

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

(21) **PI0610400-2 A2**



(22) Data de Depósito: 04/04/2006
(43) Data da Publicação: 22/06/2010
(RPI 2059)

(51) *Int.Cl.:*
H04L 29/06
G06F 21/00

(54) Título: **MÉTODO, APARELHO E PROGRAMA DE COMPUTADOR PARA PROVER UM MECANISMO GENÉRICO PARA O SERVIDOR DE APLICAÇÃO DE REDE**

(30) Prioridade Unionista: 20/07/2005 US 11/184,931,
11/04/2005 US 60/669,873, 11/04/2005 US 60/669,873

(73) Titular(es): NOKIA CORPORATION

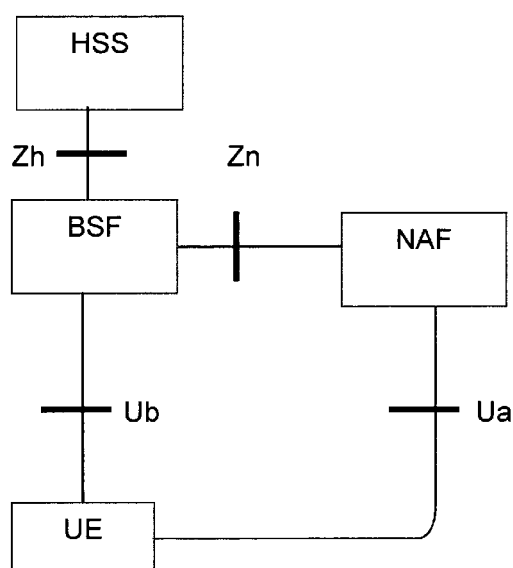
(72) Inventor(es): PEKKA LAITINEN, SILKE HOLTMANN

(74) Procurador(es): Araripe & Associados

(86) Pedido Internacional: PCT IB2006000790 de 04/04/2006

(87) Publicação Internacional: WO 2006/109122 de 19/10/2006

(57) Resumo: Método e aparelho para prover um mecanismo genérico para o servidor de aplicação de rede. O receptor recebe um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede. A unidade de determinação determina a chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário. A unidade de provimento provê a informação de autenticação para a função de aplicação de rede.



“MÉTODO, APARELHO E PROGRAMA DE COMPUTADOR PARA PROVER UM MECANISMO GENÉRICO PARA O SERVIDOR DE APLICAÇÃO DE REDE”.

Referência

5 Este pedido reivindica prioridade do Pedido de Patente Provisório US 60/669,873, depositado em 11 de abril de 2005. O assunto deste pedido depositado anteriormente é aqui incorporado por referência.

Campo da Invenção

10 Esta invenção é relacionada a um mecanismo genérico para um servidor de aplicação para determinar qual chave da Arquitetura de Autenticação Genérica (GAA) permitiria uma integração fácil dos servidores de aplicação adicionais ao estender um padrão existente para as Configurações de Segurança do Usuário (USS).

Descrição da Técnica Anterior

15 A autenticação inicial (i.e., bootstrapping) da Arquitetura de Autenticação Genérica (GAA) do Projeto de Parceiros da Terceira Geração (3GPP) é baseado no AKA (Protocolo de Acordo de Chave e Autenticação). Dependendo do terminal móvel, tal como um telefone móvel, e o Cartão de Circuito Integrado (UICC) do Sistema de Telecomunicações Móvel Universal
20 (UMTS) ou módulo de identidade do assinante inserido no terminal móvel, a Arquitetura de Autenticação Genérica (GAA) 3GPP pode ter as chaves a seguir: Ks_int_NAF, Ks_ext_NAF, e Ks_NAF. Hoje, o número de serviços que usam GAA é bem pequeno e uma definição sobre qual chave usar para um cartão inteligente particular ou módulo de identidade do assinante pode ser implementado
25 diretamente em um servidor de Função de Aplicação de Rede (NAF) que oferece o serviço ao usuário. Porém, tal implementação no servidor não é muito escalável ou fácil para o administrador no caso de mudanças, tal como novos casos de uso e mudanças ou atualizações nos serviços existentes, ou o usuário que adquire um novo cartão inteligente. As mudanças ou atualizações no NAF requereria uma
30 configuração manual, que é especialmente difícil, se o NAF reside não na rede de

origem do usuário ou assinante, mas em uma rede de terceira parte.

A chave de Ks_int_NAF é usada para segurar o Protocolo de Transporte de Hipertexto (HTTPS) entre o cartão inteligente ou módulo de identidade do assinante e o servidor de aplicação NAF. A aplicação residiria no cartão inteligente ou módulo de identidade do assinante e o terminal móvel apenas atuaria como um modem. Este mecanismo pode ser usado como uma alternativa para apresentar as mensagens de configuração OTA SMS para carregar as novas atualizações ou outras aplicações SAT.

O único caso de uso para a chave Ks_int_NAF definida hoje é no Serviço de Multidifusão/Rádiodifusão de Multimídia (MBMS). No MBMS, o NAF é configurado de acordo com as definições na especificação TS 33.246 3GPP, acoplada aqui como Apêndice A, os conteúdos deste sendo incorporados aqui por referência. No MBMS, uma escolha sobre qual chave usar é definido pela descrição das chaves específicas na especificação TS 33.246. Então para este caso de uso, nenhum mecanismo de escolha de chave é requerido porque a chave é implementada diretamente no NAF que está oferecendo o serviço MBMS para o usuário.

Resumo da Invenção

De acordo com uma incorporação da presente invenção, é provido um método para prover um mecanismo genérico para o servidor de aplicação de rede. O método inclui receber um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede. O método inclui determinar uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário. O método inclui prover a informação de autenticação para a função de aplicação de rede.

De acordo com uma incorporação da presente invenção, é provido um aparelho para prover um mecanismo genérico para o servidor de aplicação de rede. Um dispositivo receptor para receber um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede. Um

dispositivo de determinação para determinar uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário. Um primeiro dispositivo de provimento para prover a informação de autenticação para a função de aplicação de rede.

De acordo com uma incorporação da presente invenção, é provido um aparelho para prover um mecanismo genérico para o servidor de aplicação de rede. O receptor recebe um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede. Uma unidade de determinação determina uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário. Uma unidade de provimento provê a informação de autenticação para a função de aplicação de rede.

Breve Descrição das Figuras

Os desenhos apensos são incluídos para prover um melhor entendimento da invenção e são incorporados e constituem uma parte desta especificação, ilustrando as incorporações da invenção que junto com a descrição serve para explicar os princípios da invenção, onde:

Figura 1A – ilustra um aparelho para prover um mecanismo genérico para o servidor de aplicação de rede, de acordo com uma incorporação da presente invenção;

Figura 1B – ilustra uma arquitetura de rede exemplar na qual uma Função de Aplicação de Rede está na rede visitada, de acordo com uma incorporação da presente invenção;

Figura 2 – ilustra um aparelho para prover um mecanismo genérico para o servidor de aplicação de rede, de acordo com uma incorporação da presente invenção;

Figura 3 – ilustra um método para prover um mecanismo genérico para o servidor de aplicação de rede, de acordo com uma incorporação da

presente invenção; e

Figura 4 – ilustra um método para prover um mecanismo genérico para o servidor de aplicação de rede, de acordo com uma incorporação alternativa da presente invenção.

