



INPI
INSTITUTO
NACIONAL
DA PROPRIEDADE
INDUSTRIAL
Assinado
Digitalmente

REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

CARTA PATENTE Nº PI 0710257-7

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE DE INVENÇÃO, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito: PI 0710257-7

(22) Data do Depósito: 26/03/2007

(43) Data da Publicação Nacional: 09/08/2011

(51) Classificação Internacional: H04L 29/06; H04L 9/08; H04L 9/32; H04W 12/04; H04W 12/06.

(52) Classificação CPC: H04L 63/062; H04L 9/0833; H04L 9/321; H04L 9/3271; H04L 63/0853; H04W 12/04; H04W 12/06; H04L 63/083; H04L 2209/80; H04L 2463/061.

(30) Prioridade Unionista: US 60/786,357 de 28/03/2006.

(54) Título: MÉTODO PARA AUTENTICAR UMA APLICAÇÃO COM UMA APLICAÇÃO DE SERVIDOR E TERMINAL MÓVEL PARA AUTENTICAÇÃO DE UMA APLICAÇÃO

(73) Titular: NOKIA TECHNOLOGIES OY. Endereço: Karakaari 3, FI-02610, Espoo, FINLÂNDIA(FI)

(72) Inventor: SHREEKANTH LAKSHMESHWAR; PHILIP GINZBOORG; PEKKA LAITINEN; SILKE HOLTMANN.

(87) Publicação PCT: WO 2007/110468 de 04/10/2007

Prazo de Validade: 10 (dez) anos contados a partir de 05/11/2019, observadas as condições legais

Expedida em: 05/11/2019

Assinado digitalmente por:
Liane Elizabeth Caldeira Lage
Diretora de Patentes, Programas de Computador e Topografias de Circuitos Integrados

“MÉTODO PARA AUTENTICAR UMA APLICAÇÃO COM UMA APLICAÇÃO DE SERVIDOR E TERMINAL MÓVEL PARA AUTENTICAÇÃO DE UMA APLICAÇÃO”.

Antecedentes da Invenção:

Campo da invenção:

[001] A presente invenção refere-se à autenticação. Em particular, a presente invenção se refere a métodos, programas de computador e terminais móveis inusitados e aperfeiçoados para autenticar uma aplicação de um cliente.

Descrição da Técnica Relacionada:

[002] O desenvolvimento atual em direção à computação e à formação de rede verdadeiramente móvel causou a evolução de diversas tecnologias de acesso, as quais também fornecem aos usuários acesso à Internet quando estão fora de sua rede doméstica. Até o momento, o uso da Internet foi dominado por comunicações de pessoa-para-máquina, isto é, serviços de informação. A evolução em direção às chamadas redes sem fio de terceira geração (3G) traz consigo comunicações de multimídia móveis, as quais também irão alterar a maneira com que os serviços baseados em IP são utilizados em redes móveis públicas. O Subsistema de Multimídia IP (IMS), conforme especificado pelo Projeto de Parceria de Terceira Geração (3GPP), integra as comunicações móveis de voz com tecnologias de Internet, permitindo serviços de multimídia baseados em IP sejam utilizados nas redes móveis.

[003] Os novos terminais móveis com capacidade para multimídia (telefones multimídia) fornecem uma plataforma de desenvolvimento aberta para Os usuários podem, por sua vez, fazer a transferência por download de novos serviços/aplicações para seus terminais móveis e utilizá-los nos mesmos. Por exemplo, a especificação técnica 3GPP TS33.220 revela a Arquitetura Genérica de Autocarregamento (GBA) que faz parte da Arquitetura de Autenticação (GAA). Um modelo de rede geral da GBA é revelado na Figura 1. O modelo revelado na Figura 1 inclui quatro entidades diferentes: Um Equipamento de Usuário (EU) 14, uma Função de Servidor de Autocarregamento 12, Função de Aplicação de Rede (NAF) 16 e um Sistema

Doméstico de Assinante (HSS) 10. A Figura 1 revela, ainda, as interfaces entre as entidades.

[004] A Figura 2 é um diagrama que ilustra o procedimento de autocarregamento na GBA. Quando um UE 200 quer interagir com uma NAF e sabe que o procedimento de autocarregamento é necessário, o mesmo deve desempenhar, em primeiro lugar, uma autenticação de autocarregamento. Quando o autocarregamento é iniciado, o UE 200 envia (21) uma solicitação de http em direção à BSF 202. A BSF 202 restaura (22) o conjunto completo de ajustes de segurança de usuário da GBA e um Vetor de Autenticação (AV, AV RAND AUTN XRES CK IK) através do ponto de referência Zh a partir de um HSS 204. Em seguida, a BSF 202 encaminha o RAND e o AUTN para o UE 200 na mensagem 401 (23) (sem o CK, IK e XRES). Isso ocorre para exigir que o UE 200 autentique a si próprio. O UE 200 verifica (24) o AUTN para confirmar que o desafio é proveniente de uma rede autorizada. O UE 200 também calcula CK, IK e RES. Isso resultará em chaves de sessão IK e CK na BSF 202 e no UE 200. O UE 200 envia (25) outra solicitação de HTTP, que contém a resposta Digest AKA (calculada usando-se RES), para a BSF 202. A BSF 202 autentica (26) o UE 200 através da confirmação da resposta Digest AKA e gera (27) uma chave mestre Ks através da concatenação de CK e IK. Um valor B-TID também pode ser gerado. O BSF envia (28) uma mensagem de OK 200, que inclui B-TID, para o UE 200 com o objetivo de indicar o sucesso da autenticação. Além disso, na mensagem de OK 200, a BSF 202 deve fornecer a vida útil da chave Ks. A chave Ks é gerada no UE 200 através da concatenação de CK e IK. O UE 200 e a BSF 202 podem usar a Ks para derivar a chave Ks_NAF. KDF para a GBA é definida em 3GPP TS 33.220, segurança de protocolo de NAF e Ua. A KDF deve ser implantada no equipamento móvel.

[005] Quando a aplicação no terminal quer autenticar um servidor de aplicação de rede, a mesma obtém um Ks_NAF de segredo compartilhado com NAF através de uma API oferecida por uma aplicação confiável no terminal. A aplicação confiável utiliza os procedimentos de autocarregamento descritos acima com o servidor da Função de Servidor de Autocarregamento (BSF) para derivar o Ks_NAF de segredo

compartilhado com NAF. A NAF adquire o segredo compartilhado para a aplicação do cliente através da comunicação com a BSF.

[006] Um prestador de serviço pode querer impedir que as aplicações do cliente sejam desenvolvidas e apropriadas por outros prestadores de serviço e instaladas em um terminal móvel para acessar seu serviço. Para atingir tal objetivo, ele poderia, por exemplo, autenticar uma aplicação no terminal móvel todas as vezes que o mesmo tentasse acessar o serviço. Tal método, portanto, exigiria uma associação de segurança de longo prazo entre o prestador de serviço e cada cópia distribuída da aplicação. Manter tais associações de segurança de longo prazo pode aumentar, de modo significativo, os custos do prestador de serviço.

[007] Já que a chave NAF específica, isto é, Ks_NAF , é, de fato, específica da NAF (isto é, serviço), o objetivo pode ser alcançado pelo terminal móvel através do acesso restrito a Ks_NAF para somente aquelas aplicação que são consideradas confiáveis pelo prestador de serviço da NAF. Essa restrição é possível se o hardware e o software da plataforma do terminal móvel possuem as propriedades de segurança a seguir: (1) processos podem auto-autenticar e (2) um processo não pode acessar os dados de outro processo. O terminal móvel, portanto, precisa ser configurado; o mesmo precisa saber quais aplicações têm acesso permitido a quais credenciais específicas da NAF (isto é, chaves específicas NAF). Existem, ao menos, duas opções para configurar permissões de acesso para credenciais da GBA (isto é, um conjunto de chaves específicas NAF) no terminal móvel.

