(11) Número de Publicação: **PT 1552646 E**

(51) Classificação Internacional:
H04L 9/32 (2014.01)

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

(22) Data de pedido: **2003.09.30**

(30) Prioridade(s): **2002.10.03 US 416481 P**
2003.09.10 US 659774

(43) Data de publicação do pedido: **2005.07.13**

(45) Data e BPI da concessão: **2014.03.19**
083/2014

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

(72) Inventor(es):
HENRY HAVERINEN **FI**
KALLE AHMAVAARA **FI**

(74) Mandatário:
JOSÉ RAUL DE MAGALHÃES SIMÕES
RUA CASTILHO, 167 - 2.º 1070-050 LISBOA **PT**

(54) Epígrafe: **MÉTODO E APARELHO DE PERMISSÃO DE NOVA AUTENTICAÇÃO NUM SISTEMA DE COMUNICAÇÃO CELULAR**

(57) Resumo:
UM MÉTODO (E EQUIPAMENTO CORRESPONDENTE) PARA UMA NOVA AUTENTICAÇÃO ¿ APÓS UMA PRIMEIRA AUTENTICAÇÃO COMPLETA POR PARTE DE UM PRIMEIRO SERVIDOR DE AUTENTICAÇÃO (23A) ¿ DE UMA SESSÃO DE COMUNICAÇÃO ENVOLVENDO A TROCA DE INFORMAÇÕES ENTRE UM TERMINAL (21) E UM SERVIDOR (24), O MÉTODO INCLUINDO: UMA ETAPA (11) NA QUAL SÃO ATRIBUÍDOS AO PRIMEIRO SERVIDOR DE AUTENTICAÇÃO (23A) E A CADA UM DOS OUTROS SERVIDORES DE AUTENTICAÇÃO (23B) UM NOME DE DOMÍNIO EXCLUSIVO RESPETIVO; E UMA ETAPA (13) NA QUAL, DURANTE A AUTENTICAÇÃO ENTRE O TERMINAL E O PRIMEIRO SERVIDOR DE AUTENTICAÇÃO (23A), O PRIMEIRO SERVIDOR DE AUTENTICAÇÃO (23A) TRANSMITE AO TERMINAL (21) UMA IDENTIDADE DE NOVA AUTENTICAÇÃO, INCLUINDO O NOME DE DOMÍNIO EXCLUSIVO ATRIBUÍDO AO PRIMEIRO SERVIDOR DE AUTENTICAÇÃO. EM SEGUIDA, MAIS TARDE, DURANTE A NOVA AUTENTICAÇÃO, PARA PERMITIR QUE A NOVA AUTENTICAÇÃO SEJA EFETUADA PELO MESMO SERVIDOR DE AUTENTICAÇÃO (23A) QUE EFETUOU A AUTENTICAÇÃO COMPLETA ¿ OU SEJA, O PRIMEIRO SERVIDOR DE AUTENTICAÇÃO (23A) ¿ A IDENTIDADE DE NOVA AUTENTICAÇÃO É INCLUÍDA NUM PEDIDO DE NOVA AUTENTICAÇÃO.

RESUMO

MÉTODO E APARELHO DE PERMISSÃO DE NOVA AUTENTICAÇÃO NUM SISTEMA DE COMUNICAÇÃO CELULAR

Um método (e equipamento correspondente) para uma nova autenticação - após uma primeira autenticação completa por parte de um primeiro servidor de autenticação (23a) - de uma sessão de comunicação envolvendo a troca de informações entre um terminal (21) e um servidor (24), o método incluindo: uma etapa (11) na qual são atribuídos ao primeiro servidor de autenticação (23a) e a cada um dos outros servidores de autenticação (23b) um nome de domínio exclusivo respetivo; e uma etapa (13) na qual, durante a autenticação entre o terminal e o primeiro servidor de autenticação (23a), o primeiro servidor de autenticação (23a) transmite ao terminal (21) uma identidade de nova autenticação, incluindo o nome de domínio exclusivo atribuído ao primeiro servidor de autenticação. Em seguida, mais tarde, durante a nova autenticação, para permitir que a nova autenticação seja efetuada pelo mesmo servidor de autenticação (23a) que efetuou a autenticação completa - ou seja, o primeiro servidor de autenticação (23a) - a identidade de nova autenticação é incluída num pedido de nova autenticação.

