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

(11) PI 0407702-4 B1

(22) Data do Depósito: 18/02/2004

(45) Data de Concessão: 09/05/2017

(54) Título: MÉTODO PARA CRIAR E DISTRIBUIR CHAVES CRIPTOGRÁFICAS EM UM SISTEMA DE RÁDIO MÓVEL E SISTEMA DE RÁDIO MÓVEL

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

(30) Prioridade Unionista: 20/02/2003 DE 103 07 403.1

(73) Titular(es): SIEMENS AKTIENGESELLSCHAFT

(72) Inventor(es): GÜNTHER HORN; DIRK KRÖSELBERG

Relatório Descritivo da Patente de Invenção para **"MÉTODO PARA CRIAR E DISTRIBUIR CHAVES CRIPTOGRÁFICAS EM UM SISTEMA DE RÁDIO MÓVEL E SISTEMA DE RÁDIO MÓVEL".**

A presente invenção refere-se a um método para criar e distribuir chaves criptográficas em um sistema de rádio móvel e a um sistema de rádio móvel.

No escopo da *Universal Mobile Telecommunications Systems* (UMTS) são desenvolvidos serviços multimídia baseados na Internet para melhorar a usabilidade do sistema de rádio móvel UMTS e para abrir campos de utilização adicionais.

Como uma plataforma para serviços de multimídia baseados na Internet para um sistema de rádio móvel foi padronizado no 3 GPP (*3rd Generation Partnership Project*) um chamado *IP-based Multimedia Subsystem UMTS Release 5* (IMS) que é descrito no documento - Arquitetura.

Quando um equipamento rádio móvel de um assinante de rádio móvel visita uma rede de comunicações em um sistema de rádio móvel com IMS para utilizar serviços de multimídia baseados na Internet, é feita uma autenticação do terminal de rádio móvel de acordo com a norma descrita em [1], 3GPP segundo o *IMS Authentication and Key Agreement Protocol* (Protocolo IMS-AKA).

De acordo com o Protocolo IMS-AKA, o terminal de rádio móvel e a rede de comunicações em cuja área se encontra atualmente o terminal de rádio móvel identificam-se mutuamente e são geradas duas chaves criptográficas, a chamada chave de integridade e a chamada chave de transmissão. De acordo com UMTS Release 5, a chave de integridade é utilizada para a sinalização IMS entre o terminal de rádio móvel e um computador da rede de comunicação visitada (*visited network*). O computador da rede de comunicação visitada é equipado como *Call State Control Function-Computer* (CSCF Computer) e é denominado de *Proxy-CSCF-Computer* (P-CSCF-Computer). A chave de transmissão é prevista para a codificação, isto é, para proteger a confidencialidade dos dados trocados.

Adicionalmente, para a proteção das mensagens de sinalização

IMS puras sob a utilização da chave de integração pode ser previsto que entre um computador de servidor de aplicação e o terminal de rádio móvel precisam ser trocadas mensagens eletrônicas adicionais de modo confidencial no escopo do fornecimento de serviços baseados no IP.

Um computador de servidor de aplicação no lado da rede, no contexto da presente descrição, é um computador que oferece serviços de acordo com multimídia, de preferência, previstos na camada de aplicação (camada OSI 7) e que comunica de acordo com um protocolo camada 7, isto é, um protocolo de camada de aplicação. Por exemplo, o computador de servidor de aplicação pode ser configurado como um computador de servidor de HTTP (*Hypertext Transfer Protocol*) e comunicar com o terminal de rádio móvel de acordo com o protocolo HTTP.

Além da funcionalidade básica do IMS, os computadores de servidor de aplicação são utilizados, por exemplo, na administração de ajustes de usuários no lado da rede e para armazenar e administrar dados de perfil sobre os assinantes do sistema de rádio móvel.

Exemplos para estas aplicações entre assinantes móveis (especialmente aqueles de um sistema de rádio móvel IMS) e computadores de servidores de aplicação na rede de comunicação que utilizam o protocolo http são:

- Listas de acesso para servidores de presença com os quais é possível utilizar informação de posição sobre a posição atual de um terminal de rádio móvel dentro do sistema de rádio móvel (por exemplo, dados de GPS).
- Listas do tipo *Buddy* de aplicações *Chat*, isto é listas de assinantes admitidos para uma aplicação Chat.
- serviços de gerenciamento de grupos, e
- conexões para conferências eletrônicas de multimídia.

Como mais um exemplo para tal aplicação cabe mencionar que conexões multicast entre um terminal de rádio móvel e entre um centro de serviços *multicast* são estabelecidas sob a aplicação do sistema IMS.

Para proteger por criptografia os protocolos utilizados entre o

terminal de rádio móvel e o computador de servidor de aplicação, suas mensagens precisam ser protegidas, por exemplo, no que se refere à autenticação, integridade de dados e / ou confidencialidade de dados.

Dependendo do cenário de uso concreto e do protocolo de camada de aplicação utilizado são utilizados diferentes protocolos de segurança para proteger do protocolo de camada de aplicação, por exemplo,

- para o HTTP, o protocolo de segurança HTTP-Digest, o protocolo TLS (*Transport Layer Security Protocol*) ou o protocolo WTLS (*Wireless Transport Layer Security Protocol*), e
- para a distribuição das chaves para conexões de comunicação multicast MIKEY (*Multimedia Internet KEYing*).

Em todos os protocolos criptográficos de camada de aplicação é necessário que os parceiros de comunicação envolvidos, especialmente o terminal de rádio móvel e o computador de servidor de aplicação, isto é, o computador de servidor de aplicação na rede de comunicação, dispõe de material de chave secreto, isto é, de chaves secretas que está disponível já no início da transmissão da primeira mensagem eletrônica protegida.

No caso do IMS, a infra-estrutura da chave se baseia em chaves simétricas que são utilizadas para a autenticação dos usuários do IMS no escopo do registro do IMS, isto é, no escopo do protocolo de autenticação e troca de chaves, conforme descrito em [1].

Conforme descrito em [1], um terminal de rádio móvel no IMS se registra para uma sessão de comunicação IMS na sua rede de comunicação de origem (*Home Network*) no computador previsto para tal que também é denominado de S-CSCF-Computer (*Serving Call State Control Function-Computer*).

A comunicação acontece sob a utilização de um Proxy-Computer local, o P-CSCF-Computer acima descrito na rede de comunicação visitada que representa o primeiro ponto de contato IMS para o terminal de rádio móvel e, por conseguinte, para o usuário móvel.

A autenticação de acordo com [1] acontece entre o terminal de rádio móvel e o computador S-CSCF sob a participação de um chamado

computador HSS (*Home Subscriber Server-Computer*). No escopo da autenticação são geradas no terminal de rádio móvel e no computador HSS a chave de integridade e a chave de transmissão e transmitidas de modo criptograficamente protegido para o computador S-CSCF.

O computador S-CSCF transmite de modo criptograficamente protegido a chave de integridade para o computador P-CSCF. A proteção de integridade e a autenticidade das mensagens de sinalização subseqüentes relacionadas ao IMS são garantidas localmente entre o terminal de rádio móvel e o computador P-CSCF e se baseiam na chave de integridade. De acordo com o UMTS Release 5, a chave de transmissão atualmente não é utilizada, porém, é planejado utilizar-se a chave de transmissão para a proteção adicional da confidencialidade de dados transmitidos em versões futuras da norma UMTS (Release 6 e normas subseqüentes).

Um problema surge quando a chave de transmissão e a chave de integridade que surgem de uma autenticação IMS-AKA e da geração de chave como chave de sessão, também é utilizada para a proteção de outras aplicações e não para a sinalização IMS.

O terminal de rádio móvel e a rede de comunicação de origem, em outras palavras, o usuário e o operador da rede de comunicação de origem, são considerados como mutuamente dignos de confiança.

Porém, a rede de comunicação visitada recebe (em caso de *roaming*; em caso de *não-roaming* isso corresponde à rede de comunicação de origem) a chave de integridade e a chave de transmissão. Se um computador de servidor de aplicação também receberia a chave de integridade e a chave de transmissão, então o computador de servidor de aplicação teoricamente estaria capaz de prejudicar a segurança da sinalização IMS entre o terminal de rádio móvel e a rede de comunicação visitada. Caso contrário, a rede de comunicação visitada, isto é, um computador da rede de comunicação visitada, seria capaz de prejudicar a segurança da comunicação entre o terminal de rádio móvel e o computador de servidor de aplicação quando esta se basearia diretamente na chave de integridade ou na chave de transmissão.

