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

(21) **PI0617286-5 A2**

BRPI0617286A2

(22) Data de Depósito: 10/10/2006
(43) Data da Publicação: 19/07/2011
(RPI 2115)

(51) Int.Cl.:
H04L 29/08 2006.01
H04L 12/56 2006.01
H04L 29/06 2006.01

(54) Título: **MÉTODOS PARA ESTABELECER UMA ASSOCIAÇÃO DE SEGURANÇA ENTRE UM NÓ DE SERVIÇO E UM CLIENTE, PARA ESTABELECER UMA ASSOCIAÇÃO DE SEGURANÇA ENTRE PRIMEIRO E SEGUNDO CLIENTES, E PARA PROTEGER UM NÓ CONTRA ATAQUES DE REPETIÇÃO, NÓ DE SERVIÇO, TERMINAL DE CLIENTE, E, FUNÇÃO DE GERAÇÃO DE CÓDIGO**

(30) Prioridade Unionista: 13/10/2005 US 11/248589, 19/12/2005 US 11/305329

(73) Titular(es): Telefonaktiebolaget LM Ericsson (publ)

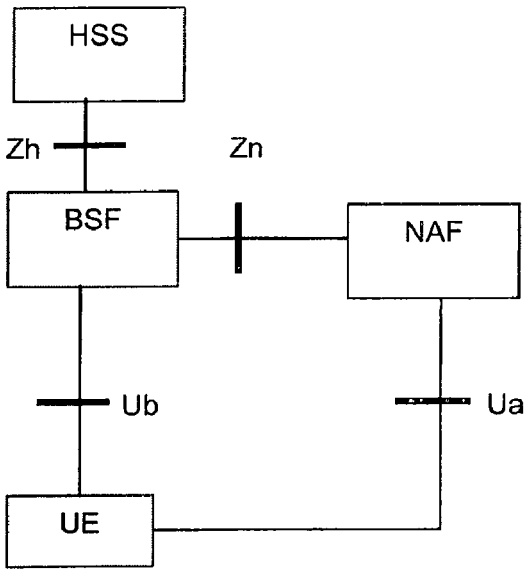
(72) Inventor(es): Karl Norrman, Rolf Blom

(74) Procurador(es): MOMSEN LEONARDOS & CIA

(86) Pedido Internacional: PCT EP2006067225 de 10/10/2006

(87) Publicação Internacional: WO 2007/042512de 19/04/2007

(57) Resumo: MÉTODOS PARA ESTABELECER UMA ASSOCIAÇÃO DE SEGURANÇA ENTRE UM NÓ DE SERVIÇO E UM CLIENTE, PARA ESTABELECER UMA ASSOCIAÇÃO DE SEGURANÇA ENTRE PRIMEIRO E SEGUNDO CLIENTES, E PARA PROTEGER UM NÓ CONTRA ATAQUES DE REPETIÇÃO, NÓ DE SERVIÇO, TERMINAL DE CLIENTE, E, FUNÇÃO DE GERAÇÃO DE CÓDIGO. Método para estabelecer uma associação de segurança entre um cliente e um nó de serviço para a finalidade de inserir informação do nó de serviço para o cliente, onde o cliente e um servidor de código compartilham um segredo básico. O método compreende enviar uma requisição para geração e provisão de um código de serviço, do nó de serviço para um servidor de código, a requisição identificando o cliente e o nó de serviço, gerar um código de serviço no servidor de código usando as identidades do cliente e do nó de serviço, o segredo básico e informação adicional, e enviar o código de serviço ao nó de serviço, juntamente com citada informação adicional, enviar citada informação adicional do nó de serviço para o cliente e, no cliente, gerar citado código de serviço usando a informação adicional recebida e o código base. Uma abordagem similar pode ser usada para prover gerenciamento de código p2p.



"MÉTODOS PARA ESTABELECER UMA ASSOCIAÇÃO DE SEGURANÇA ENTRE UM NÓ DE SERVIÇO E UM CLIENTE, PARA ESTABELECER UMA ASSOCIAÇÃO DE SEGURANÇA ENTRE PRIMEIRO E SEGUNDO CLIENTES, E PARA PROTEGER UM NÓ CONTRA ATAQUES DE REPETIÇÃO, NÓ DE SERVIÇO, TERMINAL DE CLIENTE, E, FUNÇÃO DE GERAÇÃO DE CÓDIGO"

Campo da invenção

A presente invenção relaciona-se a um método e aparelho para estabelecer uma associação de segurança entre um terminal de cliente e um nó de serviço, no sentido de fornecer um serviço tipo inserção (SMS melhorado) e, em particular, embora não necessariamente, a tal método e aparelho que emprega uma Arquitetura *Bootstrapping* Genérica.

Fundamentos da Invenção

No sentido de facilitar a provisão de serviços a terminais de usuário, uma rede móvel tal como uma rede 3G freqüentemente requererá o estabelecimento de um canal de comunicação seguro ou "associação de segurança" entre terminais de cliente (isto é, terminais móveis) e os nós de serviço baseados em rede que provêem os serviços. A Arquitetura *Bootstrapping* Genérica (GBA) é discutida na Especificação Técnica 3GPP TS 33.220 e provê um mecanismo pelo qual um terminal de cliente (UE) pode ser autenticado para uma Função de Autenticação de Rede (o nó de serviço) e códigos de sessão segura obtidos para uso entre o terminal de cliente e a Função de Autenticação de Rede. O modelo simples de rede para esta arquitetura é ilustrado na Figura 1. Este mecanismo executa *Bootstrapping* no conhecido procedimento de Autenticação e Acordo de Código (AKA) [GPP TS 33.102] que permite que um terminal de cliente seja autenticado para uma Função de Servidor de *Bootstrapping* (BSF) da rede doméstica do cliente, com base em um K secreto que é compartilhado entre o USIM do terminal de cliente e o Sistema de Assinante Doméstico (KSS) da rede doméstica do

assinante. O procedimento AKA estabelece adicionalmente códigos de sessão a partir dos quais códigos são derivados, os quais são posteriormente aplicados entre o terminal de cliente e uma Função de Aplicação de Rede (NAF). Quando um terminal de cliente e NAF desejam obter códigos de sessão a partir da BSF, a NAF envia um identificador de transação à BSF, o identificador de transação contendo um índice que a BSF usa para identificar o terminal de cliente e códigos apropriados que este envia ao NAF.

De acordo com o mecanismo GBA, o UE inicia o processo de geração de código enviando uma requisição contendo uma identidade de usuário ao BSF. A requisição também contém a identidade da NAF. A BSF recupera um vetor de autenticação a partir do Servidor de Assinante Doméstico (HSS), cada vetor de autenticação consistindo de um número randômico RAND, uma resposta esperada XRES, um código cifrado CK, um código de integridade IK e um ficha de autenticação AUTN. A BSF gera material de código KS concatenando CK e IK contidos dentro do vetor de autenticação. A BSF gera um identificador de código B-TID no formato NAI por codificação de base 64 do valor RAND e combinando o valor codificado com o nome do servidor BSF, isto é, como

base64encode(RAND)@BSF_servers_domain_name.