5

Tabela de Abreviações

3GPP	3 rd Generation Partnership Project Projeto de Parceiros da 3 ^a Geração
3GPP2	3rd Generation Partnership Project 2 2 Projeto de Parceiros da 3 ^a Geração
ACM	Address Complete Message Mensagem Alcançou o Destino
AKA	Authentication and Key Agreement Acordo de Chave e Autenticação
Auth	Authentication Autenticação
AUTHR	Authentication Response Resposta de Autenticação
AVP	Attribute-Value-Pair Par-Valor-Atributo
BS	Base Station Estação Base
BSC	Base Station Controller Controlador da Estação Base
BSF	Bootstrapping Server Function Função do Servidor de Autenticação Inicial
BTS	Base station Transceiver Subsystem Sub-sistema Transceptor da Estação Base
CK	Confidentiality Key Chave de Confidencialidade

CM	Cellular Message Mensagem Celular
GAA	Generic Authentication Architecture Arquitetura de Autenticação Genérica
GBA	Generic Bootstrapping Architecture Arquitetura de Autenticação Inicial Genérica
GBA_U	GBA with UICC-based enhancements GBA com aperfeiçoamentos baseados em UICC
GUSS	GBA User Security Settings Configurações de segurança do Usuário GBA
HSS	Home Subscriber Server Servidor do Assinante de Origem
HTTP	Hypertext Transport Protocol Protocolo de Transporte de Hipertexto
HTTPS	Secured Hypertext Transport Protocol Protocolo de Transporte de Hipertexto Seguro
IK	Integrity Key Chave de Integridade
IMS	IP Multimedia Subsystem Subsistema de Multimídia IP
IMSI	International Mobile Subscriber Identity Identidade do Assinante Móvel Internacional
IP	Internet Protocol Protocolo Internet
ISIM	IMS SIM card Cartão SIM IMS
Kc	Ciphering Key Chave de Cifragem

Ki	Individual Subscriber Authentication Key Chave de Autenticação do Assinante Individual
Ks	Key Material Material Chave
Ks_int_NAF	Derived key in GBA_U which remains on UICC Chave Derivada no GBA_U que permanece no UICC
Ks_ext_NAF	Derived key in GBA_U Chave Derivada no GBA_U
Ks_NAF	Derived Key in GBA_ME Chave Derivada no GBA_ME
MAP	Mobile Application Part Parte de Aplicação Móvel
MBMS	Multimedia Broadcast/Multicast Service Serviço de Multidifusão/Rádiodifusão de Multimídia
ME	Mobile Equipment Equipamento Móvel
MIN	Mobile Identification Number Número de Identificação Móvel
MNO	Home Mobile Network Operator
MO	Mobile Originated Originado Móvel
NAF	Network Application Function Função de Aplicação de Rede
NE	Network Element Elemento de Rede
OTA	Over The Air Sobre o Ar
PDSN	Packet Data Service Node Nó de Serviço de dados de Pacote

PLC	Private Long Code Código Longo Privado
PLCM	PLC Mask Máscara PLC
PSTN	Public Switched Telephone Network Rede de Telefonia Comutada Pública
RAN	Radio Access Network Rede de Acesso de Rádio
RAND	Random Challenge Data Dados de desafio Randômicos
SAT--	SIM Application Toolkit Conjunto de Ferramentas de Aplicação SIM
SIM	Subscriber Identity Module Módulo de Identidade do Assinante
SMS	Short Message Service Serviço de Mensagem Curta
UE	User Equipment Equipamento do Usuário
UICC	UMTS Integrated Circuit Card Cartão de Circuito Integrado UMTS
UMTS	Universal Mobile Telecommunications System Sistema de Telecomunicações Móvel Universal
USIM	Universal SIM card Cartão SIM Universal
USS	User Security Settings Configurações de Segurança do Usuário
Ub	Bootstrapping air interface (from UE to BSF) Interface Aérea de Autenticação Inicial (do UE para BSF)

Zh	HSS interface from BSF Interface HSS do BSF
----	--

Descrição Detalhada da Invenção

O 3GPP é uma infra-estrutura de autenticação proposta (3GPP TS 33.220, anexado aqui como Apêndice B, os conteúdos são incorporados aqui por referência). Esta infra-estrutura pode ser utilizada para permitir as funções de aplicação no lado de rede e no lado do usuário para comunicar nas situações onde o lado de rede e o lado do usuário não poderiam se comunicar. Esta funcionalidade é chamada de "autenticação inicial de segurança da aplicação," ou mais simplesmente como "bootstrapping" (autenticação inicial).

Os princípios gerais da autenticação inicial são que uma função do servidor de autenticação inicial genérica (BSF) permite ao equipamento do usuário (UE) autenticar com este, e concorda nas chaves de sessão. Tal autenticação pode ser baseada no acordo de chave e autenticação (AKA). Ao rodar o AKA, o terminal móvel e a rede mutuamente autenticam um ao outro e concordam nas chaves, especificamente uma chave de confidencialidade (CK) e uma chave de integridade (IK). Depois desta autenticação, o UE e a função de aplicação de rede (NAF), que também pode ser referenciada como provedor de serviço, pode rodar em algum protocolo de aplicação específica, onde a autenticação das mensagens é baseada nas chaves de sessão acordadas entre o UE e o BSF.

A função de autenticação inicial não é pretendida para ser dependente de qualquer função de aplicação de rede particular. O servidor que implementa a função de autenticação inicial deve ser de responsabilidade de um operador de origem para controlar os vetores de autenticação. As funções de aplicação de rede podem ser suportadas na rede de origem do operador, na rede visitada, ou em uma terceira rede.

A Figura 1A ilustra uma arquitetura de rede exemplar, de acordo com uma incorporação da presente invenção. A arquitetura de rede inclui um equipamento do usuário (UE) 100, pelo menos uma função de aplicação de rede

(NAF) 102, uma função do servidor de autenticação inicial (BSF) 104, e um sistema do assinante de origem (HSS) 106. O BSF 104 e HSS 106 formam parte do operador de rede móvel de origem (MNO) 108. O UE 100 conecta no MNO 108 de acordo com as técnicas de comunicação móveis conhecidas.

5 O NAF 102 é hospedado no elemento de rede, sob o controle do MNO 108, por exemplo, e o BSF pode também ser hospedado em um elemento de rede sob o controle do MNO 108. Assim, para propósitos práticos, cada NAF 102 e o BSF 104 pode ser considerado como um elemento de rede.

10 Como ilustrado na Figura 1A, o UE 100 comunica com o NAF 102 pela interface Ua 110. O UE 100 comunica com o BSF 104 pela interface Ub 112. O NAF 102 comunica com o BSF 104 pela interface Zn 114. O BSF 104 comunica com o HSS 106 pela interface Zh 116.

O NAF 102 pode ser provido em uma rede separada adicional. Por exemplo, como ilustrado na Figura 1B, uma arquitetura de rede exemplar é provida na qual NAF 102 está na rede visitada. No caso onde o UE 100 contactou um NAF 15 102 que é operado em outra rede que a rede de origem, este NAF 102 visitado usará um proxy de diâmetro (D-proxy) 118 da rede dos NAFs para comunicar com o BSF do assinante (i.e., BSF de origem) 104. O NAF 102 comunica com o BSF 104 pela interface Zn 114 para o D-Proxy 118 e pela interface Zn' 120 para o BSF 20 104. A funcionalidade D-Proxy 118 pode ser implementada como um elemento de rede separado, ou ser parte de qualquer elemento de rede (NE) na rede visitada que implementa a funcionalidade proxy de Diâmetro (exemplos de tais NE's são os BSF da rede que o NAF 102 visitado pertence, ou um servidor AAA).