Também para o caso de que um terminal de rádio móvel deseja

comunicar simultaneamente com vários computadores de servidor de aplicação, é desejável, muitas vezes até necessário, que não seja possível tirar conclusões a partir da chave criptográfica que um respectivo computador de servidor de aplicação recebe sobre a chave criptográfica que um outro computador de servidor de aplicação recebe.

Uma possibilidade de solucionar o problema acima descrito é que tanto na rede de comunicação de origem como também no terminal de rádio móvel do usuário ocorra uma derivação de uma nova chave criptográfica da chave de integridade e / ou da chave de transmissão. Um computador de servidor de aplicação recebe a chave criptográfica derivada, não conhece nem a chave de integridade nem a chave de transmissão, contando que a função criptográfica utilizada para a derivação da chave não permita conclusões plausíveis sobre a chave de integridade e / ou a chave de transmissão para o computador de servidor de aplicação.

O problema que surge com essa idéia é que se precisa de uma função de derivação de chave que o computador da rede de comunicação visitada não possa repetir. Um chamado *Keyed-Hash* que utiliza como parâmetros de entrada, por exemplo, a chave de integridade ou a chave de transmissão, e como valor aleatório, o parâmetro aleatório gerado dentro do escopo da autenticação de acordo com [1] também pode ser calculado pelo computador na rede de comunicação visitada.

Um novo parâmetro aleatório que seria combinado entre o terminal de rádio móvel do usuário e a rede de comunicação de origem para fins de derivação de chave somente poderia ser obtido através de uma alteração em protocolos de comunicação ou de segurança já existentes, isto é, através de uma alteração, por exemplo, do Protocolo IMS-AKA ou na comunicação entre o computador S-CSCF e o computador HSS.

Mas, esta alteração deve ser evitada, uma vez que uma modificação de normas de comunicação ou de normas de segurança já existentes não pode ser executada de modo simples e, por conseguinte, seria muito cara.

Uma lista dos mecanismos de segurança previstos na norma *UMTS-Standard Release 5*, encontra-se em [2].

As funções de autenticação de mensagens e as funções de geração de chave utilizadas no escopo do Protocolo IMS-AKA são descritas em [3] e [4]. Além disso, [4] descreve uma função de codificação de cifra de bloco denominado de função de Rijndael.

Uma lista de diversas funções de derivação de chaves pode ser encontrada em [5].

Um outro método de derivação de chaves é descrito em [6].

Da patente EP 1 156 694 A1 é conhecido um equipamento de comunicação por rádio e um método para a comunicação por rádio que permitem a um terminal móvel garantir uma função de codificação e uma função de integridade nas camadas de transmissão de dados dois ou mais alto. Para tal, o terminal móvel possui uma unidade de processamento de codificação ou de processamento de integridade respectivamente, que é comutada entre uma unidade de controle de comunicação por rádio e uma unidade de conexão. Nisso, a unidade de processamento de codificação de integridade somente executa um processamento de codificação com chamados dados transparentes, tais como, por exemplo, dados de voz que são transmitidas entre a unidade de conexão e a unidade de comunicação. A unidade de processamento de codificação de integridade executa ainda um processamento de codificação e / ou um processamento de integridade com dados não-transparentes, que são transmitidos para o e a partir do dispositivo de controle de comunicação por rádio.

A presente invenção tem a tarefa de aumentar a proteção criptográfica em um sistema de rádio móvel.

O problema é solucionado com a ajuda do método para criar e distribuir chaves criptográficas em um sistema de rádio móvel e através do sistema de rádio móvel com as características de acordo com as reivindicações independentes.

Um método para gerar e distribuir chaves criptográficas em um sistema de rádio móvel parte de pelo menos um primeiro computador, de preferência, de um computador de uma rede de comunicação visitada (*visited network*), um computador de uma rede de comunicação de origem (*ho-*

me network) e pelo menos um segundo computador, de preferência configurado como um computador de servidor de aplicação. O pelo menos um terminal de rádio móvel encontra-se de preferência na área da rede de comunicação visitada e identificou-se perante a rede de comunicação de origem e a rede de comunicação visitada. Neste contexto cabe mencionar que a rede de comunicação visitada e a rede de comunicação de origem podem ser idênticas. No escopo da autenticação foi gerado material chave de autenticação que é disponível e armazenado no terminal de rádio móvel e no computador da rede de comunicação de origem. Durante o processo, o terminal de rádio móvel e o computador da rede de comunicação de origem criam respectivamente, sob a utilização do material de chave de autenticação uma primeira chave criptográfica e uma segunda chave criptográfica. Assim sendo, no terminal de rádio móvel e no computador da rede de comunicação de origem são disponíveis e armazenados respectivamente a primeira chave e a segunda chave.

O primeiro e o segundo computador podem alternadamente ser configurado como computador de servidor de aplicação.

A primeira chave criptográfica é transmitida, de preferência, pelo computador da rede de comunicação de origem (alternativamente pelo terminal de rádio móvel) do primeiro computador, de preferência, portanto, o computador da rede de comunicação visitada. Além disso, a segunda chave criptográfica é transmitida para o segundo computador, de preferência, o computador de servidor de aplicação, de preferência pelo computador da rede de comunicação de origem, como alternativa, pelo terminal de rádio móvel.

Um sistema de rádio móvel possui pelo menos um terminal de rádio móvel onde como resultado de uma autenticação entre o terminal de rádio móvel e um computador de uma rede de comunicação de origem do terminal de rádio móvel é armazenado material de chave de autenticação. Além disso, o sistema de rádio móvel possui um primeiro computador, de preferência, um computador de uma rede de comunicação visitada e um computador da rede de comunicação de origem. No computador da rede de comunicação de origem, também como resultado da autenticação do termi-

nal de rádio móvel na rede de comunicação de origem, material de chave de autenticação. Também no sistema de rádio móvel é previsto pelo menos um segundo computador, de preferência configurado como um computador de servidor de aplicação. O terminal de rádio móvel encontra-se na rede de comunicação visitada. O terminal de rádio móvel e o computador da rede de comunicação de origem possuem cada vez uma unidade criptográfica para a respectiva formação de uma primeira chave criptográfica e de uma segunda chave criptográfica sob utilização do material de chave de autenticação. O computador da rede de comunicação visitada possui ainda uma memória para armazenar uma primeira chave criptográfica que foi transmitida ao computador pelo terminal de rádio móvel ou pelo computador da rede de comunicação de origem. O computador de servidor de aplicação possui também uma memória para armazenar a segunda chave criptográfica que foi transmitido ao computador de servidor de aplicação pelo terminal de rádio móvel ou pelo computador da rede de comunicação de origem.

Como ilustração, a presente invenção pode ser visto no fato de que o material de chave de autenticação formado no escopo da autenticação não é transmitido diretamente e completamente para os computadores de servidor de aplicação e para o computador da rede de comunicação visitada, e sim, que de pelo menos uma parte do material de chave de autenticação são derivados chaves de sessão que são utilizadas no escopo da comunicação posterior entre o terminal de rádio móvel e os computadores de servidor de aplicação ou o computador da rede de comunicação visitada, por exemplo, para codificar os dados a serem protegidos. Com isso, a proteção criptográfica no escopo da comunicação entre o terminal de rádio móvel e o respectivo computador de servidor de aplicação é protegida contra um acesso por parte do computador na rede de comunicação visitada, e também a comunicação entre o terminal de rádio móvel e o computador da rede de comunicação visitada é protegida contra ataques por parte do computador de servidor de aplicação, uma vez que o computador de servidor de aplicação e o computador da rede de comunicação visitada possuem cada um chaves que não aos apropriadas para tirar conclusões sobre a respectiva outra chave o que

poderia possibilitar uma decodificação dos dados codificados com a chave da respectiva outra instância.

A segurança criptográfica elevada é alcançada de acordo com a presente invenção sem que seja necessário modificar o protocolo de comunicação padronizado no escopo de UMTS.

Aperfeiçoamentos preferidos da presente invenção resultam das reivindicações dependentes.

As seguintes realizações da presente invenção referem-se tanto ao método para criar e distribuir chaves criptográficas em um sistema de rádio móvel como também ao sistema de rádio móvel.

A primeira chave criptográfica e a segunda chave criptográfica são criadas de acordo com uma realização da presente invenção, sob utilização de uma função de derivação de chave.

De acordo com a presente invenção é previsto que a primeira chave criptográfica e a segunda chave criptográfica são criadas de tal modo que

- não é possível, a partir da primeira chave criptográfica, tirar conclusões sobre a segunda chave criptográfica;
- não é possível a partir da segunda chave criptográfica, tirar conclusões sobre a primeira chave criptográfica;
- não é possível a partir da primeira chave criptográfica ou da segunda chave criptográfica, tirar conclusões sobre o material de chave de autenticação.