[008] Primeiramente, o terminal móvel pode adquirir os dados de configuração com permissões para todas as aplicações NAF a partir de uma fonte externa. Nesse caso, exige-se que os dados de configuração tenham origem em uma fonte confiável e sejam inteiramente protegidos. As permissões para acessar as credenciais da GBA podem ser entregues a ME em conjunto com outros dados de configuração usando-se uma estrutura de gerenciamento de dispositivo (por exemplo, procedimentos de Gerenciamento de Dispositivo OMA), a qual implanta aquelas exigências. A segurança dos dados de configuração pode ser baseada em criptografia 1) simétrica

ou 2) assimétrica. Tal opção também pode ser utilizada sem uma estrutura de gerenciamento de dispositivo externo. Por exemplo, o terminal móvel pode ser configurado antes que seja entregue para o usuário final, por exemplo, na fábrica pelo fabricante, ou em uma loja pelo vendedor do terminal móvel. Após o terminal móvel ter alcançado seu usuário final, permissões podem ser modificadas manualmente: Por exemplo, o terminal móvel questionará seu próprio proprietário para configurar cada nova permissão. Portanto, a configuração manual do terminal móvel pode prejudicar a prática do uso do serviço, de modo que seja melhor configurar as permissões, de modo automático, da forma mais proveitosa possível. Ademais, uma desvantagem potencial dessa opção é que os prestadores de serviço devem confiar na fonte dos dados de configuração, pois a mesma define as permissões para todas as aplicações NAF. Em segundo lugar, os direitos de acesso para cada aplicação podem ser configurados no terminal um a um com base na comunicação com a fonte externa.

[009] Outro método para configurar os direitos de acesso, de modo individual, para cada aplicação é usar a Infra-estrutura de Chave Pública (PKI) e as aplicações assinadas. De modo típico, a assinatura da aplicação assinada pode ser verificada usando-se um certificado digital específico para aplicação. Pode ser que o sistema PKI usado para certificar e verificar as aplicações inclua uma possibilidade de definir o serviço, ou serviços, que essa aplicação tem permissão para acessar (isto é, a quais credenciais específicos NAF a aplicação tem direito a acesso). Tal informação pode ser codificada no próprio certificado de aplicação, ou pode ser uma parte dos metadados da aplicação. De maneira típica, tal informação consistiria nos identificadores que identificam cada credencial específica NAF de modo único.

[010] A segurança da configuração com chaves simétricas GBA é baseada no fato de que a NAF e o terminal móvel compartilham a chave Ks_NAF . Dois métodos principais para implantar essa alternativa são: (1) Se uma aplicação assinada pela Ks_NAF , então, pode-se confiar na mesma para adquirir acesso a instâncias futuras daquelas credenciais de NAF e (2) se uma aplicação pode provar uma vez para o

terminal móvel que reconhece Ks_NAF, então, pode-se confiar na mesma para adquirir acesso a instâncias futuras daquelas credenciais de NAF.

[011] Quando as aplicações do cliente estão instaladas em um terminal móvel, é necessário estabilizar uma confiança entre tal aplicação e um servidor GAA_ME (isto é, a aplicação confiável que desempenha o procedimento de autocarregamento com a BSF) instalado no terminal móvel se tal aplicação quer adquirir as chaves específicas NAF. Portanto, existe uma maneira de assinar a aplicação usando-se um certificado digital específico NAF e usar a assinatura para estabilizar a confiança de aplicação no terminal. Por exemplo, essa maneira está sendo adotada nos terminais Symbrian. Portanto, o servidor GAAJYEE não teria conhecimento de quais, de todas as aplicações instaladas (confiáveis), seriam somente dotadas de chaves específicas NAF.

[012] O problema supramencionado pode ser resolvido através do acréscimo de itens a um certificado que informa que essa aplicação assinada pela aplicação deveria ser dotada de uma capacidade de cliente GAA (isto é, credencias NAF podem ser adquiridas a partir do servidor GAA-ME para uma aplicação de terminal móvel). Tal solução precisa de mecanismos entre o servidor GAA_ME e a plataforma (com segurança de plataforma) para coordenar a confiança. Quando as aplicações do cliente estão localizadas no dispositivo mais próximo, como um laptop (caso de uso de terminal seccionado), o qual quer utilizar o servidor GAA_ME do telefone, tal solução se torna difícil de implantar.

[013] Com base no que foi dito acima, existem diversos problemas nas soluções da técnica anterior que precisam resolvidos. Por exemplo, quais aplicações em um terminal móvel possuem permissão para acesso às credencias NAF e como configurá-las. Ademais, outro problema é como autenticar uma aplicação a um servidor GAA ME em um terminal móvel.

SUMÁRIO DA INVENÇÃO:

[014] De acordo com um aspecto da invenção, é fornecido um método de autenticação de uma aplicação. O método compreende executar, com uma aplicação

de servidor confiável, procedimentos de autocarregamento entre a aplicação de servidor confiável e uma função de servidor de autocarregamento; derivar uma chave compartilhada com base em, ao menos, uma chave ajustada com o servidor de função de servidor de autocarregamento durante os procedimentos de autocarregamento e um identificador de função de aplicação de rede; fornecer uma aplicação com um identificador de transação de autocarregamento, sendo que o identificador de transação de autocarregamento é recebido a partir do servidor de função de servidor de autocarregamento durante os procedimentos de autocarregamento; receber uma resposta proveniente da aplicação; e autenticar a aplicação através da validação da resposta com a chave compartilhada.

[015] De acordo com um aspecto da invenção, é fornecido um método de autenticação de uma aplicação com uma aplicação de servidor confiável. O método compreende receber, com uma aplicação, a partir de uma aplicação de servidor confiável, ao menos um identificador de transação de autocarregamento; abrir um enlace de comunicação com um servidor de função de aplicação de rede; fornecer ao servidor de função de aplicação de rede ao menos o identificador de transação de autocarregamento através do enlace de comunicação; receber, em resposta ao fornecimento do identificador de transação de autocarregamento, ao menos, uma resposta proveniente do servidor de função de aplicação de rede; e autenticar a aplicação através do fornecimento à aplicação de servidor confiável de, ao menos, a resposta recebida a partir do servidor de função de aplicação de rede. De acordo com um aspecto da invenção, é fornecido um método de derivação de uma chave de autenticação. O método compreende abrir um enlace de comunicação com uma aplicação; receber, a partir da aplicação, ao menos, um identificador de transação de autocarregamento através do enlace de comunicação; enviar uma solicitação para um servidor de função de servidor de autocarregamento para receber uma chave compartilhada, sendo que a solicitação compreende, ao menos, um identificador de transação de autocarregamento; receber, a partir do identificador de transação de autocarregamento, a chave compartilhada em resposta à solicitação; derivar uma

resposta usando-se, ao menos, a chave compartilhada; e enviar, ao menos, a resposta para a aplicação.

[016] Cada um dos aspectos supramencionados pode ser implantado como um programa de computador que pode ser incorporado em um meio de comunicação legível por computador. De acordo com um aspecto da invenção, é fornecido um terminal móvel para autenticar uma aplicação. O terminal móvel compreende uma aplicação de servidor confiável configurada para executar procedimentos de autocarregamento entre a aplicação de servidor confiável e uma função de servidor de autocarregamento; derivar uma chave compartilhada com base em, ao menos, um material de chave recebido a partir do servidor de função de servidor de autocarregamento durante os procedimentos de autocarregamento e um identificador de função de aplicação de rede; fornecer uma aplicação com um identificador de transação de autocarregamento, sendo que o identificador de transação de autocarregamento é recebido a partir do servidor de função de servidor de autocarregamento durante os procedimentos de autocarregamento; receber uma resposta proveniente da aplicação; e autenticar a aplicação através da validação da resposta com a chave compartilhada.

