(11) Número de Publicação: **PT 1844595 E**

(51) Classificação Internacional:
H04W 12/06 (2009.01)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2006.01.17**

(30) Prioridade(s): **2005.02.03 EP 05002300**
2005.04.19 US 108848

(43) Data de publicação do pedido: **2007.10.17**

(45) Data e BPI da concessão: **2011.03.02**
067/2011

(73) Titular(es):
NOKIA CORPORATION
KEILALAHDENTIE 4 02150 ESPOO FI

(72) Inventor(es):
PEKKA LAITINEN FI

(74) Mandatário:
MANUEL ANTÓNIO DURÃES DA CONCEIÇÃO ROCHA
AV LIBERDADE, Nº. 69 1250-148 LISBOA PT

(54) Epígrafe: **AUTENTICAÇÃO USANDO A FUNCIONALIDADE GAA PARA LIGAÇÕES DE REDE UNIDIRECIONAL**

(57) Resumo:
MÉTODOS, UMA ENTIDADE DE CLIENTE, ENTIDADES DE REDE, UM SISTEMA E UM PRODUTO DE PROGRAMA INFORMÁTICO REALIZAM A AUTENTICAÇÃO ENTRE UMA ENTIDADE DE CLIENTE E UMA REDE. A REDE INCLUI, NO MÍNIMO, UMA ENTIDADE DE FUNÇÃO DE SERVIDOR DE BOOTSTRAP E UMA ENTIDADE DE FUNÇÃO DE APLICAÇÃO DE REDE. A ENTIDADE DE CLIENTE NÃO É CAPAZ DE COMUNICAR COM AMBAS AS ENTIDADES DE REDE DE UM MODO BIDIRECIONAL. O PONTO DE REFERÊNCIA UB DO PADRÃO 3GPP ENTRE A ENTIDADE DE CLIENTE E A ENTIDADE DE FUNÇÃO DE SERVIDOR DE BOOTSTRAP NÃO É UTILIZADO PARA EFEITOS DE AUTENTICAÇÃO, COMO, POR EXEMPLO, A AUTENTICAÇÃO USANDO A FUNCIONALIDADE GAA PARA LIGAÇÕES DE REDE UNIDIRECIONAL.

RESUMO

"AUTENTICAÇÃO USANDO A FUNCIONALIDADE GAA PARA LIGAÇÕES DE REDE UNIDIRECIONAL"

Métodos, uma entidade de cliente, entidades de rede, um sistema e um produto de programa informático realizam a autenticação entre uma entidade de cliente e uma rede. A rede inclui, no mínimo, uma entidade de função de servidor de bootstrap e uma entidade de função de aplicação de rede. A entidade de cliente não é capaz de comunicar com ambas as entidades de rede de um modo bidirecional. O ponto de referência Ub do padrão 3GPP entre a entidade de cliente e a entidade de função de servidor de bootstrap não é utilizado para efeitos de autenticação, como, por exemplo, a autenticação usando a funcionalidade GAA para ligações de rede unidirecional.

DESCRIÇÃO

"AUTENTICAÇÃO USANDO A FUNCIONALIDADE GAA PARA LIGAÇÕES DE REDE UNIDIRECIONAL"

Campo da Invenção

A presente invenção refere-se a métodos, entidades de rede, um sistema e um produto de programa informático para a autenticação entre uma entidade de cliente e uma rede, em que a entidade de cliente não é capaz de comunicar com a rede de um modo bidirecional. Em particular, a presente invenção refere-se à autenticação usando funcionalidades de acordo com uma arquitetura de autenticação genérica, GAA, por ex. em cenários de transmissão.

Antecedentes da Invenção

Nos últimos anos desenvolveram-se várias espécies de sistemas de comunicação, em particular móvel e/ou sistemas de comunicação baseados em IP (IP: Protocolo de Internet), assim como, uma série de serviços oferecidos nestes sistemas.

Nestes sistemas de comunicação avançados, como por ex. as redes de comunicação móvel da Terceira Geração, que estão atualmente em desenvolvimento pelo Programa de Parceria de Terceira Geração (3GPP), os aspetos relacionados com a segurança e fiabilidade desempenham um papel cada vez mais importante.

A começar pelo conceito de certificados de assinante, que suporta serviços que os operadores móveis fornecem e

cuja provisão ajuda os operadores móveis, e considerando a necessidade de mais capacidades de segurança genéricas, a padronização 3GPP concentra-se ultimamente na evolução de uma arquitetura de autenticação genérica (GAA). Como se pode deduzir da Figura 1, que mostra uma vista geral de um ambiente de arquitetura de autenticação genérica em inter-relação com um sistema de assinante doméstico HSS 14, um equipamento de utilizador UE 12 e uma entidade de rede NE 13, a GAA 11 consiste basicamente de três subaspetos. Ou seja, uma arquitetura de bootstrap genérica (GBA) 11b, certificados de assinante 11a e uma procuração de autenticação (AP) 11 c por ex. baseada em HTTPS (Protocolo de Transporte de Hipertexto Seguro). Deste modo, a arquitetura de bootstrap genérica (GBA) também constrói uma base para ambos os outros subaspetos nessa GBA oferecerem capacidade de autenticação genérica para várias aplicações baseadas num segredo partilhado. Normalmente, a funcionalidade GBA é inicializar (bootstrap) a autenticação e certificação por chave para a segurança da aplicação, e baseia-se no mecanismo HTTP Digest AKA (Autenticação e Certificação por Chave) de acordo com IETF RFC 3310.

A Figura 2 ilustra um modelo de rede para o bootstrap genérico. Uma função de servidor de bootstrap BSF 13a e o equipamento de utilizador UE 12, que estão ligados via uma ligação bidirecional Ub, autenticam mutuamente usando o protocolo AKA protocolo e certificam chaves de sessão. Estas chaves destinam-se depois a ser usadas para uma sessão de bootstrap e a ser usadas entre o equipamento de utilizador 12 e uma função de aplicação de rede NAF 13b controlada por operador, que está também ligada ao equipamento do utilizador 12 através de uma ligação

bidirecional Ua. Depois do procedimento de bootstrap, que é descrito em pormenor mais abaixo, o equipamento de utilizador 12 e a função de aplicação de rede 13b pode executar algum protocolo específico da aplicação, em que a autenticação de mensagens se baseia nessas chaves de sessão criadas durante a autenticação mútua. Correspondentemente, GAA/GBA pode geralmente ser entendido como um cenário de autenticação de 3 partes, em que a função de servidor de bootstrap 13a está ainda ligada a um sistema de assinante doméstico HSS 14 que suporta por ex. definições de segurança do utilizador (USS).

Os pontos de referência (interfaces) entre as entidades individuais na Figura 2 estão identificados por Ub, Ua, Zn, e Zh. As interfaces Zn e Zh baseiam-se no Diâmetro (de acordo com o Protocolo de Diâmetro Base que é especificado em IETF RFC 3588), a interface Ub baseia-se numa reutilização de mensagens HTTP Digest AKA, e o protocolo usado na interface Ua depende da aplicação a ser executada.

A utilização da arquitetura de bootstrap genérica está dividida em duas fases. A primeira fase, isto é, o procedimento de bootstrap (genérico) como tal, é ilustrado na Figura 3, e a segunda fase, isto é, o procedimento de utilização bootstrap genérico, é ilustrado na Figura 4.

No procedimento de bootstrap de acordo com a Figura 3, o equipamento de utilizador UE 12 envia um pedido HTTP para a função de servidor de bootstrap BSF 13a (passo S31). No passo S32, a BSF 13a restaura o perfil de utilizador e um desafio, isto é, um vetor de autenticação (AV), através da interface Zh do sistema de assinante doméstico HSS 14. De seguida, no passo S33, a BSF 13a reencaminha parâmetros de

autenticação RAND e AUTN ao UE 12 para exigir que o UE 12 se autentique a si próprio. O UE 12 calcula um código de autenticação de mensagens (MAC) para verificar o desafio da rede de autenticação, assim como, calcula chaves de sessão CK, IK, e RES. Por conseguinte, as chaves de sessão CK, IK, e RES estão disponíveis em BSF 13a e também em UE 12. No passo S35, o UE 12 envia novamente um pedido à BSF 13a, e a BSF 13a verifica, no passo S36, se o parâmetro recebido é calculado usando RES e se é igual ao parâmetro que é similarmente calculado usando XRES, que foi obtido anteriormente como parte do vetor de autenticação a partir do HSS 14. Se estes parâmetros forem iguais, o UE 12 é autenticado, e a BSF 13a cria uma chave ("chave principal") Ks, concatenando as chaves de sessão CK e IK (passo S37). A chave Ks é depois usada para proteger a interface Ua. No passo S38, a BSF 13a envia uma mensagem de OK, incluindo um identificador de transação B-TID e outros possíveis dados (como por exemplo um vitalício para a chave Ks), ao UE 12, que indicam o sucesso da autenticação. Ao concatenar as chaves de sessão CK e IK, a chave Ks para proteger a interface Ua é depois também criada no UE 12 (passo S39). Deste modo, uma sessão de bootstrap entre o equipamento de utilizador (cliente) e a função de servidor de bootstrap foi iniciada com sucesso.

A Figura 4 apresenta um procedimento exemplificativo que usa uma associação de segurança de bootstrap. Depois de ter iniciado uma sessão de bootstrap (S40a), o UE 12 pode começara a comunicar com a função de aplicação de rede NAF 13b. Assim sendo, a chave principal Ks criada durante o procedimento de bootstrap no UE 12 e na BSF 13a é usada para derivar a chave Ks-NAF específica de NAF (passo S40b).

Um pedido de aplicação (passo S41) inclui o identificador de transação B-TID obtido durante o bootstrapping, um conjunto de dados específicos da aplicação referenciado por msg, e todas as credenciais referenciadas por MAC. No passo S42, a NAF 13b pede uma ou mais chaves e, possivelmente, os dados de perfil do utilizador correspondentes à informação fornecida pelo UE 12 através da interface zn a partir da BSF 13a. Um pedido deste pode, por exemplo, basear-se no identificador de transação. Entre os passos S42 e S43, a chave Ks-NAF específica de NAF é criada na entidade BSF 13a. No passo S43, a BSF 13a responde fornecendo a ou as chaves pedidas (incluindo Ks-NAF e uma parte específica da aplicação do perfil de utilizador que é referenciada por Prof) à NAF 13b, que a NAF 13b usa diretamente ou com as quais a NAF 13b deriva mais chaves necessárias para proteger o protocolo usado através da interface Ua em direção ao UE 12, que é uma funcionalidade específica da aplicação e não endereçada em especificações GAA. Este tipo de derivação é realizada do mesmo modo como UE 12 o fez anteriormente.

De seguida, a entidade NAF 13b guarda (passo S44) pelo menos os parâmetros Ks-NAF, Prof, e vitalício da chave. Depois disso, a NAF 13b continua com o protocolo usado através da Ua, enviando uma resposta da aplicação ao UE 12 (passo S45). Para mais detalhes sobre a arquitetura de bootstrap genérica, faz-se referência à especificação técnica 3GPP TS 33.220 (versão 6.3.0) de dezembro de 2004.

Tendo em conta a convencional arquitetura de autenticação genérica e a arquitetura de bootstrap genérica acima descrita, estamos perante o seguinte problema.

Em resumo, o convencional comportamento GAA 3GPP normal é que o cliente, ou seja, um equipamento de utilizador inicializa (bootstrap) com a entidade BSF, usando um vetor de autenticação AKA. Como resultado, obtêm-se as chamadas credenciais GAA que consistem de uma chave partilhada Ks e de um identificador de transação de bootstrap (B-TID). Estas credenciais GAA são ainda usadas para derivar uma chave específica de servidor (Ks-NAF). As chaves específicas de NAF (isto é, B-TID e Ks-NAF) podem depois ser usadas entre o cliente UE e o servidor NAF, como por ex. um nome/palavra-passe de utilizador no protocolo existente, cujo caso é referenciado pelo termo "genérico".