O material de chave de autenticação pode possuir pelo menos duas chaves criptográficas, por exemplo, para o caso de que o sistema de rádio móvel é um sistema de rádio móvel baseado em uma norma 3GPP que preferencialmente possui um subsistema de multimídia baseado no IP, e precisamente uma chave de integridade e uma chave de transmissão.

Neste caso, de preferência a primeira chave criptográfica e a segunda chave criptográfica são derivadas da chave de transmissão.

Em outras palavras isto significa que de acordo com esta realização da presente invenção no terminal de rádio móvel e no computador da

rede de comunicação de origem são derivadas outras chaves criptográficas da chave de transmissão.

Ao contrário da chave de integridade que a rede de comunicação de origem de acordo com [1] transmite diretamente para a proteção de integridade da sinalização IMS para o computador da rede de comunicação visitada, de preferência, para um computador P-CSCF, a chave de transmissão propriamente dito, de acordo com a presente invenção, não é transmitida pelo computador da rede de comunicação de origem, de preferência, pelo computador S-CSCF. A chave de transmissão, em contrapartida, é utilizada para derivar uma ou várias chaves novas pelo uso de uma função de derivação de chave apropriada, sendo que a função de derivação de preferência se baseia em uma pseudofunção aleatória. A primeira chave derivada formada por meio da função de derivação de chave é transmitida como primeira chave criptográfica pelo computador S-CSCF para o computador P-CSCF quando a primeira chave criptográfica será utilizada para a proteção da confidencialidade de dados transmitidos.

No sistema de rádio móvel podem ser previstos a princípio qualquer número de redes de comunicação e de terminais de rádio móvel, e qualquer número de computadores de servidor de aplicação.

Em uma maioria de computadores de servidor de aplicação é previsto, de acordo com uma execução da presente invenção que o terminal de rádio móvel e o computador da rede de comunicação de origem formam uma chave criptográfica adicional para cada computador de servidor de aplicação adicional utilizando o material de chave de autenticação. A respectiva chave criptográfica adicional é transmitida para o computador de servidor de aplicação competente - de preferência pelo computador da rede de comunicação de origem.

Nesse caso é vantajoso gerar a maioria ou a variedade de chaves criptográficas através da mesma função de derivação de chave, porém, utilizando parâmetros de entrada apropriados diferentes. Através da utilização de parâmetros de entrada apropriados, de preferência de um número aleatório de um valor qualitativamente alto é garantido para função de deri-

vação de chave que o receptor da chave derivada, por exemplo, um computador de servidor de aplicação ou o computador da rede de comunicação visitada, não seja capaz de tirar conclusões sobre a chave básica, isto é, a chave de transmissão, em geral, o material de chave de autenticação.

Tais parâmetros de entrada tanto podem ser parâmetros conhecidos tanto para o terminal de rádio móvel e também para o computador da rede de comunicação de origem, como, por exemplo, os parâmetros que resultam da respectiva autenticação atual de acordo com o Protocolo IMS-AKA. Através da segunda chave criptográfica é derivada, para a proteção de mais mensagens além da sinalização IMS, por exemplo, para a proteção de mensagens http, que são previstas entre o terminal de rádio móvel e um computador de servidor de aplicação configurado como um *Presence Server* computador, ou de mensagens configuradas de acordo com o protocolo MIKEY entre o terminal de rádio móvel e um *Multicast-Service-Centre-Computer* derivado da chave de transmissão.

De acordo com a presente invenção é previsto, derivar em caso de demanda qualquer número de outras chaves criptográficas a partir da chave de transmissão, em geral, do material de chave de autenticação.

Como método de derivar chaves, a princípio, pode ser utilizado qualquer método criptográfico apropriado para derivar uma chave criptográfica, por exemplo, os métodos descritos em [5], como alternativa, uma variação do método de derivar chaves de acordo com MILENAGE descrito em [3] e [4].

Se para a formação de um grande número de chaves criptográficas como chaves de sessão for utilizada a mesma função de derivação de chave, então somente precisa ser implementada uma função de derivação de chave criptográfica tanto no terminal de rádio móvel como também no computador da rede de comunicação de origem. Uma outra vantagem da presente invenção é o fato de que um usuário de um terminal de rádio móvel somente precisa identificar-se uma vez para o acesso para o IMS e os serviços oferecidos através dele. Para o acesso às aplicações ou aos serviços baseados no IMS não são necessárias quaisquer identificações.

Além disso, de acordo com a presente invenção evita-se altera-

ções em protocolos padronizados já existentes, por exemplo, não precisarão ser alterados o protocolo de autenticação IMS-AKA descrito em [1] ou o protocolo para a comunicação entre o computador S-CSCF e o computador HSS, já que não precisam mais ser trocados parâmetros adicionais entre os respectivos computadores envolvidos.

Por meio da utilização da chave de transmissão (e não da chave de integridade) como chave base para a derivação de chaves evita-se também que surjam diferenças na utilização da chave entre diversas versões da norma (UMTS-3GPP Release 5 e UMTS-3GPP Release 6, etc.) que causariam dispêndios de padronização e de integração maiores.

Além disso, de acordo com a presente invenção é possível de configurar a derivação de chaves de tal modo que a chave somente é utilizada para as relações de segurança entre o terminal de rádio móvel e uma determinada unidade de rede e não para outras relações de segurança e não permita nenhuma conclusão para outras relações de segurança, especialmente nenhuma investigação das chaves criptográficas utilizadas no escopo de outras relações de segurança.

Também é possível configurar a derivação de chaves de tal modo que o terminal de rádio móvel e o computador S-CSCF calculam a chave derivada somente a partir da chave de transmissão, de parâmetros que resultam da respectiva autenticação atual de acordo com o protocolo de comunicação IMS-AKA e da identidade do computador de servidor de aplicação.

Isso tem a vantagem adicional de que a chave derivada para um determinado computador de servidor de aplicação pode ser calculada independentemente pelas chaves para outros computadores de servidor de aplicação. Isto é particularmente importante naquele caso quando a necessidade para o cálculo de chaves criptográficas derivadas para computadores de servidor de aplicação não surge simultaneamente, uma vez que o usuário não contata diversos computadores de servidor de aplicação em momentos diferentes e alguns, nunca.

Como parâmetros adicionais para a função de derivação de cha-

ve, de acordo com uma outra execução da presente invenção, é utilizada pelo menos uma das chaves criptográficas anteriormente criada. Em outras palavras, isso significa que um ou várias chaves criptográficas criadas anteriormente e agora disponíveis são utilizadas como valores de entrada para a função de derivação de chave , portanto, servindo como base para a criação de chaves criptográficas posteriores.

Por meio da presente invenção é então solucionado o problema de proteger na base de uma infra-estrutura de segurança IMS já existente em um sistema de rádio móvel uma comunicação adicional entre o terminal de rádio móvel e os computadores de servidor de aplicação para aplicações ou serviços na base do IMS que até agora não são cobertos pela segurança do sistema de rádio móvel IMS.

Tal comunicação pode ser baseada, por exemplo, no protocolo http e no protocolo MIKEY, de uma maneira geral, em qualquer protocolo de comunicação da camada OSI 7, isto é, da camada de aplicação.

Para garantir a comunicação, o mecanismo descrito cria chaves de sessão que são derivadas da chave de integridade e / ou chave de transmissão criada no escopo de uma autenticação IMS segundo [1]. O problema é solucionado principalmente pelo fato de que várias instâncias da rede como o computador de servidor de aplicação e o computador P-CSCF recebem chaves diferentes que não permitem conclusões sobre outras chaves criptográficas, de modo que também uma instância de rede, isto é, um computador de uma rede de comunicação visitada, não pode violar a confidencialidade das mensagens que o usuário troca com uma outra instância de rede, isto é, com um outro computador de uma rede de comunicação.

Adicionalmente, de acordo com a presente invenção, é utilizado um mecanismo que permite criar com apenas uma função de derivação de chave chaves criptográficas independentes para diferentes aplicações. Com isso, o dispêndio de implementar várias dessas funções de derivação de chave pode ser evitado.

Conforme descrito acima, adicionalmente se evita várias autenticações do usuário, isto é, do terminal de rádio móvel.

Como ilustração, a presente invenção pode ser visto no fato de que a partir da chave de transmissão criada no escopo do registro IMS são derivadas outras chaves criptográficas que são utilizadas para a codificação entre mensagens que podem ser utilizadas entre o terminal de rádio móvel e o computador P-CSCF e para as relações de segurança entre o terminal de rádio móvel e os computadores de servidor de aplicação, são de tal maneira derivadas que as vantagens acima descritas são obtidas.