A BSF retém o código KS em associação com o identificador de transação B-TID e a identidade NAF. O B-TID e AUTN são enviados pela BSF ao UE, o USIM do terminal de cliente verificando o valor AUTN usando o K secreto compartilhado e retornando uma compilação do resultado esperado XRES à BSF. O USIM também gera o material de código KS usando o K secreto e o valor RAND (recuperado) do B-TID.

Em seguida à conclusão deste procedimento, o UE comunica à NAF, o B-TID recebido. A NAF e a BSF são autenticadas uma à outra, e a NAF envia à BSF o B-TID recebido juntamente com sua própria identidade. A BSF usa o B-TID e a identidade da NAF para localizar o código KS correto

e usa KS para gerar um código NAF. Outra informação tal como a identidade NAF é também usada na geração do código NAF. O código NAF gerado é retornado à NAF. O UE é similarmente capaz de gerar o código NAF usando o código KS que este já tenha gerado.

Após o mecanismo GBA ter sido executado pela primeira vez, requisições subseqüentes para estabelecer uma associação de segurança entre o UE e a mesma ou uma NAF diferente pode usar o material de código KS já estabelecido, desde que aquele código não tenha expirado. Entretanto, isto ainda requererá que o UE inicie uma requisição para estabelecimento de uma associação de segurança enviando seu B-TID à NAF.

Sumário da Invenção

Há ocasiões nas quais é desejável permitir que a NAF inicie o estabelecimento de uma associação de segurança com o UE. Por exemplo, pode-se considerar um serviço tipo inserção que fornece informação de notícias, esportes, e finanças, etc., a usuários que tenham se registrado previamente para um serviço. Um procedimento operacional típico para obter isto pode ser para o provedor de serviço enviar uma mensagem SMS ao UE que requisita ao usuário para abrir uma conexão segura. Entretanto, há muitas ameaças relacionadas a este modelo pois uma SMS pode ser manipulada, enviada por uma parte não autorizada, ser repetida, etc. Se existiu uma associação de segurança, ou o nó de serviço pôde iniciar uma, antes que os dados de serviços reais sejam enviados, os procedimentos de segurança poderiam ser baseados nisto e a maioria dos problemas poderiam ser minimizada.

De acordo com um primeiro aspecto da presente invenção, é provido um método para estabelecer uma associação de segurança entre um primeiro nó e um segundo nó para a finalidade de inserir informação a partir do primeiro nó para o segundo nó, onde o segundo nó e uma função de geração de código compartilham um segredo básico, o método

compreendendo:

- enviar uma requisição para geração e provisão de um código de serviço a partir do primeiro nó para a função de geração de código, a requisição contendo identidades do primeiro e segundo nós;
- gerar um código de serviço na função de geração de código, usando a identidade do primeiro nó, o segredo básico e informação adicional, e enviar o código de serviço ao primeiro nó juntamente com a citada informação adicional;
- enviar a citada informação adicional e a citada identidade do primeiro nó, a partir do primeiro nó para o segundo nó; e
- no segundo nó, gerar o citado código de serviço usando a informação adicional recebida, a primeira identidade de usuário e o segredo básico.

Será verificado que a função de geração de código pode ser um nó isolado ou pode ser um servidor distribuído. No caso de uma rede 3G empregando a Arquitetura *Bootstrapping* Genérica, uma Função de Servidor de *Bootstrapping* e um Servidor de Assinante Doméstico (HSS) podem juntos prover a função de geração de código, onde a Função de Servidor de *Bootstrapping* se comunica com o nó de serviço e com o Servidor de Assinante Doméstico. No caso de uma rede 2G, a função de geração de código pode ser uma combinação de uma Função de Servidor de *Bootstrapping* e um servidor AuC.

No caso de uma rede 3G empregando a Arquitetura *Bootstrapping* Genérica, o nó de serviço compreende uma Função de Aplicação de Rede. A etapa de gerar um código de serviço na função de geração de código, compreende as etapas de:

- gerar material de código KS usando a citado segredo básico; e
- gerar o código de serviço usando o citado material de

código KS, a identidade do nó de serviço e a citada informação adicional.

A etapa de gerar o código de serviço no cliente também compreende estas duas etapas.

Citada etapa de gerar um código de serviço no servidor de código pode utilizar valores diferentes daqueles enviados ao cliente pelo nó de serviço. O cliente pode obter certos outros valores do servidor de código.

Citada informação adicional pode compreender um ou mais dentre:

um valor randômico;

marcação de tempo;

número de seqüência;

outros identificadores

No caso da Arquitetura *Bootstrapping* Genérica, citado valor randômico é o parâmetro RAND e é levado dentro do B-TID.

Citada informação adicional pode compreender um identificador de transação no formato de NAI, e compreendendo um valor randômico codificado.

Citada informação adicional pode ser enviada do nó de serviço para o cliente em uma mensagem também contendo dados de serviço, os dados de serviço sendo criptografados com o código de serviço, onde o cliente pode decriptografar os dados criptografados uma vez que este tenha gerado o código de serviço.

Em uma realização da invenção, a função de geração de código envia ao nó de serviço um valor de autenticação de rede. O nó de serviço redireciona este valor ao cliente, juntamente com a citada informação adicional. O cliente usa o segredo básico e o valor de autenticação para autenticar a função de geração de código. Somente se a função de geração de código é autenticada o cliente gera e usa o código de serviço.

Em uma realização alternativa da invenção, o cliente requisita

um valor de autenticação a partir da função de geração de código após ter recebido a citada informação adicional do nó de serviço. Somente quando o cliente tiver autenticado a função de geração de código, o código de serviço é gerado e usado.

O terminal pode compreender meios para receber do nó de serviço um código de autenticação de mensagem, o terminal compreendendo meios para gerar um código ou códigos de autenticação a partir de pelo menos uma parte da informação de geração de código, e usando o(s) código(s) de autenticação para autenticar o código de autenticação de mensagem. Os meios de geração podem ser um USIM/ISIM.

Citado código de serviço pode ser um código de Diffie-Hellman para o segundo nó, o método adicionalmente compreendendo a etapa de prover ao primeiro nó um código de Diffie-Hellman para aquele primeiro nó, e enviar o código de Diffie-Hellman para o primeiro nó ao segundo nó, citada associação de segurança sendo estabelecida com base nos dois códigos de Diffie-Hellman diferentes.

De acordo com um segundo aspecto da presente invenção, é provido um nó de serviço para fornecer um serviço de inserção a um cliente, via um enlace de comunicação seguro, o nó de serviço compreendendo:

- meio para enviar uma requisição para geração e provisão de um código de serviço a uma função de geração de código, a requisição identificando o cliente e o nó de serviço;
- meio para receber da função de geração de código um código de serviço, juntamente com a citada informação adicional;
- meio para redirecionar citada informação adicional ao cliente; e
- meio para criptografia e/ou informação de serviço de proteção de integridade, usando o código de serviço e para enviar a informação criptografada e/ou informação protegida ao cliente.