25 Para as Figuras 1A e 1B, o princípio de autenticação inicial é que o UE 100 e a função de autenticação inicial mutuamente se autenticam, por exemplo, usando o protocolo AKA, e concordam na secreta mestre compartilhada. Após, a secreta mestre compartilhada ser usada para derivar uma ou mais secretas mestres compartilhadas específicas da função de aplicação de rede que são aplicadas entre o UE 100 e a função de aplicação de rede particular (NAFs) 30 em questão. O material NAF específico da secreta mestre compartilhada é gerado

especificamente e independentemente para cada função de aplicação de rede. Após a operação de autenticação inicial ter sido completada, o UE 100 e a função de aplicação de rede podem rodar em algum protocolo específico, onde a segurança das mensagens será baseada nestas chaves geradas durante a autenticação mútua entre o UE 100 e a função do servidor de autenticação inicial. Assim, as chaves podem ser usadas para autenticação e proteção de integridade, e para confidencialidade. A função de aplicação de rede é então capaz de adquirir o NAF específico da secreta compartilhada derivada da secreta mestre compartilhada estabelecida entre o equipamento do usuário e a função do servidor de autenticação inicial.

A interface de comunicação Ub 112 suporta a autenticação inicial e o protocolo de acordo de chave e autenticação, para prover a autenticação mútua e o acordo de chave entre o UE 100 e o BSF 104. Este protocolo pode ser baseado no protocolo AKA 3GPP, por exemplo.

A interface Zh 116 permite ao BSF 104 buscar qualquer informação de autenticação requerida e a informação de perfil do assinante do HSS 106. A interface Ua 110 suporta qualquer protocolo de aplicação específica que seja seguro usando o NAF específico da secreta compartilhada derivada da secreta mestre compartilhada acordada entre o UE 100 e o BSF 104, baseado no protocolo suportado pela interface Ub 112. A interface Zn 114 é usada pelo NAF 102 para buscar o NAF específico da secreta compartilhada que tem derivado da secreta mestre compartilhada acordada no protocolo suportado na interface Ub 112 do BSF 104. A interface Zn 114 também podem ser usada para buscar a informação de perfil do assinante do BSF 104.

A mensagem transmitida do BSF 104 para o NAF 102 inclui a informação de autenticação inicial. A informação de autenticação inicial pode incluir um identificador de transação, um NAF específico da secreta compartilhada, e a informação de perfil do assinante opcional ("prof_naf" ou "qualquer NAF específico USSs"). O NAF específico da secreta compartilhada, denotado por Ks_NAF, é estabelecido entre o UE 100 e o BSF 104, e pode ser modificado para

uso específico para as comunicações entre o UE 100 e o NAF específico. Ks_NAF é derivada de Ks ao usar os parâmetros especificados no Anexo B 3GPP TS 33.220 (Apêndice A). Ks é a secreta mestre compartilhada, e Ks_NAF é um NAF específico da secreta mestre compartilhada. A informação de autenticação inicial transmitida para cada NAF é então única para este NAF, de acordo com Ks_NAF específico da secreta compartilhada para este NAF.

Um conjunto de todas as configurações de segurança do usuário (GUSS) contém o elemento de informação específico BSF e o conjunto de todos os USSs específicos-aplicação. O conjunto de todas as configurações de segurança do usuário (USSs), i.e. GUSS, é armazenado no HSS. No caso onde o assinante tem múltiplas assinaturas, i.e., múltiplos ISIM ou aplicações USIM no UICC, o HSS conterá um ou mais GUSSs que podem ser mapeados para qualquer de uma ou mais identidades, por exemplo IMPIs (Identidade Privada de Multimídia IP) e IMSIs (Identidade do Assinante Móvel Internacional).

O desenvolvimento de um novo caso de uso, dois NAF específicos da secreta compartilhada no GBA_U , sendo um usado no UICC (Ks_int_NAF) e o outro usado no equipamento móvel (Ks_ext_NAF). Este caso de uso necessita de alguma "decisão lógica" do que a chave ter, i.e., Ks_int_NAF , ou Ks_ext_NAF . Adições de novos serviços para esta 'lógica' deveriam ser possíveis sem uma nova configuração de cartão inteligente no terminal móvel. No caso do NAF suportar mais de um tipo de chave, qualquer tipo de ação de ataque do nível de segurança precisa ser prevenido. Este ataque pode ser que o NAF é enganado ao usar uma chave de nível mais baixo de segurança em vez de requerer o uso do Ks_int_NAF .

De acordo com uma incorporação da presente invenção, é provido um mecanismo genérico para o servidor de aplicação obter o conhecimento sobre qual chave de uma Arquitetura de Autenticação Genérica (GAA) permitiria uma integração fácil dos servidores de aplicação adicionais ao estender um padrão existente para as Configurações de Segurança do Usuário (USS). Os Pares-Valor-Atributo AVP (AVPs) são definidos nas mensagens de Pedido-Info-Autenticação Inicial/Resposta da interface Zn GAA 3GPP TS 29.109, anexado aqui como

Apêndice C, os conteúdos deste são incorporados aqui por referência, e novos Diâmetro adicionais AVP são definidos no 3GPP TS 29.229, anexado aqui como Apêndice D, os conteúdos deste sendo incorporados aqui por referência.

Um mecanismo genérico pode ser implementado através de uma codificação rígida ou ao configurar localmente o uso da chave diretamente no software em cada NAF durante a configuração do NAF (local no NAF), por codificação rígida do uso da chave no BSF (BSF dita ao entregar apenas a chave pertinente a NAF), ao prover um campo(s) adicional na configuração de segurança do usuário (USS) armazenado no Servidor do Assinante de Origem (HSS) que é transferido ao BSF, e/ou ao usar o AVP armazenado no BSF que indica o uso da chave. Se o BSF entregasse apenas as chaves pertinentes ao NAF, o NAF não estaria atento à qualidade de segurança fornecida e ao tipo de chave que está usando.

O 3GPP padronizado e as Configurações de Segurança do Usuário (USS) existentes poderiam ser estendidos e usados para indicar qual chave usar. Isto proporcionaria ao operador-origem do usuário o controle total e flexível, especialmente no caso em que o serviço é oferecido por um NAF de terceira parte e a tarifação do serviço é feita pelo operador-origem.

De acordo com uma incorporação da presente invenção, pode haver pelo menos duas possíveis incorporações. Em uma primeira incorporação da presente invenção, o USS poderia indicar que tipo de cartão inteligente ou ambiente seguro o usuário possui. Também, a primeira incorporação proveria se o SIM Universal do assinante móvel (USIM), o cartão IMS SIM (ISIM) é ou não permitido para GBA_U. Na primeira incorporação, pode haver um campo indicador que indica se o cartão ou ambiente seguro é permitido para GBA_U.

Em uma segunda incorporação da presente invenção, o USS pode incluir um ou dois campos indicadores de autorização que são transportados no USS de uma especificação existente 3GPP TS 29.109, anexado aqui como Apêndice D, os conteúdos deste sendo incorporados aqui por referência. No primeiro campo indicador, se este campo estiver presente e indicar o uso da

secreta compartilhada baseado no UICC (Ks_int_NAF) este é obrigatório. O segundo campo indicador pode ser um campo opcional onde se este segundo campo indicador estiver presente este indica o uso da secreta compartilhada (Ks_ext_NAF ou Ks_NAF).

5 Se o assinante móvel é provisionado por um operador de origem com um novo módulo de identidade do assinante, então o USS pode ser facilmente atualizado para requerer que de agora em diante uma chave Ks_int_NAF mais segura seja usada. Ambas as alternativas impedem as ações de ataque de segurança, i.e., a chave Ks_ext_NAF sendo usada em vez da chave
10 Ks_int_NAF mais segura.