Exemplos de execução da presente invenção são mostrados nas figuras e serão explicados detalhadamente a seguir.

Eles mostram:

A figura 1 mostra um diagrama em bloco de um sistema de rádio móvel de acordo com um exemplo de execução da presente invenção;

A figura 2 mostra um fluxograma de mensagens onde o fluxo de mensagens para criar e distribuir chaves criptográficas é mostrado de acordo com um exemplo de execução da presente invenção;

A figura 3 mostra um diagrama de bloco, onde é mostrada a criação de chaves criptográficas de acordo com um exemplo de execução da presente invenção.

Muito embora no exemplo de execução seguinte, por motivos da apresentação mais simples, são mostrados apenas um terminal de rádio móvel, uma rede de comunicação de origem e uma rede de comunicação visitada, a presente invenção pode ser aplicada a qualquer número de terminais de rádio móvel e redes de comunicação.

O sistema de rádio móvel 100 mostrado na figura 1 é configurado de acordo com o *UMTS Standard Release 5*.

O sistema de rádio móvel 100 de acordo com o exemplo de execução preferido possui uma rede de comunicação de origem 101 (*home network*), uma rede de comunicação visitada 102 (*visited network*), um terminal de rádio móvel 103 e computadores de servidor de aplicação 106, 107 que se encontram em outras redes de comunicação 104, 105.

A seguir somente serão explicados brevemente os elementos relevantes para a presente invenção do sistema de rádio móvel 100 de acor-

do com o *UMTS Standard Release 5*.

Na rede de comunicação de origem 101 é previsto um *Home Subscriber Server Computer* (HSS Computer) 108. No computador HSS são armazenados dados característicos, por exemplo, um perfil de serviço de usuário para cada terminal de rádio móvel 103 e o proprietário do terminal de rádio móvel 103 conjugados à rede de comunicação de origem 101.

Ao computador HSS 108 é acoplado um *Serving Call State Control Function Computer* (computador S-CSCF) 109 por meio de uma primeira conexão de comunicação 110.

Todo o gerenciamento de chamada, tanto por meio de pacote como também por linha, é controlado por um computador CSCF. Algumas outras tarefas dos computadores CSCF são a administração de faturamento (*billing*), a administração de endereços e a colocação a disposição de mecanismos de disparo para disparar serviços e nós especiais predeterminados.

Por meio de uma segunda conexão de comunicação 111, um *Interrogating CSCF Computer* (computador I-CSCF) 112 é acoplado ao computador S-CSCF 109. No computador I-CSCF 112 que se encontra na rede de comunicação de origem 101 e armazenada o endereço IP do respectivo HSS Computer 108 responsável, de modo que no início da autenticação de um terminal de rádio móvel 103 se torna possível na rede de comunicação de origem 101 determinar o HSS Computer 108 competente para a autenticação. O computador I-CSCF 112 estabelece de forma clara a "interface de comunicação" da rede de comunicação visitada 102 com a rede de comunicação de origem 101.

Na rede de comunicação visitada 102 é previsto um *Proxy CSCF Computer* (computador P-CSCF) 113 que junto com as estações rádio base existentes na rede de comunicação visitada 102 coloca à disposição uma interface de ar para o estabelecimento de uma ligação por rádio 114 com o terminal de rádio móvel 103 que se encontra na área à qual é conjugado o computador P-CSCF 113.

O computador P-CSCF 113 é ligado através de uma ligação por rádio ou de uma conexão de comunicação de rede fixa 115 por meio de

qualquer número de outras redes de comunicação com o computador I-CSCF 112 da rede de comunicação de origem 101.

Além disso, com o computador S-CSCF 109 da rede de comunicação de origem 101 são acoplados os computadores de servidor de aplicação 106, 107 nas outras redes de comunicação 104, 105 de acordo com o presente exemplo de execução por meio de outras ligações por rádio ou conexão de comunicação de rede fixa 116, 117. Por meio de ligações por rádio adicionais ou conexão de comunicação de rede fixa 118, 119, os computadores de servidor de aplicação 106, 107 são acoplados ao terminal de rádio móvel 103.

De acordo com este exemplo de execução, os diversos computadores possuem cada vez um microprocessador, uma ou várias memórias e respectivas interfaces de comunicação, de modo que é viabilizada uma troca de mensagens eletrônicas entre os diversos computadores e o terminal de rádio móvel 103.

Os computadores e o terminal de rádio móvel 103 são ainda configurados de tal maneira que os passos do método descritos a seguir podem ser realizados e as mensagens eletrônicas descritas em seguida podem ser geradas, codificadas ou decodificadas e transmitidas ou recebidas.

Para gerar as mensagens eletrônicas, de acordo com o presente exemplo de execução, pelo menos em parte é utilizado o *Session Initiation Protocol* (SIP).

Para que um terminal de rádio móvel 103 possa utilizar um serviço colocado à disposição por computadores de servidor de aplicação 106, 107 é necessário que ocorra e seja realizada uma autenticação mutua entre o terminal de rádio móvel 103 e a rede de comunicação de origem 101.

No início do processo de autenticação e para criar e distribuir chaves criptográficas que são utilizadas no escopo da sinalização e no escopo da troca de mensagens eletrônicas codificadas, o terminal de rádio móvel 103 envia uma mensagem de registro SIP 201 para o computador P-CSCF 113, conforme mostra o fluxograma de mensagens 200 na figura 2. A mensagem de registro SIP 201 é transferida depois de ter sido recebida pelo

computador P-CSCF 113 para o computador I-CSCF 112 na rede de comunicação de origem 101 do terminal de rádio móvel 103 que envia a mensagem de registro SIP 201. O computador I-CSCF 112 também transfere a mensagem de registro SIP 201, e precisamente para o computador S-CSCF 109 pertencente da rede de comunicação de origem 101.

Depois do recebimento da mensagem de registro SIP 201, o computador S-CSCF 109 verifica se o terminal de rádio móvel 103 que emite a mensagem de registro SIP 201 já foi registrado no computador S-CSCF 109 ou não. Em caso negativo, o computador S-CSCF 109 envia através da primeira conexão de comunicação 110 uma mensagem de requisição de dados de autenticação Cx 202 ao computador HSS 108 com a qual o computador S-CSCF 109 solicita no computador HSS 108 novos dados de autenticação para o terminal de rádio móvel 103.

No computador HSS 108. como reação à mensagem de requisição de dados de autenticação Cx 202, são geradas uma ou várias seqüências de dados de autenticação do modo descrito a seguir e transmitidas para o computador S-CSCF 109 em uma mensagem de dados de autenticação 203.

Em uma forma de execução alternativa os dados de autenticação são gerados pelo próprio computador S-CSCF 109.

O computador HSS 108, como alternativa, um *Authentication Center Computer* conjugado ao computador HSS 108, gera um número de seqüência corrente SQN 302 (passo 301).

Além disso, em um passo adicional (passo 303) é gerado um número aleatório RAND 304.

Além disso, um chamado *Authentication Management Field AMF* 305 predeterminado é utilizado como parâmetro de entrada para as operações descritas a seguir.

Além disso, uma chave secreta K 306 que somente o computador HSS 108 (na forma de execução alternativa o computador S-CSCF 109), e o terminal de rádio móvel 103 conhecem, é utilizada no escopo das operações descritas em seguida.

Nesse contexto cabe mencionar que a geração de um vetor de

autenticação AV, descrito a seguir, também pode acontecer no computador S-CSCF 109 ou em um outro elemento da rede comparável na rede de comunicação de origem 101, caso em que os valores acima descritos estão disponíveis na respectiva unidade de computador.

Sob a utilização da chave secreta K 306, do campo *Authentication Management Field AMF* 305, do número de seqüência SQN 302 e do número aleatório RAND 304, uma primeira função de autenticação de mensagens f1 307, descrita por exemplo, em [3] e [4], gera um *Message Authentication Code MAC* 308, de acordo com a seguinte norma:

$$MAC = f1_K (SQN \mid RAND \mid AMF). \quad (1)$$

O símbolo "|" simboliza no escopo dessa descrição uma concatenação dos valores que ficam à esquerda ou à direita do símbolo.

As funções f1 e f2 de autenticação de mensagens utilizadas a seguir e as funções de geração de chave f3, f4, f5 são descritas em [3] e [4].