No caso da Arquitetura *Bootstrapping* Genérica, citada informação adicional compreende um B-TID contendo um valor RAND. Citado meio para envio é também arranjado para enviar ao cliente uma identidade do nó de serviço.

De acordo com um terceiro aspecto da invenção é provido um terminal de cliente para receber um serviço inserção fornecido por um nó de serviço, o terminal de cliente compreendendo:

- meio de memória para armazenar um segredo que é compartilhado com uma função de geração de código;
- meio para receber informação de geração de código do citado nó de serviço;
- meio para gerar um código de serviço usando o citado segredo compartilhado e citada informação de geração de código; e
- meio para usar o citado código de serviço para decriptografar e/ou verificar a integridade das comunicações com o nó de serviço.

De acordo com um quarto aspecto da presente invenção, é provida uma função de geração de código para uso ao estabelecer uma associação de segurança entre um cliente e um nó de serviço para a finalidade de inserir informação do nó de serviço para o cliente, o servidor de código compreendendo:

- meio de memória para armazenar um segredo que é compartilhado com o citado cliente;
- meio para receber uma requisição para geração e provisão de um código de serviço a partir do citado nó de serviço, a requisição identificando o cliente e o nó de serviço; e
- meio para gerar um código de serviço usando as identidades do cliente e o nó de serviço, o segredo básico, uma informação adicional, e para enviar o código de serviço ao nó de serviço, juntamente com

a citada informação adicional.

De acordo com um quinto aspecto da presente invenção, é provido um método para estabelecer uma associação de segurança entre o primeiro e segundo clientes, para a finalidade de inserir informação do primeiro cliente para o segundo cliente, onde o primeiro e segundo clientes têm relações acreditadas com o primeiro e segundo servidores de código, respectivamente, e compartilham um segredo com seus respectivos servidores de código, o método compreendendo:

- enviar uma requisição para geração e provisão de um código de serviço do primeiro cliente para o segundo servidor de código, via primeiro servidor de código, a requisição identificando o primeiro e segundo nós;
- gerar um código de serviço no segundo servidor de código usando a identidade do primeiro nó, o segredo básico, e informação adicional, e enviar o código de serviço ao primeiro nó juntamente com a citada informação adicional;
- enviar citada informação adicional do primeiro nó para o segundo nó; e

no segundo nó, gerar citado código de serviço usando a informação adicional recebida e o segredo básico.

De acordo com um sexto aspecto da presente invenção, é provido um método para proteger um nó contra ataques de repetição, o método compreendendo:

gerar um código de serviço em uma função de servidor de *bootstrapping*;

prover o código de serviço a um primeiro nó, juntamente com informação requerida para gerar o código de serviço;

enviar uma mensagem de geração de código do primeiro nó para o segundo nó, a mensagem incluindo a citada informação, um valor de

prevenção de repetição, e um código de autenticação de mensagem calculado através do corpo da mensagem, incluindo o valor de prevenção de repetição, o valor de prevenção de repetição sendo incrementado ou decrementado para cada execução do procedimento;

receber citada mensagem de geração de código no citado segundo nó e armazenar o valor de prevenção de repetição contido nela; e

no segundo nó, cada vez que uma mensagem de geração de código é recebida, verificar o citado código de autenticação de mensagem, determinar se o valor de prevenção de repetição contido na mensagem já foi armazenado ou não no segundo nó, e caso afirmativo, rejeitar a mensagem.

Realizações deste aspecto da invenção permitem que o segundo nó rejeite ataques de repetição com base em mensagens previamente enviadas ao segundo nó, com respeito a um procedimento GBA válido. Se o atacante fosse meramente incrementar aquele valor de prevenção de repetição para um valor não usado previamente, o segundo nó detectaria esta mudança com base no valor MAC incorreto, e daí detectaria o ataque. Novamente, o primeiro nó pode ser um servidor NAF, com o segundo nó sendo um cliente, ou ambos primeiro e segundo nós podem ser clientes. Será verificado que características do primeiro ao quinto aspectos da presente invenção podem ser combinados com aqueles do sexto aspecto, e vice-versa.

Breve Descrição dos Desenhos

Figura 1 ilustra um modelo simples de rede para a Arquitetura *Bootstrapping* Genérica;

Figuras 2 a 7 ilustram fluxos de sinalização associados a respectivos procedimentos para estabelecer uma associação de segurança entre um cliente (UE) e NAF; e

Figuras 8 e 9 ilustram fluxos de sinalização associados a respectivos procedimentos para estabelecer uma associação de segurança entre um par de clientes (UE_A e UE_B).

Descrição Detalhada de Certas Realizações

A Arquitetura *Bootstrapping* Genérica (GBA) para redes 3G têm sido descrita com referência à Figura 1, que ilustra as interfaces (Ua, Ub, Zn e Zh) entre as várias entidades. Devia ser considerado que a descrição está em um nível relativamente alto e implementações reais podem "parecer" diferentes, embora empregando a mesma funcionalidade geral. Por exemplo, é possível que, quando uma BSF recebe uma requisição de código de serviço de uma NAF (como será descrito abaixo), a BSF receptora precisa executar uma etapa de resolução de endereço para identificar uma BSF de "serviço" para a NAF ou cliente (UE) e, se a BSF de recepção não é a BSF de serviço, a requisição é redirecionada para a BSF de serviço.

A descrição é concernente à provisão de um serviço inserção para um cliente. Tipicamente, o cliente estará pré registrado com o provedor de serviço, mas a iniciativa de inserir informação particular é tomada pelo provedor de serviço. Em tal situação, o provedor de serviço e o cliente já não terão uma associação de segurança estabelecida um com o outro (associações de segurança são tipicamente de vida curta) e precisa ser estabelecida.

Uma primeira solução proposta aqui considera a abordagem de que a NAF solicita à BSF um código (ou serviço) NAF. A BSF retorna à NAF, o código NAF juntamente com o identificador de transação de cliente (B-TID) e o valor de autenticação de rede correspondente (AUTN). Como foi estabelecido acima, o B-TID contém o valor RAND codificado (como o prefixo NAI) que pode ser usado pelo cliente para derivar o código base (KS). A NAF pode agora compor uma mensagem contendo o B-TID, AUTN e dados adicionais incluindo a identidade NAF que o cliente requer no sentido de derivar o código NAF, e enviar esta mensagem ao cliente. Esta mensagem pode ser uma mensagem que somente dispara a configuração de um SA (isto é, compartilhamento de um código de serviço) ou poderia conter dados de serviço (isto é, dados de carga útil) criptografados com o código de serviço.

Em ambos os casos, os valores B-TID, AUTN e outros dados requeridos pelo cliente para gerar KS são enviados em texto comum, mas são "assinados" com um Código de Autenticação de Mensagem. Notar que o(s) código(s) na SA são derivados usando o código compartilhado entre o HSS e o UE, e que o AUTN está incluído na mensagem. Portanto, não é possível "enganar" mensagens, embora o código usado para proteger a integridade da mensagem seja derivado do verdadeiro SA que é destinado a estabelecer.