[017] A presente invenção possui diversas vantagens sobre as soluções da técnica anterior. Nenhuma aplicação de vírus ou, até mesmo, quaisquer aplicações de terceiros podem solicitar credenciais GAA a partir do servidor GAA_ME instalado no equipamento móvel, a menos que esses possam autenticar algumas NAF e derivar um segredo compartilhado (isto é, KS_NAF_install) a ser usado para registro no servidor GAA_ME.

[018] Ademais, a invenção fornece uma solução para derivar um segredo compartilhado entre o servidor GAA_ME e uma aplicação em um terminal próximo.

[019] A solução revelada na invenção pode ser usada para autenticar a aplicação próxima dirigida ao servidor GAA_ME. Portanto, isso pode exigir que também exista algum tipo de computação confiável (segurança de plataforma) nos dispositivos próximos.

[020] Ademais, a invenção fornece para os operadores uma opção atrativa de distribuir suas aplicações. Os operadores que já possuem autenticação com base em nome de usuário-senha (ou algum outro mecanismo de autenticação), a solução revelada na invenção facilita o desenvolvimento até o uso de credencial com base em GAA.

[021] Ademais, a invenção pode ser usada, ainda, para que os dois dispositivos gerem uma chave compartilhada por grupo que, então, é usada para uma comunicação em grupo e pode ser distribuída, de modo adicional, para outros usuários, por exemplo, para ser usada com o objetivo de ajustar túneis seguros entre eles e trocar certificados, ajustar Redes Virtuais Particulares (VPN) entre eles ou somente ajustar a Segurança da Camada de Transporte (TLS) entre eles.

[022] Em geral, a solução revelada na invenção pode ser usada para a instalação de aplicação específica de operador e para o estabelecimento de confiança entre um componente existente e um componente recentemente instalado.

Breve Descrição dos Desenhos:

[023] Os desenhos em anexo, os quais são incluídos para fornecer uma compreensão adicional da invenção e constituir uma parte dessa especificação, ilustram modalidades da invenção e, em conjunto com a descrição, auxiliam a explicar os princípios da invenção. Nos desenhos:

A Figura 1 é um diagrama em bloco que ilustra uma arquitetura da técnica anterior de Arquitetura Genérica de Autocarregamento (GBA).

A Figura 2 é um diagrama de sinalização que ilustra um procedimento de autocarregamento da técnica anterior,

A Figura 3 é um diagrama em bloco que ilustra diversos elementos de acordo com uma modalidade da invenção, e

A Figura 4 é um diagrama de sinalização que ilustra uma modalidade para autenticar uma aplicação dirigida para uma aplicação de servidor em equipamento móvel de acordo com uma modalidade da presente invenção. A Figura 5 é um diagrama de sinalização que ilustra outra modalidade para autenticar uma aplicação

dirigida para uma aplicação de servidor em equipamento móvel de acordo com uma modalidade da presente invenção.

Descrição Detalhada das Modalidades Preferidas:

[024] Agora será feita referência detalhada às modalidades da presente invenção, exemplos das mesmas são ilustrados nos desenhos em anexo.

[025] A Figura 3 revela um diagrama em bloco que ilustra diversos elementos que fazem parte da solução revelada na presente invenção. A Figura 3 revela cinco entidades diferentes: Equipamento Móvel (ME) 300, uma Função de Servidor de Autocarregamento (BSF), uma Função de Aplicação de Rede (NAF) 306, um Sistema Doméstico de Assinante (HSS) 304 e um computador 308. O diagrama em bloco da Figura 3 também leva em consideração uma situação de terminal seccionado. Em uma situação de terminal seccionado, uma aplicação local 320 reside, por exemplo, em um computador 308. A aplicação local é conectada a um servidor GAA_ME do equipamento móvel 314 através de um módulo GAA 318 e de um módulo próximo 312. A conexão atual entre o equipamento móvel 314 e o computador 308 é realizada, por exemplo, através de um enlace próximo, por exemplo, Bluetooth. O APP_ME 310 é uma aplicação (de cliente) que é instalada no equipamento móvel 300. Em outras palavras, a aplicação pode ser instalada no próprio equipamento móvel ou em um computador 308 que possui uma conexão local com o equipamento móvel 300.

[026] A arquitetura GAA fornece uma maneira de gerar um segredo compartilhado entre o equipamento móvel 300 e a NAF 306. O segredo é utilizado quando o equipamento móvel 300 quer ser autenticado pela NAF 306. A aplicação no equipamento móvel 300 precisa de credenciais USIM (ou ISIM ou SIM) para executar o autocarregamento da GAA para gerar chaves NAF específicas. A capacidade de adquirir credenciais USIM a partir de USIM não deve estar disponível, de preferência, para todas as aplicações no equipamento móvel 300 devido a uma ameaça à segurança. Portanto, um servidor GAA ME confiável 314 posteriormente, sendo que o servidor possui a capacidade de adquirir as credenciais USIM a partir de USIM e, sendo assim, possui a capacidade de realizar o autocarregamento para gerar

credenciais NAF. Portanto, uma aplicação de um cliente (APP_ME) usaria os serviços do servidor GAA_ME 314 para adquirir as credenciais NAF específicas. Tal aplicação de cliente GAA_ME é preparada e empacotada pelo fornecedor NAF. Essa aplicação é assinada usando-se uma assinatura digital que a plataforma (symbian, xp, Linux, Java e etc.) compreende. Após a instalação, tal aplicação é registrada pelo servidor GAA_ME 314 durante sua primeira execução.

[027] O equipamento móvel 300 e a função de aplicação de rede 306 podem incluir uma memória ou memórias (não reveladas na Figura 3) que também podem incluir um programa de computador (ou parte do mesmo), o qual, quando executado em uma unidade de processamento de dados, desempenha, ao menos, algumas das etapas da invenção. A unidade de processamento de dados também pode incluir uma memória ou uma memória pode ser associada àquela, a qual pode incluir o programa de computador (ou parte do mesmo) que, quando executado na unidade de processamento de dados, desempenha, ao menos, algumas das etapas da invenção.

[028] A Figura 4 é um diagrama de sinalização que ilustra uma modalidade para registrar e autenticar uma aplicação por uma aplicação de servidor em equipamento móvel de acordo com uma modalidade da presente invenção. A Figura 4 revela três entidades diferentes: uma Função de Servidor de Autocarregamento (BSF), um servidor de Função de Aplicação de Rede (NAF) 404 e um Equipamento Móvel (ME) 400. Um equipamento móvel 404 inclui uma aplicação de cliente APPME 406 e uma aplicação de servidor GAA_ME 408 já reveladas na Figura 3. Em outra modalidade, uma aplicação de cliente APP_ME pode residir no exterior do equipamento móvel 404, ou seja, por exemplo, em um dispositivo externo conectado ao equipamento móvel 404. Na modalidade da Figura 4, a APP_ME 406 envia uma solicitação de registro (410) para o servidor GAA_ME 408. A solicitação indica para o servidor GAA_ME 408 que a APPME quer se auto-autenticar para o servidor GAA_ME 408. A solicitação pode conter, ainda, um identificador NAF e/ou um identificador de instância de aplicação. O fornecedor de aplicação pode ter estabelecido o código rígido da

aplicação ou, de alguma forma, ter configurado o funcionamento do identificador NAF e da instância de aplicação.