O procedimento de bootstrap convencional requer que o cliente possua uma ligação bidirecional à entidade BSF, e o uso posterior das credenciais específicas de NAF entre o UE e a NAF normalmente também requer o mesmo. Por conseguinte, o problema reside no fato dos mecanismos convencionais GAA e/ou GBA não funcionarem, isto é, não poderem ser usados para autenticação, no caso de não haver um canal de retorno desde o equipamento de utilizador até à rede. Um exemplo para um cenário destes são as redes de transmissão, por exemplo sendo o equipamento de utilizador uma caixa adaptadora (STB; ou caixa digital) para a transmissão de vídeo digital. Num cenário destes, GAA e/ou GBA não podem, de acordo com a técnica anterior, ser usados, uma vez que o UE não pode ser inicializado (bootstrap) com a BSF nem pode comunicar com a NAF de um modo bidirecional, como é exigido.

Numa contribuição para o consórcio DVB-H (Transmissão de Vídeo Digital para Portáteis) e o ETSI (Instituto Europeu de Padrões de Telecomunicação), a Vodafone

apresentou uma proposta para uma interface para um elemento baseado em cartão USIM do mecanismo usado para derivar chaves para a proteção do serviço. No entanto, esta proposta não é adequada para ultrapassar o problema acima descrito e as desvantagens relacionadas.

Por conseguinte, é necessário arranjar uma solução para o problema e as desvantagens acima referidas para providenciar segurança neste tipo de cenários que são cada vez mais importantes para uso futuro.

Sumário da Invenção

Consequentemente, um objeto da presente invenção é eliminar as desvantagens acima referidas inerentes à técnica anterior e providenciar respetivamente métodos melhorados, entidades de rede, um sistema e um produto de programa informático.

O objeto acima referido é obtido por métodos, aparelhos e produtos de programas informáticos, conforme definido nas reivindicações anexas.

De acordo com um primeiro aspeto da presente invenção, este objetivo é por exemplo concretizado por um método que compreende a realização da autenticação entre uma entidade de cliente (UE) e uma rede que compreende, no mínimo, uma entidade de função de servidor de bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) possui uma ligação de rede unidirecional sem um canal de retorno para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que a autenticação compreende: transmitir (S62) um pedido de informação de

autenticação a partir da entidade de função de aplicação de rede até à entidade de função de servidor de bootstrap, compreendendo o referido pedido uma identidade privada da entidade de cliente, quando a entidade de função de aplicação de rede precisa de transmitir, com segurança, dados à entidade de cliente; processar (S63) o pedido e recuperar a informação de autenticação na entidade de função de servidor de bootstrap, em que a referida recuperação compreende a criação de dados de sessão de bootstrap para a entidade de cliente; transmitir (S64) uma resposta, incluindo a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente, a partir da entidade de função de servidor de bootstrap, à entidade de função de aplicação de rede; transmitir (S66) a informação de autenticação, que inclui os dados de sessão de bootstrap para a entidade de cliente e os dados por transmitir a partir da entidade de função de aplicação de rede, à entidade de cliente; e autenticar (S67) a rede usando a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente na entidade de cliente, em que a referida autenticação compreende a realização de uma autenticação, incluindo uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

De acordo com um segundo aspeto da presente invenção, este objetivo é por exemplo concretizado por um programa informático incorporado num meio de leitura informático, estando o programa informático configurado para carregar para uma memória de um meio de processamento digital e para controlar o referido meio de processamento digital, de modo a realizar o método de acordo com o primeiro aspeto.

De acordo com um terceiro aspeto da presente invenção, este objetivo é por exemplo concretizado por um aparelho operável como uma entidade de cliente para ser usado dentro de uma arquitetura de autenticação para realizar a autenticação entre a entidade de cliente (UE) e uma rede, compreendendo a rede pelo menos uma

entidade de função de servidor de bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) é operável para ter uma ligação de rede unidirecional sem um canal de retorno a partir da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), compreendendo o referido aparelho: meios de receção (87) para receber, a partir da entidade de função de aplicação de rede, informação de autenticação a partir da entidade de função de servidor de bootstrap e dados a serem transmitidos a partir da entidade de função de aplicação de rede até à entidade de cliente, compreendendo a referida informação de autenticação dados de sessão de bootstrap para a entidade de cliente, e meios de autenticação (81) para autenticar a rede usando a informação de autenticação recebida que compreende os dados de sessão de bootstrap para a entidade de cliente, em que a referida autenticação compreende a realização de uma autenticação, incluindo uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

De acordo com um quarto aspeto da presente invenção, este objetivo é por exemplo concretizado por um método, que compreende a realização da autenticação entre uma entidade de cliente (UE) e uma rede incluindo pelo menos uma entidade de função de servidor de bootstrap (BSF) e uma

entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) tem uma ligação de rede unidirecional sem um canal de retorno a partir da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), compreendendo a referida autenticação receber (S66) a partir da entidade de função de aplicação de rede, informação de autenticação a partir da função de servidor de bootstrap e dados a serem transmitidos a partir da entidade de função de aplicação de rede, compreendendo a referida informação de autenticação dados de sessão de bootstrap para a entidade de cliente, e autenticar (S67) a rede usando a informação de autenticação recebida que compreende os dados de sessão de bootstrap para a entidade de cliente, em que a referida autenticação compreende a realização de uma autenticação de acordo com uma arquitetura de autenticação genérica.

De acordo com um quinto aspeto da presente invenção, este objetivo é por exemplo concretizado por um programa informático incorporado num meio de leitura informático, estando o programa informático configurado para carregar para uma memória de um meio de processamento digital e para controlar o referido meio de processamento digital, de modo a realizar o método de acordo com o quarto aspeto.

De acordo com um sexto aspeto da presente invenção, este objetivo é por exemplo concretizado por um aparelho operável como uma entidade de função de aplicação de rede para usar dentro de uma arquitetura de autenticação para realizar a autenticação entre uma entidade de cliente (UE) e uma rede, compreendendo a rede pelo menos o aparelho que opera como uma entidade de função de aplicação de rede

(NAF) e uma entidade de função de servidor de bootstrap (BSF), em que a entidade e cliente (UE) é operável para ter uma ligação de rede unidirecional sem um canal de retorno desde a entidade de cliente até à entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que o aparelho compreende:

meios transcetores (91) para enviar para a entidade de cliente

e para enviar para e receber da entidade de função de servidor de bootstrap, em que os meios transcetores são adaptados para transmitir um pedido de informação de autenticação para a entidade de função de servidor de bootstrap, compreendendo este pedido uma entidade privada da entidade de cliente, quando a entidade de função de aplicação de rede tem de transmitir com segurança dados para a entidade de cliente, recebendo uma resposta incluindo a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente desde a entidade de função de servidor de bootstrap, e transmitir a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente e os dados por serem transmitidos à entidade de cliente,

em que a referida informação de autenticação está adaptada a uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

De acordo com um sétimo aspeto da presente invenção, este objetivo é por exemplo concretizado por um método que

compreende a realização da autenticação entre uma entidade de cliente (UE) e uma rede que compreende, no mínimo, uma entidade de função de servidor de bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) possui uma ligação de rede unidirecional sem um canal de retorno para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que a autenticação inclui transmitir (S62) um pedido de informação de autenticação para a entidade de função servidor de bootstrap, compreendendo o referido pedido uma identidade privada da entidade de cliente, quando a entidade de função de aplicação de rede precisa de transmitir com segurança dados à entidade de cliente, receber (S64) uma resposta, incluindo a informação de autenticação que compreende os dados de sessão de bootstrap, para a entidade de cliente a partir da entidade de função de servidor de bootstrap, e transmitir (S66) a informação de autenticação que inclui os dados de sessão de bootstrap para a entidade de cliente e os dados por transmitir à entidade de cliente, em que a referida informação de autenticação está adaptada a uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

De acordo com um oitavo aspeto da presente invenção, este objetivo é por exemplo concretizado por um programa informático A incorporado num meio de leitura informático, estando o programa informático configurado para carregar para uma memória de um meio de processamento digital e para controlar o referido meio de processamento digital, de modo a realizar o método de acordo com o sétimo aspeto.

De acordo com um nono aspeto da presente invenção, este objetivo é por exemplo concretizado por um aparelho operável como uma entidade de função de servidor de bootstrap para usar dentro de uma arquitetura de autenticação para realizar a autenticação entre uma entidade de cliente (UE) e uma rede, compreendendo a rede pelo menos o aparelho que opera como uma entidade de função de servidor de bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) é operável para possuir uma ligação de rede unidirecional sem um canal de retorno a partir da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que o aparelho compreende: meios transcetores (101) para enviar para e para receber da entidade de função de aplicação de rede, e meios de processamento e de recuperação (102) para processar um pedido recebido da entidade de função de aplicação de rede, compreendendo o referido pedido uma entidade privada da entidade de cliente, e para recuperar informação de autenticação, em que esses meios de processamento e de recuperação incluem ainda meios de criação (104) para criar dados de sessão de bootstrap para a entidade de cliente, em que os meios transcetores (101) estão configurados para receber o pedido da entidade de função de aplicação de rede e para transmitir a informação de autenticação que compreende os dados de sessão de bootstrap criados para a entidade de cliente à entidade de função de aplicação de rede, em que a referida informação de autenticação está adaptada a uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

De acordo com um décimo aspeto da presente invenção, este objetivo é por exemplo concretizado por um método que compreende a realização da autenticação entre uma entidade de cliente (UE) e uma rede que compreende, no mínimo, uma entidade de função de servidor de bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) possui uma ligação de rede unidirecional sem um canal de retorno desde a entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que a autenticação compreende receber (S62) um pedido de informação de autenticação da entidade de função de aplicação de rede, em que o referido pedido compreende uma identidade privada da entidade de cliente, processar (S63) o pedido recebido da entidade de função de aplicação de rede e recuperar informação de autenticação, compreendendo ainda a criação de dados de sessão de bootstrap para a entidade de cliente, transmitir (S64) uma resposta incluindo a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente à entidade de função de aplicação de rede, em que a referida informação de autenticação está adaptada a uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

De acordo com um décimo primeiro aspeto da presente invenção, este objetivo é por exemplo concretizado por um programa informático incorporado num meio de leitura informático, estando o programa informático configurado para carregar para uma memória de um meio de processamento digital e para controlar o referido meio de processamento

digital, de modo a realizar o método de acordo com o décimo aspeto.

Outros desenvolvimentos vantajosos e/ou modificações de qualquer um dos aspetos acima referidos são definidos em respetivos aspetos das reivindicações anexas. Por exemplo, pelo menos um dos seguintes pode ser aplicado:

- a transmissão do pedido é ativada por um meio diferente da entidade de cliente;
- o pedido inclui ainda uma identidade da entidade de função de aplicação de rede;
- a recuperação da informação de autenticação compreende captar a informação de autenticação de um sistema de assinante doméstico;
- a informação de autenticação inclui ainda, no mínimo, um parâmetro de desafio aleatório ou um parâmetro de autenticação de rede;
- a resposta inclui ainda uma chave da entidade de função de aplicação de rede;
- a transmissão da informação de autenticação inclui ainda transmitir uma identidade da entidade de função de aplicação de rede;
- a autenticação da rede compreende ainda a criação de uma chave da entidade de função de aplicação de rede na entidade de cliente;
- a autenticação da rede compreende ainda estabelecer uma sessão de bootstrap entre a entidade de cliente e a entidade de função de servidor de bootstrap;
- o estabelecimento de uma sessão de bootstrap baseia-se na informação de autenticação da entidade de função de aplicação de rede;

- a autenticação da rede compreende ainda guardar os dados de sessão de bootstrap na entidade de cliente;
- existe uma sessão de bootstrap válida entre a entidade de cliente e a entidade de função de servidor de bootstrap;
- uma sessão de bootstrap válida existe permanentemente;
- o processamento do pedido compreende ainda ativar a entidade de cliente para estabelecer uma sessão de bootstrap válida;
- a autenticação de informação compreende, no mínimo, dados de sessão de bootstrap;
- a resposta inclui ainda uma chave da entidade de função de aplicação de rede;
- a autenticação da rede compreende ainda a criação de uma chave da entidade de função de aplicação de rede na entidade de cliente;
- o método compreende ainda contactar inicialmente a entidade de função de aplicação de rede e enviar a sua entidade privada, através da entidade de cliente;
- o método compreende ainda ativar, através da entidade de função de aplicação de rede, a entidade de cliente para estabelecer uma sessão de bootstrap válida;
- o método compreende ainda ativar, através da entidade de função de aplicação de rede, a entidade de função de servidor de bootstrap, de modo a ativar um procedimento de bootstrap não solicitado com a entidade de cliente;

- o método compreende ainda codificar os dados a serem transmitidos na entidade de função de aplicação de rede, usando a sua chave;
- o método compreende ainda descodificar os dados na entidade de cliente, usando a chave da entidade de função de aplicação de rede;
- a rede compreende uma rede de transmissão;
- um aparelho compreende, no mínimo, um equipamento de utilizador e pode ser ligado a um módulo universal de identidade de assinante;
- a entidade de cliente compreende uma caixa adaptadora;
- a informação da identidade do utilizador disponível no aparelho está acessível;
- a informação de identidade do utilizador é guardada num cartão inteligente que pode ser ligado à entidade de cliente; e/ou
- um aparelho é configurado para transmitir transmissões.