Através de uma segunda função de autenticação de mensagens f2 309, sob utilização de uma chave segreda K 306 e do número aleatório RAND 304 é criado um valor de resposta XRES esperado 310 :

$$XRES = f2_K (RAND) \quad (2)$$

Através de uma primeira função de geração de chaves f3 311, sob a utilização da chave segreda K 306 e do número aleatório RAND 304 é criada uma chave de transmissão CK 312 de acordo com a seguinte norma :

$$CK = f3_K (RAND) \quad (3)$$

Além disso, sob a utilização de uma segunda função de geração de chaves f4 313 e sob a utilização da chave segreda K 306 e do número aleatório RAND 304, é criada uma chave de integridade IK 314 de acordo com a seguinte norma :

$$IK = f4_K (RAND) \quad (4)$$

Através de uma terceira função de geração de chaves f5 315, sob a utilização também da chave segreda K 306 e do número aleatório RAND 304, é calculada uma chave de anonimato AK 316 de acordo com a seguinte norma :

$$AK = f5_K RAND) \quad (5)$$

O computador HSS 108 cria ainda um token de autenticação AUTN 320 de acordo com a seguinte norma :

$$AUTN = SQN \oplus AK \mid AMF \mid MAC \qquad (6)$$

Os valores calculados acima descritos, isto é, o token de autenticação AUTN 320, o valor de resposta XRES esperado 310, a chave de transmissão CK 312 e a chave de integridade IK 314, são transmitidos para o computador S-CSCF 109.

De acordo com a presente invenção, sob a utilização de uma função de derivação de chave f 317 da chave de transmissão CK 312 no computador S-CSCF 109, sob a utilização de parâmetros de entrada 318 descritos a seguir, é criada uma primeira chave derivada CK1 319 da seguinte maneira :

Como função de derivação de chave f 317, de acordo com um primeiro exemplo de execução da presente invenção, é utilizada uma pseudo-função aleatória PRF que se baseia, por exemplo, no método HMAC-SHA1. A função de derivação de chave f 317 é configurada essencialmente de acordo com o método de derivar chaves especificado em [6], parágrafo 5.5.

Portanto, a primeira chave derivada CK1 é criada de acordo com a seguinte norma:

$$CK1 = f_K(CK \mid Pari \mid \text{escolha aleatória (random)}) \qquad (7)$$

onde o parâmetro de entrada Pari é otimizado e onde escolha aleatória (random) é material aleatório apropriado, por exemplo, formado de acordo com a seguinte norma :

$$\text{Escolha aleatória (random)} = RAND \mid AUTN \mid XRES \qquad (8)$$

onde RAND | AUTN é transmitido durante o processo de autenticação de acordo com [1] para o terminal de rádio móvel 103 como uma mensagem de requisição de autenticação 204 descrita a seguir.

O terminal de rádio móvel 103 utiliza para a formação do valor aleatório escolha aleatória (random) no lugar do valor de resposta esperado XRES o valor de resposta RES criado por ele.

Um valor deduzido do valor RES é transmitido no escopo do processo de acordo com [1] descrito a seguir é transmitido pelo terminal de

rádio móvel 103 como resposta de autenticação para o computador S-CSCF 109.

Neste contexto cabe mencionar que a criação das chaves criptográficas derivadas pode ocorrer no computador S-CSCF 109 ou em um elemento de rede comparável na rede de comunicação de origem 101.

Além disso, o computador S-CSCF 109 cria de acordo com a seguinte norma o vetor de autenticação AV 321 exigido :

$$AV = RAND \mid XRES \mid CK1 \mid IK \mid AUTN \qquad (9)$$

O computador S-CSCF 109 transmite a mensagem de requisição de autenticação SIP 204 para o computador I-CSCF 112, e este o transmite para o computador P-CSCF 113 da rede de comunicação visitada 102. Na mensagem de requisição de autenticação SIP 204 estão contidos o número aleatório RAND 306, o token de autenticação 320 e a chave de integridade IK. Ao contrário do processo de autenticação de acordo com [1], de acordo com a presente invenção não é contida a chave de transmissão CK e, portanto, também não é transmitida no computador P-CSCF na rede de comunicação visitada para um usuário. Em vez disso, a mensagem de requisição de autenticação SIP 204 contém a primeira chave derivada CK1.

No terminal de rádio móvel 103, sob a utilização das funções de autenticação de mensagens f1 e f2 e da função de criação de chaves f3, f4 e f5 também são criados valores acima descritos e utilizados para a autenticação da rede de comunicação visitada 102. Para este fim, as funções f1, f2, f3, f4 e f5 também são implementadas no terminal de rádio móvel 103.

Além disso, o terminal de rádio móvel 103 dispõe naturalmente da chave secreta K e ao número aleatório RAND 306. Além disso, também estão disponíveis no terminal de rádio móvel 103 para a criação das chaves derivadas sob a utilização da função de derivação de chave 317 as informações adicionais descritas a seguir sobre os parâmetros Pari.

Antes de transferir a mensagem de requisição de autenticação 204 o computador P-CSCF 113 armazena a chave de integridade IK 314 e a primeira chave derivada SK1, retira estas da mensagem de requisição de autenticação 204 e transmite uma mensagem de requisição de autenticação

reduzida 205 para o terminal de rádio móvel 103.

Assim sendo, a chave de integridade IK 314 é disponível no computador P-CSCF 113, porém, não no terminal de rádio móvel 103.

No terminal de rádio móvel 103, sob a utilização da chave secreta K 306 e do número aleatório RAND 304 disponível no terminal de rádio móvel 103, sob a utilização da quinta e da terceira função de geração de chaves f5 315, é criada a chave de anonimato AK 316.

Com utilização do primeiro campo do token de autenticação 320, criando o conteúdo do primeiro campo (SQN ⊕ AK) é criado um entrelaçamento EXCLUSIVO - OU com a chave de anonimato AK 316, e como resultado, o terminal de rádio móvel 103 recebe o número de seqüência SQN 302.

Utilizando o número de seqüência, o *Authentication Management Field AMF* 305 contido no token de autenticação 320, do número aleatório RAND 304, a chave segreda K 306 e a primeira função de autenticação de mensagens fl 307 é criado um *Message Authentication Code* de terminais que é comparado com o *Message Authentication Code MAC* 308 contido no token de autenticação 320.

Esses dois valores coincidindo, então a autenticação da rede de comunicação visitada 102 perante o terminal de rádio móvel 103 foi bem sucedida, e o terminal de rádio móvel 103 calcula um valor de resposta\ RES sob utilização do número aleatório RAND 304, da chave segreda K 306 e da segunda função de autenticação de mensagens f2 309 e transmite um valor de resposta derivado de RES em uma mensagem de resposta de autenticação SIP 206 para o computador P-CSCF 113, conforme é descrito em [1].

Cabe notar que o terminal de rádio móvel 103 calcula também, utilizando a primeira função de geração de chaves f3 311 e da chave segreda K 306 a chave de transmissão 312, e utilizando a segunda função de geração de chaves f4 313 e a chave segreda K 306 calcula a chave de integridade IK 314.

O computador P-CSCF 113 transmite a mensagem de resposta de autenticação SIP 206 para o computador I-CSCF 112, e este o transmite para o computador S-CSCF 109.

O computador S-CSCF 109 ou o computador HSS 108 examinam o valor de resposta derivado de RES, comparando o mesmo com o valor derivado de maneira analógica da resposta esperada XRES. Em caso de coincidência dos dois valores, a autenticação do terminal de rádio móvel 103 diante do computador S-CSCF 109 foi bem sucedida.

Agora o valor *escolha aleatória (random)* também pode ser criado no terminal de rádio móvel 103 de acordo com a norma (8), e em seguida, a primeira chave derivada SK1 de acordo com a norma (7).

Uma mensagem de confirmação de autenticação 207 é transmitida pelo computador S-CSCF 109 para o computador I-CSCF 112, e este a transmite para o computador P-CSCF 113.

A mensagem de confirmação de autenticação 208 é transmitida para o terminal de rádio móvel 103 para confirmar a autenticação mutua bem sucedida.

Além disso, o computador S-CSCF 109 cria através de nova utilização da função de derivação de chave f 317 e opcionalmente utilizando um parâmetro de entrada adicional Par2, uma segunda chave derivada CK2 322 de acordo com a seguinte norma :

$$CK@ = f_K (CK, CK1 \mid Par2 \mid \text{escolha aleatória (random)}) \qquad (10)$$

A segunda chave derivada CK2 322 é transmitida em uma mensagem de chave 209 para o computador de servidor de aplicação 106 que no contexto com a codificação futura utiliza a segunda chave derivada CK2 322.

O terminal de rádio móvel 103 cria de modo correspondente ao do computador S-CSCF 109 também a segunda chave derivada CK2 322.