[029] O servidor 408 executa (412) um protocolo de autocarregamento com a BSF 400. O protocolo de autocarregamento é revelado em maiores detalhes, por exemplo, na especificação técnica 3GPP de referência 3GPP TS 33.220 V7.2.0 (2005-12). Durante o autocarregamento, o servidor GAA_ME 408 recebe, ao menos, um BTID (Identificador de Transação de Autocarregamento) e a vida útil de uma chave proveniente da BSF 400 e passa (414), ao menos, o BTID de volta para o APP_ME 406. Já que o servidor GAA_ME 408 é capaz de derivar materiais Ks e reconhecer o identificador NAF, o mesmo deriva, ainda, a chave Ks_NAF, a qual é um segredo compartilhado entre o servidor GAA_ME 408 e a NAF 402. O servidor GAA_ME 408 derivará, em seguida, (422) uma chave de instalação KS _ NAF_ install usando-se KS _ NAF e, de modo opcional, o identificador de instância de aplicação mencionado anteriormente que usa qualquer método apropriado.

[030] Após receber a BTID a partir do servidor GAA_ME 408, o APP_ME 406 abre um enlace de comunicação com a NAF 402. Pode-se manter o enlace de comunicação seguro para que a ação humana seja suavizada usando-se, por exemplo, a Camada de Soquetes Segura (SSL) ou qualquer outro método adequado.

[031] Após isso, o APP_ME 406 se auto-autentica (416) para a NAF 402 usando-se um procedimento de autenticação adequado. Existem diversos métodos de autenticação aplicáveis na técnica anterior que podem ser utilizados. O procedimento de autenticação pode incluir os listados a seguir:

[032] Senha única com código rígido estabelecido para a aplicação. Nesse caso, é preferível que o código da aplicação seja ofuscado de modo que se torne muito difícil restaurar a senha simplesmente através do exame do código.

[033] O nome de usuário e a senha adquiridos fora da banda (como lançar ou visitar uma loja). - Registro para a NAF online para adquirir as credenciais.

[034] Ademais, o método de autenticação e a segurança do canal podem ser específicos da NAF. A chave compartilhada TLS pode, ainda, ser usada no caso de

segredos compartilhados. Ademais, os métodos de autenticação HTTP-DIGEST são bastante utilizados para autenticação.

[035] Uma vez que o APP_ME 406 foi autenticado para a NAF 402, a NAF 402 irá buscar (418) a chave específica KS_NAF da NAF a partir da BSF 400 usando-se a BTID e irá derivar (420) KS_NAF_install (similar à etapa 422). Em seguida, a mesma transferirá (424) o KS_NAF_install para o APP_ME 406. Tal transferência deve ser, de preferência, confidencial.

[036] Agora, o APP_ME 406 pode se auto-autenticar (426) para o GAA_ME_Server 408 usando-se KS_NAF_install como um segredo compartilhado. Se a autenticação é bem sucedida, o servidor GAA_ME 408 pode adicionar (428) a aplicação na sua lista de aplicações confiáveis dependendo de sua configuração local. Portanto, a etapa 428 pode ser, ainda, uma etapa opcional. Se a aplicação está em uma lista de aplicações confiáveis, quando, no futuro, o APP_ME 406 solicita chaves NAF, o servidor GAA_ME 408 autocarrega e fornece as chaves NAF sem qualquer autorização adicional proveniente da NAF 402.

[037] Na modalidade revelada na Figura 4, as duas caixas de derivação de chave de instalação (420, 422) são posicionadas no mesmo nível. Portanto, cada uma pode ser movida de modo ascendente ou descendente dependendo da solicitação. A derivação da chave de instalação pode ser realizada usando-se, por exemplo, transformação de chaves, usando-se KS_(ext)_NAF e o identificador de instância de aplicação ou usando-se somente a própria KS_(ext)_NAF como KS NAF install.

[038] O segredo compartilhado utilizado para autenticar, de modo inicial, o APP_ME 406 e a NAF 402 também pode ser uma senha única. A senha pode ser deletada na NAF 402 uma vez que o terminal estabelece uma confiança com o servidor GAA_ME do cliente 408. O segredo compartilhado também pode ser derivado com base em algumas características do terminal móvel. Ademais, o protocolo de autenticação entre o APP_ME 406 e a própria NAF 402 pode ser quaisquer dos protocolos de autenticação bem conhecidos. Uma vez que a autenticação foi executada, o método para garantir a segurança da comunicação entre o AP_ME 406

e a NAF 402 pode ser um dos métodos bem conhecidos. Caso um segredo compartilhado (por exemplo, nome de usuário e senha) seja usado, o protocolo TLS de chave compartilhada é uma alternativa.

[039] Em uma modalidade da invenção, quando o servidor GAA_ME 408 autenticou, de modo bem sucedido, o APP_ME 406 usando uma determinada identidade de NAF, o servidor GAA_ME 408 pode conceder o acesso APP_ME somente para as instâncias futuras de chave Ks_NAF que pertencem a mesma identidade de NAF e outras chaves NAF específicas não seriam acessíveis. Em outra modalidade da invenção, um acesso irrestrito é concedido para o APP_ME 406, isto é, o mesmo pode adquirir chaves KS_NAF de qualquer NAF.

[040] Ademais, em uma modalidade da invenção, durante o procedimento, múltiplas chaves Ks_NAF podem ser usadas para conceder acesso a diversas chaves, isto é, a NAF 402 busca chaves múltiplas Ks_NAF a partir da BSF 400 (sob autorização) e a NAF 402 deriva múltiplas chaves Ks_NAF_install e as envia para o APP_ME 406. O APP_ME 406 pode, em seguida, registrá-las com o servidor GAA_ME 408. Desta maneira, o APP_ME 406 obteria o acesso a mais de uma chave NAF específica. A Figura 5 é um diagrama de sinalização que ilustra uma modalidade para registrar e autorizar uma aplicação para uma aplicação de servidor em equipamento móvel de acordo com uma modalidade da presente invenção. A Figura 5 revela três entidades diferentes: uma Função de Servidor de Autocarregamento (BSF) 500, um servidor de Função de Aplicação de Rede (NAF) 502 e um Equipamento Móvel (ME) 504. Um equipamento móvel 504 inclui uma aplicação de cliente APP_ME 506 e uma aplicação de servidor GAA_ME 508 já reveladas na Figura 3. Em outra modalidade, uma aplicação de cliente APP_ME pode residir no exterior do equipamento móvel 504, ou seja, por exemplo, em um dispositivo externo conectado ao equipamento móvel 504.

[041] Na modalidade da Figura 5, a APP_ME 506 envia uma solicitação de registro (510) para o servidor GAA_ME 508. A solicitação indica para o servidor GAA_ME 508 que a APP_ME quer se auto-autorizar para o servidor GAA_ME 508.

A solicitação pode conter, ainda, um identificador NAF e/ou um identificador de instância de aplicação. O fornecedor de aplicação pode ter estabelecido o código rígido da aplicação ou, de alguma forma, ter configurado o funcionamento do identificador NAF e da instância de aplicação.

