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

(21) BR 112019028219-0 A2

(22) Data do Depósito: 03/08/2018

(43) Data da Publicação Nacional: 07/07/2020

(54) Título: MÉTODO PARA AUTENTICAR UMA TRANSAÇÃO DESEMPENHADA POR UM EQUIPAMENTO DE USUÁRIO DE COMUNICAÇÃO MÓVEL

(51) Int. Cl.: H04M 15/00; H04W 12/04; H04W 12/06; H04W 12/10.

(30) Prioridade Unionista: 03/08/2017 EP 17184733.8.

(71) Depositante(es): IPCOM GMBH & CO. KG.

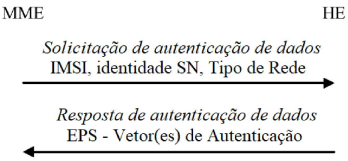
(72) Inventor(es): ACHIM LUFT; MARTIN HANS.

(86) Pedido PCT: PCT EP2018071160 de 03/08/2018

(87) Publicação PCT: WO 2019/025603 de 07/02/2019

(85) Data da Fase Nacional: 30/12/2019

(57) Resumo: A presente invenção provê um método para autenticar uma transação desempenhada por um equipamento de usuário de comunicação móvel, UE, dispositivo que tenha desempenhado um procedimento de autenticação e acordo de chave entre o dispositivo UE e uma entidade de gerenciamento móvel de uma rede visitada, a fim de estabelecer um contexto seguro entre o dispositivo UE e a rede visitada, o método compreendendo enviar uma mensagem de validação de serviço do dispositivo UE para a rede visitada, a mensagem de validação de serviço que é assinada digitalmente pelo dispositivo UE usando uma chave de proteção de integridade compartilhada entre o dispositivo UE e uma rede de operadora doméstica; e encaminhar a mensagem de validação de serviço da rede visitada para a rede de operadora doméstica.



MÉTODO PARA AUTENTICAR UMA TRANSAÇÃO DESEMPENHADA POR UM EQUIPAMENTO DE USUÁRIO DE COMUNICAÇÃO MÓVEL

[0001] A presente invenção se refere à transmissão de mensagens de validação de serviço por um dispositivo de equipamento de usuário (UE) em um sistema de comunicações móveis.

[0002] As redes GSM, UMTS e EPC (núcleo de pacote evoluído) proveem funções que implementam mecanismos de cobrança off-line e/ou online nos portadores, níveis de subsistema e serviço. A fim de suportar esses mecanismos de cobrança, a rede desempenha o monitoramento em tempo real do uso de recursos nos três níveis acima, a fim de detectar os eventos cobráveis relevantes.

[0003] Na cobrança *off-line*, um uso de recurso é relatado de uma rede para um domínio de faturamento (BD) depois que o uso do recurso tenha ocorrido. Na cobrança *on-line*, uma conta de assinante, localizada em um sistema de cobrança *on-line* (OCS), é consultada antes de conceder permissão para usar os recursos de rede solicitados.

[0004] Exemplos típicos de uso de recurso de rede são chamadas de voz de determinada duração, o transporte de um determinado volume de dados ou o envio de uma mensagem multimídia de um determinado tamanho. Os pedidos de utilização de recursos de rede podem ser iniciados pelo UE ou pela rede.

[0005] A cobrança off-line é um processo onde as informações de cobrança para uso de recurso de rede são coletadas simultaneamente com esse uso de recurso. A informação de cobrança é então passada através de uma cadeia de funções lógicas de cobrança. No final desse processo, os arquivos de registro de dados de cobrança (CDR) são gerados pela rede, que são então transferidos para o domínio de faturamento da operadora de rede para o faturamento de assinante e/ou contabilidade entre operadoras (ou funções adicionais, por exemplo, estatísticas, à critério da operadora). O BD tipicamente compreende sistemas de pós-

processamento, tais como o sistema de faturamento da operadora ou do dispositivo de mediação de faturamento. Em conclusão, a cobrança *off-line* é um mecanismo onde a informação de cobrança não afeta, em tempo real, o serviço prestado.

[0006] A cobrança *on-line* é um processo em que as informações de cobrança para uso de recurso de rede são coletadas simultaneamente com esse uso de recurso da mesma maneira que a cobrança *off-line*. Contudo, a autorização para o uso de recurso de rede deve ser obtida pela rede antes que o uso real dos recursos ocorra. Esta autorização é concedida pelo OCS mediante solicitação da rede.