É vantajoso na presente invenção providenciar uma solução sobre como o conceito 3GPP GAA pode ser usado em cenários onde o cliente não tem um canal de retorno à rede.

As versões da presente invenção basicamente eliminam a fase de bootstrap entre o cliente e a função de servidor de bootstrap. Além disso, é vantajoso que esta fase de bootstrap seja parcialmente combinada com o meta-protocolo (ou as mensagens individuais) entre a função de aplicação de rede e o cliente.

Outra vantagem da presente invenção é o fato de suportar o bootstrap da autenticação e certificação por

chave em cenários de falta de canal de retorno, isto é, falta de uma ligação bidirecional à rede.

Através da presente invenção, o conceito GAA/GBA é, assim, alargado na sua área de aplicação.

Breve Descrição dos Desenhos

Passamos a descrever a presente invenção em pormenor através de versões da mesma e de exemplos comparativos que fazem referência aos desenhos anexos, nos quais

a Figura 1 ilustra uma vista geral de um ambiente de arquitetura de autenticação genérica,

a Figura 2 ilustra um modelo de rede para a transmissão genérica,

a Figura 3 ilustra um procedimento de bootstrap genérico de acordo com a técnica anterior,

a Figura 4 ilustra um procedimento de utilização de bootstrap genérico de acordo com a técnica anterior,

a Figura 5 ilustra um diagrama de sinalização de um método de acordo com um primeiro exemplo comparativo,

a Figura 6 ilustra um diagrama de sinalização de um método de acordo com uma versão da presente invenção,

a Figura 7 ilustra um diagrama de sinalização de um método de acordo com um segundo exemplo comparativo,

a Figura 8 ilustra um diagrama de bloco de uma entidade de cliente de acordo com uma versão da presente invenção,

a Figura 9 ilustra um diagrama de bloco de uma entidade de função de aplicação de rede de acordo com uma versão da presente invenção, e

a Figura 10 ilustra um diagrama de bloco de uma entidade de função de servidor de bootstrap de acordo com uma versão da presente invenção.

Descrição detalhada de versões da presente invenção

A presente invenção é aqui descrita através de versões, bem como, exemplos comparativos com referência a cenários particulares exemplificativos e não limitativos. Um profissional da área entende que a invenção não se limita a estes exemplos e que pode ser aplicada de um modo mais expansivo.

A presente invenção e as suas versões são, a título de exemplo, dirigidas a casos para ambientes GAA e/ou GBA, em que um cliente ou equipamento de utilizador não tem um canal de retorno à rede. Com a rede que compreende, no mínimo, uma entidade de função de aplicação de rede e uma entidade de função de servidor de bootstrap, isto significa que um equipamento de utilizador (entidade de cliente) não é capaz de comunicar com ambas as entidades de rede de um modo bidirecional. Por outras palavras, isto quer dizer que o equipamento de utilizador (entidade de cliente) não tem

uma ligação bidirecional, ou seja, um canal de retorno, à entidade de função de aplicação de rede ou à entidade de função de servidor de bootstrap ou a ambas estas entidades.

A Figura 5 ilustra um diagrama de sinalização de um método de acordo com um primeiro exemplo comparativo. A Figura 5 apresenta um cenário, no qual a entidade de cliente ou equipamento de utilizador UE 12 não tem um canal de retorno à rede, isto é, a entidade de cliente não é capaz de comunicar com a entidade de função de aplicação de rede (NAF) 13b nem com a entidade de função de servidor de bootstrap (BSF) 13a de um modo bidirecional. Por conseguinte, a entidade de cliente não pode realizar um procedimento de bootstrap com a entidade BSF. Um exemplo para um cenário destes pode ser uma caixa adaptadora (STB; ou caixa digital) que é equipada com um leitor de cartões UICC (Cartão de Circuitos Integrado Universal).

Passamos a descrever um método para realizar a autenticação entre a entidade de cliente e a rede, de modo a utilizar as funcionalidades GAA.

No passo S51, a entidade NAF 13b precisa de entregar alguns dados (por ex., chaves de transmissão) ao cliente UE 12. A entidade NAF 13b conhece a identidade privada do assinante, isto é, o IMPI do assinante (identidade privada do subsistema da rede de núcleo multimédia IP), e os dados que têm de ser entregues ao UE 12. No passo S52, a entidade NAF 13b envia um pedido incluindo o IMPI do assinante, a sua própria identidade NAF-ID (isto é, nome anfitrião NAF), e opcionalmente um ou mais GSIDs (identificadores do serviço GAA para pedir definições de segurança do utilizador específico de NAF) através do ponto de

referência Zn para a entidade de função do servidor de bootstrap (BSF) 13a.

Note-se que a transmissão do pedido (do passo 2) pode ser ativada através de meios diferentes da entidade de cliente. Por exemplo no caso de DVB-H, o procedimento de autenticação (bootstrap) ou a sua necessidade pode ser ativado na rede (por exemplo na própria entidade NAF) pela necessidade de atualizar chaves de transmissão na entidade terminal.

Depois de receber o pedido da entidade NAF 13b, a entidade BSF 13a verifica no passo S53 se a entidade NAF 13b está autorizada a pedir informação de autenticação, como por exemplo um elemento de autenticação da rede (AUTN) e um desafio aleatório (RAND). Em caso afirmativo, a entidade BSF 13a capta vetores de autenticação de um sistema de assinante doméstico HSS 14, calcula a chave Ks-NAF da entidade NAF baseada na identidade NAF-ID da entidade NAF e outros parâmetros de derivação. Também extrai as definições de segurança do utilizador pedidas USSs (se existirem) a partir das definições de segurança do utilizador GBA do assinante (GUSS).

Num quarto passo S54, a entidade BSF 13a envia depois os parâmetros AUTN, RAND, Ks-NAF, vitalício de Ks-NAF, e as USSs pedidas (se existirem) à entidade NAF 13b. A NAF 13b usa a chave Ks-NAF para codificar (ou proteger de outro modo qualquer) os dados a serem transmitidos à entidade de cliente 12 (passo S55). Opcionalmente, no caso de GBA que suporta UICC (isto é, GBA-U) ambas as chaves Ks-int-NAF e Ks-ext-NAF podem ser usadas para este efeito. No entanto, a funcionalidade de codificação (assim como a descodificação abaixo) é opcional.

No passo S56, a entidade NAF 13b usa o canal de transmissão entre si mesmo e o UE 12 para enviar os parâmetros AUTN, RAND, NAF-ID e os dados codificados ao UE 12. AUTN, RAND, NAF-ID e os dados codificados podem ainda ser protegidos com outros meios conhecidos (por ex., usando uma chave pública do certificado do dispositivo do UE). Quando o UE 12 recebe os dados da NAF 13b, começa por usar os parâmetros AUTN e RAND para autenticar a rede. Se tiver sucesso, vai derivar a chave de bootstrap (Ks) das chaves de sessão CK e IK, e continuar a derivar a chave Ks-NAF específica de NAF usando Ks, NAF-ID e outros parâmetros de derivação de chaves. Pode, depois, descodificar os dados, usando a chave Ks-NAF e usar os dados (por ex., chaves de transmissão) no UE 12.

Consequentemente, o ponto de referência Ub não é, de modo algum, usado no método apresentado.

A Figura 6 ilustra um diagrama de sinalização de um método de acordo com uma versão da presente invenção. É, mais uma vez, apresentado um cenário em que a entidade de cliente UE 12 não tem canal de retorno à rede e, por isso, não pode executar um procedimento de bootstrap diretamente com a entidade BSF 13a. Em vez disso, o bootstrap realiza-se com a ajuda de uma entidade NAF. Por conseguinte, este tipo de procedimento pode ser referido como bootstrap inverso.

Um procedimento de bootstrap inverso de acordo com a presente versão realiza-se entre a entidade de cliente UE 12 e a entidade de função de servidor de bootstrap BSF 13a via uma entidade de função de aplicação de rede NAF 13b. O procedimento é descrito abaixo.

No passo S61, a entidade NAF 13b precisa de entregar alguns dados (por ex., chaves de transmissão) ao cliente UE 12. A entidade NAF 13b conhece a identidade do assinante, isto é, o IMPI do assinante (ver acima), e os dados que têm de ser entregues ao UE 12. De acordo com procedimentos convencionais, o UE 12 tem sempre ligação à entidade NAF 13b e entrega um identificador de transação de bootstrap B-TID antes da entidade NAF 13b ser capaz de pedir chaves correspondentes GBA da entidade BSF 13a.

No método de acordo com a presente invenção, a entidade NAF 13b é ativada para captar os dados GBA por outros meios.

No passo S62, a entidade NAF 13b envia o IMPI do assinante, a sua própria NAF-ID (isto é, nome anfitrião NAF), e opcionalmente um ou mais GSIDs (identificadores do serviço GAA para pedir definições de segurança do utilizador específico de NAF) através do ponto de referência Zn para a entidade BSF 13a. De acordo com procedimentos convencionais, o identificador B-TID é usado para captar as chaves GBA da BSF 13a. Em oposição a isso, a entidade NAF 13b usa aqui o IMPI do assinante para captar os dados GBA da BSF 13a.

Depois de receber o pedido da entidade NAF 13b, a BSF 13a verifica no passo S63 se a entidade NAF 13b está autorizada a pedir informação de autenticação, como os parâmetros AUTN e RAND, e fazer parte de um procedimento de bootstrap inverso de acordo com a presente versão. Em caso afirmativo, a entidade BSF 13a capta vetores de autenticação de um sistema de assinante doméstico HSS 14, calcula a chave Ks-NAF baseada na identidade NAF-ID e outros parâmetros de derivação. Também extrai as definições

de segurança do utilizador pedidas USSs (se existirem) a partir das GUSS do assinante. De seguida, ainda no passo S63, a entidade BSF 13a cria dados de sessão de bootstrap para o assinante que pode ser usado mais tarde com outros NAFs 13b, também.

De acordo com procedimentos da técnica anterior, a entidade BSF 13a deve conter os dados de sessão de bootstrap existentes (identificados pelo identificado de transação de bootstrap B-TID) e calcular a chave Ks-NAF conforme mencionado também em cima. Em oposição a isso, a entidade BSF 13a de acordo com esta versão cria dados de sessão de bootstrap sem comunicar com a entidade de cliente UE 12, que se destinam a ser usados para o cálculo de Ks-NAF e uma seleção de USSs. No passo S64, a entidade BSF 13a envia parâmetros AUTN, RAND, B-TID, Ks-NAF, vitalício de Ks-NAF, e os USSs pedidos (se existirem) à NAF. Também AUTN, RAND e B-TID regressam à NAF. De seguida, a NAF usa (no passo 5) opcionalmente a chave Ks-NAF para codificar (ou proteger de outro modo) os dados a serem transmitidos. De acordo com as especificações atuais, isto é uma funcionalidade específica de NAF. (Note que as especificações GBA estão muito abertas ao que acontece na NAF 13b e em como a NAF 13b usa as chaves GBA.) Conforme acima mencionado, a funcionalidade de codificação (e descodificação) de dados a serem transmitidos é meramente opcional no quadro da realização da autenticação.

No passo S66, a entidade NAF usa o canal de transmissão (unidirecional) entre si mesmo e o UE 12 para enviar os parâmetros AUTN, RAND, B-TID, NAF-ID e os dados codificados ao UE 12. AUTN, RAND, NAFID e os próprios dados codificados podem ainda ser protegidos com outros meios

(por ex., OMA DRM 2.0 [2] e usando uma chave pública do certificado do dispositivo do UE).