Quando o cliente recebe a mensagem, este recupera a parte RAND do B-TID (revertendo a codificação) e o AUTN e os aplica ao USIM/ISIM para derivar o código base Ks. Então este usa os dados adicionais para derivar o código NAF e verifica a mensagem recebida usando o MAC.

As trocas de sinalização associadas a este procedimento são ilustradas na Figura 2.

No sentido de evitar a manipulação dos dados adicionais (requeridos pelo cliente) pela NAF, a BSF pode assinar aqueles dados usando um derivado de KS. Isto pode ser importante, por exemplo, para evitar que a NAF estenda o tempo de vida de um código.

A solução apresentada acima permite que a NAF insira no cliente a informação requerida para estabelecer uma associação de segurança entre as duas partes. Então, o cliente não tem que configurar uma conexão com a BSF para realizar estas tarefas. Isto representa uma solução extremamente eficiente no tempo. Entretanto, requer que a NAF comute toda informação relacionada a código (tempo de vida de código, Add-info, etc.) de uma forma protegida a partir da BSF para o UE. O B-TID e os outros dados podem então compreender realmente uma grande estrutura de dados. Isto pode ser problemático no caso em que o volume de dados que pode ser incorporado na estrutura de mensagem entre o cliente e a NAF, por exemplo, onde esta estrutura é SMS.

No sentido de reduzir o volume de dados requerido, trocado

entre a NAF e o cliente para estabelecer a associação de segurança, a solução acima pode ser modificada omitindo o valor AUTN dos dados enviados pela BSF à NAF. A NAF agora compõe uma mensagem contendo o B-TID e outros dados necessários (incluindo a identidade NAF) que o terminal necessita para derivar o código NAF e os envia ao cliente. Novamente, esta mensagem poderia ser uma mensagem que apenas dispara a configuração de uma associação de segurança, ou poderia conter dados de carga útil criptografados.

Quando o cliente recebe a mensagem da NAF, conecta a BSF, transmitindo o B-TID a ela, autentica-se e requisita a informação restante necessária para derivar o material de codificação associado ao B-TID, isto é, por exemplo, AUTN. Depois de ter recebido esta informação, este deriva o código de serviço (NAF) e verifica a integridade da mensagem. Como o cliente tem que se conectar à BSF, pode ao mesmo tempo obter toda a informação relacionada ao material de codificação, isto é, Add-Info, tempo de vida de código, etc., reduzindo então a quantidade de informação "administrativa" que tem que ser transmitida da NAF para o cliente.

A troca de sinalização associada a este procedimento, supondo o cenário de geração Ks (isto é, análogo à Figura 2) é mostrada na Figura 3.

Pode ser indesejável em algumas circunstâncias revelar o valor RAND à NAF. Isto pode ser evitado formando o B-TID usando uma referência para o valor RAND real (ou o RAND efetivo, RANDe) de tal modo que a NAF vê apenas o valor de referência. O RAND efetivo (RANDe) teria então que ser sinalizado juntamente com AUTN, da BSF para o cliente. Este procedimento modificado é ilustrado na Figura 4.

A vantagem principal das soluções descritas com referência às Figuras 3 e 4 é que a BSF terá uma oportunidade adicional para controlar a geração de código no cliente. O cliente necessita AUTN para derivar o código. Por outro lado, o cliente terá que se conectar à BSF e se autenticar

para a BSF, requerendo uma nova variante do protocolo GBA através da interface Ub.

Uma ameaça às soluções das Figuras 3 e 4 é que um atacante pode gerar um lote de mensagens (implicando em conter um B-TID válido) e enviá-las a diferentes clientes para iniciar um ataque Negação-de-Serviço (DoS). Como os clientes não possuem meios para autenticar as mensagens (isto é, um AUTN) estes se conectarão à BSF em uma tentativa de autenticar as mensagens recebidas. Tal ataque, se não houver resistência, consumirá consideráveis recursos em parte da BSF. Para tornar tal ataque DoS mais difícil, seria desejável habilitar o cliente a verificar imediatamente o MAC da mensagem inserida pela NAF, no sentido de validara a mensagem sem ter que se conectar à BSF. Para obter isto, o cliente tem que ser capaz de derivar o código que é usado para geração do MAC da mensagem. Como o AUTN não é enviado ao cliente na mensagem *push*, esta derivação tem que ser baseada somente no RAND (ou valor derivado, Figura 4) no B-TID.

Uma solução é o uso só RAND (ou valor derivado) no B-TID para derivar dois códigos Ck' e Ik' na BSF. A BSF então deriva um código MAC usando esses códigos, e envia o código MAC à NAF. Este código de integridade deveria preferivelmente também depender da identidade NAF. Usar uma "impressão digital" das outras informações necessárias para derivar o código NAF na derivação do código de integridade, seria o único meio de obter isto sem ter que enviar toda a informação ao UE. A NAF computa um segundo MAC (curto) através de pelo menos uma parte dos dados a serem enviados ao cliente, e inclui o MAC na mensagem enviada ao cliente. No cliente, o USIM/ISIM usa os algoritmos AKA para gerar Ck' e Ik' e daí o segundo código MAC, e o cliente pode então verificar a mensagem. Alternativamente, a BSF pode prover os códigos Ck' e Ik' à NAF para habilitar a NAF a gerar o próprio segundo código MAC. Isto não interrompe a repetição da mensagem antiga (embora isto possa ser equacionado com o uso

de marcações de tempo) mas interrompe atacantes gerando mensagens randômicas.

Em uma solução alternativa, ilustrada no diagrama de sinalização da Figura 5, a BSF não gera e envia o próprio código NAF à NAF, em resposta à requisição NAF para um código *PUSH* para um dado usuário. Ao invés disso, a BSF envia um valor público de Diffie-Hellman $g^{NAF\ Key}$ baseado no Código NAF (ou em algum outro valor baseado no segredo associado Ks) e dados relacionados à identidade das partes envolvidas e uso pretendido do código. A NAF pode agora escolher um valor secreto RAND próprio, e anexar o valor correspondente público de Diffie-Hellman g^{RAND} para aquele valor secreto à informação enviada ao UE. Ambas as partes podem então derivar um código compartilhado comum, S_Key = $g^{RAND*NAF\ Key}$. O S_Key é usado para codificar o MAC. É notado que os esquemas Diffie-Hellman podem ser implementados através de diferentes tipos de grupos. Aqui, usamos a notação padrão quando o grupo é Zp e o elemento de geração g usado é denotado por g.

De acordo ainda com uma solução alternativa, ilustrada no diagrama de sinalização da Figura 6, quando a NAF requer um código *PUSH* para um dado usuário, a BSF não inclui um código NAF padrão, mas ao invés disso deriva um código que se apóia adicionalmente em ambos UE_identity e NAF_identity (em adição a quaisquer dados adicionais). Tal código é denotado "NAF_UE_Key" na Figura. No sentido de assegurar o fornecimento do código à NAF a partir da BSF, a BSF inclui na mensagem para a BSF um MAC calculado usando o NAF_UE_Key.