[0007] Quando recebe uma solicitação de uso de recurso de rede, a rede reúne as informações de cobrança relevantes e gera um evento de cobrança para o OCS em tempo real. O OCS, então, retorna uma autorização de uso de recurso apropriada. A autorização de uso de recurso pode ser limitada em seu âmbito (por exemplo, volume de dados ou duração), portanto, a autorização pode ter que ser renovada de tempo em tempo, desde que o uso de recursos de rede do usuário persista.

[0008] A cobrança *on-line* é um mecanismo onde as informações de cobrança podem afetar, em tempo real, o serviço prestado e, portanto, é solicitada uma interação direta do mecanismo de cobrança com o controle do uso de recurso de rede.

[0009] Uma função de ativação de cobrança (CTF) gera eventos de cobrança com base na observação do uso de recurso de rede. Uma função de dados de cobrança (CDF) recebe eventos de cobrança da CTF por meio do chamado ponto de referência Rf. A CDF então usa as informações contidas nos eventos de cobrança para construir CDRs. Os CDRs produzidos pela CDF são transferidos imediatamente para uma função de *gateway* de cobrança (CGF) por meio do chamado ponto de referência Ga. A CGF atua como um *gateway* entre a rede 3GPP e o BD. Ela usa o chamado ponto de referência Bx para a transferência de arquivos

CDR para o BD. A OCF consiste em dois módulos distintos, ou seja, uma função de cobrança com base em sessão (SBCF) e uma função de cobrança com base em eventos (EBCF).

[0010] A SBCF é responsável pela cobrança *on-line* de rede/sessões de usuário, por exemplo, chamadas de voz, portadores de IP CAN, sessão de IP CAN ou sessões de IMS.

[0011] A EBCF desempenha cobrança on-line com base em evento em conjunto com qualquer servidor de aplicativos ou serviço NE, inclusive servidores de aplicativos SIP.

[0012] Uma função de avaliação (RF) determina um valor do uso de recurso de rede (descrito no evento de cobrança recebido pelo OCF da rede) em nome da OCF.

[0013] Um sistema de cobrança *off-line* (OFCS) é um agrupamento de funções de cobranças usadas para cobrança *off-line*. Ele coleta e processa eventos de cobrança de um ou mais CTFs e gera CDRs para os processos de faturamento a jusante *off-line* posteriores.

[0014] Caso um assinante esteja em *roaming* e servido por uma rede visitada, ambos os sistemas de cobrança (na rede visitada e na rede doméstica) cobrarão o assinante separadamente. As cobranças de *roaming* geralmente são por minuto para chamadas de voz (cobrança diferente para chamadas de voz originadas e terminadas por celular), por SMS e por volume de dados por *megabyte*. Por questões de cobrança, ambas as redes se comunicam por meio de um procedimento de conta transferida (TAP). O mecanismo de transferência para TAP é um mecanismo chamado de aplicativos customizados para lógica aprimorada de rede móvel (CAMEL).

[0015] Para todos os serviços providos por uma rede visitada que são roteados através da rede doméstica, por exemplo, chamadas de voz, SMS, IMS, é possível que a operadora da rede doméstica valide todas as cobranças transferidas da rede de atendimento por meio do TAP. Já

existem alguns serviços que atualmente não são roteados pela rede doméstica, como interrupção local ao acesso de *internet* ou chamadas de voz por IP localmente roteadas (VoIP). Esses serviços servidos localmente provavelmente se tornarão mais populares. A operadora doméstica não possui um mecanismo para verificar as cobranças transferidas da rede de atendimento por meio do TAP para serviços roteados localmente. Atualmente, as operadoras devem confiar umas nas outras que os serviços pelos quais a rede de atendimento transmite cobranças foram realmente providos ao assinante em *roaming*. Há uma necessidade de um mecanismo que possibilite que a operadora doméstica valide as cobranças de *roaming*.

[0016] O documento US 2002/0161723 A1 descreve uma técnica na qual a identidade de um UE é validada usando chaves armazenadas no UE e um centro de autenticação de maneira convencional. Quando o UE está conectado a uma rede local que não a sua rede doméstica, uma chave secreta compartilhada, compartilhada pela operadora de rede doméstica e o UE, é usada para validar o UE com a operadora de rede local. Se um usuário do UE desejar fazer uma compra fazendo uso do UE para autorizar o pagamento, as mensagens serão trocadas com um vendedor usando uma rede de comunicação diferente, com o UE assinando uma mensagem do vendedor para indicar a aceitação da transação. Um serviço de verificação de assinatura de rede é então usado para verificar a assinatura. O serviço de verificação de assinatura é diferenciado da rede doméstica e da rede local. Como descrito, tanto o UE quanto o serviço de verificação de assinatura são providos com a chave de assinatura.