[042] O servidor GAA_ME 508 executa (512) um protocolo de autocarregamento com a BSF 500. O protocolo de autocarregamento é revelado em maiores detalhes, por exemplo, na especificação técnica 3GPP de referência 3GPP TS 33.220 V7.2.0 (2005-12). Durante o autocarregamento, o servidor GAA_ME 508 recebe, ao menos, um BTID (Identificador de Transação de Autocarregamento) e a vida útil de uma chave proveniente da BSF 500. Já que o servidor GAA_ME 508 é capaz de derivar a chave Ks e reconhecer o identificador NAF, o mesmo deriva, ainda, a chave Ks_NAF (514), a qual é um segredo compartilhado entre o servidor GAA_ME 508 e a NAF 502. O servidor GAA_ME 508 também irá gerar (514) um desafio remoto para o APP_ME (506). Após isso, o servidor GAA_ME 15 508 passa (514), ao menos, o BTID e o desafio para o APP_ME 506.

[043] Após receber a BTID e o desafio a partir do servidor GAA_ME 508, o APP_ME 506 abre um enlace de comunicação com a NAF 502 e passa (518) o BTID e o desafio para a NAF 502. Pode-se manter o enlace de comunicação seguro para que uma possível ação humana seja suavizada.

[044] A NAF 502 busca (520) a chave NAF específica KS_NAF a partir da BSF 400 usando-se o BTID e deriva (522) uma resposta para o desafio através do uso de Ks_NAF. A resposta pode ser calculada, por exemplo, através do uso de uma função de sinal numérico unidirecional ou um código de autenticação de mensagem de sinal numérico dotado de chaves (HMAC) em que os parâmetros de entrada incluem, ao menos, a Ks_NAF e o desafio. A NAF 502 pode, ainda, assinar dados com a Ks_NAF. Os dados podem incluir um ou mais sinais numéricos de aplicações que a NAF 502 autoriza para ter acesso às chaves NAF específicas (Ks_NAFs). Um desses sinais numéricos pode ser o sinal numérico da aplicação APP_ME (506) que foi instalado no ME (504) anteriormente. Deve-se compreender que o sinal numérico da aplicação é

meramente uma possibilidade. Quaisquer outras informações, ou seja, uma caracterização da aplicação, podem ser usadas no lugar de um sinal numérico. Por exemplo, se a aplicação reside em outro dispositivo que é conectado ao terminal do usuário através de uma rede local, como WLAN ou Bluetooth, então, a caracterização da aplicação pode ser o endereço da rede do dispositivo. Ademais, uma caracterização possível de uma aplicação em um dispositivo externo pode ser o número de série daquele dispositivo. Ademais, uma caracterização possível poderia ser uma chave pública de assinatura de conteúdo. Ademais, em uma modalidade da invenção, a solicitação (518) da NAF 502 pode incluir alguma caracterização da plataforma (por exemplo, "dispositivo Nokia que executa a Série 60 v3.1"), a qual, em seguida, ajuda a NAF 502 a enviar a correta caracterização aceitável da aplicação de volta. Em seguida, a NAF 502 (524) transfere a resposta e os dados possivelmente assinados para o APP_ME 506.

[045] Os dados assinados referem-se, por exemplo, a alguns dados extras que a NAF 502 adiciona à mensagem que é assinada usando-se a Ks_NAF. Desta forma, o servidor GAA_ME pode verificar a assinatura desses dados extra e certificar-se de que é proveniente de uma fonte confiável, a qual reconhece a Ks_NAF. Agora, o APP_ME 506 pode se auto-autorizar (526) para o GAA_ME_Server 508 através do uso da resposta e dos dados assinados. Se a autorização for bem sucedida, isto é, a resposta e a assinatura dos dados assinados estão corretos, o servidor GAA_ME 508 continua com o procedimento de autorização e concede a Ks_NAF ao APP_ME 506. De modo adicional, o servidor GAA_ME 508 também pode calcular o sinal numérico do APP_ME 506 e verificar se esse sinal numérico está nos dados assinados. Se ao menos uma das verificações for bem sucedida, o servidor GAA_ME 508 pode adicionar (528) a aplicação na sua lista de aplicações confiáveis dependendo de sua configuração local. Se a aplicação está em uma lista de aplicações confiáveis, quando, no futuro, o APP_ME 506 solicita chaves NAF, o servidor GAA_ME 508 autocarrega e fornece as chaves NAF sem qualquer autorização adicional proveniente da NAF.

[046] A adição possível da aplicação na sua lista de confiáveis torna possível ter "concessões únicas" e "concessões integrais". No primeiro caso, o APP_ME teria sempre que adquirir a autorização extra (dados assinados ou de resposta ou ambos) para cada solicitação por Ks_NAF ou, no segundo caso, o APP_ME adquiriria uma concessão permanente e não teria que adquirir uma autorização extra nas solicitações futuras por Ks_NAF. Enfim, se as verificações feitas acima foram bem sucedidas, o servidor GAA_ME 508 (530) indica para o APP_ME que o procedimento foi bem sucedido e inclui, possivelmente, a Ks_NAF a essa mensagem.

[047] Em uma modalidade da invenção, quando o servidor GAA_ME 508 autenticou, de modo bem sucedido, o APP_ME 506, o servidor GAA_ME 408 pode conceder o acesso APP_ME somente para as chaves NAF específicas Ks_NAF que foram usadas durante o procedimento e outras chaves NAF específicas não seriam acessíveis. De modo especial, esse pode ser o caso se os dados assinados não foram enviados a partir da NAF 502 para o servidor GAA_ME 508 através do APP_ME 506. Em outra modalidade da invenção, um acesso irrestrito é concedido para o APP_ME 506, isto é, o mesmo pode adquirir todas as chaves KS NAF possíveis.

[048] Em outra modalidade da invenção, a KS_(ext)_NAF é usada como uma chave de grupo para garantir a segurança de uma comunicação em grupo e pode ser compartilhada com outros dispositivo que podem não ter qualquer forma de geração de chave GBA ou nenhuma capacidade de solicitação. Essa modalidade pode ser usada para garantir a segurança de um enlace de comunicação, por exemplo, em um ambiente domestico com muitos dispositivos de baixa capacidade, ou pode ser usada para ajustar uma VPN pessoal (rede particular virtual).

[049] Ademais, em uma modalidade da invenção, a NAF_ID pode ser enviada a partir do APP_ME 506 para o servidor GAA_ME 508 na etapa 510, conforme descrito acima, ou na etapa 526.

[050] Ademais, em uma modalidade da invenção, durante o procedimento, múltiplas chaves Ks_NAF podem ser usadas para conceder acesso a diversas chaves, isto é, a NAF 502 busca chaves múltiplas Ks_NAF a partir da BSF 500 (sob

autorização) e a NAF 502 calcula múltiplas respostas para o desafio usando essas chaves Ks_NAF e também assina, de modo opcional, os dados usando todas ou um subconjunto das chaves e as envia para o APP_ME 506. O APP_ME 506 pode, em seguida, registrá-las com o servidor GAA-ME 508. Desta maneira, o APP_ME 506 obteria o acesso a mais de uma chave NAF específica.

[051] Ademais, esse método pode ser aplicado em muitos outros casos em que o equipamento de terminal é configurado para confiar em um prestador de serviço (por exemplo, um fabricante de equipamento ou através de um operador de rede) e, então, o equipamento e o prestador de serviço possuem, ou concordam, em uma chave compartilhada. Descrevemos em detalhes que, se uma nova aplicação pode provar para o terminal que possui a confiança de um determinado prestador de serviço, então, a mesma pode ser marcada como "confiável" e pode ser instalada no terminal do usuário. Tal evidência é baseada no conhecimento da chave compartilhada entre o terminal e o prestador de serviço. Por exemplo, ao invés da aplicação ser instalada no terminal, poderia haver um dispositivo periférico ou outro terminal em uma rede próxima (por exemplo, rede Bluetooth ou WLAN) que iria querer conectar-se ao terminal do usuário. O procedimento de estabelecimento de confiança é o mesmo também nesses casos.