Se no contexto da comunicação com computadores de servidor de aplicação adicionais será necessário material de chave adicional, isto é, chaves derivadas adicionais, então são criadas chaves derivadas adicionais CKi (i = 1, ..., n, - n significa o número de chaves derivadas criadas) 323, 324, a princípio qualquer número de chaves adicionalmente derivadas de acordo com a seguinte norma, e transmitida para o respectivo computador de servidor de aplicação :

$$CKi = f_K (CK, CKi \mid Pari \mid \text{escolha aleatória (random)}) \qquad (11)$$

Neste caso, Pari (i = 1, ..., n) pode representar a identidade, por exemplo, o endereço IP, do respectivo computador de servidor de aplicação 106, 107.

O respectivo parâmetro Pari pode ainda conter outras informações sobre a utilização da chave, por exemplo, informações sobre a utilização para a codificação ou para a proteção da integridade, informações sobre a direção do fluxo de mensagens (saindo do terminal de rádio móvel 103 ou para o terminal de rádio móvel 103), para o qual a chave deve ser utilizada.

Depois da chave de integridade IK 314 e a chave de transmissão CK 312 estarem disponíveis no terminal de rádio móvel 103 e no computador S-CSCF 109, a função de derivação de chave f 317 é executada tantas vezes até que para todas as aplicações a serem protegidas haja as chaves criptográficas necessárias. Isto ocorre, conforme descrito acima, tanto no terminal de rádio móvel 103 como também no computador S-CSCF 109.

Em seguida, são utilizadas as chaves derivadas, por exemplo, pelo computador P-CSCF 113 (primeira chave derivada CK 318) para a proteção das próprias mensagens IMS e as outras chaves derivadas 322, 323, 324 estão colocadas à disposição de uma aplicação a ser protegida ou utilizadas de modo apropriado para elas.

Em alternativa pode ser gerada uma seqüência de chaves pela concatenação das diversas chaves derivadas criadas CK1, CK2, Cki, CKn 318, 322, 323, 324. Isto é vantajoso quando as chaves derivadas com seu comprimento não correspondem às exigências do processo de proteção utilizado ou quando, por exemplo, duas chaves unidirecionais são necessárias para uma aplicação.

Nesse caso, uma chave derivada resulta de acordo com a seguinte norma :

$$KEYMAT = CK1 \mid CK2 \mid \ldots \mid CKi \ldots \qquad (12)$$

Desta seqüência de chaves KEYMAT serão então, começando da esquerda e em seqüência sucessivamente para as seguintes aplicações, retiradas as chaves criptográficas necessárias.

A seguir serão indicados exemplos de execução alternativos pa-

ra a criação das chaves derivadas 318, 322, 323, 324.

O seguinte exemplo de execução é semelhante ao método MILENAGE descrito em [3] e [4].

Material aleatório apropriado para *escolha aleatória (random)*, criado, por exemplo, de acordo com a norma (8). Para a criação do valor aleatório *escolha aleatória (random)* é utilizado o método de acordo com a exemplo de execução acima descrito. Além disso, supõe-se que ASi-ID significa a identidade, por exemplo, o endereço do IP, do computador de servidor de aplicação ASi para i = 1, 2, ..., n. Suponha-se que h é uma função *hash* como, por exemplo, SHA-1. E é uma função de codificação de cifras de bloco apropriada, contendo valores de entrada, valores de saída e chaves com comprimento de bit de respectivamente 128. Quando o valor de entrada é x, a chave é k e o valor de saída é y, então o valor de saída y é determinado de acordo com a seguinte norma :

$$Y = E[x]k \qquad (13)$$

Um exemplo para uma função de codificação de cifra de bloco é o chamado método de Rijndael, como descrito, por exemplo, em [4].

Um valor de 128 bit x_i é derivado da identidade do computador de servidor de aplicação e da chave de transmissão CK 312 de acordo com a seguinte norma :

$$X_i = ASi - ID \oplus E[ASi - ID]_{CK} \qquad (14)$$

Um valor intermediário TEMP do comprimento de 128 bit é calculado de acordo com a seguinte norma :

$$TEMP = E[\text{escolha aleatória (random)} \oplus x_i]_{CK} \qquad (15)$$

Uma respectiva chave derivada CKi agora é calculada como segue :

$$CKi(r, c) = E[rot(TEMP \oplus x_i, r) \oplus c]_{CK} \oplus x_i \qquad (16)$$

onde r e c são constantes apropriadas predeterminávels, como por exemplo, descrito em [4].

Como também descrito em [4], é possível, de acordo com a presente invenção, derivar pela seleção apropriada de outras constantes r e c outras chaves CKi (r, c) para o mesmo computador de servidor de aplicação.

De acordo com um exemplo de execução alternativo da presente invenção que segue o método de derivação de chaves de acordo com RSA PKCS nº 5, novamente é utilizado o valor aleatório *escolha aleatória (random)* que é obtido do mesmo modo como de acordo com o primeiro exemplo de execução.

Novamente, como de acordo com o segundo exemplo de execução, ASi-ID é a identidade do computador de servidor de aplicação ASi para i = 1, 2, ..., n. Novamente h é uma função *hash* como, por exemplo, SHA1 e PRF é uma pseudo-função aleatória.

Os seguintes valores são calculados :

X_0 = h ("chave de cifra para computador P-CSCF"), (17)

X_i = h (ASi - ID) . para i = l, ..., n (18)

Em seguida, as chaves derivadas CKi são calculadas de acordo com a seguinte norma para i = 0, 1, 2, ..., n :

CKi = F (CK, *escolha aleatória (random)*, c, i) = U_l (i) \XOR U_2 (i) \ XOR ... \ XOR U_c (i) (19)

onde c é um número inteiro apropriado que pode ser predeterminado de modo apropriado, e

U_l (i) = PRF (CK, *escolha aleatória (random)* | x_i) (20)

U_2 (i) = PRF (CK, U_l (i)) (21)

...

U_c (i) = PRF (CK, U_{c-1} (i)) (22)

De acordo com uma outra forma de execução alternativa é previsto combinar os procedimentos de acordo com o primeiro exemplo de execução e o segundo exemplo de execução no seguinte sentido.

Primeiro é calculado uma chave derivada CKi para o computador de servidor de aplicação ASi, conforme é descrito no segundo exemplo de execução. Em seguida, o procedimento é aplicado de acordo com o primeiro exemplo de execução para obter mais material de chave para o computador de servidor de aplicação ASi, substituindo-se a chave de transmissão CK 312 no primeiro exemplo de execução pela chave respectivamente derivada CKi que foi obtido do processo de acordo com o segundo exemplo de exe-

cução .

Então resultam para as chaves adicionalmente derivadas :

$$CKi1 = f(CKi, \textit{escolha aleatória (random)}) \quad (23)$$

$$CKi2 = f(CKi, CKi1 \mid \textit{escolha aleatória (random)}) \quad (24)$$

$$CKi3 = f(CKi, CKi2 \mid \textit{escolha aleatória (random)}) \quad (25)$$

etc..

Agora existe tudo para a codificação das respectivas mensagens no escopo das aplicações necessárias tanto no terminal de rádio móvel 103, no computador P-CSCF 113 e nos computadores de servidor de aplicação 106, 107, sem que o computador P-CSCF 113 possa tirar conclusões sobre as chaves derivadas CKi, 318, 322, 323, 324 nos computadores de servidor de aplicação 106, 107, e vice-versa, sem que os computadores de servidor de aplicação 106, 107 possam tirar conclusões sobre o material de chave armazenado e utilizado no computador P-CSCF 113.

Sob a utilização das chaves derivadas 318, 322, 323, 324 acontece em seguida a codificação dos dados úteis a serem transmitidos.

No presente pedido foram citadas as seguintes publicações:

[1] 3GPP TS 33.203 V5.3.0 - Technical Specification, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Access Security for IP-based services (Release 5).

[2] G. Horn, D. Kröselberg, K. Müller : Security for IP multimedia services in the 3GPP third generation mobile system, Proceedings of the Third International Networking Conference INC`2002, páginas 503 a 512, Plymouth, UK, 16 a 18 de julho de 2002.

[3] 3GPP TS 35.205 V5.0.0 - Technical Specification, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the MILENAGE Algorithm Set : An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*, Document 1 : General (Release 5).

[4] 3GPP TS 35.206 V5.0.0 - Technical Specification, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3 GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 e f5*, Documento 2 : Algorithm Specification (Release 5).

[5] IST-2000-25350 - SHAMAN, D13 - WP1 contribution, Final technical reporte comprising the complete technical results, specification and conclusion, capítulo 4.7, páginas 114 a 122, novembro de 2002.