[0017] O documento WO 2005/004456 descreve um mecanismo para cobrar um usuário de um UE que usa uma rede visitada na qual uma rede doméstica emite certificados contábeis que são enviados ao UE, que possibilita que o UE proveja esses ao provedor de serviços da rede visitada.

[0018] A presente invenção provê um método para autenticar uma transação desempenhada por um equipamento de usuário de comunicação móvel, UE, dispositivo que tenha desempenhado um procedimento de autenticação e acordo de chave entre o dispositivo UE e uma entidade de gerenciamento móvel de uma rede visitada, a fim de estabelecer um contexto de segurança entre o dispositivo UE e a rede visitada, o método compreendendo enviar uma mensagem de validação de serviço do dispositivo UE para a rede visitada, a mensagem de validação de serviço que é assinada digitalmente pelo dispositivo UE usando uma chave de proteção de integridade compartilhada entre o dispositivo UE e uma rede doméstica; e encaminhar a mensagem de validação de serviço da rede visitada para a rede doméstica.

[0019] A presente invenção provê um mecanismo que fornece à operadora doméstica mais controle sobre as cobranças de *roaming* transferidas por meio do TAP. O consentimento do usuário pode fazer parte desse mecanismo. Um aspecto desse mecanismo é estabelecer um segredo compartilhado entre um UE e uma operadora doméstica e usar esse segredo compartilhado para gerar mensagens de validação de serviço protegidas por integridade. O segredo compartilhado também poderia ser usado para enviar mensagens protegidas por integridade da rede de operadora doméstica para o UE; por exemplo, uma lista com redes visitadas preferenciais ou permitidas. Várias alternativas são providas sobre como transferir essas mensagens de validação de serviço do UE para a operadora doméstica. A opção mais benéfica é aprimorar a CTF na rede visitada, assim as mensagens de validação de serviço geradas no UE em roaming são adicionadas aos CDRs gerados na rede de atendimento e encaminhadas à operadora doméstica por meio de mensagens de cobrança TAP. Existem também várias alternativas para compartilhar um segredo entre um UE e uma rede doméstica que é desconhecida da rede visitada. Uma opção é executar uma função de autenticação e acordo de chave

(AKA) duas vezes, mas não compartilhar a chave de proteção de integridade com a rede visitada na segunda execução. Uma vantagem desse método é que não há impacto nos cartões SIM existentes. Nas fases posteriores da padronização 5G, é possível que uma função de derivação de chave (KDF) será usada para derivar todas as chaves de sessão da rede doméstica para a rede visitada, isto é, a rede visitada não recebe as chaves da rede doméstica, mas as chaves dedicadas à rede visitada derivadas das chaves da rede doméstica. Nesse caso, a chave de proteção de integridade da rede doméstica, agora desconhecida da rede visitada, pode ser usada.

[0020] Aspectos particulares da invenção podem oferecer à operadora controle sobre as cobranças de *roaming* e/ou estabelecer cobranças mais confiáveis de *roaming* de acordos comerciais. Uma implementação da invenção pode ser com base em meios técnicos, em vez de confiança, e a invenção possibilita que um usuário evite fraudes relacionadas às cobranças de *roaming*.

[0021] Modalidades preferenciais da invenção serão agora descritas, somente a título de exemplos, em referência às figuras anexas, nas quais:

A Figura 1 é uma representação esquemática de uma entidade de gerenciamento móvel que solicita vetores de autenticação de um ambiente doméstico;

A Figura 2 é uma representação esquemática de um procedimento de autenticação e acordo de chave; e

A Figura 3 é um fluxograma de mensagem que ilustra uma modalidade da invenção.

[0022] Em uma primeira modalidade, um conhecido mecanismo de resposta de desafio inicial chamado de "autenticação e acordo de chave" (AKA), no qual as chaves de sessão são geradas, é executado duas vezes para gerar duas chaves de integridade diferentes. Em um cenário de

roaming de legado LTE, a AKA é desempenhada entre um UE e uma entidade de gerenciamento de mobilidade (MME) da rede de atendimento uma vez. A MME solicita um vetor de autenticação da operadora doméstica, que inclui o desafio, a chave da sessão raiz K_{ASME} e a resposta esperada para o desafio. A MME envia o desafio para o UE; o UE calcula a resposta a este desafio e a chave da sessão raiz correspondente. O UE envia a resposta de volta para a MME. A MME verifica a resposta com a ajuda da resposta esperada. A chave de sessão gerada é armazenada junto com um identificador KSI_{ASME} no UE e na MME e é usada para estabelecer um contexto de segurança para o UE. O procedimento AKA é descrito no 3GPP TS 33.401 v15.0.0.