DESCRIÇÃO

MÉTODO E APARELHO DE PERMISSÃO DE NOVA AUTENTICAÇÃO NUM SISTEMA DE COMUNICAÇÃO CELULAR

CAMPO TÉCNICO

A presente invenção pertence a um mecanismo de Protocolo de Autenticação Extensível (EAP - Extensible Authentication Protocol) para a autenticação e distribuição de chave de sessão num sistema de comunicação, tal como o mecanismo EAP para Autenticação e Acordo (de distribuição) de Chave (de sessão) (AKA - Authentication and (session) Key (distribution) Agreement) do Sistema Universal de Telecomunicações Móveis (UMTS - Universal Mobile Telecommunications System), e igualmente tal como o mecanismo EAP para AKA conforme implementado no Módulo de Identidade do Subscritor (SIM - Subscriber Identity Module) utilizado no Sistema Global para Comunicações Móveis (GSM - Global System for Mobile Communications). Mais particularmente, a presente invenção pertence à nova autenticação nos sistemas de comunicação que utilizam os mecanismos EAP para a autenticação SIM GSM ou AKA UMTS.

ANTECEDENTES DA TÉCNICA

O AKA baseia-se em mecanismos desafio-resposta e na criptografia simétrica, e no UMTS é conforme apresentado na TS (Technical Specification - Especificação Técnica) do 3GPP (Third Generation Partnership Program - Programa de Parceria de Terceira Geração) 33.102 V3.6.0: "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999)", *3rd Generation Partnership Project*, novembro de 2000. Habitualmente, o AKA é executado num Módulo de Identidade

do Subscritor UMTS (USIM - UMTS Subscriber Identity Module), um dispositivo tipo *smart card* (cartão inteligente). Contudo, a aplicabilidade de AKA não é limitada a dispositivos cliente com *smart cards*; por ex. os mecanismos AKA também podem ser implementados em *software* anfitrião. O AKA fornece igualmente compatibilidade com versões anteriores ao mecanismo de autenticação GSM apresentado em GSM 03.20 (ETS 300 534): "Digital cellular telecommunication system (Phase 2); Security related network functions", European Telecommunications Standards Institute, agosto de 1997. Em comparação com o mecanismo GSM, o AKA fornece comprimentos de chave substancialmente maiores e também autenticação do lado do servidor (bem como do lado do cliente).

Relativamente a um dispositivo cliente, tal como um terminal sem fios (mais especificamente, tal como uma estação móvel), para a utilização dos serviços fornecidos por um servidor, tal como um servidor num sistema de comunicação fornecido e gerido por uma operadora (ou, na realidade, os serviços de um servidor de qualquer tipo de rede, incluindo, por ex., a Internet), o terminal ou o utilizador tem, em alguns casos (para algumas redes e para alguns serviços dessas redes), de autenticar-se a si mesmo no servidor e vice-versa (o segundo, pelo menos, em algumas redes, especialmente UMTS), ou seja, cada um tem de provar ao outro que é quem afirma ser. Nas redes de acesso telefónico, LANs sem fios, redes LAN com fios e várias redes de Linha de Subscritor Digital (xDSL - Digital Subscriber Line), a operadora da rede utiliza habitualmente o que é muitas vezes designado por servidor AAA (Authentication, Authorization and Accounting - Autenticação, Autorização e Contabilidade) para autenticar um cliente e para autenticar o servidor da rede da operadora à qual o cliente endereçou um pedido de serviços

(ou para autenticar a rede da operadora independentemente de qualquer servidor específico). Um servidor AAA pode ser responsável pelo armazenamento de informações confidenciais partilhadas e outras informações de credenciais necessárias para a autenticação de utilizadores (terminais com componentes específicos de um determinado utilizador e que, como tal, identificam o mesmo), ou um servidor AAA pode utilizar um servidor de base de dados de utilizador separado para armazenar as informações de credenciais. O Protocolo de Autenticação Extensível (EAP) é frequentemente utilizado em redes que utilizam servidores AAA para a autenticação entre um servidor AAA e um terminal. Se a operadora da rede for uma operadora celular de uma rede UMTS ou GSM, o método EAP pode encapsular uma autenticação GSM e acordo de chave melhores, tal como em EAP SIM, ou uma autenticação UMTS e acordo de chave melhores, tal como em EAP AKA. O terminal troca pacotes de autenticação com um dispositivo de serviço na rede local. O dispositivo de serviço é diferente em tipos diferentes de redes, mas pode ser, por exemplo, um ponto de acesso LAN sem fios, um comutador Ethernet ou um Servidor de Acesso à Rede (NAS - Network Access Server) de acesso telefónico. Normalmente, o dispositivo de serviço funciona como o que é designado por cliente AAA, e o cliente AAA e o servidor AAA realizam a autenticação utilizando o que é designado por protocolo AAA.

No início de uma sessão de comunicação estabelecida com EAP SIM ou EAP AKA, o terminal e o servidor AAA realizam o que é aqui designado por autenticação completa, ou seja, a autenticação que começa a partir de um estado no qual nem o terminal nem o servidor AAA têm qualquer base para autenticar o outro.