[052] 3GPP GBA é uma das maneiras de derivar a chave compartilhada e estabelecer a confiança entre o terminal e o prestador de serviço. Outras maneiras também podem ser consideradas. Por exemplo, com uma infra-estrutura de chave pública (PKI) em funcionamento, ambas as partes trocariam certificados de suas chaves públicas, verificariam mutuamente suas assinaturas e procederiam para derivar uma chave compartilhada. Como outro exemplo, uma chave compartilhada a longo prazo pode ser pré-instalada no terminal pelo operador da rede ou pelo fabricante do terminal.

[053] Fica evidente para uma pessoa versada na técnica que, com o avanço da tecnologia, a ideia básica da invenção pode ser implantada de diversos modos. A

invenção e suas modalidades não são, portanto, limitadas aos exemplos descritos acima, ao invés disso, essas podem variar dentro do escopo das reivindicações.

REIVINDICAÇÕES

1. Método para autenticar uma aplicação (310, 320) com uma aplicação de servidor confiável (314) em um terminal móvel (300), a aplicação de servidor confiável (314) sendo externa a um cartão de circuito integrado universal, sendo que o método é **CARACTERIZADO** pelo fato de que compreende:

executar, com uma aplicação de servidor confiável (314), procedimentos de autocarregamento entre a aplicação de servidor confiável (314) e uma função de servidor de autocarregamento (302);

derivar, pela aplicação de servidor confiável (314), uma chave compartilhada com base em, ao menos, uma chave recebida a partir do servidor de função de servidor de autocarregamento (302) durante os procedimentos de autocarregamento e um identificador de função de aplicação de rede;

fornecer, pela aplicação de servidor confiável (314), para a aplicação (310, 320) um identificador de transação de autocarregamento, sendo que o identificador de transação de autocarregamento é recebido a partir do servidor de função de servidor de autocarregamento (302) durante os procedimentos de autocarregamento;

receber, pela aplicação de servidor confiável (314), uma resposta proveniente da aplicação (310, 320);

autenticar, pela aplicação de servidor confiável (314), a aplicação (310, 320) através da validação da resposta com a chave compartilhada; e

marcar, pela aplicação de servidor confiável (314), a aplicação (310, 320) como confiável se a autenticação for bem sucedida.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a autenticação da aplicação (310, 320) compreende:

autenticar a aplicação (310, 320) através da comparação da chave compartilhada com a resposta.

3. Método, de acordo com a reivindicação 1, que compreende adicionalmente: gerar um desafio; fornecer para a aplicação (310, 320) um desafio; e **CARACTERIZADO** pelo fato de que a etapa de autenticação compreende autenticar

a aplicação (310, 320) através da validação da resposta com o desafio e a chave compartilhada.

4. Método, de acordo com a reivindicação 3, que compreende adicionalmente: Receber dados assinados com a resposta; e **CARACTERIZADO** pelo fato de que a etapa de autenticação compreende, de modo adicional, verificar os dados assinados com a chave compartilhada.

5. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que compreende adicionalmente: receber uma solicitação de registro a partir da aplicação (310, 320), sendo que a solicitação compreende, ao menos, um identificador de função de aplicação de rede e um identificador de instância de aplicação antes de fornecer para a aplicação (310, 320) um identificador de transação de autocarregamento.

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que compreende adicionalmente: receber uma solicitação de registro a partir da aplicação (310, 320), antes de fornecer para a aplicação (310, 320) um identificador de transação de autocarregamento.

7. Método, de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que a solicitação de registro compreende um identificador de instância de aplicação.

8. Método, de acordo com qualquer uma das reivindicações 5 a 7, **CARACTERIZADO** pelo fato de que a derivação da chave compartilhada compreende: Derivar a chave compartilhada com base na chave recebida a partir do servidor de função servidor de autocarregamento (302) durante os procedimentos de autocarregamento, o identificador de função de aplicação de rede e o identificador de instância de aplicação.

9. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que compreende adicionalmente: fornecer para a aplicação (310, 320) uma chave compartilhada.

10. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que compreende adicionalmente: receber a partir da aplicação (310, 320) uma solicitação de uma chave de função de aplicação de rede; e

enviar para a aplicação a chave de função de aplicação de rede em resposta à solicitação.

11. Terminal móvel (300) para autenticação de uma aplicação (310, 320), **CARACTERIZADO** pelo fato de que compreende uma aplicação de servidor confiável (314) no terminal móvel (300), a aplicação de servidor confiável (314) sendo configurada para executar procedimentos de autocarregamento entre a aplicação de servidor confiável (314) e uma função de servidor de autocarregamento (302); derivar uma chave compartilhada com base em, ao menos, uma chave recebida a partir do servidor de função de servidor de autocarregamento (302) durante os procedimentos de autocarregamento e um identificador de função de aplicação de rede; fornecer para a aplicação (310, 320) um identificador de transação de autocarregamento, sendo que o identificador de transação de autocarregamento é recebido a partir do servidor de função de servidor de autocarregamento (302) durante os procedimentos de autocarregamento; receber uma resposta proveniente da aplicação (310, 320); autenticar a aplicação (310, 320) através da validação da resposta com a chave compartilhada; e marcar a aplicação com o confiável se a autenticação (310, 320) for bem sucedida.

12. Terminal móvel (300), de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que a aplicação de servidor (314) é configurada para autenticar a aplicação (310, 320) através da comparação da chave compartilhada com a resposta.

13. Terminal móvel (300), de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que a aplicação do servidor confiável (314) é configurada para gerar um desafio; fornecer para a aplicação (310, 320) o desafio; e validar a resposta com o desafio e a chave compartilhada.

14. Terminal móvel (300), de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que a aplicação de servidor confiável (314) é configurada para receber dados assinados com a resposta; e a etapa de autenticação compreende, de modo adicional, verificar os dados assinados com a chave compartilhada.

15. Terminal móvel (300), de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que a aplicação de servidor confiável (314) é configurada para receber uma solicitação de registro a partir da aplicação (310, 320), sendo que a solicitação compreende, ao menos, um identificador de função de aplicação de rede e um identificador de instância de aplicação antes de fornecer para a aplicação (310, 320) um identificador de transação de autocarregamento.

16. Terminal móvel (300), de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que a aplicação de servidor confiável (314) é configurada para receber uma solicitação de registro a partir da aplicação (310, 320) antes de fornecer para a aplicação um identificador de transação de autocarregamento.

17. Terminal móvel (300), de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que a solicitação de registro compreende um identificador de instância de aplicação.

18. Terminal móvel (300), de acordo com qualquer uma das reivindicações 15 ou 17, **CARACTERIZADO** pelo fato de que a aplicação de servidor confiável (314) é configurada para derivar a chave compartilhada com base na chave recebida a partir do servidor de função servidor de autocarregamento (302) durante os procedimentos de autocarregamento, no identificador de função de aplicação de rede e no identificador de instância de aplicação.

19. Terminal móvel (300), de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que a aplicação de servidor confiável é configurada para fornecer para a aplicação (310, 320) a chave compartilhada.

20. Terminal móvel (300), de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que a aplicação de servidor confiável (314) é configurada para receber a partir da aplicação (310, 320) uma solicitação de uma chave de função de aplicação de rede; e enviar para a aplicação (310, 320) a chave de função de aplicação de rede em resposta à solicitação.