[0023] Nesta modalidade, o procedimento AKA é desempenhado duas vezes. A primeira execução é como descrita acima. Na segunda execução, apenas o desafio e a resposta esperada são transferidos da rede doméstica para a rede de atendimento, isto é, uma chave raiz da sessão $K_{ASME}2$ é mantida na rede doméstica e não é fornecida à rede de atendimento (visitada). Uma raiz para a hierarquia de chaves da sessão para o contexto de segurança entre a rede de atendimento e o UE é o $K_{ASME}1$ e a chave de proteção de integridade para a mensagem de confirmação de serviço é derivada da $K_{ASME}2$. Uma vez que a rede de atendimento não tem conhecimento da $K_{ASME}2$, as mensagens de validação de serviço protegidas por integridade, assinadas com a chave de proteção de integridade que somente o UE e a operadora doméstica compartilham entre si, não podem ser geradas pela rede de atendimento, mas somente pelo UE. Caso a rede de atendimento altere o conteúdo da mensagem de validação de serviço, a verificação de integridade na rede doméstica irá falhar.

[0024] A Figura 1 ilustra uma MME solicitando um ou mais vetores de autenticação de um banco de dados de assinante no ambiente

doméstico (HE) da rede da operadora doméstica. O procedimento AKA é ilustrado na Figura 2 (estado da técnica).

[0025] Em lançamentos de padronização posteriores, as chaves de sessão atuais conhecidas na rede doméstica podem não ser encaminhadas da operadora doméstica para a rede de atendimento. Por conseguinte, em uma segunda modalidade, as chaves de sessão da operadora doméstica permanecem somente com a operadora doméstica e, em vez disso, as chaves de sessão usadas na rede de atendimento serão derivadas das chaves existentes na rede doméstica e no UE. Neste caso, o procedimento acima de uma segunda execução de AKA é obsoleto, pois o UE e a operadora doméstica podem proteger por integridade a sua comunicação por meio das chaves de sessão da operadora doméstica.

[0026] Se as mensagens de validação de serviço são uma característica opcional que é somente desempenhada pelo UE e pela rede de atendimento no caso de solicitação da rede doméstica, é então necessário sinalizar a solicitação da rede da operadora doméstica para a rede de atendimento. É benéfico adicionar as informações na resposta para a solicitação de autenticação do HE para a MME na rede de atendimento. Em uma terceira modalidade, a rede da operadora doméstica solicita mensagens de validação de serviço em uma ou mais mensagens dedicadas à rede de atendimento. Em uma quarta modalidade, o HE solicita mensagens de autenticação de serviço da rede de atendimento de maneira implícita ao responder com um vetor de autenticação mais do que o solicitado.

[0027] Além disso, o UE precisa receber uma solicitação para gerar mensagens de validação de serviço. Essa solicitação pode ser enviada como informação adicional da rede da operadora doméstica ou da rede de atendimento no processo de autenticação, por exemplo, em uma mensagem de comando no modo de segurança *non-access stratum* (NAS). Em outra modalidade, as mensagens de validação de serviço são

solicitadas pela rede de atendimento para o UE em uma ou mais mensagens dedicadas. Em uma modalidade, a rede de atendimento solicita mensagens de validação de serviço durante um procedimento de conexão, por exemplo, durante o processo de autenticação ou instalação do contexto de segurança. Em outra modalidade, a rede de atendimento solicita mensagens de validação de serviço por portador durante o procedimento de instalação de portador. É benéfico para a rede de atendimento solicitar uma periodicidade correspondente para a geração de mensagens de validação de serviço no UE. Em outra modalidade, o UE decide a periodicidade com base nas informações de política armazenadas providas pela rede da operadora doméstica.

[0028] Se as mensagens de validação de serviço são solicitadas e em que periodicidade o UE é solicitado para gerar mensagens de validação de serviço é a critério da operadora doméstica. Pode ser uma política por assinante ou por classe de acesso ou com base nas capacidades do UE. Em uma modalidade, uma política de mensagens de validação de serviço é armazenada no HE da rede da operadora doméstica. Em outra modalidade, a política de mensagens de validação de serviço faz parte de uma função de controle e cobrança de política (PCCF).

[0029] As mensagens de validação de serviço enviadas do UE por meio da rede visitada para a rede doméstica têm que ser protegidas contra ataques de repetição. Isso poderia ser realizado com estampas temporais ou números de sequência de mensagens ou ambos. A primeira mensagem de validação de serviço poderia ser uma validação antecipada, isto é, ela valida a instalação ou a recepção de uma configuração para instalação de um serviço sem que uma provisão de serviço significativa seja validada. Essa primeira mensagem de validação de serviço deve incluir uma estampa temporal ou o número de sequência 1 e quando a segunda mensagem de validação pode ser esperada; por exemplo, em um minuto ou no tráfego de dados em *roaming* de 100 *Kbytes* ou no final de uma ligação.