Depois de estabelecida a autenticação completa, é

possível que, após algum tempo predeterminado ou no caso de ser cumprida alguma outra condição, seja necessária a nova autenticação para reduzir a probabilidade de alguém mal-intencionado ter começado a fazer-se passar pela entidade originalmente autenticada utilizando algum outro dispositivo (um dispositivo servidor ou um dispositivo cliente), ou ter de alguma forma adquirido controlo físico do dispositivo originalmente autenticado (por ex. um utilizador deixou um terminal autenticado ligado e foi-se embora) e ter começado a enviar pedidos. A nova autenticação também pode ser necessária para verificar se o terminal ainda está a utilizar os recursos de rede, conforme exigido pelas mensagens de contabilidade enviadas pela rede local. Igualmente, é possível utilizar uma nova autenticação para negociar novas chaves de segurança nos casos em que a duração das chaves é limitada por razões de segurança. A nova autenticação é idêntica em EAP SIM (para GSM) e EAP AKA (para UMTS).

O estado da técnica dos protocolos EAP SIM e EAP AKA permite a nova autenticação através da utilização das identidades de utilizador de nova autenticação separadas fornecidas a partir do servidor AAA ao terminal que está a ser novamente autenticado. A nova autenticação baseia-se nas chaves de sessão e noutras informações de contexto estabelecidas durante a autenticação completa.

Uma operadora pode implementar diversos servidores AAA numa rede para balanceamento de carga e por outras razões. Uma vez que um servidor AAA pode ser selecionado aleatoriamente para autenticar um terminal, ou pode ser selecionado através de algum mecanismo predeterminado, tal como um mecanismo circular (*round-robin*), um terminal (utilizador) pode nem sempre autenticar com o mesmo servidor AAA. Numa rede dessas, a nova autenticação torna-

se um problema, uma vez que as informações de contexto só são armazenadas no servidor AAA que efetuou a autenticação completa. Uma vez que a nova autenticação assume a disponibilidade de algumas informações fornecidas durante a autenticação completa, a mesma não irá funcionar (ou seja, não pode ser efetuada) se um pedido AAA de terminal de nova autenticação for transmitido a um servidor AAA diferente do servidor AAA que efetuou a autenticação completa.

O documento de SCHAEFER, G.; KARL, H.; FESTAG, A.: "Current Approaches to Authentication in Wireless and Mobile Communications Networks", TECHNICAL REPORT TKN-01-002, 26 de março de 2001 (26-03-2001), XP002369479, obtido a partir da Internet: URL:http://www.gallileus.info/gallileus/members/m_HolgerKarl/publications/100859230709/100859303169 [obtido a 24-02-2006] fornece uma visão geral das principais técnicas de autenticação utilizadas para redes móveis e sem fios no momento da respetiva publicação.

Deste modo, é necessária uma forma que permita que a nova autenticação funcione em redes em que um pedido de nova autenticação possa ser transmitido a um servidor AAA diferente do servidor AAA que efetuou a autenticação completa.

DIVULGAÇÃO DA INVENÇÃO

A invenção é definida através das reivindicações em anexo.

BREVE DESCRIÇÃO DAS FIGURAS

Os objetos, as características e vantagens acima e outros da invenção tornar-se-ão evidentes a partir de uma

consideração da descrição detalhada subsequente apresentada em conjunto com as figuras em anexo, em que:

a Fig. 1 é um fluxograma de um método para a nova autenticação de um terminal (com um servidor de autenticação que funciona como um agente de autenticação), de acordo com a invenção; e

a Fig. 2 é um diagrama de blocos/fluxograma de um terminal que autentica e, em seguida, autentica novamente com um servidor de autenticação, de acordo com a invenção.

MODO PREFERENCIAL DE REALIZAÇÃO DA INVENÇÃO

Esta invenção fornece uma solução para o problema de como garantir o funcionamento da nova autenticação em redes em que um pedido de nova autenticação possa ser transmitido a um servidor AAA diferente do servidor AAA que efetuou a autenticação completa. Para resolver o problema, a invenção permite selecionar como servidor AAA na nova autenticação o servidor AAA que efetuou a autenticação completa.

A invenção é descrita abaixo em conjunto com o mecanismo de Protocolo de Autenticação Extensível (EAP) para a autenticação e distribuição de chave de sessão na Autenticação e Acordo de Chave (AKA) do Sistema Universal de Telecomunicações Móveis (UMTS), conforme apresentado em 3GPP TS 33.102 V3.6.0: "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999)", *3rd Generation Partnership Project*, novembro de 2000, e no documento de rascunho IETF (Internet Engineering Task Force), "EAP AKA Authentication", draft-arkko-pppext-eap-aka-04.txt, de J. Arkko e H. Haverinen, junho de 2002. O UMTS é um padrão de