A Figura 2 ilustra um aparelho 150 para prover um mecanismo genérico para o servidor de aplicação de rede, de acordo com uma incorporação da presente invenção. O aparelho 150 inclui uma unidade receptora 152 para receber o pedido de um equipamento do usuário para prover a informação de
15 autenticação para uma função de aplicação de rede. O aparelho 150 inclui uma unidade de determinação 154 para determinar uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário. O aparelho 150 também inclui uma primeira unidade de provimento 156 para prover
20 a informação de autenticação à função de aplicação de rede.

A Figura 3 ilustra um método para prover um mecanismo genérico para o servidor de aplicação de rede, de acordo com uma incorporação da presente invenção. Na operação 200, o método recebe um pedido do equipamento do usuário para prover a informação de autenticação para uma função de
25 aplicação de rede. Na operação 210, o método determina uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender um padrão existente para as configurações de segurança do usuário. Na operação 220, prover a informação de autenticação à função de aplicação de rede. De acordo com uma incorporação da presente
30 invenção, o USS poderia indicar que tipo de cartão inteligente o usuário possui, ou

que tipo (i.e., Ks_ext_NAF ou Ks_int_NAF), de secreta compartilhada deve ser usado. Na operação 230, o método determina se o SIM Universal do assinante móvel (USIM), o cartão IMS SIM (ISIM) ou outro ambiente seguro é ou não permitido para o GBA_U. Na primeira incorporação, pode haver um campo

5 indicador que indica se o cartão ou o ambiente seguro é habilitado ao GBA_U.

A Figura 4 ilustra um método para prover um mecanismo genérico para o servidor de aplicação de rede, de acordo com uma incorporação alternativa da presente invenção. Na operação 300, o método recebe um pedido do equipamento do usuário para prover a informação de autenticação para uma

10 função de aplicação de rede. Na operação 310, o método determina uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender um padrão existente para as configurações de segurança do usuário. Na operação 320, prover a informação de autenticação à função de aplicação de rede. De acordo com uma incorporação da

15 presente invenção, o USS poderia indicar que tipo de cartão inteligente ou ambiente seguro o usuário possui, ou que tipo de secreta compartilhada deva ser usado. Na operação 330, o método determina se o USS inclui um ou dois campos indicadores a serem transportados no cabeçalho de Autorização da especificação existente 3GPP TS 29.109, anexado como Apêndice C. No primeiro campo

20 indicador, se este campo estiver presente este indica que o uso da secreta (Ks_int_NAF) compartilhada baseada em UICC é obrigatório. O segundo campo indicador pode ser um campo opcional, onde se este segundo campo indicador estiver presente, este indica o uso da secreta (Ks_ext_NAF ou Ks_NAF) compartilhada baseado no ME.

25 Se um novo servidor de aplicação for configurado na rede do operador, este não necessita saber qual chave usar para qual usuário ou se o usuário será provisionado em um futuro próximo com um novo cartão SIM. O NAF obteria a informação de escolha da chave necessária do BSF.

De acordo uma incorporação da presente invenção, um novo AVP

30 poderia ser usado para indicar o tipo de chave derivada sendo usado. Por

exemplo, o novo AVP pode indicar se a chave derivada é Ks_int_NAF ou algum outro tipo de chave. O novo AVP indicaria se o cartão ou ambiente seguro é habilitado ao GBA_U ou, como uma alternativa, qual chave usar. Dependendo do indicador, o NAF pode usar a chave secreta compartilhada (Ks_int_NAF) baseado no UICC quando indicado. Quer dizer, o AVP indica que o cartão ou o ambiente seguro é habilitado ao GBA_U ou o AVP indica o uso de Ks_int_NAF explicitamente. O NAF requereria então que esta chave fosse usada e não alguma outra chave com um nível de segurança mais baixo.

Para o servidor de rede em um ambiente seguro, por exemplo um cartão inteligente, o cliente residiria no Cartão de Circuito Integrado (UICC) do Sistema de Telecomunicações Móvel Universal (UMTS) e a aplicação também residiria em um ambiente seguro. Isto seria tipicamente uma aplicação Java, uma aplicação XML, uma aplicação C++, uma aplicação de Perl, ou uma aplicação Visual Basic ou outros tipos semelhantes de aplicações. Então, o UICC também pode atuar como um servidor de aplicação que oferece um serviço de rede para outras entidades, onde uma delas poderia residir em outro domínio confiável, por exemplo, em uma segunda área segura no telefone e a Ks_int_NAF pode ser usada para comunicações seguras entre as entidades de serviço de rede. O NAF baseado em UICC teria o papel de um WSP (Provedor de Serviço de Rede) como esboçado pela Especificação de Estrutura de Serviço de Rede de Liberdade de Aliança (ID-WSF) <http://www.projectliberty.org/resources/specifications.php>. O UICC pode atuar como um provedor de serviço de rede de acordo com a Liberdade de Aliança que provê uma entidade solicitante (i.e., o consumidor do serviço de rede) com uma informação sensível que pode ser autenticada/seguira pela Ks_int_NAF. Outras chaves baseadas em GAA podem ser usadas também na estrutura de serviço de rede para identificação e segurança da mensagem. Além disso, o TS 24.109 3GPP especifica a interface de autenticação inicial (Ub) e a interface da função de aplicação de rede (Ua), anexado aqui como Apêndice E, os conteúdos deste sendo incorporados aqui por referência. TS 29.109 3GPP especifica as interfaces Zh e Zn baseadas no protocolo de diâmetro, anexado aqui

como Apêndice F, os conteúdos deste sendo incorporados aqui por referência.

A presente invenção pode permitir ao operador-origem do assinante ter total controle do nível de segurança usado. A atualização das configurações de segurança do usuário, no caso do usuário possuir um novo UICC poderia
5 acontecer centralmente no Servidor de Serviço de Origem (HSS) e não seria requerido atualizar todos os NAFs individualmente. A lógica de decisão pode residir no HSS ou BSF controlado pelo operador. Em adição, os ataques de segurança também não seriam mais possíveis para as novas aplicações.

A descrição precedente tem sido direcionada às incorporações
10 específicas desta invenção. Será aparente, porém, que outras variações e modificações às incorporações descritas podem ser feitas, com a realização de algumas ou todas as suas vantagens. Então, é o objetivo das reivindicações apenas cobrir todas as tais variações e modificações dentro do conceito inventivo e escopo da invenção.

REIVINDICAÇÕES

1. Método para prover um mecanismo genérico para o servidor de aplicação de rede, o método é **CARACTERIZADO** pelo fato de que compreende:

- receber um pedido do equipamento do usuário para prover a
5 informação de autenticação para a função de aplicação de rede;

- determinar uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário;

- prover a informação de autenticação para a função de aplicação de
10 rede.

2. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que também compreende:

- prover os dados relativos ao tipo de cartão inteligente ou ambiente seguro no equipamento do usuário nas configurações de segurança do usuário; e

- prover um campo indicador indicativo de se a arquitetura de
15 autenticação inicial genérica com os melhoramentos baseados em circuito integrado (GBA-U) permite o módulo de identidade do assinante universal, o módulo de identidade do assinante, o cartão IMS SIM ou outro ambiente seguro.

3. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo
20 fato de que também compreende:

- prover o primeiro e o segundo campos indicadores nas configurações de segurança do usuário que são transportados no cabeçalho de autorização de uma especificação, onde no primeiro campo indicador, a primeira chave derivada (Ks_int_NAF) nos melhoramentos baseados nos circuitos
25 integrados (GBA_U) é usado, e no segundo campo indicador, a segunda chave derivada (Ks_ext_NAF) ou a terceira chave derivada (Ks_NAF) são usadas.

4. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o passo de determinação compreende determinar ao menos:

- configurar localmente o uso da chave diretamente na função de
30 aplicação de rede durante a configuração da função de aplicação de rede;

- configurar localmente o uso da chave na função do servidor de autenticação inicial;

- prover um campo adicional na configuração de segurança do usuário armazenada no servidor do assinante de origem que é transferido para a função do servidor de autenticação inicial; e

- usar o par-valor-atributo armazenado na função do servidor de autenticação inicial que indica o uso da chave.