A discussão acima considerou a aplicação da invenção à provisão de códigos relacionados a serviços a usuários e nós de serviço. Uma outra aplicação da presente invenção relaciona-se à provisão de códigos a terminais de cliente para permitir que um terminal de cliente insira mensagens a um terminal de cliente de rede não hierárquica de uma maneira segura, quer

dizer gerenciamento de código "*peer-to-peer*" (p2p).

De acordo com uma solução, um UE inicial, isto é, UE_A, emprega o método ilustrado em geral na Figura 7. Esta abordagem se apóia em uma relação de confiança explícita entre a BSF_A e a BSF_B. A parte inicial primeiramente executa um procedimento GBA padrão com a BSF_A de sua rede doméstica, no sentido de obter um código base, Ks_A. UE_A então usa o código base para derivar uma RAND atrelada à outra parte UE_B à qual UE_A deseja inserir uma mensagem. Isto pode ser feito do mesmo modo que os códigos NAF são derivados. A segunda ação executada pelo UE_A é requisitada informação de código para UE_B. Esta requisição, contendo as identidades de ambos os clientes, é enviada à BSF_A, que envia a requisição à BSF dentro da rede doméstica do UE_B, isto é, BSF_B.

A BSF_B retorna a UE_A, via BSF_A, um valor público de Diffie-Hellman para UE_B, a saber $g^{NAF\ Key}$. Este também retorna o B-TID (contendo o valor RAND usado para gerar o NAF Key), AUTN, e dados adicionais requeridos. A parte inicial UE_A então forma uma mensagem contendo seu valor de Diffie-Hellman público, g^{RAND}, e a informação necessária pelo receptor para derivar o KS_B, o NAF_Key relacionado, e daí o código de sessão $g^{RAND*NAF\text{-}Key}$, UE_A pode naturalmente derivar o mesmo código de sessão.

Uma solução de gerenciamento de código p2p alternativa é ilustrada na Figura 8 e requer que a BSF_B gere o código para ser compartilhado pelas redes não hierárquicas. A primeira ação pela a parte inicial UE_A é requisitar um código para a outra parte UE_B. Esta requisição é enviada ao início da parte BSF_A, que redireciona a requisição à BSF_B da parte de recepção. A parte inicial inclui sua identidade bem como aquela da parte de recepção na requisição, e a BSF_B deriva o código a ser compartilhado, NAF_UE_Key. O código derivado, juntamente com B-TID, AUTN, etc., é então fornecido ao UE_A.

Com este esquema, a parte de recepção recebe uma verificação implícita da identidade reivindicada do remetente, pois esta identidade é usada na derivação de NAF_UE_Key. A parte de recepção poderia também obter uma autenticação explícita se a BSF_B inclui um MAC baseado em um "NAF_Key" cobrindo todos os dados, conforme descrito acima.

Será verificado pela pessoa especialista na técnica que várias modificações podem ser feitas à realizações acima descritas, sem se afastar do escopo da presente invenção. Por exemplo, embora as soluções apresentadas acima tenham sido relacionadas a GBA, a invenção tem aplicabilidade geral a arquiteturas onde a informação deve ser inserida de um provedor de serviço, e onde o provedor de serviço e o cliente não compartilham um segredo comum. Em uma outra modificação, onde soluções múltiplas são implementadas em paralelo, a requisição de autenticação enviada à BSF contém um seletor indicando qual solução a NAF/UE empregará.

REIVINDICAÇÕES

1. Método para estabelecer uma associação de segurança entre um primeiro nó e um segundo nó, para finalidade de inserir informação do primeiro nó para o segundo nó, onde o segundo nó e uma função de geração de código compartilham um segredo básico, o método caracterizado pelo fato de compreender:

- enviar uma requisição para geração e provisão de um código de serviço a partir do primeiro nó para a função de geração de código, a requisição contendo identidades do primeiro e segundo nós;
- gerar um código de serviço na função de geração de código, usando a identidade do primeiro nó, o segredo básico e informação adicional, e enviar o código de serviço ao primeiro nó juntamente com a citada informação adicional;
- enviar a citada informação adicional e a citada identidade do primeiro nó, a partir do primeiro nó para o segundo nó; e
- no segundo nó, gerar o citado código de serviço usando a informação adicional recebida, a primeira identidade de usuário e o segredo básico.

2. Método de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que o citado primeiro nó e um nó de serviço e o citado segundo nó é um cliente.

3. Método de acordo com a reivindicação 2, caracterizado pelo fato de que o citado cliente é um terminal de cliente de uma rede 3G empregando uma Arquitetura *Bootstrapping* Genérica, citado nó de serviço compreendendo uma Função de Aplicação de Rede e citada função de geração de código compreendendo uma Função de Servidor de *Bootstrapping*.

4. Método de acordo com a reivindicação 3, caracterizado pelo fato de que a citada função de geração de código compreende adicionalmente um Sistema de Assinante Doméstico ou um Registro de Localização

Doméstica/Centro de Autenticação, citado segredo básico sendo conhecida ou acessível pelo Sistema de Assinante Doméstico ou HE/Centro de Autenticação.

5. Método de acordo com a reivindicação 3 ou 4, caracterizado pelo fato de que a citada etapa de gerar um código de serviço na função de geração de código compreende as etapas de:

- gerar material de código KS usando a citado segredo básico; e
- gerar o código de serviço usando o citado material de código KS, a identidade do nó de serviço e a citada informação adicional.

6. Método de acordo com a reivindicação 3, caracterizado pelo fato de que citada etapa de gerar citado código de serviço no cliente compreende:

- gerar material de código KS usando a citado segredo básico; e
- gerar o código de serviço usando citado material de código KS, e citada informação adicional.

7. Método de acordo com a reivindicação 6, caracterizado pelo fato de que a citado segredo básico é armazenada em um ISIM/USIM do cliente, e citada etapa de gerar o material de código KS é efetuada dentro do ISIM/USIM.

8. Método de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato da citada etapa de gerar um código de serviço na função de geração de código utilizar valores diferentes daqueles enviados ao cliente pelo nó de serviço.

9. Método de acordo com a reivindicação 8, caracterizado pelo fato de que pelo menos certos daqueles outros valores são obtidos pelo cliente a partir da função de geração de código.

10. Método de acordo com qualquer uma das reivindicações

precedentes, caracterizado pelo fato de que a citada informação adicional compreende um ou mais dentre:

um identificador de transação; e

um valor de autenticação de rede.

11. Método de acordo com qualquer uma das reivindicações 1 a 9, caracterizado pelo fato de que a citada informação adicional compreende um identificador de transação no formato de uma NAI, o identificador de transação compreendendo um valor randômico codificado gerado pela função de geração de código, o valor randômico codificado sendo usado para gerar o código de serviço.