rede móvel de terceira geração global. A invenção também se destina obviamente à utilização em conjunto com os mecanismos EAP para a autenticação e distribuição de chave de sessão utilizando o Módulo de Identidade do Subscritor (SIM) do Sistema Global para Comunicações Móveis (GSM), conforme apresentado na Especificação Técnica GSM 03.20 (ETS 300 534): "Digital cellular telecommunication system (Phase 2); Security related network functions", European Telecommunications Standards Institute, agosto de 1997, e no documento de rascunho IETF, "EAP SIM Authentication", de H. Haverinen, draft-haverinen-pppext-eap-sim-05.txt, 2 de julho de 2002. Embora a invenção seja descrita em particular para a utilização com o Protocolo de Autenticação Extensível e respetivos métodos para UMTS e GSM, convém compreender que nada sobre a invenção a restringe à utilização no Protocolo de Autenticação Extensível ou nos sistemas de comunicação celular de acordo com normas UMTS ou GSM; na realidade, a invenção destina-se à utilização em qualquer sistema de comunicação que permita a autenticação de uma forma semelhante ou comparável à utilização do Protocolo de Autenticação Extensível em conjunto com protocolos AAA. A invenção no caso da forma de realização descrita utiliza o chamado EAP (Protocolo de Autenticação Extensível), conforme apresentado em RFC 2284, intitulado "PP Extensible Authentication Protocol (EAP)", publicado pelo Network Working Group do IETF. O (PPP) EAP é um protocolo geral para a autenticação; o mesmo suporta múltiplos mecanismos e autenticação.

Relativamente agora às Figs. 1 e 2, para garantir que a nova autenticação é sempre possível, a invenção fornece um método que inclui uma primeira etapa 11, na qual é atribuído a cada servidor AAA 23a, 23b (nas mesmas ou diferentes redes de operadora) um nome de domínio exclusivo, e no caso de UMTS ou GSM e autenticação para

serviços IP, corresponde a um nome de um tipo que pode ser utilizado (como uma parte, ou seja, como por ex. em utilizador@dominio, em que "dominio" corresponde ao nome de domínio exclusivo) num Identificador de Acesso à Rede (NAI - Network Access Identifier), que é o identificador (de um terminal) utilizado em protocolos AAA em conjunto com a autenticação para o acesso à rede. Em protocolos EAP e AAA estabelecidos, o pedido de autenticação inclui o Identificador de Acesso à Rede do utilizador. Em caso de autenticação completa, EAP SIM e EAP AKA especificam o formato de identidade que o terminal deverá utilizar para pedir a autenticação completa. De acordo com as especificações estabelecidas, a parte do nome de utilizador do NAI inclui o Identificador de Subscritor Móvel Internacional (IMSI - International Mobile Subscriber Identifier) ou um identificador temporário que é designado por pseudónimo nas especificações de EAP SIM e EAP AKA. O nome de domínio utilizado no NAI é habitualmente um identificador comum da operadora local. Diversos servidores AAA podem ter sido utilizados para servir pedidos que são transmitidos a este nome de domínio. Deste modo, de acordo com o estado da técnica, em geral, um nome de domínio no NAI pode ser partilhado por diversos servidores AAA. Por exemplo: os subscritores de My-Operator (A Minha Operadora) podem utilizar o nome de domínio *myoperator.com*, e as mensagens AAA serão encaminhadas para um dos servidores AAA de myoperator.com. Se o domínio indicar possivelmente um grupo de servidores AAA, trata-se da autenticação completa EAP SIM e EAP AKA. Contudo, de acordo com a invenção, será igualmente atribuído a cada servidor AAA um nome de domínio exclusivo, tal como, por exemplo, *servidorX.my-operator.com*, e estes são os nomes de domínios exclusivos que serão utilizados nas identidades de nova autenticação. Neste caso, o nome de terceiro nível *servidorX* torna o nome de domínio *servidorX.myoperator.com* num nome de domínio

exclusivo. O formato estruturado do nome de domínio pode permitir que alguns dos elementos AAA encaminhem todos os domínios que terminam com *my-operator.com* para o salto seguinte correto sem considerar qualquer nome de terceiro nível que possa ter sido necessário adicionar para tornar exclusivo um nome de domínio; por exemplo, o dispositivo de serviço 21a pode não ter necessidade de se preocupar com o nome de domínio completo e, em vez disso, pode utilizar uma regra simples: "Encaminhar **.my-operator.com* para o *proxy* AAA MyOperator" (em que o caráter * funciona como um caráter universal, ou seja, indica qualquer conjunto de carateres permitidos num nome).