[6] D. Harkins e D. Carrel, The Internet Key Exchange (IKE), RFC 2409, páginas 17 a 19 , novembro de 1998.

REIVINDICAÇÕES

1. Método para criar e distribuir chaves criptográficas (318, 322) em um sistema de rádio móvel (100) que possui pelo menos um terminal de rádio móvel (103), um primeiro computador (113), um computador de uma rede de comunicação de origem (109) e um segundo computador (106, 107), sendo que o terminal de rádio móvel (103) e o computador da rede de comunicação de origem (109) contêm como resultado de autenticação material de chave de autenticação (312, 314), caracterizado pelo fato de que

- são criadas pelo terminal de rádio móvel (103) e pelo computador da rede de comunicação de origem (109) respectivamente sob utilização do material de chave de autenticação (312) uma primeira chave criptográfica (318) e uma segunda chave criptográfica (322);
- a primeira chave criptográfica (318) é transmitida para o primeiro computador (113);
- a segunda chave criptográfica (322) é transmitida para o segundo computador (106);
- a primeira chave criptográfica (318) e a segunda chave criptográfica (322) são criadas de tal modo que
  - não é possível tirar conclusões sobre a segunda chave criptográfica (322) a partir da primeira chave criptográfica (318),
  - não é possível tirar conclusões sobre a primeira chave criptográfica (318) a partir da segunda chave criptográfica (322),
  - não é possível tirar conclusões sobre o material de chave de autenticação (312, 314) a partir da primeira chave criptográfica (318) ou da segunda chave criptográfica (322).

2. Método de acordo com a reivindicação 1,

- onde o primeiro computador (113) é um computador de uma rede de comunicação visitada, sendo que o terminal de rádio

móvel (103) se encontra na rede de comunicação visitada (102), e

- onde o segundo computador é um computador de servidor de aplicação (106, 107).

3. Método de acordo com a reivindicação 1,

- onde o primeiro computador (113) é um primeiro computador de servidor de aplicação (106) e
- onde o segundo computador é um segundo computador de servidor de aplicação (107).

4. Método de acordo com uma das reivindicações 1 a 3, onde a primeira chave criptográfica (318) e a segunda chave criptográfica (322) são criadas sob utilização de pelo menos uma função de derivação de chave (317).

5. Método de acordo com uma das reivindicações 1 a 4, onde o material de chave de autenticação (312, 314) possui pelo menos duas chaves criptográficas.

6. Método de acordo com uma das reivindicações 1 a 5, onde o sistema de rádio móvel (100) é configurado como um sistema de rádio móvel baseado na norma 3GPP.

7. Método de acordo com a reivindicação 6, onde o sistema de rádio móvel (100) possui um *IP multimedia subsystem.*

8. Método de acordo com uma das reivindicações 1 a 7, onde o material de chave de autenticação (312, 314) possui uma chave de integridade (314) e uma chave de transmissão (312).

9. Método de acordo com a reivindicação 8, onde a primeira chave criptográfica (318) e a segunda chave criptográfica (322) são derivadas da chave de transmissão (312).

10. Método de acordo com uma das reivindicações 1 a 9, onde o terminal de rádio móvel (103) e o computador da rede de comunicação de origem (109) criam para computadores de servidor de aplicação (107) respectivamente sob utilização do material de chave de autenticação (312, 314) chaves criptográficas adicionais (323, 324) que são transmitidas para os

respectivos computadores de servidor de aplicação (107).

11. Método de acordo com uma das reivindicações 1 a 10, onde é utilizada a mesma função de derivação de chave para a criação das chaves criptográficas (318, 322, 323, 324).

12. Método de acordo com uma das reivindicações 1 a 11, onde para a criação das chaves criptográficas (318, 322, 323, 324) são utilizados parâmetros de entrada adicionais diferentes (319) para a função de derivação de chave (317).

13. Método de acordo com a reivindicação 12 onde como parâmetros de entrada adicionais (319) para a função de derivação de chave (317) são utilizados parâmetros que são formados no escopo da autenticação.

14. Método de acordo com a reivindicação 13, onde pelo menos uma das chaves criptográficas (318, 322, 323, 324) anteriormente criadas é utilizada como parâmetro de entrada adicional para a função de derivação de chave.

15. Sistema de rádio móvel (100)

- com pelo menos um terminal de rádio móvel (103) onde como resultado de uma autenticação é armazenado material de chave de autenticação (312, 314),
- com um primeiro computador (113),
- com um computador de uma rede de comunicação de origem (109) onde como resultado de uma autenticação é armazenado o material de chave de autenticação (312, 314),
- com pelo menos um segundo computador (106, 107), caracterizado pelo fato de que
- o terminal de rádio móvel (103) e o computador da rede de comunicação de origem (109) possuem respectivamente uma unidade criptográfica para a criação de uma primeira chave criptográfica (318) e de uma segunda chave criptográfica (322) sob utilização do material de chave de autenticação (312, 314), sendo que a primeira chave criptográfica (318) e a segunda

chave criptográfica (322) são executadas de tal modo que

- não é possível tirar conclusões sobre a segunda chave criptográfica (322) a partir da primeira chave criptográfica (318),
- não é possível tirar conclusões sobre a primeira chave criptográfica (318) a partir da segunda chave criptográfica (322),
- não é possível tirar conclusões sobre o material de chave de autenticação (312, 314) a partir da primeira chave criptográfica (318) ou da segunda chave criptográfica (322).

• o primeiro computador (113) possui uma memória para armazenar a primeira chave criptográfica (318), e

• o segundo computador (106, 107) possui uma memória para armazenar a segunda chave criptográfica (322).

FIG 1

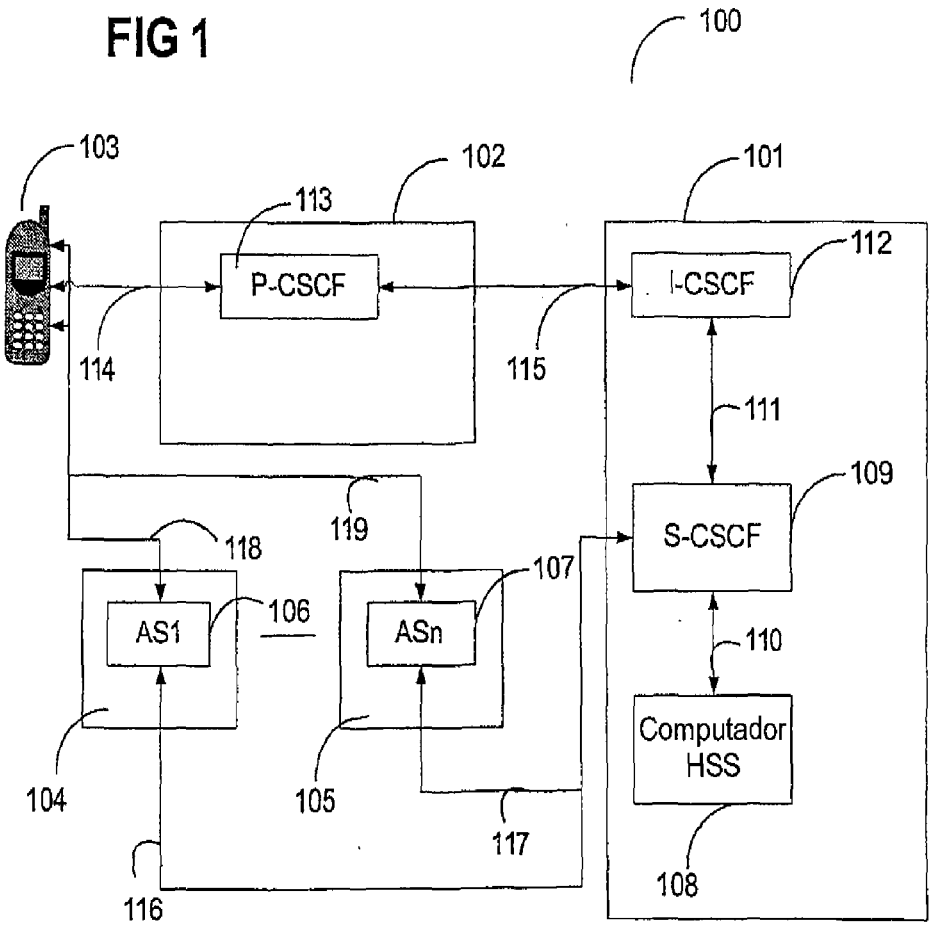

100
103
102
101
113
P-CSCF
I-CSCF
112
114
115
111
109
119
118
S-CSCF
107
AS1
106
ASn
110
Computador
HSS
104
105
117
116
108