De acordo com os padrões da técnica anterior, o identificador B-TID é transferido do UE 12 para a NAF 13b. Isto aconteceria mesmo antes do passo S61 num procedimento GBA normal. De acordo com a presente versão, o identificador B-TID, bem como, os parâmetros AUTN e RAND são enviados da entidade NAF 13b para o cliente UE 12.

Quando o UE recebe os dados da NAF 13b (passo S67), começa por usar os parâmetros AUTN e RAND para autenticar a rede. Se tiver sucesso, vai derivar a chave de bootstrap (Ks) das chaves de sessão CK e IK, e continuar a derivar a chave Ks-NAF específica de NAF usando Ks, NAF-ID e outros parâmetros de derivação de chaves. Pode, depois, descodificar os dados, usando a chave Ks-NAF e usar os dados (por ex., chaves de transmissão) no UE 12. O UE 12 também pode ser configurado para guardar os dados de sessão de bootstrap que podem ser usados, mais tarde, com outra NAF 13b. O UE 12 estabelece depois uma sessão de bootstrap através dos parâmetros recebidos B-TID, AUTN e RAND. Além disso, na presente versão, a derivação de chave é manuseada nesta fase do procedimento (uma vez que a sessão de bootstrap fica válida). O UE 12 também pode usar uma sessão de bootstrap recentemente criada com outras NAFs 13b enquanto a sessão for válida ou for criada uma sessão de bootstrap.

Também aqui, o ponto de referência Ub não é, de modo algum, usado no método apresentado.

A Figura 7 ilustra um diagrama de sinalização de um outro método de acordo com um segundo exemplo comparativo. É apresentado um cenário no qual o cliente UE 12 não tem

canal de retorno para a entidade NAF 13b, mas tem uma ligação bidirecional a outros elementos de rede como a BSF 13a. Ou seja, de modo idêntico aos cenários acima mencionados, a entidade de cliente UE 12 não é capaz de comunicar com nenhum dos dois elementos de rede relevantes NAF 13b e BSF 13a de um modo bidirecional. No entanto, no presente caso, o cliente pode realizar um procedimento de bootstrap com a entidade BSF 13a. Um exemplo para esse tipo de cenário pode ser um terminal móvel com funcionalidades 3G, por ex. conectividade IP, mas está também equipado com um instrumento para receber, por exemplo, transmissão de vídeo digital vídeo para terminais portáteis, isto é, suporta DVB-H.

Este cenário assume que o UE 12 tem uma sessão de bootstrap válida com a BSF 13a a toda a hora (isto podia ser uma opção de configuração no UE 12) ou que assume que a BSF 13a é capaz de ativar o UE 12 para estabelecer uma sessão de bootstrap (por ex., usando o Protocolo de Iniciação de Sessão (SIP). O presente método que utiliza as funcionalidades GAA é descrito abaixo.

No passo S71, a entidade NAF 13b precisa de entregar alguns dados (por ex., chaves de transmissão) à entidade de cliente UE 12. Conhece a identidade do assinante, isto é, o seu IMPI e os dados que têm de ser entregues ao UE 12. A entidade NAF 13b envia o IMPI do assinante, a sua própria NAF-ID (isto é, nome anfitrião NAF), e opcionalmente um ou mais GSIDs (identificadores do serviço GAA para pedir definições de segurança do utilizador específico de NAF) através do ponto de referência Zn (passo S72). Até este momento, o método é mais idêntico ao da versão acima descrita.

Depois de receber o pedido da entidade NAF 13b, a entidade BSF 13a verifica no passo S73 se o assinante possui uma sessão de bootstrap válida, e pode ser encontrada nas suas bases de dados. Se não estiver presente, a entidade BSF 13a pode indicar um erro à entidade NAF 13b ou ativar a entidade de cliente UE 12 para executar um procedimento de estabelecimento de bootstrap. Depois, a entidade BSF 13a calcula a chave Ks-NAF baseada na identidade NAF-ID e outros parâmetros de derivação de chaves. Também extrai as definições de segurança do utilizador pedidas USSs (se existirem) a partir das GUSS do assinante. A entidade BSF 13a envia os parâmetros B-TID, Ks-NAF, vitalício de Ks NAF, os USSs pedidos (se existirem) à entidade NAF 13b. Por conseguinte, a entidade NAF 13b fica a conhecer o identificador de transação de bootstrap válido B-TID quando recebe isto da entidade BSF 13a. No quinto passo, a entidade NAF 13b pode, opcionalmente, usar a sua chave Ks-NAF para codificar (ou proteger de outro modo qualquer) os dados a serem transmitidos. A entidade NAF 13b usa o canal de transmissão entre si mesmo e o UE 12 para enviar os parâmetros B-TID, NAF-ID e os dados codificados à entidade de cliente UE. Os parâmetros B-TID, NA-FID e os próprios dados codificados podem ainda ser protegidos com outros meios (por ex., OMA DRM 2.0 [2] e usando uma chave pública do certificado do dispositivo do UE 12).

Quando o UE 12 recebe, no passo S77, os dados da entidade NAF 13b, ele usa B-TID e NAF-ID para derivar a chave Ks-NAF específica de NAF, usando Ks (identificado por B-TID), NAF-ID e outros parâmetros de derivação de chaves. Pode, depois, se estiver codificado, descodificar os dados,

usando a Ks-NAF e usar os dados (por ex., chaves de transmissão) no UE 12. A funcionalidade relacionada com a utilização da chave GBA no UE 12 (como na NAF 13b, ver o passo S75) é específica de NAF. A derivação de chave é manuseada nesta fase do procedimento.

As extensões/modificações, quando implementam os métodos - de acordo com qualquer uma das versões da presente invenção e com os exemplos comparativos - numa arquitetura GBA de acordo com a técnica anterior, são as seguintes:

- a NAF 13b é capaz de pedir AUTN e RAND (mas não RES, CK, IK) e a chave GBA derivada de CK e IK (isto é, Ks-NAF, por exemplo), usando a identidade privada do assinante (por ex. IMPI ou IMSI) em vez de B-TID;
- a BSF 13a é capaz de criar dados de sessão de bootstrap para um assinante baseado num pedido de NAF para AUTN e RAND;
- adicionalmente aos dados normais que regressam da BSF 13a, também AUTN e RAND são devolvidos (mas não RES, CK, IK);
- o UE 12 é capaz de criar dados de sessão de bootstrap com base em AUTN, RAND, B-TID, e chave vitalícia recebidos da NAF 13b; e
- A NAF 13b é capaz de pedir dados de sessão de bootstrap (B-TID, específico de NAF, etc.), usando o IMPI do assinante.

No sentido de outra versão da presente invenção, pode-se conceber um caso em que a entidade de cliente 12 não pode chegar à BSF 13a, mas tem um canal de 2 vias para a

NAF 13b. Por exemplo, este é o caso quando o UE 12 usa GBA para a autenticação de acesso. O protocolo GBA inverso básico não pode ser usado porque a NAF 13b não conhece o IMPI do assinante do UE 12. Este tipo de cenário também podia estar presente, por exemplo, num caso de WLAN (Rede de Área Local Sem Fios), em que a entidade de cliente 12 precisa de autenticar, mas não tem uma ligação por ex. ao servidor de EAP (Protocolo de Autenticação Extensível) que podia operar como a entidade NAF 13b num caso desses. Correspondentemente, a entidade de cliente UE 12 realiza um procedimento de bootstrap (com a entidade BSF 13a) via a entidade NAF 13b. A sinalização é idêntica aos procedimentos acima descritos, excetuando o fato de, antes do primeiro passo, o UE 12 contactar a entidade NAF 13b e enviar a sua identidade privada IMPI.

Outra versão ainda reside num caso, no qual a entidade NAF 13b tem apenas um canal unidirecional para o UE 12, mas a BSF 13a tem um canal bidirecional para o UE 12.

Nesta versão, é possível que (1) a entidade NAF 13b ative o UE 12 para estabelecer uma sessão de bootstrap válida; ou (2) a entidade NAF 13b ativa a entidade BSF 13a, de modo a ativar um procedimento de bootstrap não solicitado com a entidade de cliente UE 12.

De acordo com outras versões da presente invenção, são apresentadas uma entidade de cliente, uma entidade de função de aplicação de rede, uma entidade de função de servidor de bootstrap e um sistema para realizar a autenticação entre a entidade de cliente e a rede de acordo com qualquer um dos métodos da presente invenção.

A Figura 8 ilustra um diagrama de bloco de uma entidade de cliente de acordo com uma versão da presente invenção.

Uma entidade de cliente 12 de acordo com uma versão compreende meios de receção 87 para receber transmissões da entidade de função de aplicação de rede NAF 13b e meios de autenticação 81 para autenticar a rede, usando a informação de autenticação recebida.

De acordo com outras versões, a entidade de cliente UE 12 compreende ainda opcionalmente um ou vários dos seguintes aspetos (como se pode deduzir da Figura 8):

- meios de criação de chaves 82 para criar uma chave da entidade de função de aplicação de rede (por ex. Ks-NAF);
- meios de estabelecimento 84 para estabelecer uma sessão de bootstrap entre a entidade de cliente 12 e a entidade de função de servidor de bootstrap 13a;
- meios de armazenamento 85 para guardar dados de sessão de bootstrap; e/ou
- meios de descodificação 83 para descodificar dados codificados recebidos a partir da entidade de função de aplicação de rede 13b, usando uma chave da entidade de função de aplicação de rede 13b, que é fornecida pelos meios de criação de chaves 82.

A entidade de cliente 12 de acordo com a versão apresentada na Figura 8 compreende ainda meios de processamento e de controlo 86 configurados para processar dados e sinalizar, e para controlar a entidade de cliente 12 como um todo, assim como, os seus constituintes, como

por ex. os meios de estabelecimento 84. Para este efeito, os meios de processamento e controlo 86 possuem dados bidirecionais e/ou ligações de controlo a qualquer um dos meios constituintes apresentados.

A entidade de cliente de acordo com a presente versão compreende ainda, pelo menos, um equipamento de utilizador e/ou pode ser ligada a um módulo universal de identidade do assinante de acordo com, por exemplo, os padrões 3GPP.

Além disso, a entidade de cliente de acordo com outra versão da presente invenção é uma caixa adaptadora (ou caixa digital). Neste caso e sendo a entidade de cliente uma caixa adaptadora deste tipo, ela é configurada para ser operada de acordo com qualquer técnica apropriada conhecida, como por exemplo de acordo com os padrões DVB-H.

Na versão acima referida, os meios de autenticação 81 da entidade de cliente são configurados para aceder à informação de identidade do utilizador disponível na entidade de cliente. Este tipo de informação da identidade do utilizador é, por exemplo, usado adicionalmente à informação de autenticação recebida, para efeitos de autenticação. A informação da identidade do utilizador é, por exemplo, guardada num cartão inteligente que pode ser ligado à entidade de cliente, como por ex. um UICC, um módulo universal da identidade de assinante (USIM), ou um cartão inteligente compatível para ser usado de acordo com os padrões DVB-H.

A Figura 9 ilustra um diagrama de bloco de uma entidade de função de aplicação de rede de acordo com uma versão da presente invenção.

Uma entidade de rede, em particular uma entidade de função de aplicação de rede 13b de acordo com uma versão,

compreende meios transcetores 91 configurados para enviar transmissões a uma entidade de cliente 12, e para enviar para e receber de uma entidade de função de servidor de bootstrap 13a. Os meios transcetores 91 estão por ex. configurados para transmitir um pedido de informação de autenticação para a entidade de função de servidor de bootstrap 13a quando a entidade de função de aplicação de rede 13b precisa de transmitir com segurança dados à entidade de cliente 12, para receber uma resposta, incluindo a informação de autenticação da entidade de função de servidor de bootstrap 13a, e para transmitir a informação de autenticação e os dados por transmitir à entidade de cliente 12.

De acordo com outras versões, a entidade de função de aplicação de rede NAF 13b compreende ainda opcionalmente meios de codificação 92 para codificar os dados por transmitir à entidade de cliente 12, usando a chave da própria entidade de função de aplicação de rede 13b. De acordo com a Figura 9, os dados por transmitir estão representados por um símbolo de base de dados com a etiqueta DATA 93.