Numa etapa seguinte 12, um primeiro 23a dos servidores AAA 23a, 23b recebe um pedido de um dispositivo de serviço 21a (ou seja, um cliente AAA e, em particular, por ex. um ponto de acesso de serviço) através de um servidor AAA de *proxy* 22 para a autenticação (completa) relativamente a um terminal 21, de modo a que o dispositivo de serviço 21a possa garantir o acesso do terminal 21 a uma rede 24 (tal como a Internet). A Fig. 2 não ilustra (por motivos de clareza) vários dos elementos de uma ou mais redes de operadora que permitem a comunicação sem fios entre o terminal 21 e os servidores AAA 23a, 23b (ou seja, em particular, as redes de acesso rádio para cada rede de operadora), bem como outros elementos que encaminham as comunicações para um ou outro dos servidores AAA 23a, 23b.

Numa etapa seguinte 13, o primeiro servidor AAA 23a transmite ao terminal 21 (através do servidor *proxy* 22 e do dispositivo de serviço 21a) uma identidade de nova autenticação (para a utilização pelo terminal numa nova autenticação posterior), e inclui o nome de domínio exclusivo na identidade de nova autenticação, que também inclui uma parte do nome de utilizador. A identidade de

nova autenticação é diferente da identidade baseada em IMSI e da identidade de pseudónimo que são utilizadas na autenticação completa. A etapa 13 é efetuada como parte do procedimento de autenticação completa, que inclui outras etapas que foram omitidas da Fig. 1 por motivos de clareza. A parte de nome de utilizador da identidade de nova autenticação é um nome de utilizador único escolhido pelo servidor. Pode ser um número ou um identificador escolhido aleatoriamente. Como tal, uma identidade de nova autenticação pode ser, por exemplo:

1209834387@servidor15.myoperator.com.

Numa etapa seguinte 14, para efetuar a nova autenticação (baseada habitualmente em alguma condição que foi cumprida), o terminal 21 envia um pedido de nova autenticação utilizando a identidade de nova autenticação, incluindo o nome de domínio exclusivo. Em geral, existem várias formas possíveis de iniciar a nova autenticação. Uma forma é o dispositivo de serviço 21a poder iniciar a nova autenticação. Neste caso, na LAN sem fios, em que o "pedido de nova autenticação" que é reencaminhado com base no nome de domínio exclusivo contém um pacote de resposta de identidade EAP, o dispositivo de serviço 21a envia o pacote de pedido de identidade EAP ao terminal 21, e o terminal responde com uma resposta de identidade EAP que contém a identidade de nova autenticação. Em seguida, este pacote é reencaminhado, através de um protocolo AAA, para o servidor AAA correto. Em alternativa, o próprio terminal 21 pode iniciar a nova autenticação. Na LAN sem fios, o terminal 21 envia um pacote EAPOL-Início (EAP sobre início LAN) ao dispositivo de serviço 21a. Na receção de EAPOL-Início, o dispositivo de serviço 21a emite o pacote de pedido de identidade EAP para o terminal, e a troca de nova autenticação avança conforme descrito abaixo.

Numa etapa seguinte 15, qualquer elemento de rede AAA (o dispositivo de serviço 21a, o *proxy* 22 e os servidores AAA 23a, 23b) que receba o pedido examina a identidade de nova autenticação incluída no pedido para determinar para onde encaminhar o pedido (com base na identidade de nova autenticação, que indica o primeiro servidor AAA 23a através do nome de domínio). O encaminhamento baseia-se, por exemplo, numa tabela de encaminhamento ou noutros meios de encaminhamento AAA normais, conforme apropriado. Habitualmente, o servidor *proxy* 22 examina o nome de domínio e encaminha diretamente o pedido para o primeiro servidor AAA 23a. Deste modo, o pedido é recebido mais cedo ou mais tarde pelo servidor AAA que efetuou a autenticação completa, ou seja, o primeiro servidor AAA 23a.

Numa etapa seguinte 16, o primeiro servidor AAA 23a responde ao pedido de nova autenticação através de um protocolo estabelecido para a nova autenticação. Nas etapas subsequentes 17, as comunicações subsequentes entre o terminal 21 e o primeiro servidor AAA 23a são efetuadas através de protocolos AAA estabelecidos entre o terminal 21 e o primeiro servidor AAA 23a por meio do dispositivo de serviço 21a. As comunicações subsequentes podem ser encaminhadas diretamente entre o dispositivo de serviço 21a e o primeiro servidor AAA 23a ou podem ser encaminhadas através dos elementos AAA intermédios. Os protocolos AAA estabelecidos incluem habitualmente meios para garantir que o servidor AAA 23a que efetua a autenticação não muda durante uma troca de autenticação.

Em alguns casos, o terminal 21 pode ter comunicação através de diversas sessões diferentes em simultâneo, utilizando o procedimento de autenticação completa para cada sessão. As sessões podem ser autenticadas pelo mesmo servidor AAA ou por diferentes servidores AAA, e podem

utilizar as mesmas ou diferentes tecnologias de rádio e as mesmas ou diferentes aplicações para efetuar a autenticação. De acordo com a invenção, para adaptar essa variabilidade, o terminal 21 mantém informações de estado separadas para cada uma dessas sessões, e o terminal 21 pode depois efetuar a nova autenticação separadamente para cada uma dessas sessões, conforme descrito relativamente à Fig. 1. Em conformidade, cada servidor AAA 23a, 23b utilizado na autenticação para uma ou mais sessões simultâneas mantém informações de estado separadas para cada sessão dessas.