5. Método de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que também compreende:

- usar o par-valor-atributo para indicar o tipo de chave derivativa sendo usada ou o tipo de cartão inteligente ou ambiente seguro permitido, onde o tipo de chave derivativa compreende Ks_int_NAF, Ks_ext_NAF, ou Ks_NAF, e o cartão inteligente ou ambiente seguro compreende o GBA_U.

6. Método de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que o par-valor-atributo indica o uso da Ks_int_NAF, também compreende requerer o uso da Ks_int_NAF pela função de aplicação de rede ao invés da chave com nível mais baixo de segurança.

7. Método de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que quando o servidor de rede está no ambiente seguro, o método também compreende:

- alocar a aplicação de rede no cartão de circuito integrado (UICC) do sistema de telecomunicações móvel universal (UMTS), onde o UICC é a função de aplicação de rede e a chave derivada (Ks_int_NAF) é usada para as comunicações seguras entre as entidades de serviço de rede.

8. Método de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que alocar a aplicação de rede compreende uma aplicação Java, uma aplicação XML, uma aplicação C++, uma aplicação Perl, ou uma aplicação Visual Basic.

9. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que também compreende:

- configurar localmente o uso da chave na função do servidor de autenticação inicial (BSF) ao prover um campo adicional nas configurações de segurança do usuário armazenadas no servidor do assinante de origem (HSS).

10. Aparelho para prover um mecanismo genérico para o servidor de aplicação de rede, o aparelho é **CARACTERIZADO** pelo fato de que compreende:

- um dispositivo receptor para receber um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede;

- um dispositivo de determinação para determinar uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário;

- um primeiro dispositivo de provimento para prover a informação de autenticação para a função de aplicação de rede.

11. Aparelho de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que também compreende:

- um segundo dispositivo de provimento para prover o tipo de ambiente seguro no equipamento do usuário nas configurações de segurança do usuário; e

- um terceiro dispositivo de provimento para prover um campo indicador indicativo de se a arquitetura de autenticação inicial genérica com os melhoramentos baseados em circuito integrado (GBA-U) permite o módulo de identidade do assinante universal, o módulo de identidade do assinante, o cartão IMS SIM ou outro ambiente seguro.

12. Aparelho de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que também compreende:

- um segundo dispositivo de provimento para prover o primeiro e o segundo campos indicadores nas configurações de segurança do usuário que são transportados no cabeçalho de autorização de uma especificação, onde no primeiro campo indicador, a primeira chave derivada (Ks_Int_NAF) nos

melhoramentos baseados nos circuitos integrados (GBA_U) é usado, e no segundo campo indicador, a segunda chave derivada (Ks_ext_NAF) ou a terceira chave derivada (Ks_NAF) são usadas.

13. Aparelho de acordo com a reivindicação 10, **CARACTERIZADO**

5 pelo fato de que mecanismo genérico compreende ao menos um:

- um primeiro dispositivo de codificação rígida para configurar localmente o uso da chave diretamente na função de aplicação de rede durante a configuração da função de aplicação de rede;

- um segundo dispositivo de codificação rígida para configurar
10 localmente o uso da chave na função do servidor de autenticação inicial;

- um segundo dispositivo de provimento para prover um campo adicional na configuração de segurança do usuário armazenada no servidor do assinante de origem que é transferido para a função do servidor de autenticação inicial; e

- 15 - um primeiro dispositivo de uso para usar o par-valor-atributo armazenado na função do servidor de autenticação inicial que indica o uso da chave.

14. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO**

pelo fato de que também compreende:

- 20 - um segundo dispositivo de uso para usar o par-valor-atributo para indicar o tipo de chave derivativa sendo usada ou o tipo de cartão inteligente ou ambiente seguro permitido, onde o tipo de chave derivativa compreende Ks_int_NAF, Ks_ext_NAF, ou Ks_NAF, e o cartão inteligente ou ambiente seguro compreende o GBA_U.

25 15. Aparelho de acordo com a reivindicação 14, **CARACTERIZADO**

pelo fato de que o par-valor-atributo indica o uso da Ks_int_NAF, também compreende requerer o uso da Ks_int_NAF pela função de aplicação de rede ao invés da chave com nível mais baixo de segurança.

16. Aparelho de acordo com a reivindicação 11, **CARACTERIZADO**

30 pelo fato de que quando o servidor de rede está no ambiente seguro também

compreende:

- alocar a aplicação de rede no cartão de circuito integrado (UICC) do sistema de telecomunicações móvel universal (UMTS), onde o UICC é a função de aplicação de rede e a chave derivada (Ks_int_NAF) é usada para as comunicações seguras entre as entidades de serviço de rede.

17. Aparelho de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que também compreende:

- um terceiro dispositivo de codificação rígida para configurar localmente o uso da chave na função do servidor de autenticação inicial (BSF) ao prover um campo adicional nas configurações de segurança do usuário armazenadas no servidor do assinante de origem (HSS).

18. Aparelho para prover um mecanismo genérico para o servidor de aplicação de rede, o aparelho é **CARACTERIZADO** pelo fato de que compreende:

- uma unidade de recepção que recebe um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede;

- uma unidade de determinação que determina uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário;

- uma unidade de provimento que provê a informação de autenticação para a função de aplicação de rede.

19. Programa de computador armazenado em um dispositivo legível de computador para prover um mecanismo genérico para o servidor de aplicação de rede, o programa de computador é **CARACTERIZADO** pelo fato de que é configurado para executar o processo que compreende:

- receber um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede;

- determinar uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão

existente para as configurações de segurança do usuário;

- prover a informação de autenticação para a função de aplicação de rede.

20. Programa de computador de acordo com a reivindicação 19,

CARACTERIZADO pelo fato de que também compreende:

- prover os dados relativos ao tipo de cartão inteligente ou ambiente seguro no equipamento do usuário nas configurações de segurança do usuário; e

- prover um campo indicador indicativo de se a arquitetura de autenticação inicial genérica com os melhoramentos baseados em circuito integrado (GBA-U) permite o módulo de identidade do assinante universal, o módulo de identidade do assinante, o cartão IMS SIM ou outro ambiente seguro.

21. Programa de computador de acordo com a reivindicação 19,

CARACTERIZADO pelo fato de que também compreende:

- prover o primeiro e o segundo campos indicadores nas configurações de segurança do usuário que são transportados no cabeçalho de autorização de uma especificação, onde no primeiro campo indicador, a primeira chave derivada (Ks_int_NAF) nos melhoramentos baseados nos circuitos integrados (GBA_U) é usado, e no segundo campo indicador, a segunda chave derivada (Ks_ext_NAF) ou a terceira chave derivada (Ks_NAF) são usadas.

22. Programa de computador de acordo com a reivindicação 19,

CARACTERIZADO pelo fato de que o passo de determinação compreende determinar ao menos:

- configurar localmente o uso da chave diretamente na função de aplicação de rede durante a configuração da função de aplicação de rede;

- configurar localmente o uso da chave na função do servidor de autenticação inicial;

- prover um campo adicional na configuração de segurança do usuário armazenada no servidor do assinante de origem que é transferido para a função do servidor de autenticação inicial; e

- usar o par-valor-atributo armazenado na função do servidor de

autenticação inicial que indica o uso da chave.