12. Método de acordo com a reivindicação 2, caracterizado pelo fato de que a citada informação adicional compreende um identificador de transação no formato de uma NAI, o identificador de transação compreendendo um indicador para um valor randômico gerado e armazenado na função de geração de código, o valor randômico sendo usado para gerar o código de serviço, o método compreendendo enviar uma requisição contendo o citado indicador, do cliente para a função de geração de código, e retornar o valor randômico ao cliente, para habilitar o cliente a gerar o código de serviço.

13. Método de acordo com a reivindicação 2, caracterizado pelo fato de que a função de geração de código envia ao nó de serviço um valor de autenticação de rede e o nó de serviço redireciona este valor ao cliente, juntamente com a citada informação adicional, o cliente usando o segredo básico e o valor de autenticação para autenticar a função de geração de código.

14. Método de acordo com a reivindicação 2, e caracterizado pelo fato de compreender enviar uma requisição do cliente para a função de geração de código para um valor de autenticação, após o cliente ter recebido a citada informação adicional do nó de serviço, receber o valor de autenticação

no cliente, e autorizar a requisição de associação de segurança recebida do nó de serviço, com base neste valor.

15. Método de acordo com a reivindicação 2, caracterizado pelo fato de que a citada informação adicional é redirecionada do nó de serviço para o cliente em uma mensagem contendo também dados de serviço, os dados de serviço sendo criptografados e/ou protegidos na integridade com o código de serviço, onde o cliente pode decriptografar os dados criptografados, uma vez que tenha gerado o código de serviço.

16. Método de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que a citada etapa de gerar um código de serviço na função de geração de código compreende usar a identidade do segundo nó.

17. Método de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que o citado código de serviço é um código de Diffie-Hellman para o segundo nó, o método compreendendo adicionalmente a etapa de prover ao primeiro nó um código de Diffie-Hellman para aquele primeiro nó, e enviar o código Diffie-Hellman para o primeiro nó ao segundo nó, citada associação de segurança sendo estabelecida com base nos dois códigos de Diffie-Hellman.

18. Método de acordo com a reivindicação 1, caracterizado pelo fato de que citados primeiro e segundo nós são primeiro e segundo clientes, respectivamente.

19. Método de acordo com a reivindicação 18, caracterizado pelo fato de que a citada função de geração de código compreende um servidor de código tendo uma relação de confiança com citado segundo cliente, e citada requisição para geração e provisão de um código de serviço é enviada ao citado servidor de código via um segundo servidor de código tendo uma relação de confiança com citado primeiro cliente.

20. Método de acordo com a reivindicação 19, e caracterizado

pelo fato de compreender enviar, do citado primeiro nó para citado segundo nó, um código de serviço obtido pelo citado primeiro nó, no primeiro e segundo nós, derivando um código de sessão usando ambos citados códigos de serviço.

21. Método de acordo com a reivindicação 18, caracterizado pelo fato de que citadas etapas de redirecionar citada informação adicional do primeiro nó para o segundo nó, e gerar citado código de serviço no segundo nó usando a informação adicional recebida e o segredo básico, fazem parte de um procedimento de troca de Diffie-Hellman.

22. Nó de serviço para fornecer um serviço de inserção a um cliente, via um enlace de comunicação segura, o nó de serviço caracterizado pelo fato de compreender:

- meio para enviar uma requisição para geração e provisão de um código de serviço a uma função de geração de código, a requisição identificando o cliente e o nó de serviço;
- meio para receber da função de geração de código um código de serviço, juntamente com a citada informação adicional;
- meio para redirecionar citada informação adicional ao cliente; e
- meio para criptografia e/ou informação de serviço de proteção de integridade, usando o código de serviço e para enviar a informação criptografada e/ou informação protegida ao cliente.

23. Terminal de cliente para receber um serviço inserido fornecido por um nó de serviço, o terminal de cliente caracterizado pelo fato de compreender:

- meio de memória para armazenar um segredo que é compartilhado com uma função de geração de código;
- meio para receber informação de geração de código do citado nó de serviço;

- meio para gerar um código de serviço usando o citado segredo compartilhado e citada informação de geração de código; e
- meio para usar o citado código de serviço para decriptografar e/ou verificar a integridade das comunicações com o nó de serviço.

24. Terminal de acordo com a reivindicação 23 e caracterizado pelo fato de compreender meio para receber do nó de serviço um código de autenticação de mensagem, o terminal compreendendo meio para gerar um código ou códigos de autenticação a partir de pelo menos uma parte da informação de geração de código, e usando o(s) código(s) de autenticação para autenticar o código de autenticação de mensagem.

25. Terminal de acordo com a reivindicação 23 e caracterizado pelo fato de que citado meio para gerar um código ou códigos de autenticação compreende um USIM/ISIM.

26. Função de geração de código para uso ao estabelecer uma associação de segurança entre um cliente e um nó de serviço para a finalidade de inserir informação do nó de serviço para o cliente, o servidor de código caracterizada pelo fato de compreender:

- meio de memória para armazenar um segredo que é compartilhado com citado cliente;
- meio para receber uma requisição para geração e provisão de um código de serviço a partir do citado nó de serviço, a requisição identificando o cliente e o nó de serviço; e
- meio para gerar um código de serviço usando a identidade do nó de serviço, o segredo básico, uma informação adicional, e para enviar o código de serviço ao nó de serviço juntamente com citada informação adicional.

27. Método para estabelecer uma associação de segurança entre primeiro e segundo clientes, para a finalidade de inserir informação do

primeiro cliente para o segundo cliente, onde o primeiro e segundo clientes possuem relações de confiança com o primeiro e segundo servidores de código, respectivamente, e compartilham um segredo com seus respectivos servidores de código, o método caracterizado pelo fato de compreender:

- enviar uma requisição para geração e provisão de um código de serviço do primeiro cliente para o segundo servidor de código, via primeiro servidor de código, a requisição identificando o primeiro e segundo nós;
- gerar um código de serviço no segundo servidor de código, usando a identidade do primeiro nó, o segredo básico e informação adicional, e enviar o código de serviço ao primeiro nó juntamente com a citada informação adicional;
- enviar a citada informação adicional do primeiro nó, para o segundo nó; e

no segundo nó, gerar o citado código de serviço usando a informação adicional recebida, e o segredo básico.

28. Método para proteger um nó contra ataques de repetição, o método caracterizado pelo fato de compreender:

gerar um código de serviço em uma função de servidor de bootstrapping;

prover o código de serviço a um primeiro nó juntamente com a informação requerida para gerar o código de serviço;

enviar uma mensagem de geração de código do primeiro nó para o segundo nó, a mensagem incluindo a citada informação, um valor de prevenção de repetição e um código de autenticação de mensagem calculado através do corpo da mensagem, incluindo o valor de prevenção de repetição, o valor de prevenção de repetição sendo incrementado ou decrementado para cada execução do procedimento;

receber citada mensagem de geração de código no citado

segundo nó e armazenar o valor de prevenção de repetição contido nele; e

no segundo nó, cada vez que é recebida uma mensagem de geração de código, verificar o citado código de autenticação de mensagem, determinar se o valor de prevenção de repetição contido na mensagem já foi armazenado ou não no segundo nó e, caso afirmativo, rejeitar a mensagem.