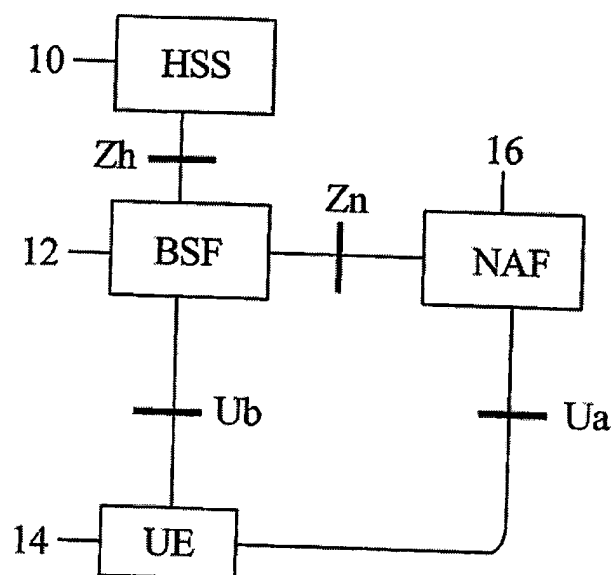


Fig. 1 (TÉCNICA ANTERIOR)

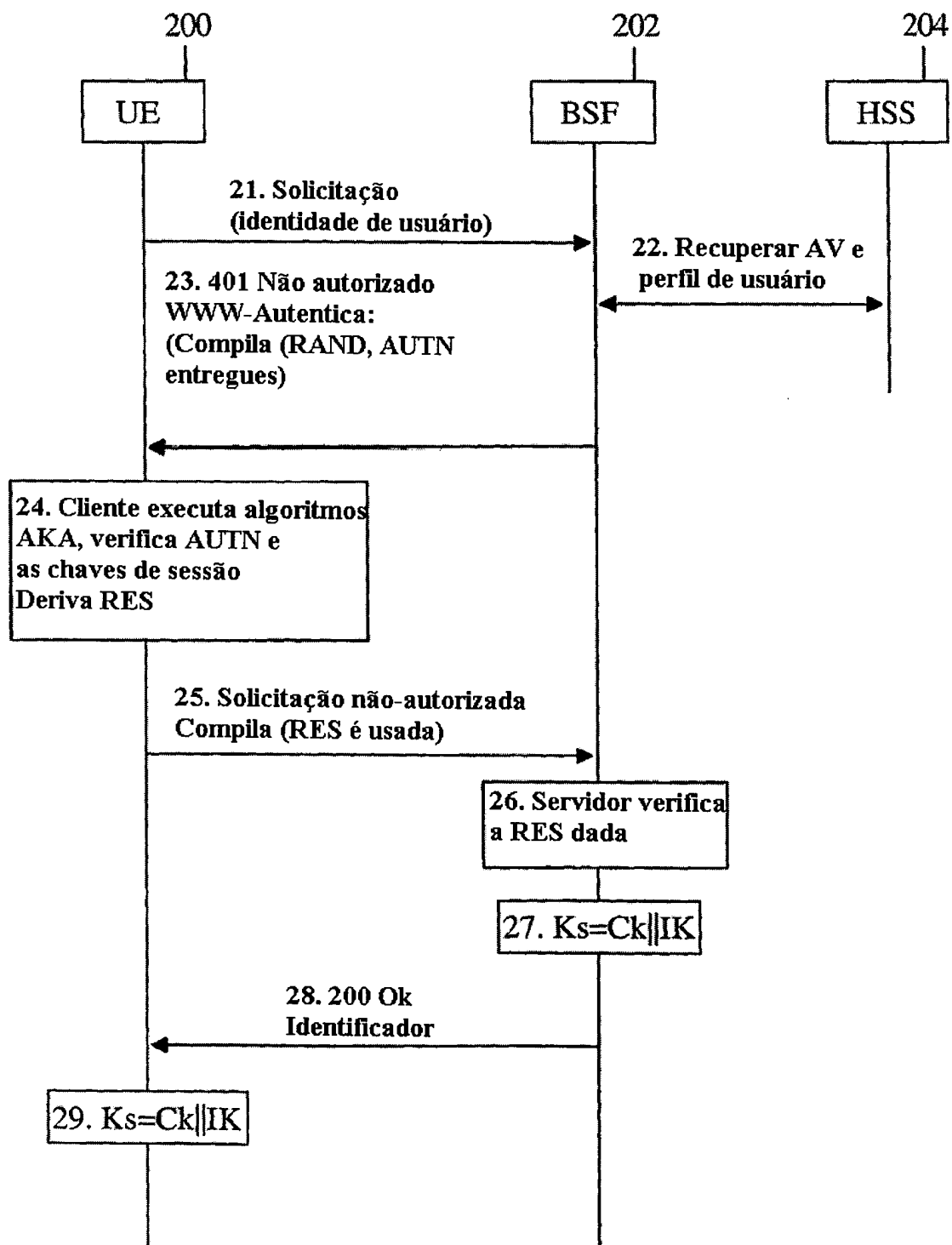


Fig. 2 (TÉCNICA ANTERIOR)