A partir da segunda mensagem de validação de serviço, (para cada serviço), as mensagens poderiam incluir informações adicionais de *feedback* do período de serviço anterior, tal como qualidade da chamada de voz do minuto anterior da chamada de voz ou taxa de dados do último tráfego de dados móveis em roaming de 100 *Kbytes*.

[0030] A seguir, é apresentado um exemplo de tal mensagem de validação de serviço.

ID	Ver	SEQ	TS	P	SID	FB	MAC

ID. Identificação do assinante; por exemplo, GUTI (ID temporária única global)

Ver: Informações sobre a versão do protocolo

SEQ: Número de sequência da mensagem; por exemplo, 16 *bits*

TS: Estampa temporal

P: Periodicidade esperada das mensagens de validação de serviço para este serviço

SID: Identificador de serviço (por exemplo, serviço de dados de interrupção local, chamada de voz, ID da sessão do portador ou da PDU)

FB: Informações de *feedback* para o serviço atual

MAC: Código de autenticação de mensagem como proteção de integridade com chave de sessão compartilhada.

[0031] Um fluxograma de mensagem exemplar é mostrado na Figura 3. Um usuário liga seu UE em um país estrangeiro. O UE encontra, durante o procedimento de registro, etapa 1, uma rede de atendimento com a qual a operadora doméstica possui um acordo de roaming. Uma lista controlada por operadora doméstica de redes permitidas é armazenada no SIM. A rede de atendimento solicita, na etapa 2, um vetor de autenticação da operadora doméstica para o usuário em *roaming*. Uma entidade de gerenciamento de mobilidade MME da rede de atendimento solicita, na etapa 3, um ou mais vetores de autenticação AV de um ambiente doméstico HE da rede doméstica. O HE responde, na etapa 4, com o vetor de autenticação solicitado e um vetor de autenticação adicional. A MME da

rede doméstica encaminha, na etapa 5, uma chave de sessão para proteção de integridade derivada do vetor de autenticação adicional para uma função de *gateway* de cobrança. A rede de atendimento recebe, na etapa 6, dois vetores de autenticação AV. Um é completo como conhecido no estado da técnica e em um segundo AV, de acordo com a invenção, a raiz da hierarquia de chave de sessão (pelo menos a chave da sessão para proteção de integridade) não está incluída. A recepção de um vetor de autenticação adicional pode sinalizar implicitamente a rede de atendimento que as mensagens de validação de serviço são solicitadas à rede da operadora doméstica. Esta solicitação também pode ser de maneira explicita com uma solicitação de validação de serviço NAS dentro de mensagens entre a MME e o HE, de acordo com o 3GPP TS 33.401. A AKA executada como parte do procedimento de autenticação no estado da técnica, de acordo com TS 33.401, não é mostrada na figura. A rede de atendimento, então, executa um segundo procedimento AKA (ou o potencial sucessor AKA*), na etapa 7, no qual a rede de atendimento sinaliza em uma mensagem de comando do modo de segurança NAS para o UE que a chave da sessão para proteção de integridade dessa execução adicional da AKA deve ser usada para assinar mensagens de validação de serviço e que essas mensagens de validação de serviço são solicitadas. O UE confirma, na etapa 8, a solicitação na mensagem completa de modo de segurança NAS para a rede de atendimento. A chave de proteção de integridade resultante da segunda execução AKA é armazenada no UE a fim de gerar o campo MAC de mensagens de validação de serviço.

[0032] O usuário agora inicia uma chamada de voz roteada localmente e, portanto, uma primeira mensagem de validação de serviço é gerada no UE e enviada, na etapa 9, uma mensagem de validação de serviço NAS para a entidade de gerenciamento de mobilidade de atendimento (MME) da rede de atendimento. A primeira mensagem de validação de serviço contém a GUTI do usuário, o número de sequência da

mensagem "1", estampa temporal atual, periodicidade esperada de um minuto, como identificador de serviço "chamada de voz local", campo de informações de *feedback* vazio e um código de autenticação de mensagem válido para os sete primeiros campos da mensagem.

[0033] A rede de atendimento MME encaminha, na etapa 10, a mensagem de validação para a função de dados de cobrança CDF. A CDF também recebe, na etapa 11, uma mensagem de eventos de cobrança da função de ativação de cobrança CTF e gera um CDR e, de acordo com esta invenção, concatena a mensagem de validação de serviço para o CDR. Conforme as mensagens de validação de serviço são geradas pelo UE de maneira autônoma, configuradas ou influenciadas pela rede doméstica ou visitada. É benéfico sincronizar uma mensagem de validação de serviço com os CDRs, de modo que com cada CDR uma mensagem de validação de serviço correspondente é concatenada, mas uma solução não síncrona também seria possível. Nesse caso, um único CDR pode incluir zero, uma ou mais mensagens de validação, dependendo da disponibilidade da mensagem no CDR. Caso mais de uma mensagem de validação de serviço esteja contida em um único CDR, algumas poderão validar CDRs anteriores que não continham mensagens de validação de serviço.