Além disso, os meios transcetores 91 podiam ser configurados para transmitir uma identidade da entidade de função de aplicação de rede 13b à entidade de cliente 12. Uma identidade destas também pode ser guardada na mesma base de dados DATA 93 dos dados por transmitir.

A entidade da rede de acordo com outra versão da presente invenção está configurada para transmitir transmissões, por exemplo, à entidade de cliente UE.

A Figura 10 ilustra um diagrama de bloco de uma entidade de função de servidor de bootstrap de acordo com uma versão da presente invenção.

Uma entidade de rede, em particular uma entidade de função de servidor de bootstrap BSF 13a, de acordo com uma versão, compreende meios transcetores 101 para enviar para e receber de uma entidade de função de aplicação de rede 13b, e meios de processamento e de recuperação 102 para processar um pedido recebido a partir da entidade de função de aplicação de rede 13b e para recuperar informação de autenticação. Na presente versão, os meios transcetores 101 estão particularmente configurados para receber o pedido da entidade de função de aplicação de rede 13b e para transmitir a informação de autenticação à entidade de função de aplicação de rede 13b.

De acordo com outras versões, a entidade de função de servidor de bootstrap BSF 13a compreende ainda opcionalmente um ou vários dos seguintes aspetos (como se pode deduzir da Figura 10):

- meios de captação 105 para captar a informação de autenticação a partir de um sistema de assinante doméstico HSS 14;
- meios de criação 104 para criar dados de sessão de bootstrap; e/ou
- meios de ativação 103 para ativar a entidade de cliente 12 para estabelecer uma sessão de bootstrap válida.

Um sistema de acordo com a presente invenção compreende, no mínimo, uma entidade de cliente 12 (que pode

ser opcionalmente uma caixa adaptadora), pelo menos uma entidade de função de aplicação de rede 13b, e pelo menos uma entidade de função de servidor de bootstrap 13a de acordo com as Figuras 8 até 10.

Note-se que nas Figuras 8 até 10 são apenas apresentados os meios e elementos funcionais que estão associados à presente invenção. Para simplificar são omitidos outros meios e elementos funcionais que os profissionais do ramo conhecem e sabem que fazem de qualquer um dos aparelhos apresentados nas suas estruturas convencionais.

De um modo geral, note-se que os elementos funcionais mencionados, ou seja, o UE, a BSF e a NAF de acordo com a presente invenção, e os seus constituintes podem ser implementados por meios conhecidos, tanto no e/ou software, respetivamente, desde que estejam configurados para executar as funções descritas das respetivas peças. Por exemplo, os meios de autenticação da entidade de cliente podem ser implementados por qualquer unidade de processamento de dados, como por ex. um microprocessador, que esteja configurada para autenticar a rede usando a informação de autenticação recebia de acordo com o método da presente invenção. As peças mencionadas também podem ser realizadas em blocos funcionais individuais ou por meios individuais, ou uma ou várias das peças mencionadas podem ser realizadas num único bloco funcional ou por meios únicos. Correspondentemente, a ilustração acima das Figuras 8 até 10 serve apenas fins ilustrativos e não restringe uma implementação da presente invenção, seja de que forma for.

Em resumo, são apresentados métodos, uma entidade de cliente, entidades de rede, um sistema e um produto de

programa informático para realizar a autenticação entre uma entidade de cliente e uma rede, compreendendo a rede pelo menos uma entidade de função de servidor de bootstrap e uma entidade de função de aplicação de rede, e em que a entidade de cliente não é capaz de comunicar com ambas as entidades de rede de um modo bidirecional, em que o ponto de referência Ub padrão entre a entidade de cliente e a entidade de função de servidor de bootstrap não é utilizado para fins de autenticação. Resumindo, a presente invenção apresenta a autenticação, usando a funcionalidade GAA para ligações de rede unidirecionais.

De acordo com um aspeto vantajoso da presente invenção, a rede é uma rede de transmissão.

Apesar de a invenção ter sido acima descrita com referência aos exemplos apresentados nos desenhos anexos, é óbvio que ela não se limita a esses. Muito pelo contrário, é evidente aos profissionais do ramo que a presente invenção pode ser modificada em muitas maneiras sem sair do âmbito da ideia da invenção conforme apresentada nas reivindicações anexas.

REIVINDICAÇÕES

1. Um método que compreende

realizar a autenticação entre uma entidade de cliente (UE) e uma rede com, no mínimo, uma entidade de função de servidor de bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) possui uma ligação de rede unidirecional sem um canal de retorno da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que a autenticação compreende:

transmitir (S62) um pedido de informação de autenticação da entidade de função de aplicação de rede à entidade de função de servidor de bootstrap, compreendendo o referido pedido uma identidade privada da entidade de cliente, quando a entidade de função de aplicação de rede precisa de transmitir, com segurança, dados para a entidade de cliente

processar (S63) o pedido e recuperar a informação de autenticação na entidade de função de servidor de bootstrap, em que a referida recuperação compreende a criação de dados de sessão de bootstrapping para a entidade de cliente;

transmitir (S64) uma resposta incluindo a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente desde a entidade de função de servidor de bootstrap até à entidade de função de aplicação de rede;

transmitir (S66) a informação de autenticação que compreende os dados de sessão de bootstrap para a

entidade de cliente e os dados por transmitir a partir da entidade de função de aplicação de rede para a entidade de cliente; e

autenticar (S67) a rede usando a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente na entidade de cliente, em que a referida autenticação compreende realizar uma autenticação que inclui uma autenticação genérica de acordo com a arquitetura de autenticação genérica.

2. O método de acordo com a reivindicação 1, em que a transmissão do pedido é ativada por um meio diferente da entidade de cliente.

3. O método de acordo com a reivindicação 1, em que o pedido compreende ainda uma identidade da entidade de função de aplicação de rede.

4. O método de acordo com a reivindicação 1, em que o processamento do pedido e a recuperação da informação de autenticação compreendem captar a informação de autenticação de um sistema de assinante doméstico (HSS).

5. O método de acordo com a reivindicação 1, em que a informação de autenticação inclui ainda, no mínimo, um parâmetro de desafio aleatório ou um parâmetro de autenticação de rede.

6. O método de acordo com a reivindicação 5, em que a resposta compreende ainda uma chave da entidade de função de aplicação de rede.

7. O método de acordo com a reivindicação 1, em que a transmissão da informação de autenticação compreende ainda transmitir uma identidade da entidade de função de aplicação de rede.

8. O método de acordo com a reivindicação 1, em que a autenticação da rede compreende ainda criar uma chave da entidade de função de aplicação de rede na entidade de cliente.

9. O método de acordo com a reivindicação 1, em que a autenticação da rede compreende ainda estabelecer uma sessão de bootstrap entre a entidade de cliente e a entidade de função de servidor de bootstrap.

10. O método de acordo com a reivindicação 9, em que o estabelecimento de uma sessão de bootstrap se baseia na informação de autenticação da entidade de função de aplicação de rede.

11. O método de acordo com a reivindicação 1, em que a autenticação da rede compreende ainda guardar os dados de sessão de bootstrap na entidade de cliente.

12. O método de acordo com a reivindicação 1, que compreende ainda determinar se existe uma sessão de

bootstrap válida entre a entidade de cliente e a entidade de função de servidor de bootstrap.

13. O método de acordo com a reivindicação 12, em que a sessão de bootstrap válida existe permanentemente.

14. O método de acordo com a reivindicação 12, em que o processamento do pedido compreende ainda ativar a entidade de cliente para estabelecer a sessão de bootstrap válida.

15. O método de acordo com a reivindicação 12, em que a resposta compreende ainda uma chave da entidade de função de aplicação de rede.

16. O método de acordo com a reivindicação 12, em que a autenticação da rede compreende ainda criar uma chave da entidade de função de aplicação de rede na entidade de cliente.

17. O método de acordo com a reivindicação 1, que compreende ainda contactar inicialmente a entidade de função de aplicação de rede e enviar uma identidade privada da entidade de cliente, através da entidade de cliente.

18. O método de acordo com a reivindicação 1, que compreende ainda ativar, através da entidade de função de aplicação de rede, a entidade de cliente para estabelecer uma sessão de bootstrap válida.

19. O método de acordo com a reivindicação 1, que compreende ainda ativar, através da entidade de função de aplicação de rede, a entidade de função de servidor de bootstrap, de modo a ativar um procedimento de bootstrap não solicitado com a entidade de cliente.

20. O método de acordo com a reivindicação 1, que compreende ainda codificar os dados por transmitir na entidade de função de aplicação de rede, usando uma chave da função de aplicação de rede.

21. O método de acordo com a reivindicação 20, que compreende ainda descodificar os dados na entidade de cliente, usando a chave da entidade de função de aplicação de rede.

22. O método de acordo com a reivindicação 1, em que a rede compreende uma rede de transmissão.

23. Um programa informático incorporado num meio de leitura informático, que está configurado para carregar para uma memória de um meio de processamento digital e para controlar o referido meio de processamento digital para realizar o método de acordo com qualquer uma das reivindicações de 1 a 22.

24. Um aparelho

operável como uma entidade de cliente para usar dentro de uma arquitetura de autenticação para realizar a autenticação entre a entidade de cliente (UE) e uma rede com, no mínimo, uma entidade de função de servidor de

bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) é operável de modo a possuir uma ligação de rede unidirecional sem um canal de retorno da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que o referido aparelho compreende:

meios de receção (87) para receber, a partir da entidade de função de aplicação de rede, informação de autenticação da entidade de função de servidor de bootstrap e dados por transmitir a partir da entidade de função de aplicação de rede até à entidade de cliente, compreendendo a referida informação de autenticação dados de sessão de bootstrap para a entidade de cliente, e

meios de autenticação (81) para autenticar a rede usando a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente, em que a referida autenticação compreende realizar uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

25. O aparelho de acordo com a reivindicação 24, que compreende ainda meios de criação de chaves (82) para criar uma chave da entidade de função de aplicação de rede.

26. O aparelho de acordo com a reivindicação 24, que compreende ainda meios de estabelecimento (84) para

estabelecer uma sessão de bootstrap entre o aparelho e a entidade de função de servidor de bootstrap.

27. O aparelho de acordo com a reivindicação 24, que compreende ainda meios de armazenamento (85) para guardar os dados de sessão de bootstrap.

28. O aparelho de acordo com a reivindicação 24, que compreende ainda meios de descodificação (83) para descodificar dados codificados recebidos a partir da entidade de função de aplicação de rede, usando uma chave da entidade de função de aplicação de rede.

29. O aparelho de acordo com a reivindicação 24, que compreende ainda meios de processamento e de controlo (86) para processar dados e sinalizar e para controlar o aparelho e os seus meios constituintes.

30. O aparelho de acordo com a reivindicação 25, em que o aparelho compreende, no mínimo, um equipamento de utilizador e pode ser ligado a um módulo universal de identidade de assinante,

31. O método de acordo com a reivindicação 24, em que a entidade de cliente compreende uma caixa adaptadora.

32. O aparelho de acordo com a reivindicação 31, em que os meios de autenticação estão configurados para aceder à informação da identidade do utilizador disponível no aparelho.

33. O aparelho de acordo com a reivindicação 32, em que a informação da entidade do utilizador é guardada num cartão inteligente que pode ser ligado à entidade de cliente.

34. Um método que compreende

realizar a autenticação entre uma entidade de cliente (UE) e uma rede com, no mínimo, uma entidade de função de servidor de bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) possui uma ligação de rede unidirecional sem um canal de retorno da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que a autenticação compreende

receber (S66), a partir da entidade de função de aplicação de rede, informação de autenticação da entidade de função de servidor de bootstrap e dados por transmitir a partir da entidade de função de aplicação de rede, compreendendo a referida informação de autenticação dados de sessão de bootstrap para a entidade de cliente, e

autenticar (S67) a rede usando a informação de autenticação recebida que compreende os dados de sessão de bootstrap para a entidade de cliente, em que a referida autenticação compreende realizar uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

35. O método de acordo com a reivindicação 34, que compreende ainda criar uma chave da entidade de função de aplicação de rede.