Note que, embora a invenção esteja relacionada com a autenticação de LAN sem fios, a mesma é igualmente relevante para xDSL, acesso telefónico, Ethernet e outros contextos de autenticação. Os métodos de Protocolo de Autenticação Extensível para autenticação UMTS e GSM são orientados para operadoras móveis que pretendem administrar WLANs ou outras redes de acesso complementares; é possível que a invenção nunca seja utilizada em redes UMTS ou GSM reais.

Convém compreender que as disposições descritas acima são apenas ilustrativas da aplicação dos princípios da presente invenção. Os peritos na técnica podem inventar diversas modificações e disposições alternativas sem sair do âmbito da presente invenção, e as reivindicações em anexo pretendem abranger essas modificações e disposições.

DOCUMENTOS REFERIDOS NA DESCRIÇÃO

Esta lista de documentos referidos pelo autor do presente pedido de patente foi elaborada apenas para informação do leitor. Não é parte integrante do documento de patente europeia. Não obstante o cuidado na sua elaboração, o IEP não assume qualquer responsabilidade por eventuais erros ou omissões.

Literatura não relacionada com patentes referida na descrição

- Technical Specification Group Services and System Aspects; 3G Security; Security Architecture. *3GPP (Third Generation Partnership Program) TS (Technical Specification) 33.102 V3.6.0,* 1999 **[0002]**
- *3rd Generation Partnership Project,* November 2000 **[0002]**
- Digital cellular telecommunication system (Phase 2); Security related network functions. GSM 03.20 (ETS 300 534. European Telecommunications Standards, Institute, August 1997 **[0002]**
- **SCHAEFER, G. ; KARL, H. ; FESTAG, A.** Current Approaches to Authentication in Wireless and Mobile Communications Networks. *TECHNICAL REPORT TKN-01-002,* 26 March 2001 **[0008]**
- Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999. *3GPP TS 33.102 V3.6.0,* 1999 **[0013]**
- **J. ARKKO ; H. HAVERINEN.** EAP AKA Authentication. *IETF,* June 2002, draft-arkko-pppext- eap-aka-04.txt **[0013]**
- **H. HAVERINEN.** EAP SIM Authentication. *IETF,* 02 July 2002, draft-haverinen-pppext-eap-sim-05.txt **[0013]**
- PPP Extensible Authentication Protocol (EAP. RFC 2284. Network Working Group of the IETF **[0013]**

Lisboa, 21 de Abril de 2014

REIVINDICAÇÕES

1. Um método para a utilização na nova autenticação de uma sessão de comunicação,

o método caracterizado por envolver a troca de informações entre um terminal (21) e um elemento de rede de autenticação (24) através de uma rede de autenticação (28), na qual são utilizados um primeiro servidor de autenticação (23a) e outros servidores de autenticação (23b) e é atribuído a cada um deles um nome de domínio exclusivo respetivo que identifica exclusivamente o servidor de autenticação respetivo,

a sessão de comunicação tendo já sido autenticada pelo terminal (21) e um primeiro servidor de autenticação (23a) da rede de autenticação (28) através de:

uma etapa (12), na qual o primeiro servidor de autenticação (23a) recebe um pedido de autenticação do terminal (21); e

uma etapa (13), na qual durante a autenticação entre o terminal e o primeiro servidor de autenticação (23a), o primeiro servidor de autenticação (23a) transmite ao terminal (21) uma identidade de nova autenticação, incluindo o nome de domínio exclusivo atribuído ao primeiro servidor de autenticação;

a nova autenticação compreendendo

uma etapa (14) na qual, para efetuar uma nova autenticação, um elemento de rede de autenticação (21a, 22, 23a, 23b) recebe um pedido de nova autenticação transmitido pelo terminal (21) utilizando a identidade de nova autenticação, incluindo o nome de

domínio exclusivo; e

uma etapa (15) na qual o elemento de rede de autenticação (21a, 22, 23a, 23b) determina, a partir da identidade de nova autenticação incluída no pedido, o nome de domínio exclusivo que indica o servidor de autenticação (23a) que efetuou a autenticação completa.

2. O método de acordo com a reivindicação 1, **caracterizado ainda por:**

uma etapa (15) na qual um elemento de autenticação de rede (21a, 22, 23b) reencaminha o pedido para o servidor de autenticação (23a) indicado pelo nome de domínio exclusivo incluído como parte da identidade de nova autenticação; e

uma etapa (16, 17) na qual o terminal (21) e o primeiro servidor de autenticação (23a) efetua a nova autenticação.