[0034] O CDR (com a mensagem de validação de serviço concatenada) produzido pela CDF é transferido imediatamente, na etapa 12, para a função de *gateway* de cobrança CGF por meio do ponto de referência Ga. A CGF gera, na etapa 13, uma mensagem de cobrança TAP com a mensagem de validação de serviço incluída, que é transferida por meio da interface CAMEL sobre SS7 para a CGF da operadora doméstica. A CGF da operadora doméstica válida, na etapa 14, a mensagem de validação de serviço solicitada antes de prosseguir com o procedimento de cobrança.

[0035] Uma alternativa ao exposto acima é a geração de mensagens de validação de serviço com base em uma ativação da rede

visitada. A CDF ou qualquer outra entidade do sistema de cobrança da rede visitada pode ativar o UE em uma nova mensagem NAS ou com novas informações em uma mensagem NAS conhecida para gerar uma mensagem de validação de serviço, de modo a garantir que cada mensagem de cobrança TAP inclua uma mensagem de validação de serviço que valida o serviço cobrado. Nesta alternativa, como o UE não controla o tempo de geração de mensagens de validação de serviço, as mensagens podem não conter nenhuma informação sobre a próxima mensagem de validação de serviço esperada, isto é, não há informações de periodicidade.

[0036] As mensagens de validação de serviço podem ser geradas no UE para validar uma instalação ou provisão de um serviço por uma rede visitada (em *roaming*). A mensagem de validação de serviço pode compreender informações de serviço relacionadas a uma instalação de serviço ou provisionada pela rede visitada e uma assinatura que valida as informações de serviço para a rede doméstica.

[0037] A invenção provê em um aspecto uma transmissão da mensagem de validação de serviço para a rede visitada para transmissão para a rede doméstica em relação a uma informação de cobrança da visitada para a rede doméstica a cerca de uma instalação ou serviço provisionado a ser cobrado (CDR).

[0038] Em suma, esta invenção provê a transmissão de mensagens de validação de serviço por uma rede visitada para a rede doméstica em relação a uma informação de cobrança (CDR) da visitada para a rede doméstica a cerca de uma instalação ou serviço provisionado a ser cobrado. As mensagens de validação de serviço podem compreender proteção de integridade com uma chave compartilhada entre o UE e a operadora doméstica, proteção de reprodução com estampas temporais ou números de sequência de mensagens ou ambos, a primeira mensagem de validação de serviço com antecedência, periodicidade esperada das

seguintes mensagens em uma primeira mensagem ou em todas as mensagens, *feedback* para o último período de serviço, uma mensagem de validação de serviço por serviço; por exemplo, serviço de tráfego de dados e chamada de voz e mensagens de validação de serviço ativadas pela rede visitada, isto é, geradas sob demanda da rede visitada. Uma chave de proteção de integridade compartilhada entre o UE e a operadora doméstica é gerada por meio de uma segunda execução AKA ou alcançada ao derivar as chaves de sessão exclusivas para a rede de atendimento.

REIVINDICAÇÕES

1. Método para autenticar uma transação desempenhada por um equipamento de usuário de comunicação móvel, UE, dispositivo que tenha desempenhado um procedimento de autenticação e acordo de chave entre o dispositivo UE e uma entidade de gerenciamento móvel de uma rede visitada, a fim de estabelecer um contexto de segurança entre o dispositivo UE e a rede visitada, o método **caracterizado** pelo fato de que compreende:

enviar uma mensagem de validação de serviço do dispositivo UE para a rede visitada, a mensagem de validação de serviço que é assinada digitalmente pelo dispositivo UE usando uma chave de proteção de integridade compartilhada entre o dispositivo UE e uma rede doméstica; e

encaminhar a mensagem de validação de serviço da rede visitada para a rede doméstica.

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a chave de proteção de integridade é obtida ao desempenhar um segundo procedimento de autenticação e acordo de chave no qual a rede doméstica provê um vetor de autenticação que não contém uma raiz de uma hierarquia de chaves de sessão ou uma chave de sessão para proteção de integridade.

3. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a chave de proteção de integridade é obtida ao desempenhar um segundo procedimento de autenticação e acordo de chave, no qual a rede doméstica provê somente um desafio e uma resposta esperada ao desafio para a rede visitada.

4. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o contexto de segurança entre o dispositivo UE e a rede visitada é estabelecido usando uma chave de proteção de integridade derivada de uma chave existente na rede doméstica.

5. Método, de acordo com qualquer reivindicação anterior, **caracterizado** pelo fato de que a mensagem de validação de serviço inclui pelo menos uma dentre uma estampa temporal e um número de sequência de mensagem.

6. Método, de acordo com qualquer reivindicação anterior, **caracterizado** pelo fato de que a mensagem de validação de serviço é transmitida em resposta a uma solicitação.

7. Método, de acordo com a reivindicação 6, **caracterizado** pelo fato de que a solicitação é transmitida como parte de uma mensagem de *non-access stratum*.

8. Método, de acordo com uma das reivindicações de 1 a 6, **caracterizado** pelo fato de que a mensagem de validação de serviço é transmitida de maneira autônoma pelo dispositivo UE.

9. Método, de acordo com qualquer reivindicação anterior, **caracterizado** pelo fato de que a mensagem de validação de serviço é concatenada com um registro de dados de carregamento pela rede visitada e a mensagem concatenada é transmitida para uma função de *gateway* de carregamento da rede doméstica.

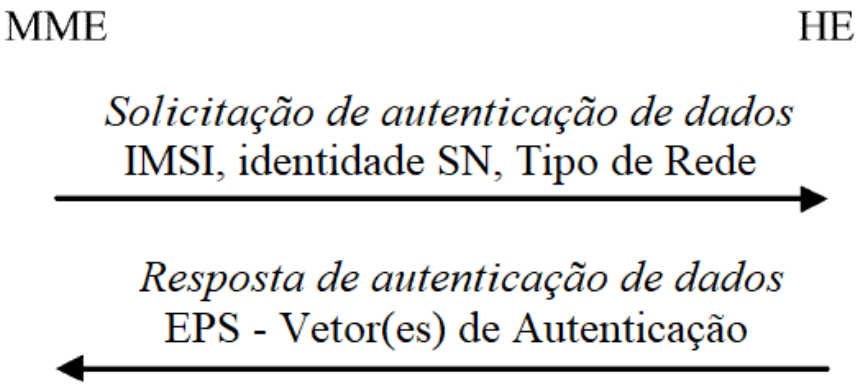

MME
HE
Solicitação de autenticação de dados
IMSI, identidade SN, Tipo de Rede
Resposta de autenticação de dados
EPS - Vetor(es) de Autenticação

Fig. 1

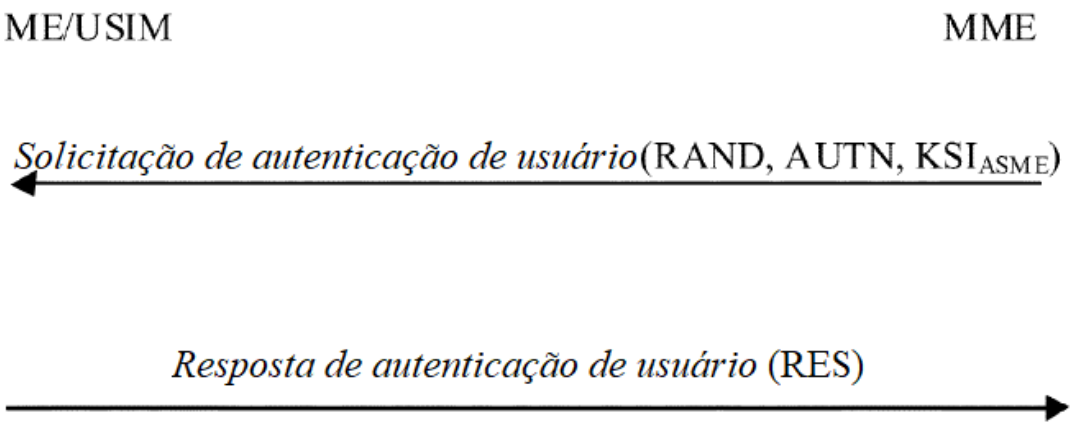

ME/USIM
MME
Solicitação de autenticação de usuário(RAND, AUTN, KSI_{ASME})
Resposta de autenticação de usuário (RES)