23. Programa de computador de acordo com a reivindicação 22, **CARACTERIZADO** pelo fato de que também compreende:

5 - usar o par-valor-atributo para indicar o tipo de chave derivativa sendo usada ou o tipo de cartão inteligente ou ambiente seguro permitido, onde o tipo de chave derivativa compreende Ks_int_NAF, Ks_ext_NAF, ou Ks_NAF, e o cartão inteligente ou ambiente seguro compreende o GBA_U.

24. Programa de computador de acordo com a reivindicação 23, **CARACTERIZADO** pelo fato de que o par-valor-atributo indica o uso da Ks_int_NAF, também compreende requerer o uso da Ks_int_NAF pela função de aplicação de rede ao invés da chave com nível mais baixo de segurança.

25. Programa de computador de acordo com a reivindicação 20, **CARACTERIZADO** pelo fato de que quando o servidor de rede está no ambiente seguro também compreende:

15 - alocar a aplicação de rede no cartão de circuito integrado (UICC) do sistema de telecomunicações móvel universal (UMTS), onde o UICC é a função de aplicação de rede e a chave derivada (Ks_int_NAF) é usada para as comunicações seguras entre as entidades de serviço de rede.

26. Programa de computador de acordo com a reivindicação 25, **CARACTERIZADO** pelo fato de que alocar a aplicação de rede compreende uma aplicação Java, uma aplicação XML, uma aplicação C++, uma aplicação Perl, ou uma aplicação Visual Basic.

27. Programa de computador de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que também compreende:

25 - configurar localmente o uso da chave na função do servidor de autenticação inicial (BSF) ao prover um campo adicional nas configurações de segurança do usuário armazenadas no servidor do assinante de origem (HSS).