36. O método de acordo com a reivindicação 34, que compreende ainda estabelecer uma sessão de bootstrap entre a entidade de cliente e a entidade de função de servidor de bootstrap.

37. O método de acordo com a reivindicação 34, que compreende ainda guardar os dados de sessão de bootstrap.

38. O método de acordo com a reivindicação 34, que compreende ainda descodificar dados codificados recebidos a partir da entidade de função de aplicação de rede, usando uma chave da entidade de função de aplicação de rede.

39. O método de acordo com a reivindicação 34, que compreende ainda processar dados e sinalizar, e controlar a entidade de cliente e os seus meios constituintes.

40. Um programa informático incorporado num meio de leitura informático, que está configurado para carregar para uma memória de um meio de processamento digital e para controlar o referido meio de processamento digital para realizar o método de acordo com qualquer uma das reivindicações de 34 a 39.

41. Um aparelho

operável como uma entidade de função de aplicação de rede para usar dentro de uma arquitetura de autenticação para realizar a autenticação entre a entidade de cliente (UE) e uma rede, em que a rede compreende, no mínimo, o aparelho que opera como uma entidade de função de aplicação de rede (NAF) e uma entidade de função de servidor de

bootstrap (BSF), em que a entidade de cliente (UE) é operável de modo a possuir uma ligação de rede unidirecional sem um canal de retorno da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que o aparelho compreende:

meios transcetores (91) para enviar à entidade de cliente e para enviar e receber da entidade de função de servidor de bootstrap,

em que os meios transcetores estão adaptados para transmitir um pedido de informação de autenticação para a entidade de função de servidor de bootstrap, compreendendo o referido pedido uma identidade privada da entidade de cliente, quando a entidade de função de aplicação de rede precisa de transmitir com segurança dados para a entidade de cliente,

receber uma resposta incluindo a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente a partir da entidade de função de servidor de bootstrap, e

transmitir a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente e os dados por transmitir à entidade de cliente,

em que a referida informação de autenticação é adaptada a uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

42. O aparelho de acordo com a reivindicação 41, em que os meios transcetores (91) estão configurados para transmitir uma identidade da entidade de função de aplicação de rede à entidade de cliente.

43. O aparelho de acordo com a reivindicação 41, que compreende ainda meios de codificação (92) para codificar os dados por transmitir à entidade de cliente, usando uma chave da entidade de função de aplicação de rede.

44. Um aparelho de acordo com a reivindicação 41, em que o aparelho está configurado para difundir transmissões.

45. Um método que compreende

realizar a autenticação entre uma entidade de cliente (UE) e uma rede com, no mínimo, uma entidade de função de servidor de bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) possui uma ligação de rede unidirecional sem um canal de retorno da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que a autenticação compreende

transmitir (S62) um pedido de informação de autenticação à entidade de função de servidor de bootstrap, em que o referido pedido compreende uma identidade privada da entidade de cliente, quando a entidade de função de aplicação de rede precisa de transmitir com segurança dados à entidade de cliente, recebendo (S64) uma resposta que inclui a informação de autenticação que compreende dados de sessão de bootstrap para a entidade de cliente a partir da entidade de função de servidor de bootstrap, e

transmitir (S66) a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente e os dados por transmitir à entidade de cliente,

em que a referida informação de autenticação é adaptada a uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

46. O método de acordo com a reivindicação 45, que compreende ainda transmitir uma identidade da entidade de função de aplicação de rede à entidade de cliente.

47. O aparelho de acordo com a reivindicação 45, que compreende ainda codificar os dados por transmitir à entidade de cliente, usando uma chave da entidade de função de aplicação de rede.

48. Um programa informático incorporado num meio de leitura informático, que está configurado para carregar para uma memória de um meio de processamento digital e para controlar o referido meio de processamento digital para realizar o método de acordo com qualquer uma das reivindicações de 45 a 47.

49. Um aparelho

operável como uma entidade de função de servidor de bootstrap para usar dentro de uma arquitetura de autenticação para realizar a autenticação entre a entidade de cliente (UE) e uma rede, em que a rede compreende, no mínimo, o aparelho que opera como uma entidade de função de servidor de bootstrap (BSF) e uma entidade de função de

aplicação de rede (NAF), em que a entidade de cliente (UE) é operável para possuir uma ligação de rede unidirecional sem um canal de retorno da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que o aparelho compreende:

meios transcetores (101) para enviar e receber da entidade de função de aplicação de rede, e

meios de processamento e recuperação (102) para processar um pedido recebido da unidade de função de aplicação de rede, em que o referido pedido compreende uma identidade privada da entidade de cliente, e para recuperar a informação de autenticação, compreendendo ainda os referidos meios de processamento e de recuperação meios de criação (104) para criar dados de sessão de bootstrap para a entidade de cliente,

em que os meios transcetores (101) estão configurados para receber o pedido da entidade de função de aplicação de rede e para transmitir a informação de autenticação que compreende os dados de sessão de bootstrap para a entidade de cliente à entidade de função de aplicação de rede,

em que a referida informação de autenticação é adaptada a uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

50. O aparelho de acordo com a reivindicação 49, que compreende ainda meios de captação (105) para captar a

informação de autenticação de um sistema de assinante doméstico (HSS).

51. O aparelho de acordo com a reivindicação 49, que compreende ainda meios de ativação (103) para ativar a entidade de cliente de modo a estabelecer uma sessão de bootstrap válida.

52. O aparelho de acordo com a reivindicação 49, em que a rede compreende uma rede de transmissão.

53. Um método que compreende

realizar a autenticação entre uma entidade de cliente (UE) e uma rede com, no mínimo, uma entidade de função de servidor de bootstrap (BSF) e uma entidade de função de aplicação de rede (NAF), em que a entidade de cliente (UE) possui uma ligação de rede unidirecional sem um canal de retorno da entidade de cliente para a entidade de função de servidor de bootstrap (BSF) e/ou a entidade de função de aplicação de rede (NAF), em que a autenticação compreende

receber (S62) um pedido de informação de autenticação da entidade de função de aplicação de rede, em que o referido pedido compreende uma identidade privada da entidade de cliente,

processar (S63) o pedido recebido da entidade de função de aplicação de rede e recuperar informação de autenticação, compreendendo ainda criar dados de sessão de bootstrap para a entidade de cliente,

transmitir (S64) uma resposta que inclui a informação de autenticação que compreende os dados de sessão de

bootstrap para a entidade de cliente à entidade de função de aplicação de rede,

em que a referida informação de autenticação é adaptada a uma autenticação que inclui uma autenticação genérica de acordo com uma arquitetura de autenticação genérica.

54. O aparelho de acordo com a reivindicação 53, que compreende ainda captar a informação de autenticação de um sistema de assinante doméstico (HSS).

55. O aparelho de acordo com a reivindicação 53, que compreende ainda ativar a entidade de cliente para estabelecer uma sessão de bootstrap válida.

56. Um programa informático incorporado num meio de leitura informático, que está configurado para carregar para uma memória de um meio de processamento digital e para controlar o referido meio de processamento digital de modo a realizar o método de acordo com qualquer uma das reivindicações de 53 a 55.

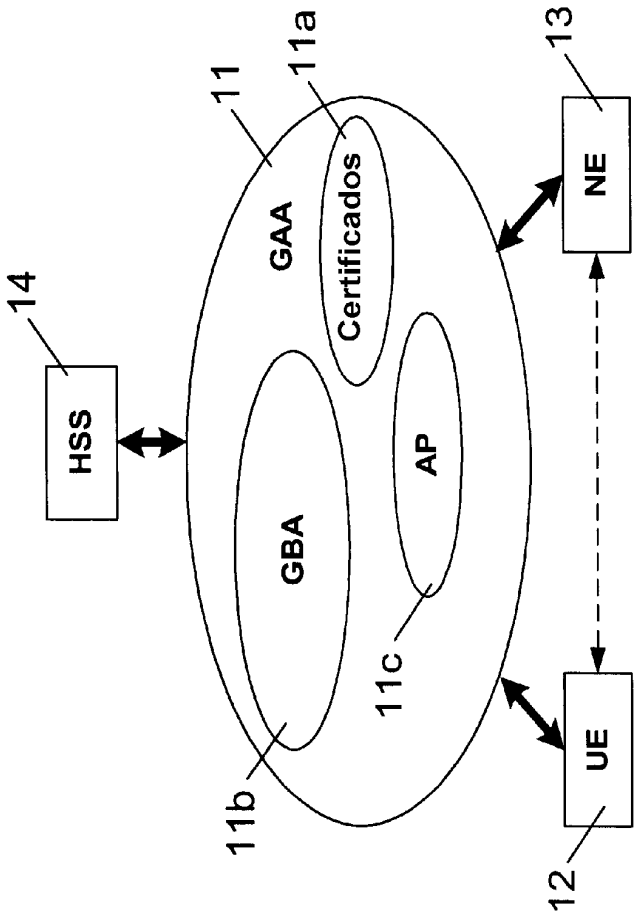

Figura 1

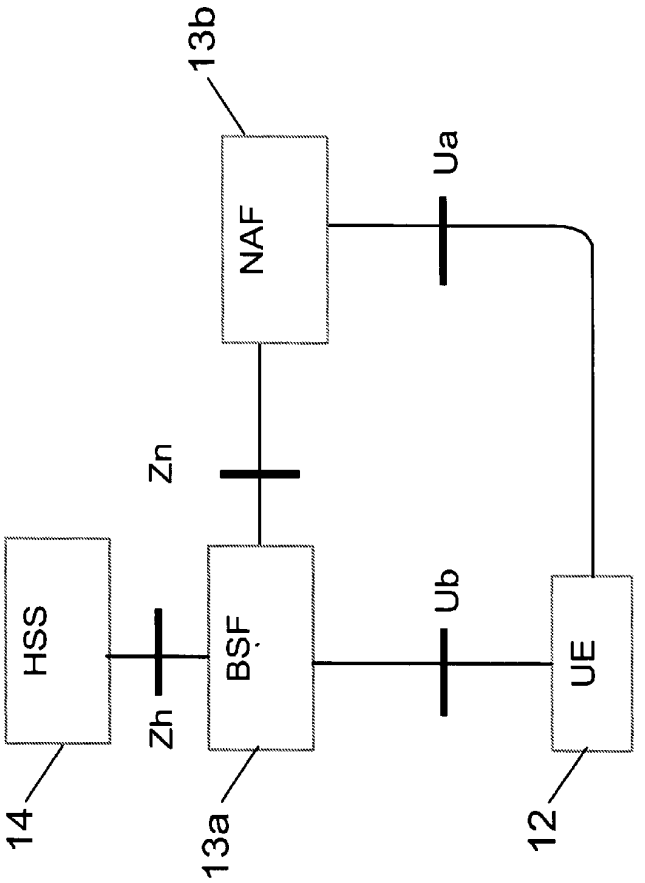

FIGURA 2

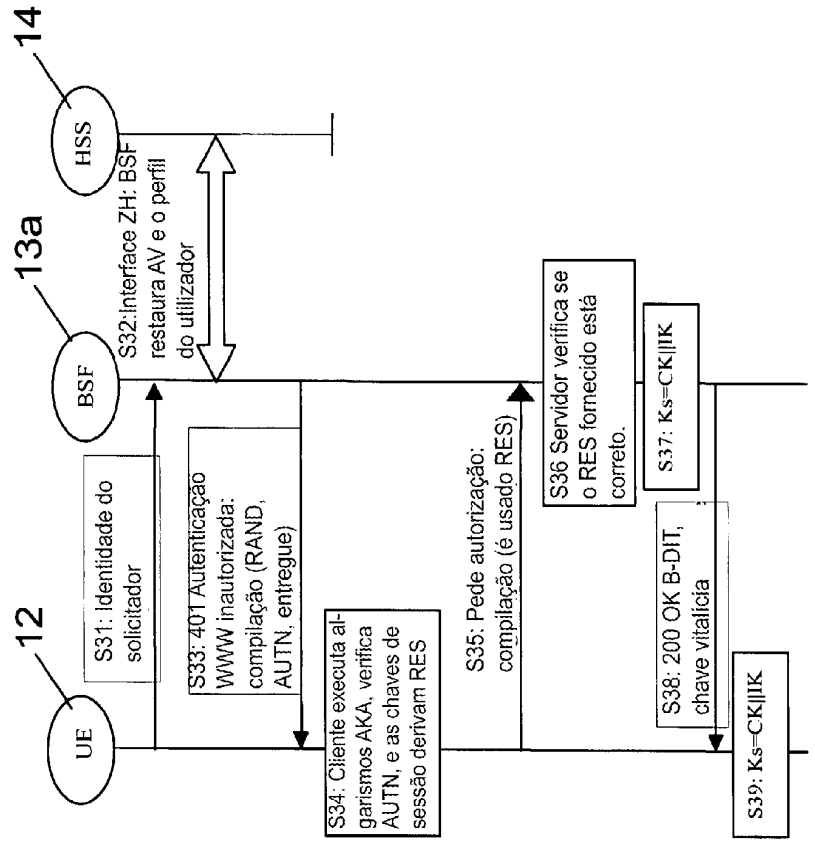
14
HSS
13a
BSF
12
UE
S32:Interface ZH: BSF restaura AV e o perfil do utilizador
S31: Identidade do solicitador
S33: 401 Autenticação WWW inautorizada: compilação (RAND, AUTN, entregue)
S34: Cliente executa algarismos AKA, verifica AUTN, e as chaves de sessão derivam RES
S35: Pede autorização: compilação (é usado RES)
S36 Servidor verifica se o RES fornecido está correto.
S37: Ks=CK||IK
S38: 200 OK B-DIT, chave vitalícia
S39: Ks=CK||IK