Fig. 2

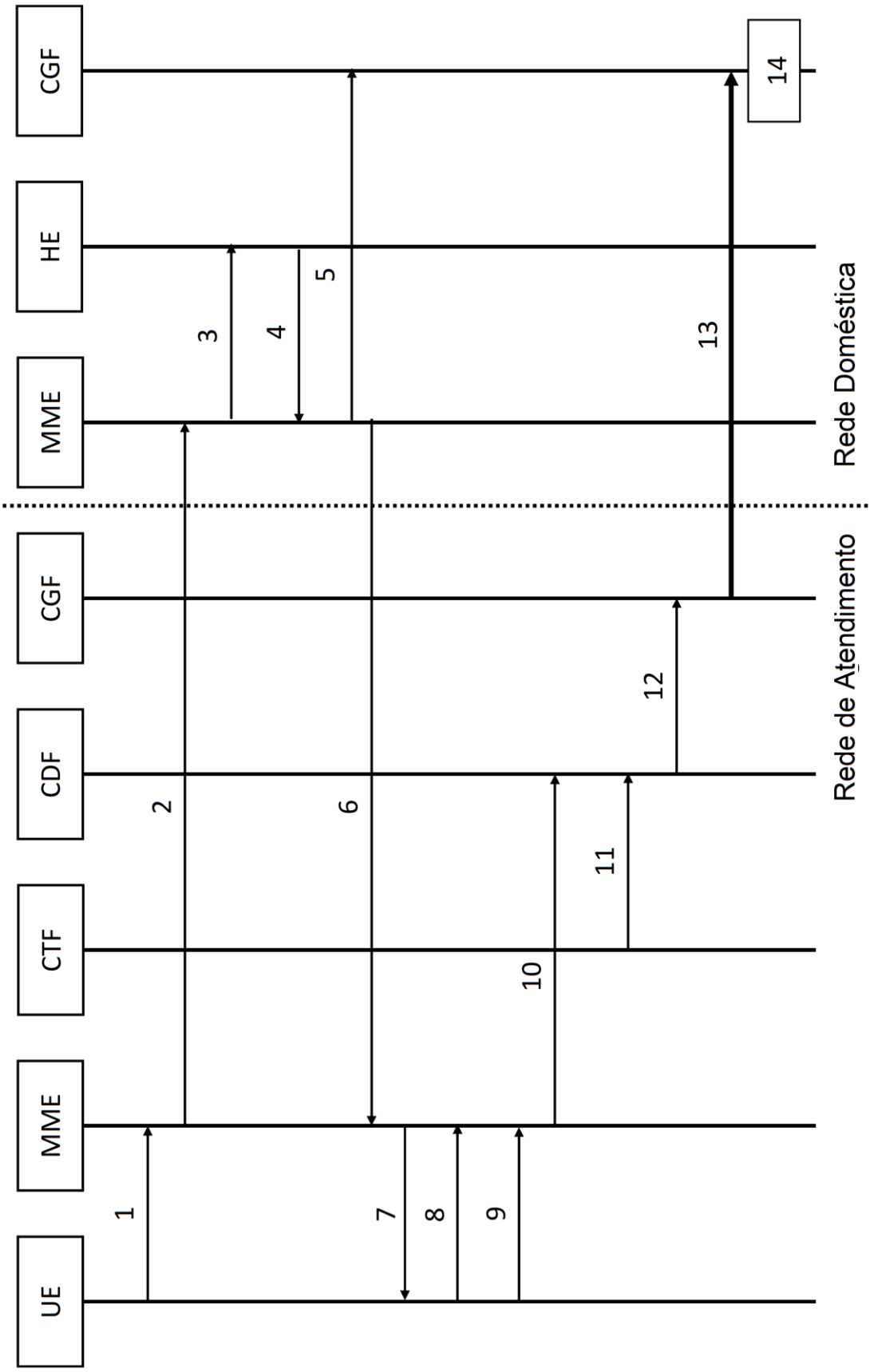

CGF
HE
MME
CGF
CDF
CTF
MME
UE
14
3
4
5
13
12
2
6
11
10
1
7
8
9
Rede Doméstica
Rede de Atendimento

Fig. 3

RESUMO

MÉTODO PARA AUTENTICAR UMA TRANSAÇÃO DESEMPENHADA POR UM EQUIPAMENTO DE USUÁRIO DE COMUNICAÇÃO MÓVEL

A presente invenção provê um método para autenticar uma transação desempenhada por um equipamento de usuário de comunicação móvel, UE, dispositivo que tenha desempenhado um procedimento de autenticação e acordo de chave entre o dispositivo UE e uma entidade de gerenciamento móvel de uma rede visitada, a fim de estabelecer um contexto seguro entre o dispositivo UE e a rede visitada, o método compreendendo enviar uma mensagem de validação de serviço do dispositivo UE para a rede visitada, a mensagem de validação de serviço que é assinada digitalmente pelo dispositivo UE usando uma chave de proteção de integridade compartilhada entre o dispositivo UE e uma rede de operadora doméstica; e encaminhar a mensagem de validação de serviço da rede visitada para a rede de operadora doméstica.