FIG 2

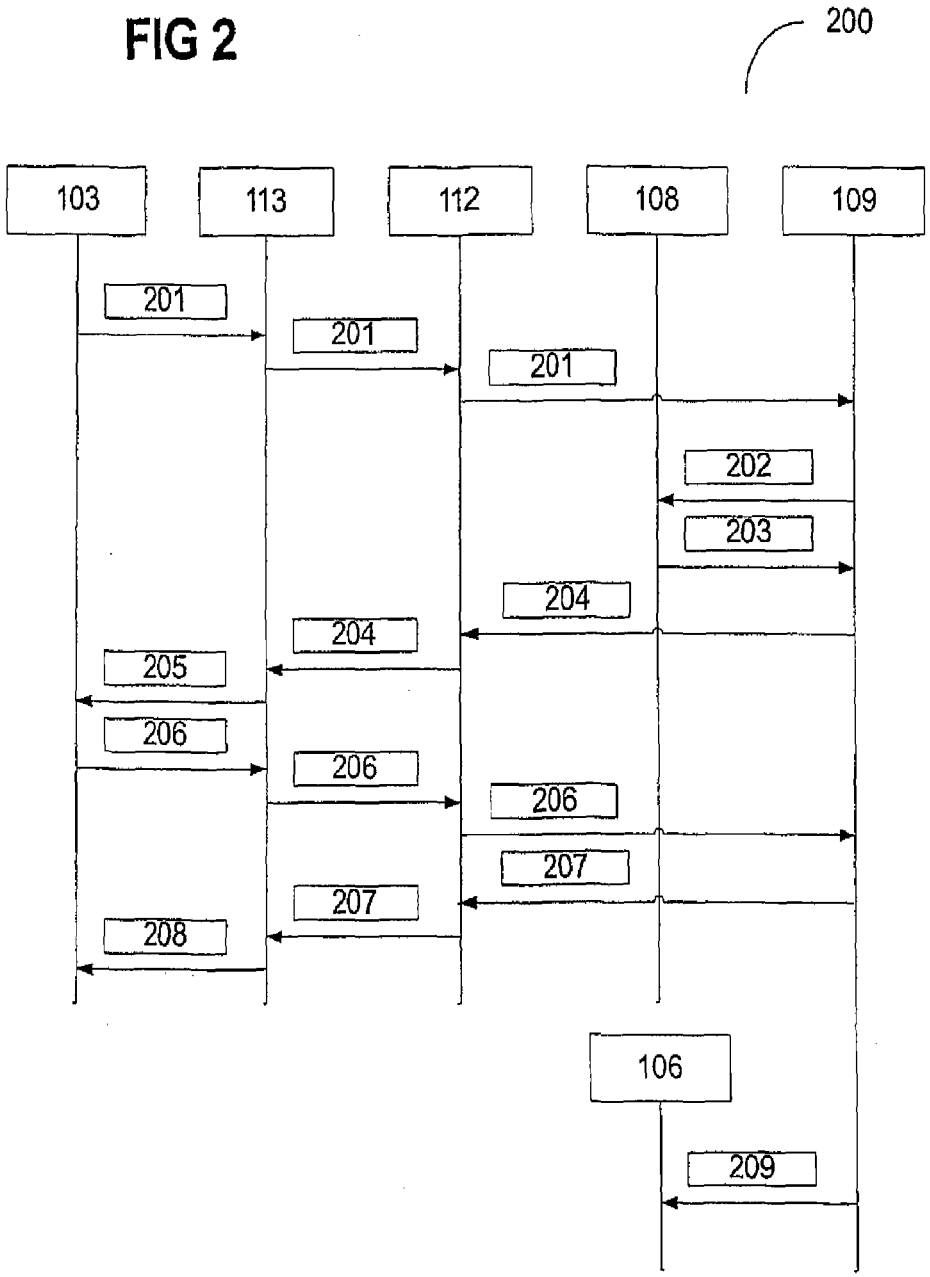
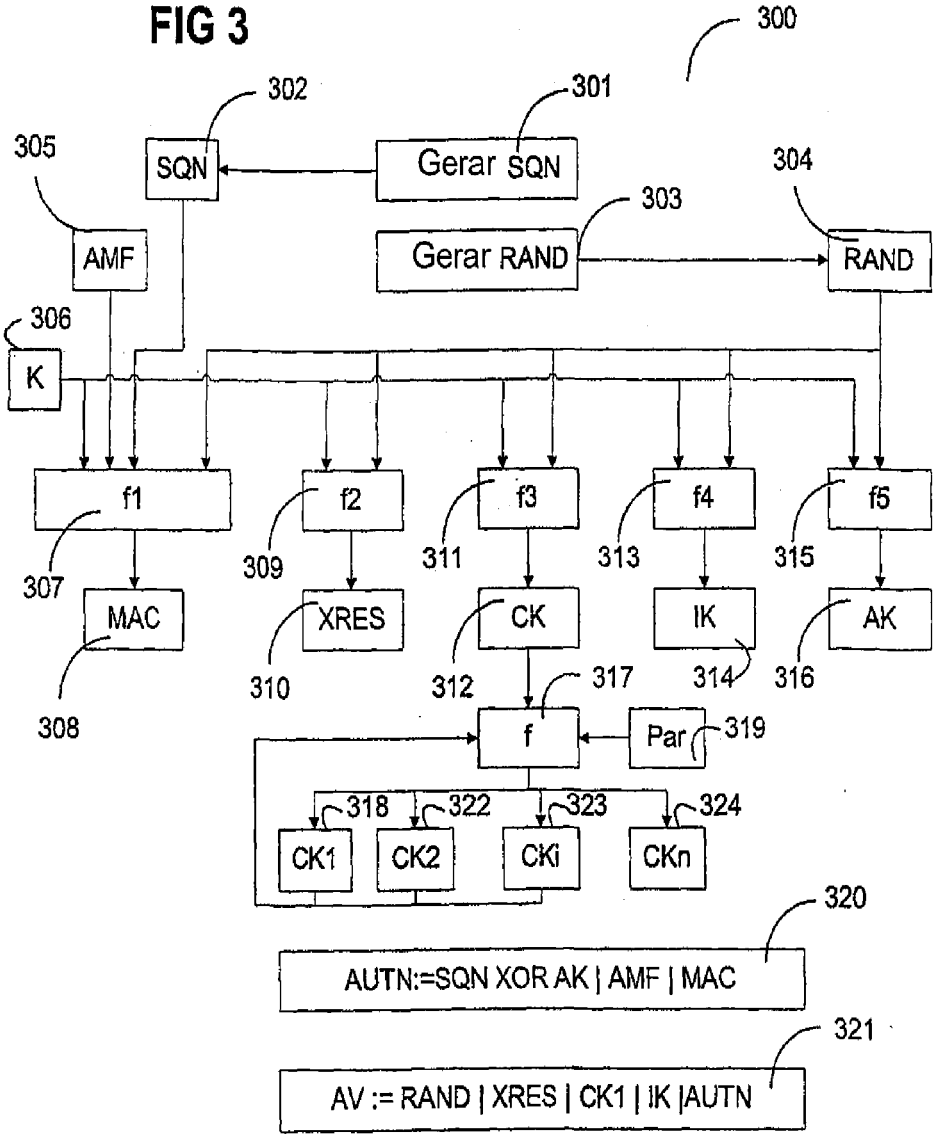

200
103
113
112
108
109
201
201
201
202
203
204
204
205
206
206
206
207
207
208
106
209

FIG 3


300
302
301
305
SQN
Gerar SQN
304
303
AMF
Gerar RAND
RAND
306
K
f1
f2
f3
f4
f5
307
309
311
313
315
MAC
XRES
CK
IK
AK
310
312
317
314
316
308
f
Par
319
318
322
323
324
CK1
CK2
CKi
CKn
320
AUTN:=SQN XOR AK | AMF | MAC
321
AV := RAND | XRES | CK1 | IK |AUTN

RESUMO

Patente de Invenção: **"MÉTODO PARA CRIAR E DISTRIBUIR CHAVES CRIPTOGRÁFICAS EM UM SISTEMA DE RÁDIO MÓVEL E SISTEMA DE RÁDIO MÓVEL".**

A presente invenção refere-se a um terminal de rádio móvel (103) e um computador da rede de comunicação de origem (108, 109) que criam respectivamente sob utilização de material de chave de autenticação (312) uma primeira chave criptográfica (318) e uma segunda chave criptográfica (322). A primeira chave criptográfica (318) é transmitida para o computador da rede de comunicação visitada (113), e a segunda chave criptográfica (322) é transmitida para um computador de servidor de aplicação (106, 107).