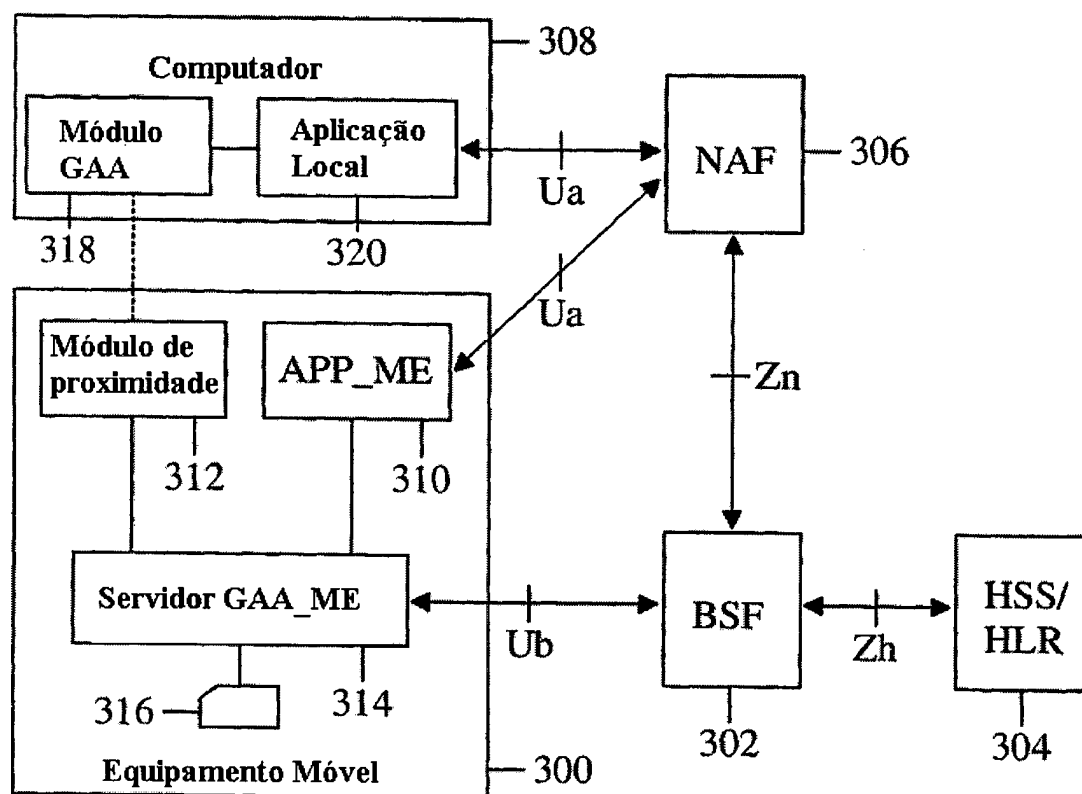


Fig. 3

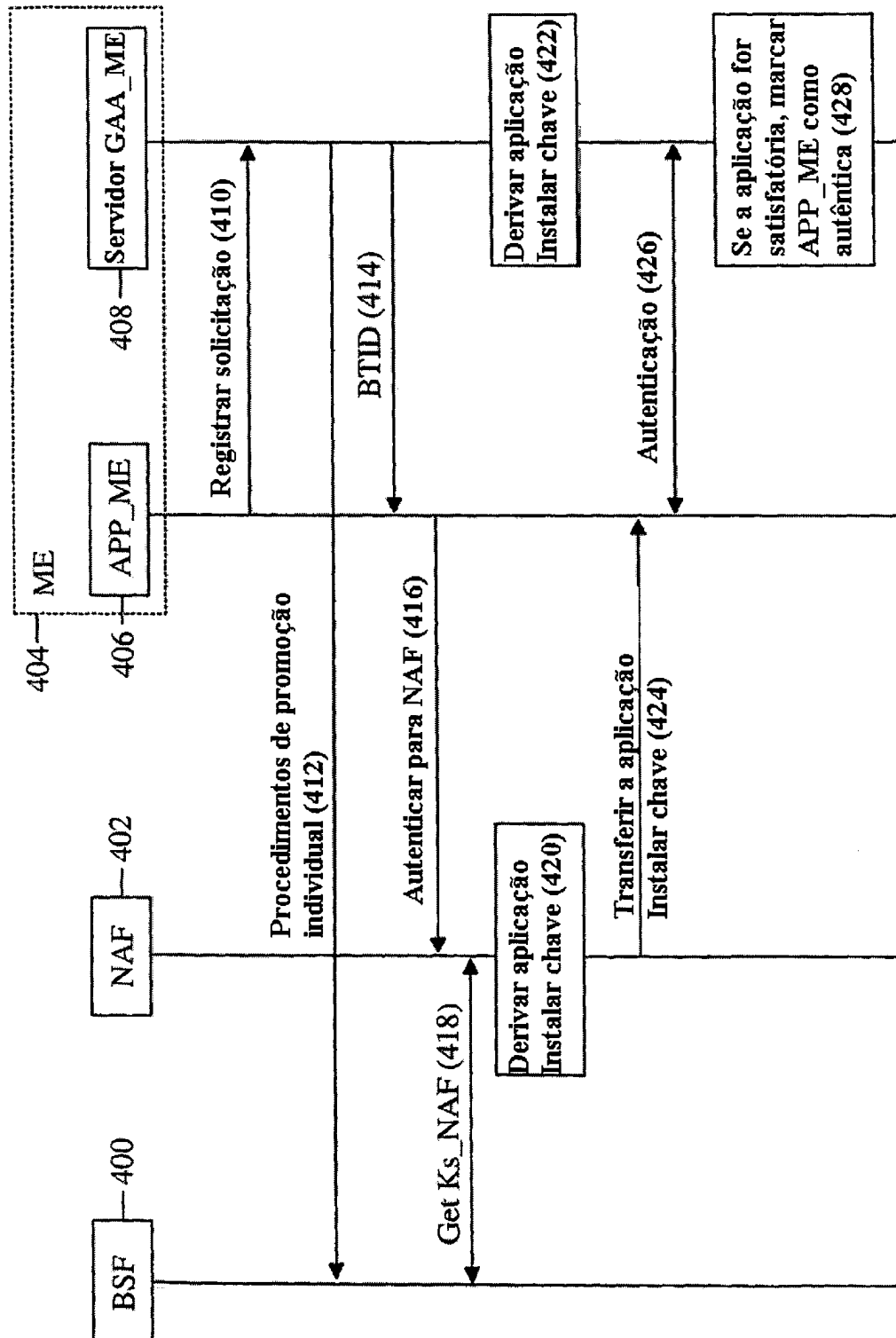


Fig. 4

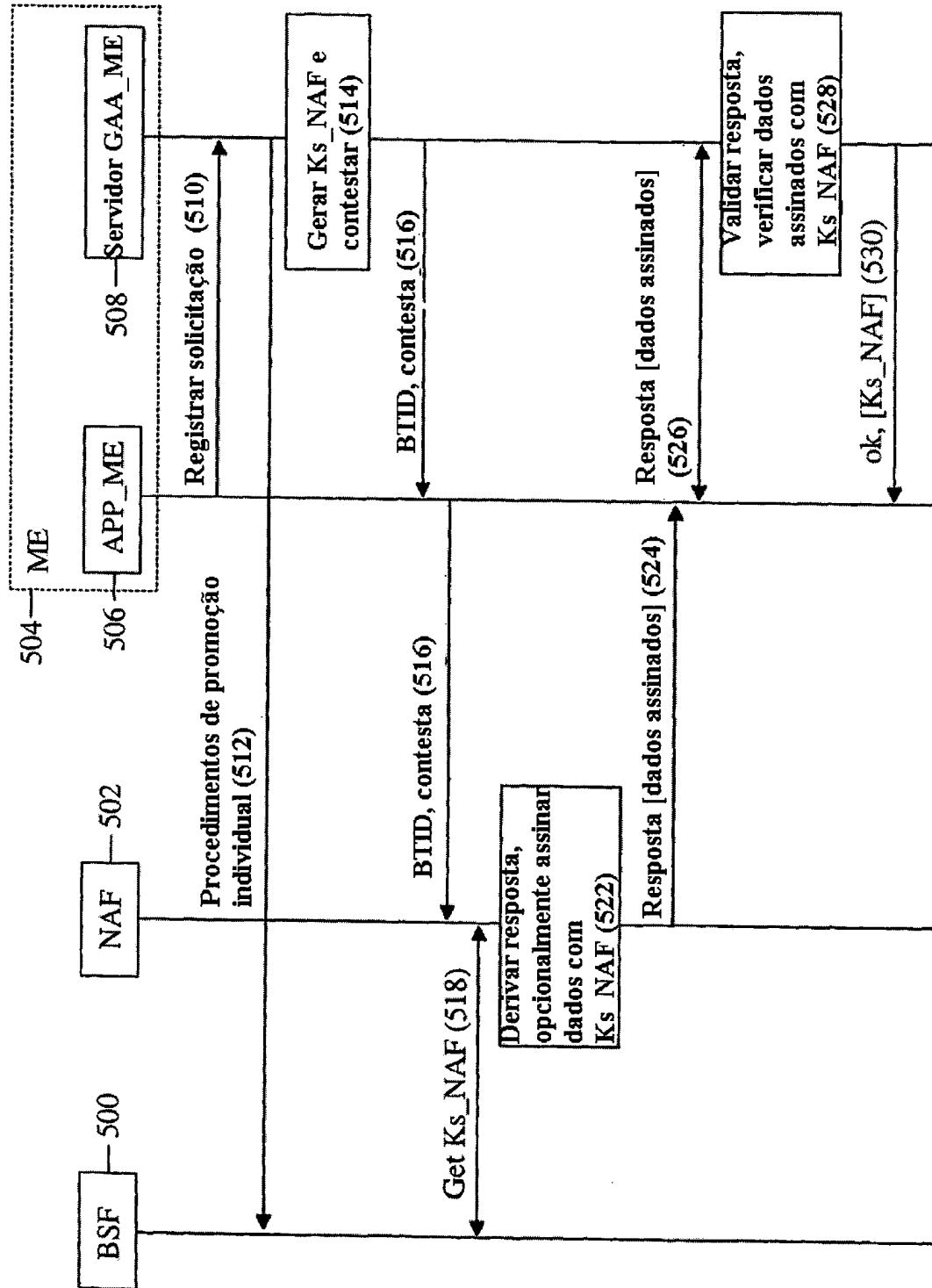


Fig. 5