com as funções de conversão para suportar o auto-carregamento.