3. Um método para a utilização por um servidor de autenticação, caracterizado por compreender:

a transmissão a um terminal que pede a autenticação de uma identidade de nova autenticação, incluindo um nome de domínio exclusivo que identifica exclusivamente o servidor de autenticação numa rede de autenticação na qual são utilizados diversos servidores de autenticação;

a receção de um pedido de nova autenticação proveniente de outro terminal, o pedido de nova autenticação incluindo outra identidade de nova autenticação, incluindo outro nome de domínio exclusivo que identifica exclusivamente outro servidor de autenticação; e

o encaminhamento do pedido de nova autenticação de acordo com o nome de domínio exclusivo incluído no pedido de nova autenticação.

4. Um método para a utilização por um terminal, caracterizado por compreender:

a receção a partir de um primeiro servidor de autenticação de uma identidade de nova autenticação gerada durante uma primeira autenticação, a identidade de nova autenticação incluindo um nome de domínio exclusivo que identifica exclusivamente o primeiro servidor de autenticação numa rede de autenticação, na qual são utilizados diversos servidores de autenticação; e

a transmissão a um elemento de rede de autenticação diferente do primeiro servidor de autenticação de um pedido de nova autenticação utilizando a identidade de nova autenticação, incluindo o nome de domínio exclusivo que identifica exclusivamente o primeiro servidor de autenticação.

5. O método de acordo com a reivindicação 4, caracterizado por a transmissão do pedido de nova autenticação compreender a inclusão da identidade de nova autenticação num pacote de resposta de identidade de acordo com um Protocolo de Autenticação Extensível.

6. Um servidor de autenticação (23a, 23b) num sistema de comunicação celular compreendendo:

meios (13) para transmitir a um terminal (21) uma identidade de nova autenticação, incluindo um nome de domínio exclusivo que identifica exclusivamente o servidor de autenticação numa rede de autenticação na qual são utilizados diversos servidores de autenticação;

meios para a nova autenticação de uma sessão de comunicação entre um terminal (21) e um servidor de

conteúdo (25), o servidor de autenticação sendo (23a, 23b) **caracterizado por:**

meios (15) para receber um pedido de nova autenticação utilizando outra identidade de nova autenticação que identifica exclusivamente outro servidor de autenticação e para determinar a partir da outra identidade de nova autenticação o nome de domínio exclusivo do outro servidor de autenticação, e meios (16) para reencaminhar o pedido de nova autenticação para o outro servidor de autenticação (23a) indicado pelo nome de domínio exclusivo do outro servidor de autenticação incluído como parte da outra identidade de nova autenticação.

7. Um terminal configurado para pedir a nova autenticação de uma sessão de comunicação entre o terminal e um servidor de conteúdo, **caracterizado por:**

ser configurado para receber a partir de um primeiro servidor de autenticação uma identidade de nova autenticação gerada durante uma primeira autenticação, a identidade de nova autenticação incluindo um nome de domínio que indica exclusivamente o primeiro servidor de autenticação numa rede de autenticação, na qual são utilizados diversos servidores de autenticação; e

ser configurado para transmitir a um elemento de rede de autenticação um pedido de nova autenticação utilizando a identidade de nova autenticação incluindo o nome de domínio exclusivo.

8. Um terminal de acordo com a reivindicação 7, caracterizado por ser configurado para transmitir a um elemento de rede de autenticação um pedido de nova

autenticação utilizando a identidade de nova autenticação, incluindo o nome de domínio exclusivo que inclui a identidade de nova autenticação num pacote de resposta de identidade de acordo com um Protocolo de Autenticação Extensível.

9. Um produto de programa de computador compreendendo:

uma estrutura de armazenamento legível por computador que inclui um código de programa de computador na mesma para a execução através de um processador de computador num servidor de autenticação (23a), com o referido código de programa de computador **caracterizado por** incluir instruções para implementar um aparelho de acordo com a reivindicação 6.

10. Um produto de programa de computador compreendendo:

uma estrutura de armazenamento legível por computador que inclui um código de programa de computador na mesma para a execução através de um processador de computador num servidor de autenticação (23a), com o referido código de programa de computador **caracterizado por** incluir instruções para efetuar todas as etapas do método de acordo com a reivindicação 3.

11. Um produto de programa de computador compreendendo:

uma estrutura de armazenamento legível por computador que inclui um código de programa de computador na mesma para a execução através de um processador de computador, com o referido código de programa de computador **caracterizado por** incluir instruções para implementar um aparelho de acordo com a reivindicação 7.