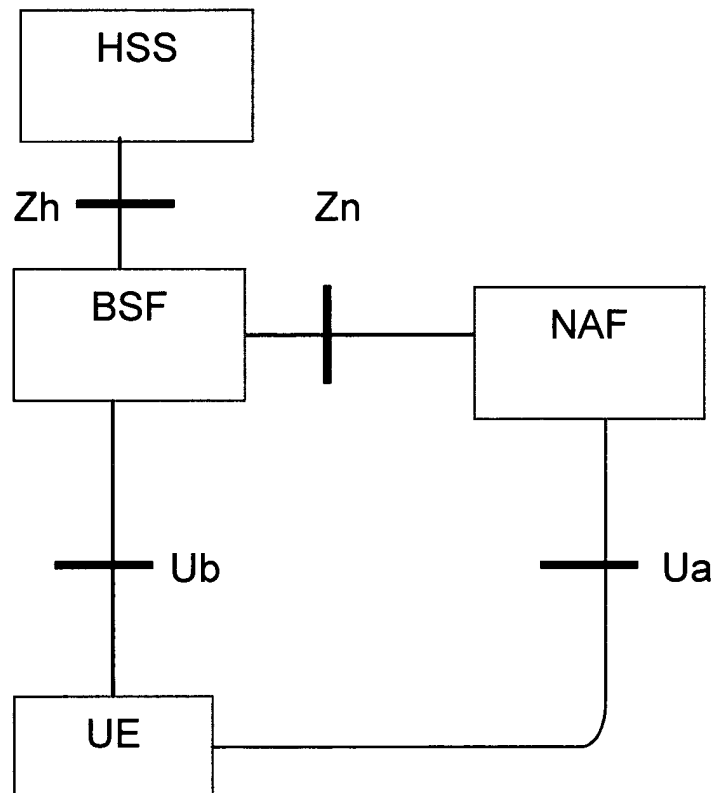
FIG. 1A

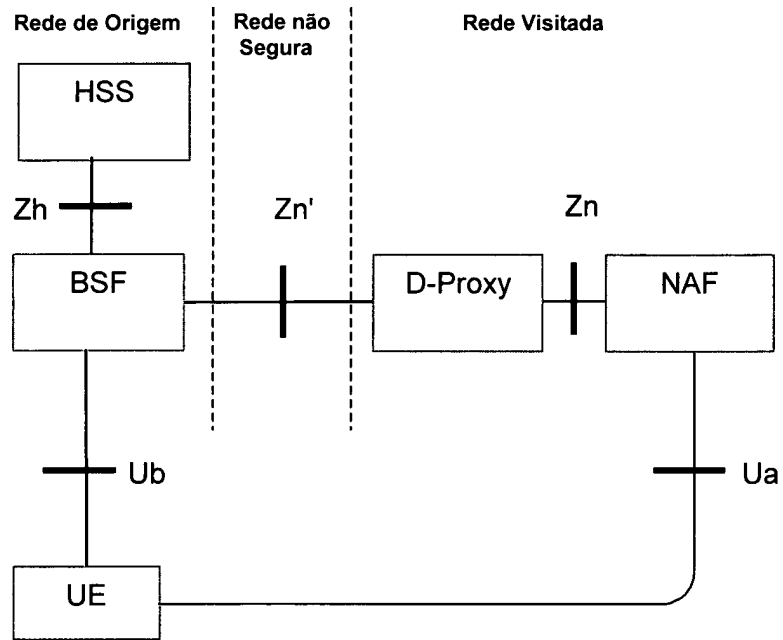
FIG. 1B

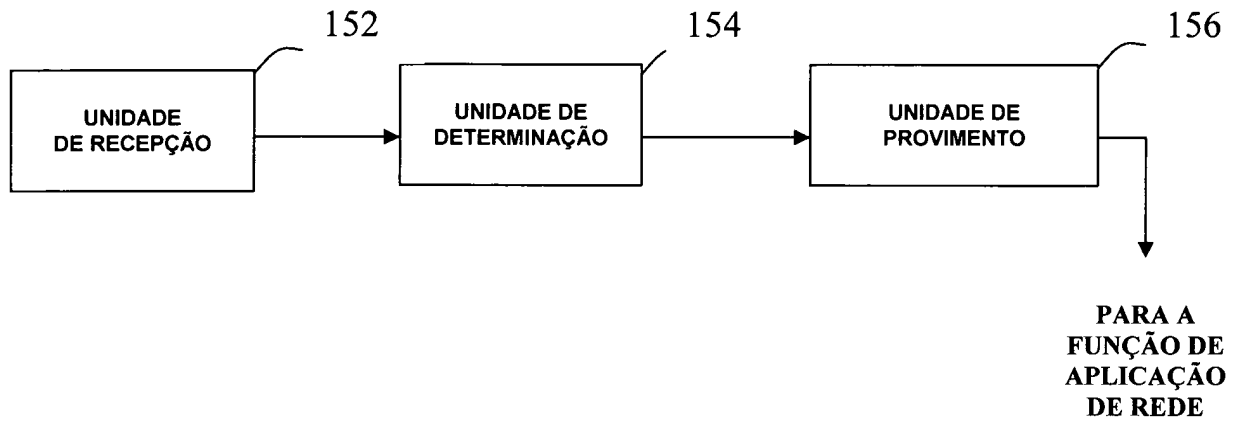
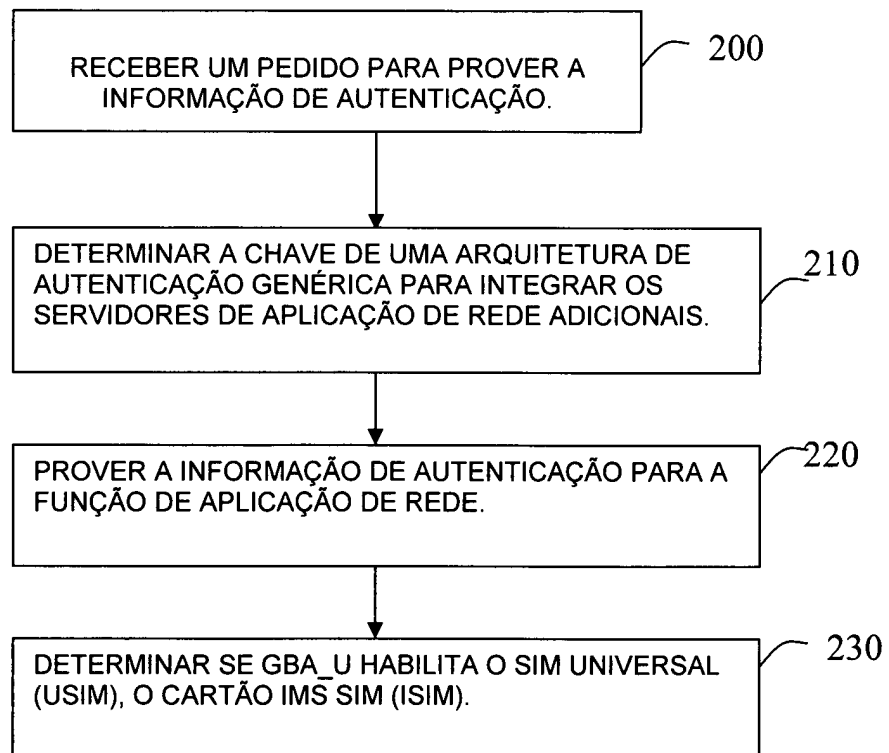
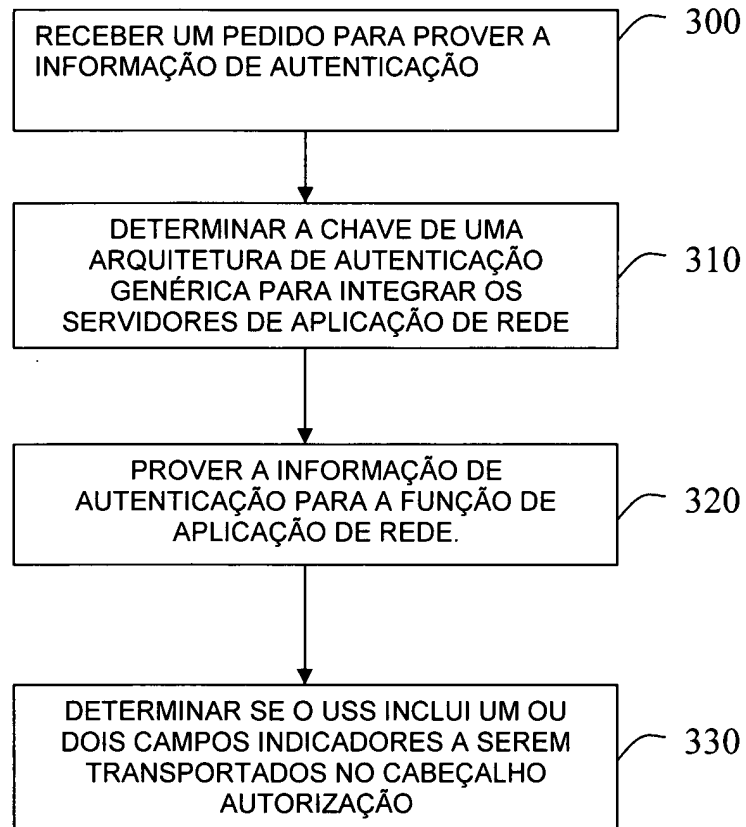
FIG. 2**FIG. 3**

FIG. 4

RESUMO

P10610400-2

“MÉTODO, APARELHO E PROGRAMA DE COMPUTADOR PARA PROVER UM MECANISMO GENÉRICO PARA O SERVIDOR DE APLICAÇÃO DE REDE”.

5 Método e aparelho para prover um mecanismo genérico para o servidor de aplicação de rede. O receptor recebe um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede. A unidade de determinação determina a chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais
10 ao estender o padrão existente para as configurações de segurança do usuário. A unidade de provimento provê a informação de autenticação para a função de aplicação de rede.

REIVINDICAÇÕES

1. Método para prover um mecanismo genérico para o servidor de aplicação de rede, o método é **CARACTERIZADO** pelo fato de que compreende:

- receber um pedido do equipamento do usuário para prover a
5 informação de autenticação para a função de aplicação de rede;

- determinar uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário;

- prover a informação de autenticação para a função de aplicação de
10 rede.

2. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que também compreende:

- prover os dados relativos ao tipo de cartão inteligente ou ambiente seguro no equipamento do usuário nas configurações de segurança do usuário; e

- prover um campo indicador indicativo de se a arquitetura de
15 autenticação inicial genérica com os melhoramentos baseados em circuito integrado (GBA-U) permite o módulo de identidade do assinante universal, o módulo de identidade do assinante, o cartão IMS SIM ou outro ambiente seguro.

3. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo
20 fato de que também compreende:

- prover o primeiro e o segundo campos indicadores nas configurações de segurança do usuário que são transportados no cabeçalho de autorização de uma especificação, onde no primeiro campo indicador, a primeira chave derivada (Ks_int_NAF) nos melhoramentos baseados nos circuitos
25 integrados (GBA_U) é usado, e no segundo campo indicador, a segunda chave derivada (Ks_ext_NAF) ou a terceira chave derivada (Ks_NAF) são usadas.

4. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o passo de determinação compreende determinar ao menos:

- configurar localmente o uso da chave diretamente na função de
30 aplicação de rede durante a configuração da função de aplicação de rede;

- configurar localmente o uso da chave na função do servidor de autenticação inicial;

- prover um campo adicional na configuração de segurança do usuário armazenada no servidor do assinante de origem que é transferido para a função do servidor de autenticação inicial; e

- usar o par-valor-atributo armazenado na função do servidor de autenticação inicial que indica o uso da chave.

5. Método de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que também compreende:

- usar o par-valor-atributo para indicar o tipo de chave derivativa sendo usada ou o tipo de cartão inteligente ou ambiente seguro permitido, onde o tipo de chave derivativa compreende Ks_int_NAF, Ks_ext_NAF, ou Ks_NAF, e o cartão inteligente ou ambiente seguro compreende o GBA_U.

6. Método de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que o par-valor-atributo indica o uso da Ks_int_NAF, também compreende requerer o uso da Ks_int_NAF pela função de aplicação de rede ao invés da chave com nível mais baixo de segurança.

7. Método de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que quando o servidor de rede está no ambiente seguro, o método também compreende:

- alocar a aplicação de rede no cartão de circuito integrado (UICC) do sistema de telecomunicações móvel universal (UMTS), onde o UICC é a função de aplicação de rede e a chave derivada (Ks_int_NAF) é usada para as comunicações seguras entre as entidades de serviço de rede.

8. Método de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que alocar a aplicação de rede compreende uma aplicação Java, uma aplicação XML, uma aplicação C++, uma aplicação Perl, ou uma aplicação Visual Basic.

9. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que também compreende:

- configurar localmente o uso da chave na função do servidor de autenticação inicial (BSF) ao prover um campo adicional nas configurações de segurança do usuário armazenadas no servidor do assinante de origem (HSS).

10. Aparelho para prover um mecanismo genérico para o servidor de aplicação de rede, o aparelho é **CARACTERIZADO** pelo fato de que compreende:

- um dispositivo receptor para receber um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede;

- um dispositivo de determinação para determinar uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário;

- um primeiro dispositivo de provimento para prover a informação de autenticação para a função de aplicação de rede.

11. Aparelho de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que também compreende:

- um segundo dispositivo de provimento para prover o tipo de ambiente seguro no equipamento do usuário nas configurações de segurança do usuário; e

- um terceiro dispositivo de provimento para prover um campo indicador indicativo de se a arquitetura de autenticação inicial genérica com os melhoramentos baseados em circuito integrado (GBA-U) permite o módulo de identidade do assinante universal, o módulo de identidade do assinante, o cartão IMS SIM ou outro ambiente seguro.