Figura 3

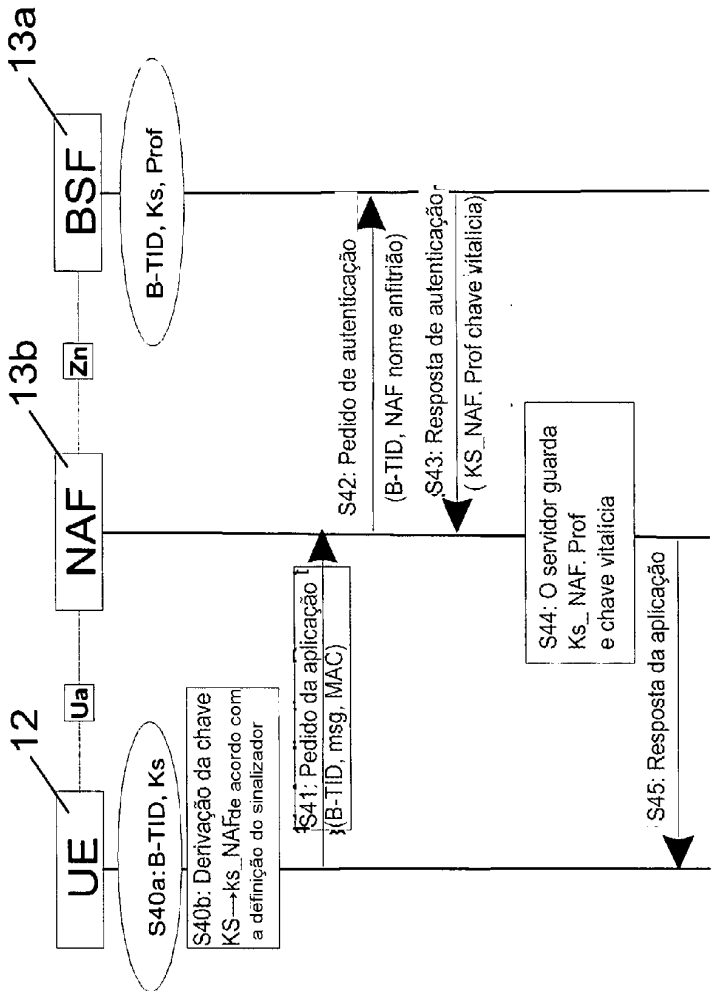
13a
BSF
B-TID, Ks, Prof
13b
Zn
NAF
12
Ua
UE
S40a: B-TID, Ks
S40b: Derivação da chave
KS→ks_NAF de acordo com
a definição do sinalizador
S41: Pedido da aplicação
(B-TID, msg, MAC)
S42: Pedido de autenticação
(B-TID, NAF nome anfitrião)
S43: Resposta de autenticação
(KS_NAF, Prof chave vitalicia)
S44: O servidor guarda
Ks_ NAF. Prof
e chave vitalicia
S45: Resposta da aplicação

Figura 4

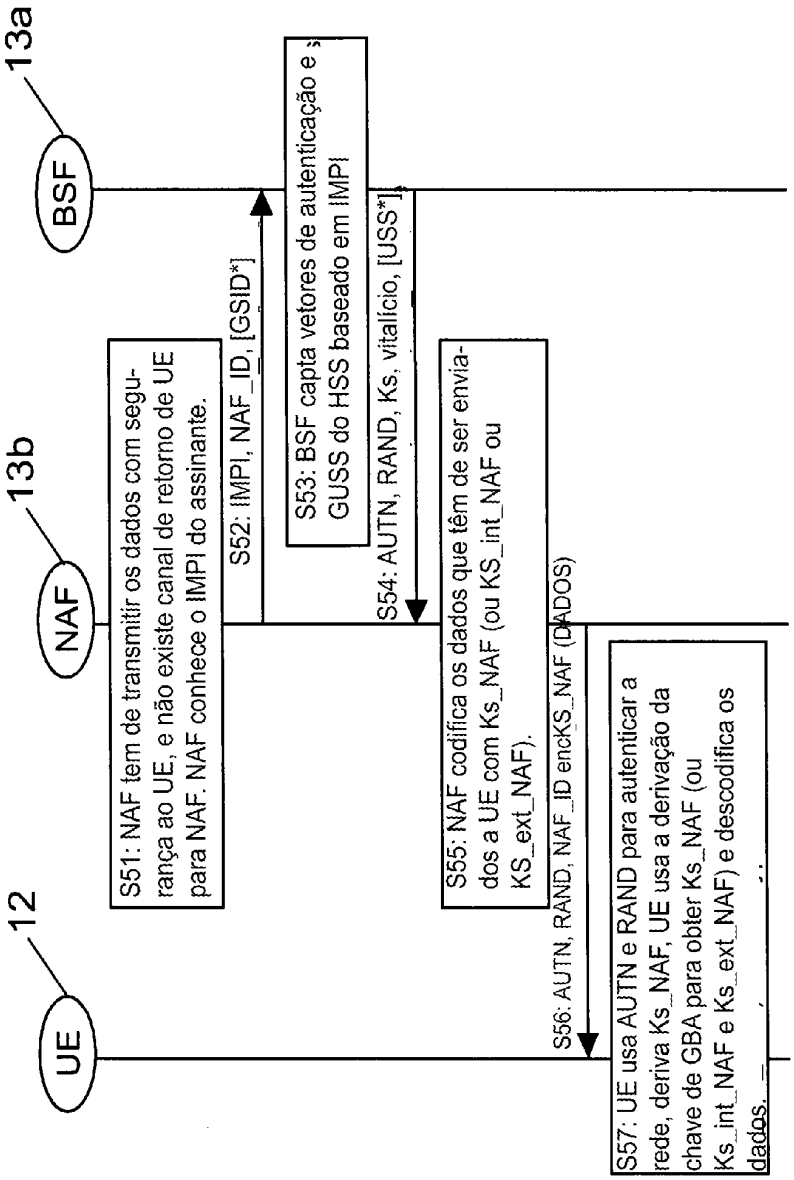
12
UE
13b
NAF
13a
BSF
S51: NAF tem de transmitir os dados com segurança ao UE, e não existe canal de retorno de UE para NAF. NAF conhece o IMPI do assinante.
S52: IMPI, NAF_ID, [GSID*]
S53: BSF capta vetores de autenticação e GUSS do HSS baseado em IMPI
S54: AUTN, RAND, Ks, vitalício, [USS*]
S55: NAF codifica os dados que têm de ser enviados a UE com Ks_NAF (ou KS_int_NAF ou KS_ext_NAF).
S56: AUTN, RAND, NAF_ID encKS_NAF (DADOS)
S57: UE usa AUTN e RAND para autenticar a rede, deriva Ks_NAF, UE usa a derivação da chave de GBA para obter Ks_NAF (ou Ks_int_NAF e Ks_ext_NAF) e descodifica os dados.

Figura 5

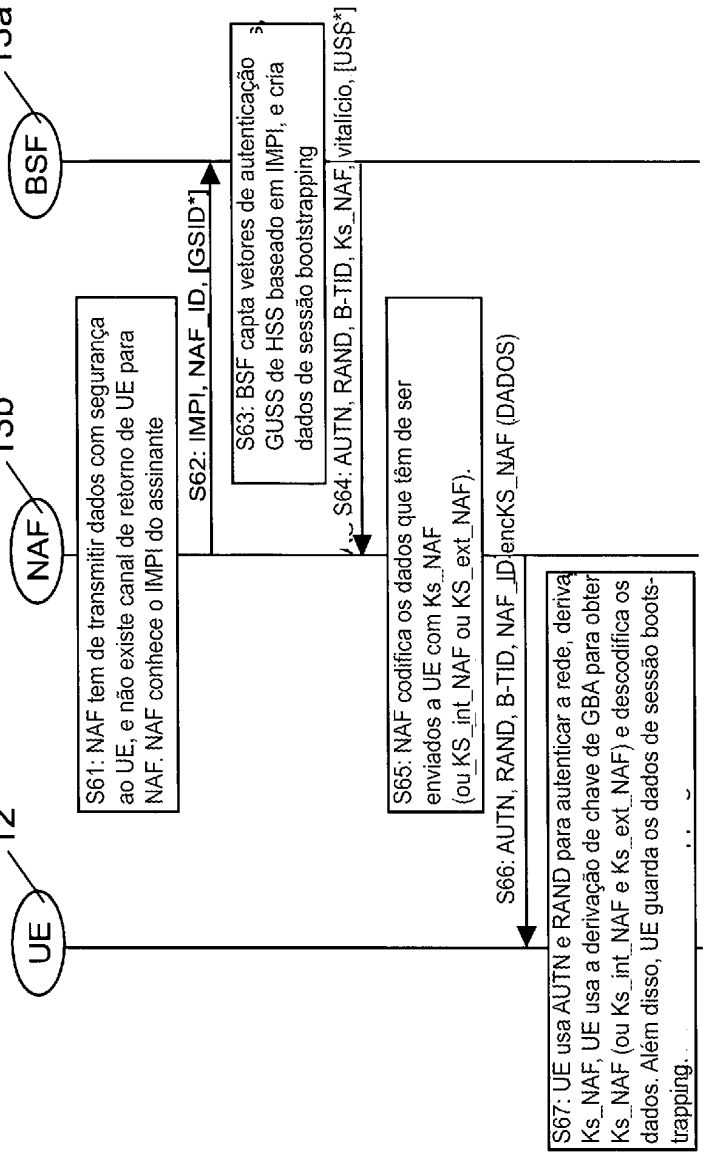
12
UE
13b
NAF
13a
BSF
S61: NAF tem de transmitir dados com segurança ao UE, e não existe canal de retorno de UE para NAF. NAF conhece o IMPI do assinante
S62: IMPI, NAF_ID, [GSID*]
S63: BSF capta vetores de autenticação GUSS de HSS baseado em IMPI, e cria dados de sessão bootstrapping
S64: AUTN, RAND, B-TID, Ks_NAF, vitalício, [USS*]
S65: NAF codifica os dados que têm de ser enviados a UE com Ks_NAF (ou KS_int_NAF ou KS_ext_NAF).
S66: AUTN, RAND, B-TID, NAF_ID, encKS_NAF (DADOS)
S67: UE usa AUTN e RAND para autenticar a rede, deriva Ks_NAF, UE usa a derivação de chave de GBA para obter Ks_NAF (ou Ks_int_NAF e Ks_ext_NAF) e descodifica os dados. Além disso, UE guarda os dados de sessão boots-trapping.