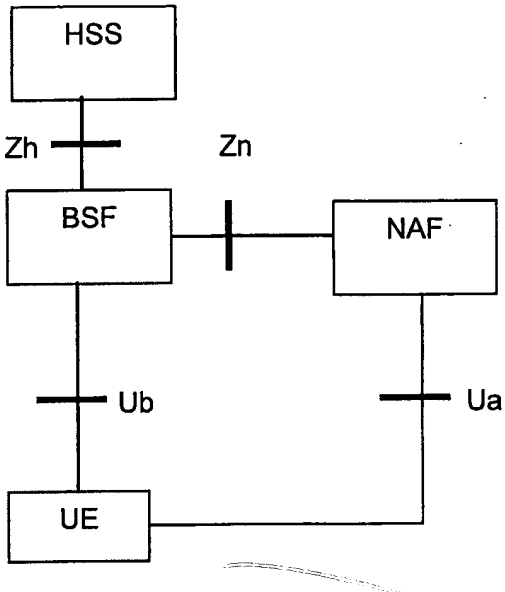


FIGURA 1

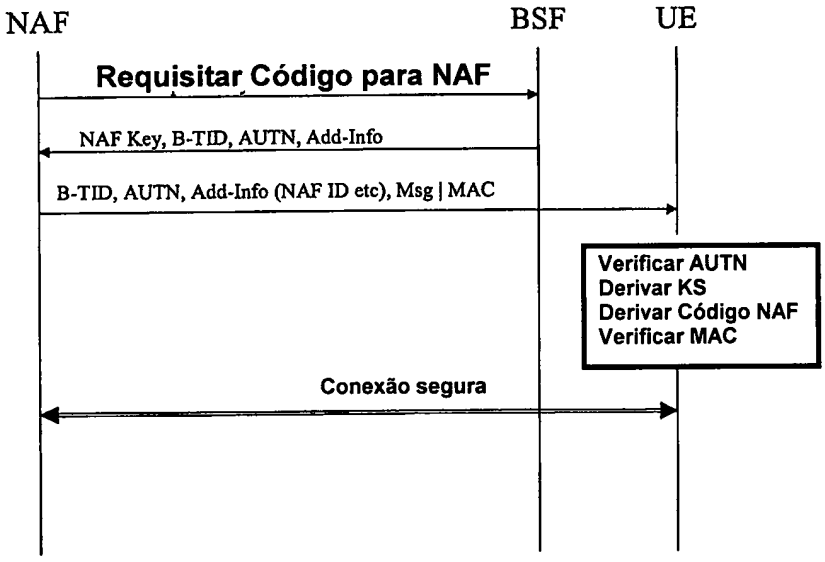


FIGURA 2

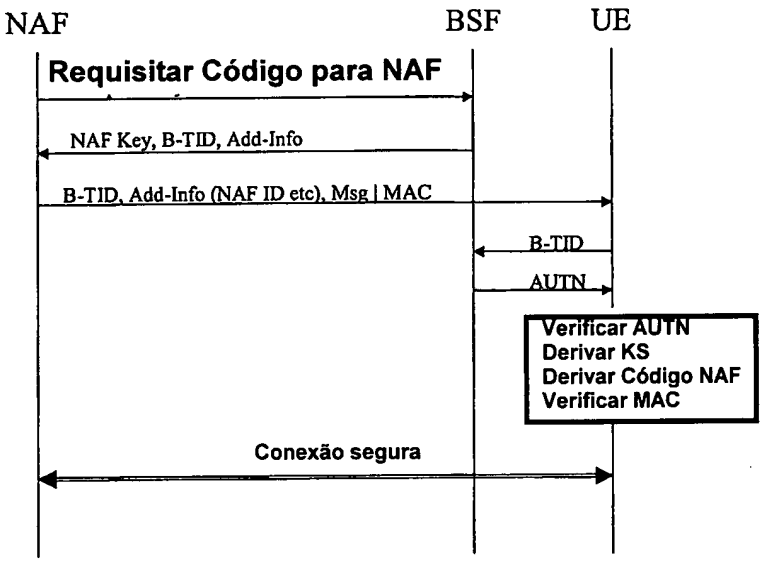


FIGURA 3

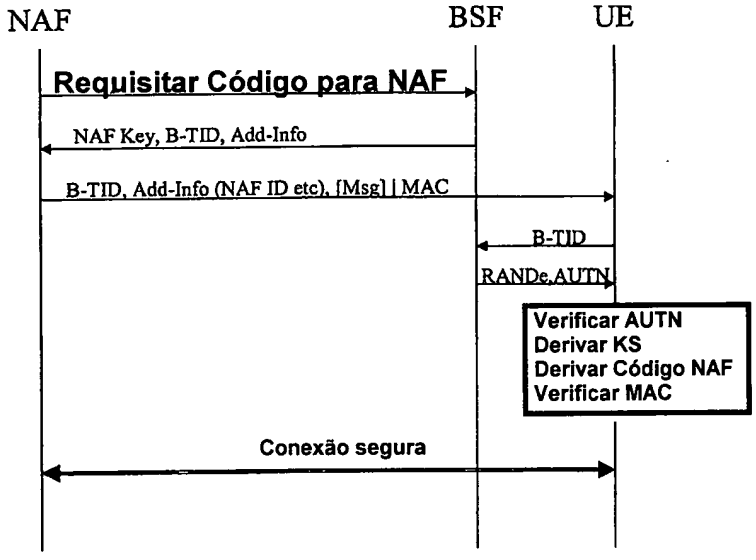


FIGURA 4

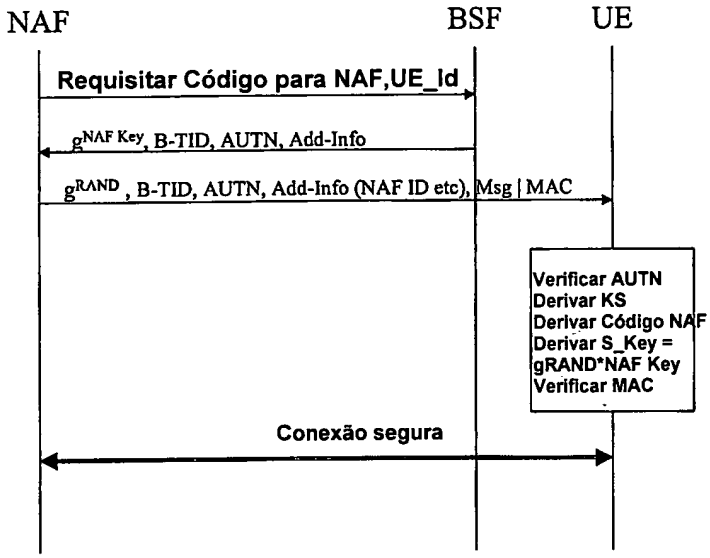


FIGURA 5

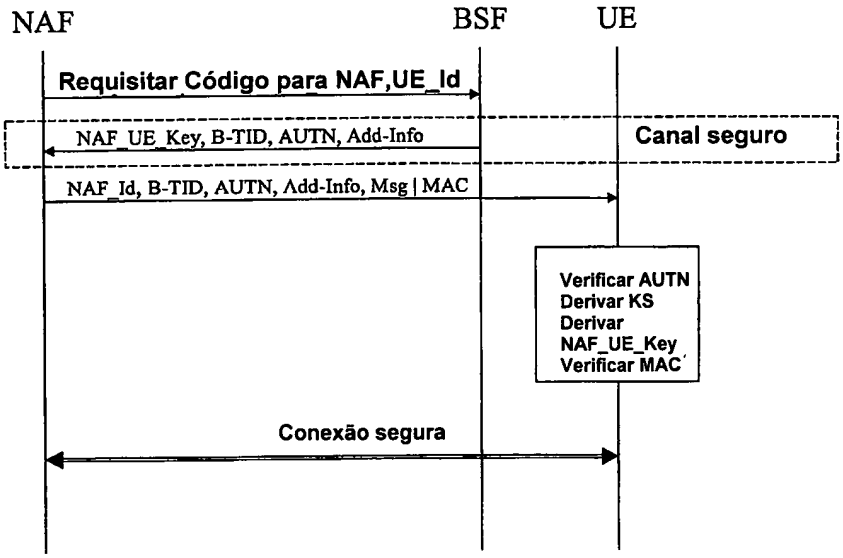


FIGURA 6

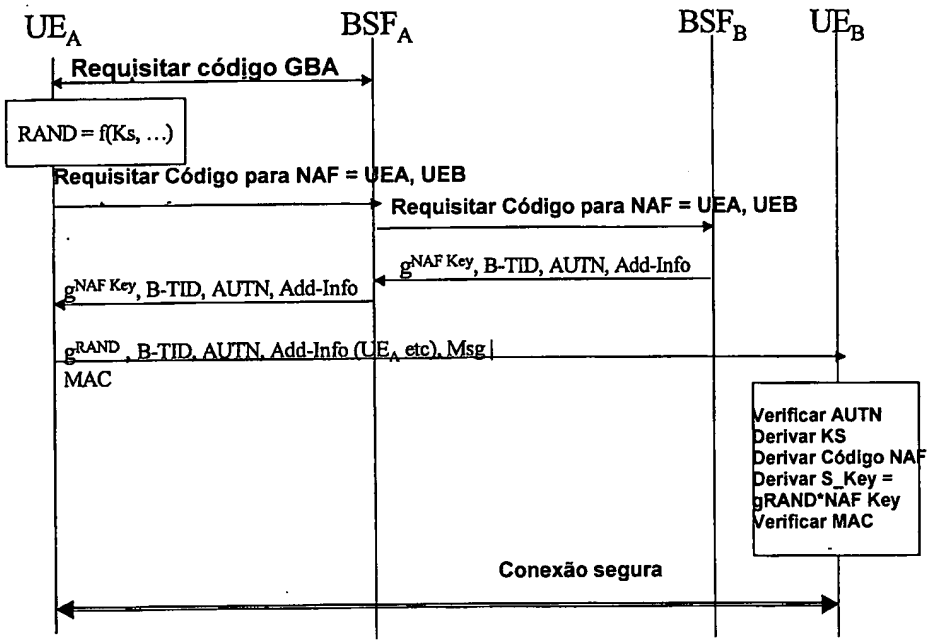


FIGURA 7

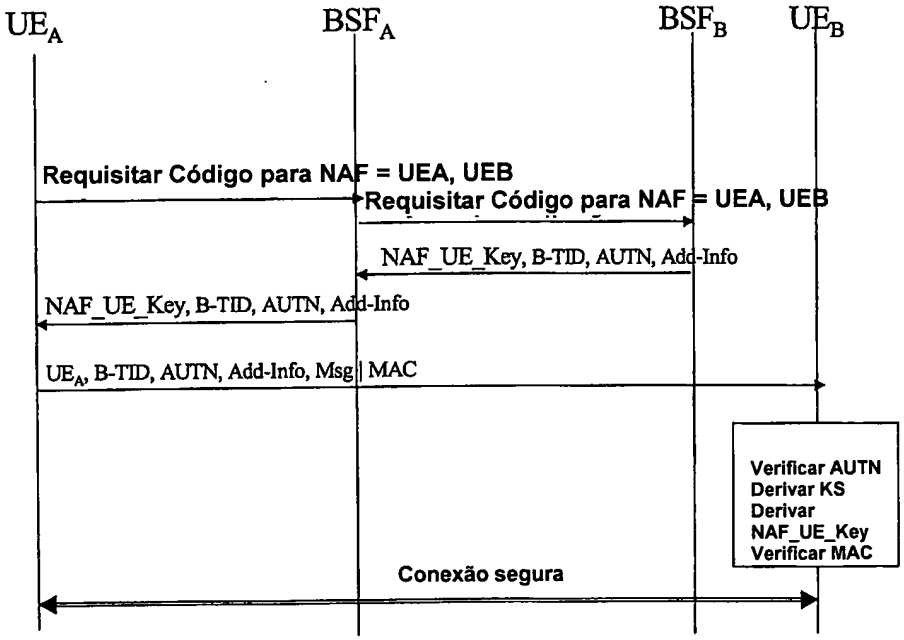


FIGURA 8

PI 0617286-5

RESUMO

"MÉTODOS PARA ESTABELECER UMA ASSOCIAÇÃO DE SEGURANÇA ENTRE UM NÓ DE SERVIÇO E UM CLIENTE, PARA ESTABELECER UMA ASSOCIAÇÃO DE SEGURANÇA ENTRE PRIMEIRO E SEGUNDO CLIENTES, E PARA PROTEGER UM NÓ CONTRA ATAQUES DE REPETIÇÃO, NÓ DE SERVIÇO, TERMINAL DE CLIENTE, E, FUNÇÃO DE GERAÇÃO DE CÓDIGO"

Método para estabelecer uma associação de segurança entre um cliente e um nó de serviço para a finalidade de inserir informação do nó de serviço para o cliente, onde o cliente e um servidor de código compartilham um segredo básico. O método compreende enviar uma requisição para geração e provisão de um código de serviço, do nó de serviço para um servidor de código, a requisição identificando o cliente e o nó de serviço, gerar um código de serviço no servidor de código usando as identidades do cliente e do nó de serviço, o segredo básico e informação adicional, e enviar o código de serviço ao nó de serviço, juntamente com citada informação adicional, enviar citada informação adicional do nó de serviço para o cliente e, no cliente, gerar citado código de serviço usando a informação adicional recebida e o código base. Uma abordagem similar pode ser usada para prover gerenciamento de código p2p.