12. Aparelho de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que também compreende:

- um segundo dispositivo de provimento para prover o primeiro e o segundo campos indicadores nas configurações de segurança do usuário que são transportados no cabeçalho de autorização de uma especificação, onde no primeiro campo indicador, a primeira chave derivada (Ks_int_NAF) nos

melhoramentos baseados nos circuitos integrados (GBA_U) é usado, e no segundo campo indicador, a segunda chave derivada (Ks_ext_NAF) ou a terceira chave derivada (Ks_NAF) são usadas.

13. Aparelho de acordo com a reivindicação 10, **CARACTERIZADO**

5 pelo fato de que mecanismo genérico compreende ao menos um:

- um primeiro dispositivo de codificação rígida para configurar localmente o uso da chave diretamente na função de aplicação de rede durante a configuração da função de aplicação de rede;

- um segundo dispositivo de codificação rígida para configurar
10 localmente o uso da chave na função do servidor de autenticação inicial;

- um segundo dispositivo de provimento para prover um campo adicional na configuração de segurança do usuário armazenada no servidor do assinante de origem que é transferido para a função do servidor de autenticação inicial; e

- 15 - um primeiro dispositivo de uso para usar o par-valor-atributo armazenado na função do servidor de autenticação inicial que indica o uso da chave.

14. Aparelho de acordo com a reivindicação 13, **CARACTERIZADO**

pelo fato de que também compreende:

- 20 - um segundo dispositivo de uso para usar o par-valor-atributo para indicar o tipo de chave derivativa sendo usada ou o tipo de cartão inteligente ou ambiente seguro permitido, onde o tipo de chave derivativa compreende Ks_int_NAF, Ks_ext_NAF, ou Ks_NAF, e o cartão inteligente ou ambiente seguro compreende o GBA_U.

25 15. Aparelho de acordo com a reivindicação 14, **CARACTERIZADO**

pelo fato de que o par-valor-atributo indica o uso da Ks_int_NAF, também compreende requerer o uso da Ks_int_NAF pela função de aplicação de rede ao invés da chave com nível mais baixo de segurança.

16. Aparelho de acordo com a reivindicação 11, **CARACTERIZADO**

30 pelo fato de que quando o servidor de rede está no ambiente seguro também

compreende:

- alocar a aplicação de rede no cartão de circuito integrado (UICC) do sistema de telecomunicações móvel universal (UMTS), onde o UICC é a função de aplicação de rede e a chave derivada (Ks_{int_NAF}) é usada para as comunicações seguras entre as entidades de serviço de rede.

17. Aparelho de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que também compreende:

- um terceiro dispositivo de codificação rígida para configurar localmente o uso da chave na função do servidor de autenticação inicial (BSF) ao prover um campo adicional nas configurações de segurança do usuário armazenadas no servidor do assinante de origem (HSS).

18. Aparelho para prover um mecanismo genérico para o servidor de aplicação de rede, o aparelho é **CARACTERIZADO** pelo fato de que compreende:

- uma unidade de recepção que recebe um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede;

- uma unidade de determinação que determina uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão existente para as configurações de segurança do usuário;

- uma unidade de provimento que provê a informação de autenticação para a função de aplicação de rede.

19. Programa de computador armazenado em um dispositivo legível de computador para prover um mecanismo genérico para o servidor de aplicação de rede, o programa de computador é **CARACTERIZADO** pelo fato de que é configurado para executar o processo que compreende:

- receber um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede;

- determinar uma chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais ao estender o padrão

existente para as configurações de segurança do usuário;

- prover a informação de autenticação para a função de aplicação de rede.

20. Programa de computador de acordo com a reivindicação 19,

5 **CARACTERIZADO** pelo fato de que também compreende:

- prover os dados relativos ao tipo de cartão inteligente ou ambiente seguro no equipamento do usuário nas configurações de segurança do usuário; e

- prover um campo indicador indicativo de se a arquitetura de autenticação inicial genérica com os melhoramentos baseados em circuito integrado (GBA-U) permite o módulo de identidade do assinante universal, o módulo de identidade do assinante, o cartão IMS SIM ou outro ambiente seguro.

21. Programa de computador de acordo com a reivindicação 19,

CARACTERIZADO pelo fato de que também compreende:

- prover o primeiro e o segundo campos indicadores nas configurações de segurança do usuário que são transportados no cabeçalho de autorização de uma especificação, onde no primeiro campo indicador, a primeira chave derivada (Ks_int_NAF) nos melhoramentos baseados nos circuitos integrados (GBA_U) é usado, e no segundo campo indicador, a segunda chave derivada (Ks_ext_NAF) ou a terceira chave derivada (Ks_NAF) são usadas.

22. Programa de computador de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que o passo de determinação compreende determinar ao menos:

- configurar localmente o uso da chave diretamente na função de aplicação de rede durante a configuração da função de aplicação de rede;

- configurar localmente o uso da chave na função do servidor de autenticação inicial;

- prover um campo adicional na configuração de segurança do usuário armazenada no servidor do assinante de origem que é transferido para a função do servidor de autenticação inicial; e

- usar o par-valor-atributo armazenado na função do servidor de

autenticação inicial que indica o uso da chave.

23. Programa de computador de acordo com a reivindicação 22, **CARACTERIZADO** pelo fato de que também compreende:

- usar o par-valor-atributo para indicar o tipo de chave derivativa sendo usada ou o tipo de cartão inteligente ou ambiente seguro permitido, onde o tipo de chave derivativa compreende Ks_int_NAF, Ks_ext_NAF, ou Ks_NAF, e o cartão inteligente ou ambiente seguro compreende o GBA_U.

24. Programa de computador de acordo com a reivindicação 23, **CARACTERIZADO** pelo fato de que o par-valor-atributo indica o uso da Ks_int_NAF, também compreende requerer o uso da Ks_int_NAF pela função de aplicação de rede ao invés da chave com nível mais baixo de segurança.

25. Programa de computador de acordo com a reivindicação 20, **CARACTERIZADO** pelo fato de que quando o servidor de rede está no ambiente seguro também compreende:

- alocar a aplicação de rede no cartão de circuito integrado (UICC) do sistema de telecomunicações móvel universal (UMTS), onde o UICC é a função de aplicação de rede e a chave derivada (Ks_int_NAF) é usada para as comunicações seguras entre as entidades de serviço de rede.

26. Programa de computador de acordo com a reivindicação 25, **CARACTERIZADO** pelo fato de que alocar a aplicação de rede compreende uma aplicação Java, uma aplicação XML, uma aplicação C++, uma aplicação Perl, ou uma aplicação Visual Basic.

27. Programa de computador de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que também compreende:

- configurar localmente o uso da chave na função do servidor de autenticação inicial (BSF) ao prover um campo adicional nas configurações de segurança do usuário armazenadas no servidor do assinante de origem (HSS).

RESUMO

“MÉTODO, APARELHO E PROGRAMA DE COMPUTADOR PARA PROVER UM MECANISMO GENÉRICO PARA O SERVIDOR DE APLICAÇÃO DE REDE”.

5 Método e aparelho para prover um mecanismo genérico para o servidor de aplicação de rede. O receptor recebe um pedido do equipamento do usuário para prover a informação de autenticação para a função de aplicação de rede. A unidade de determinação determina a chave de uma arquitetura de autenticação genérica para integrar os servidores de aplicação de rede adicionais
10 ao estender o padrão existente para as configurações de segurança do usuário. A unidade de provimento provê a informação de autenticação para a função de aplicação de rede.