Figura 6

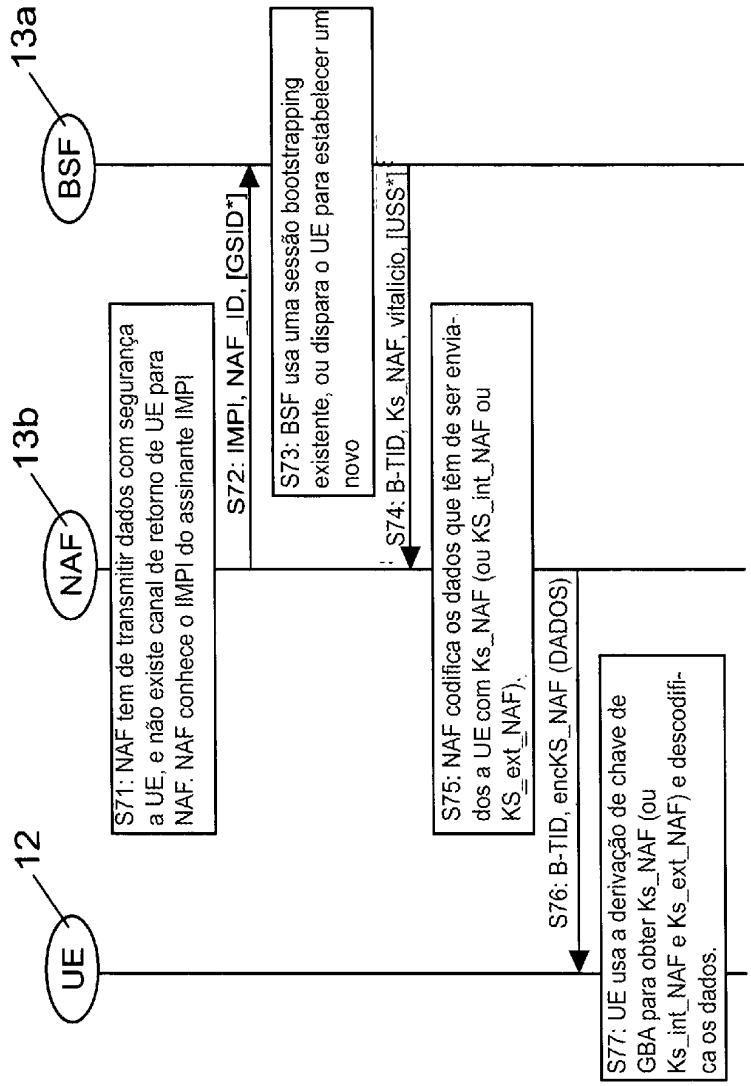
12
UE
13b
NAF
13a
BSF
S71: NAF tem de transmitir dados com segurança a UE, e não existe canal de retorno de UE para NAF. NAF conhece o IMPI do assinante IMPI
S72: IMPI, NAF_ID, [GSID*]
S73: BSF usa uma sessão bootstrapping existente, ou dispara o UE para estabelecer um novo
S74: B-TID, Ks_NAF, vitalicio, [USS*]
S75: NAF codifica os dados que têm de ser enviados a UE com Ks_NAF (ou KS_int_NAF ou KS_ext_NAF).
S76: B-TID, encKS_NAF (DADOS)
S77: UE usa a derivação de chave de GBA para obter Ks_NAF (ou Ks_int_NAF e Ks_ext_NAF) e descodifica os dados.

Figura 7

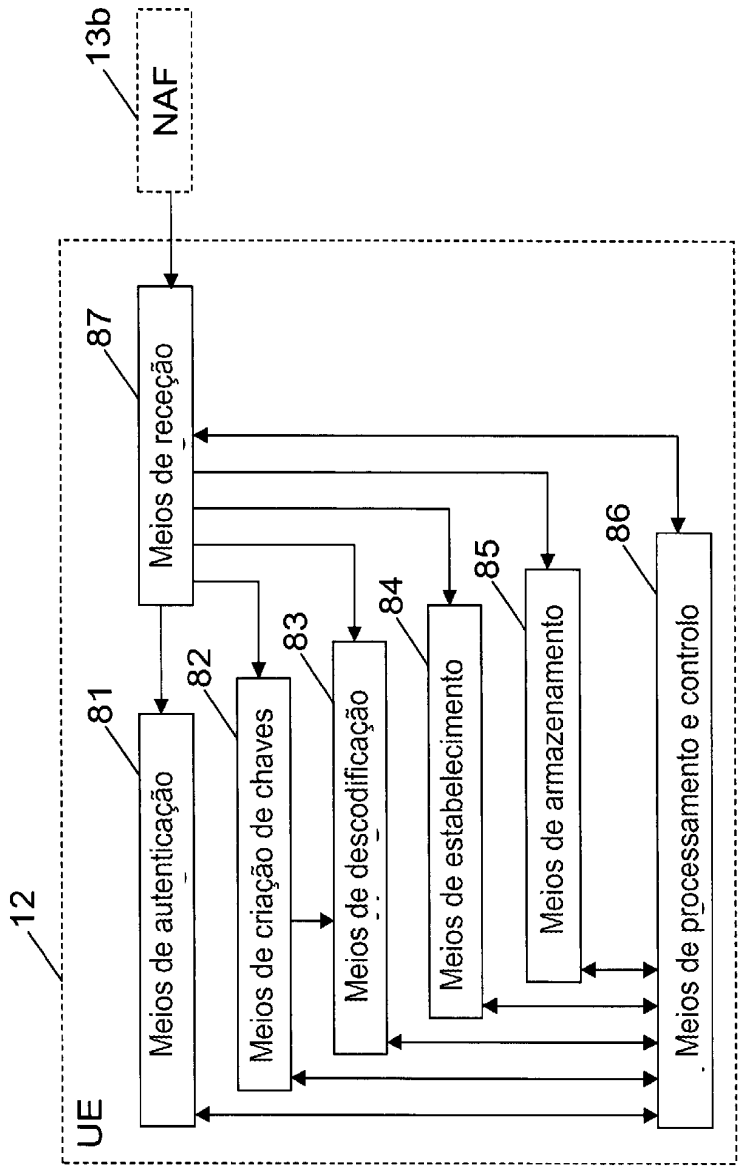
13b
NAF
12
UE
87
Meios de receção
81
Meios de autenticação
82
Meios de criação de chaves
83
Meios de descodificação
84
Meios de estabelecimento
85
Meios de armazenamento
86
Meios de processamento e controlo

Figura 8

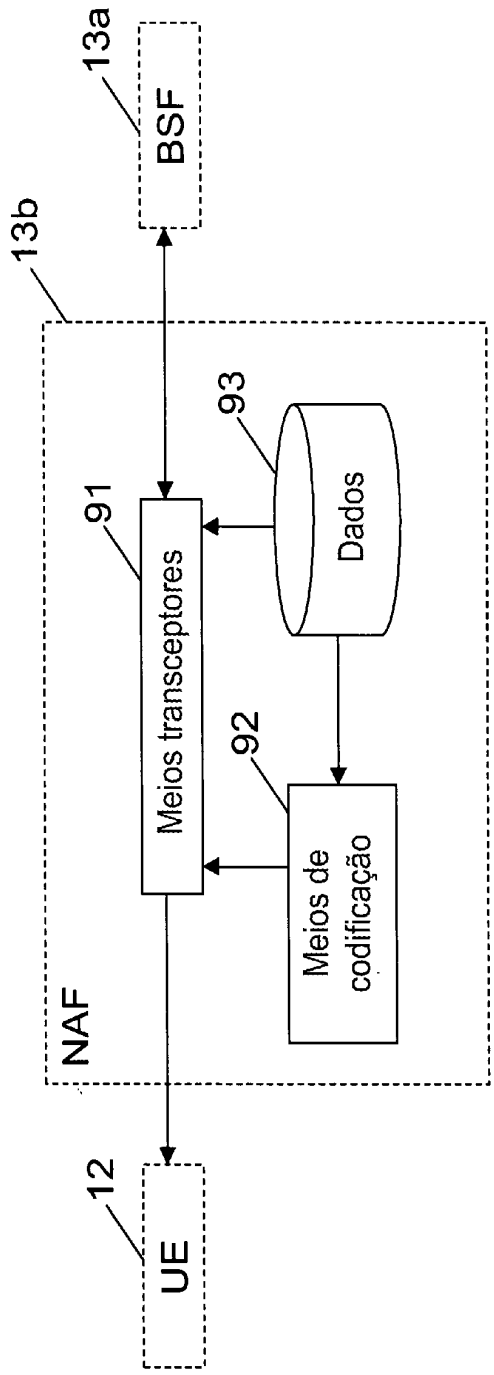
13a
BSF
13b
93
Dados
91
Meios transceptores
92
Meios de codificação
NAF
12
UE

Figura 9

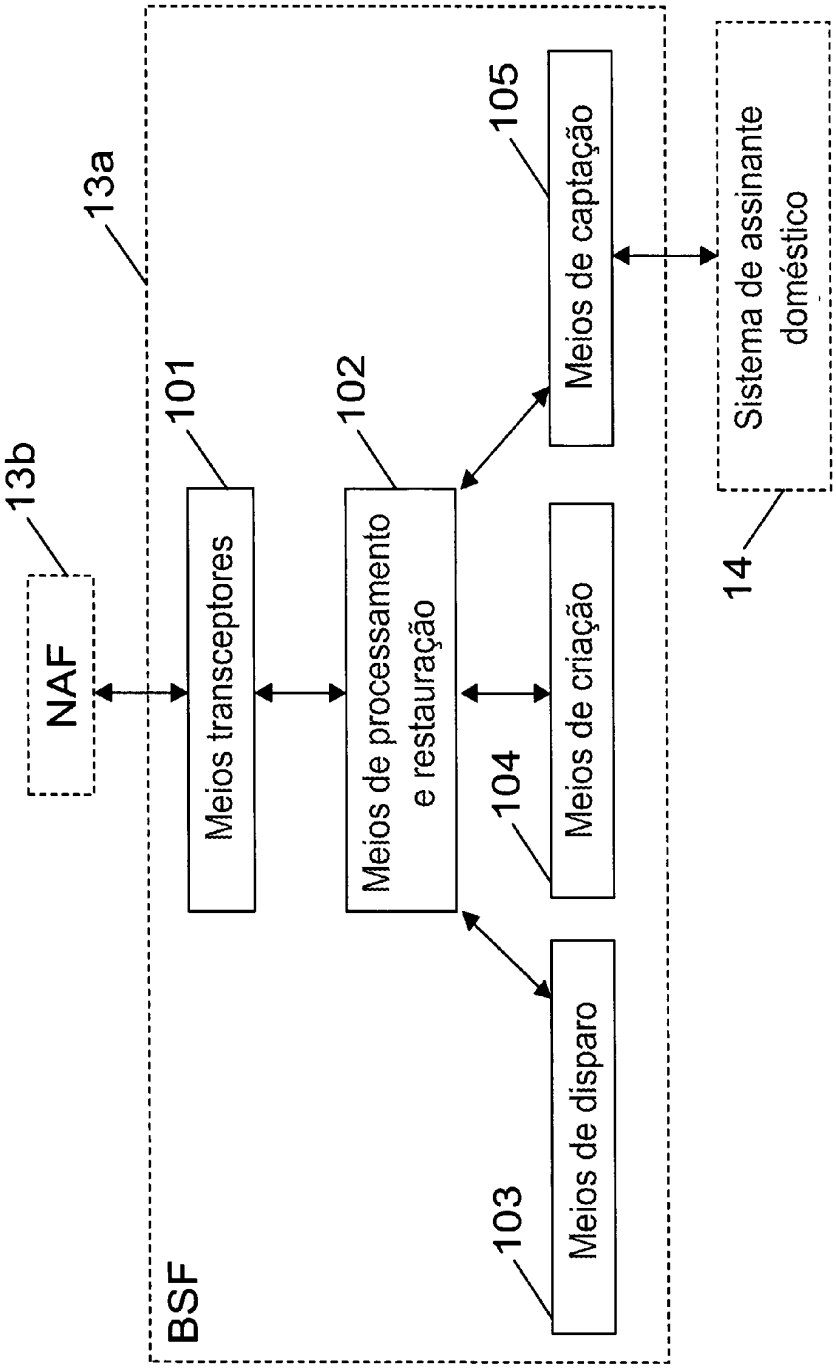
13a
13b
NAF
BSF
101
Meios transceptores
102
Meios de processamento e restauração
103
Meios de disparo
104
Meios de criação
105
Meios de captação
14
Sistema de assinante doméstico

Figura 10