12. Um sistema incluindo uma diversidade de terminais (21), uma diversidade de servidores de autenticação (23a, 23b) e, pelo menos, um servidor de conteúdo (24), em que os terminais (21) funcionam de modo a pedir conteúdo ao servidor de conteúdo (24) após a autenticação e a nova autenticação com um ou outro dos servidores de autenticação (23a, 23b), o sistema **caracterizado por**, pelo menos, dois dos servidores de autenticação (23a, 23b) estarem de acordo com a reivindicação 6.

Lisboa, 21 de Abril de 2014

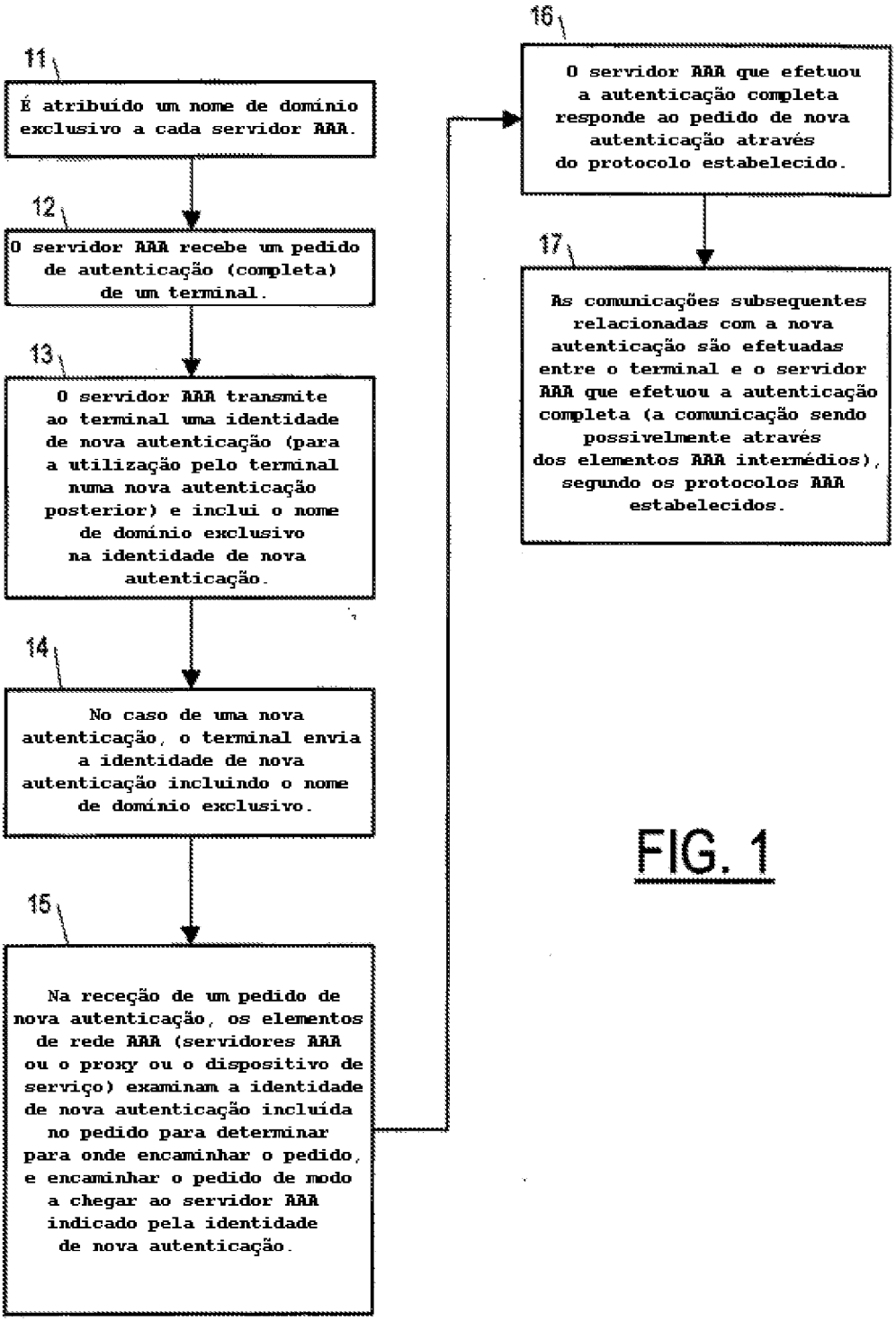
11
É atribuído um nome de domínio exclusivo a cada servidor AAA.
12
O servidor AAA recebe um pedido de autenticação (completa) de um terminal.
13
O servidor AAA transmite ao terminal uma identidade de nova autenticação (para a utilização pelo terminal numa nova autenticação posterior) e inclui o nome de domínio exclusivo na identidade de nova autenticação.
14
No caso de uma nova autenticação, o terminal envia a identidade de nova autenticação incluindo o nome de domínio exclusivo.
15
Na receção de um pedido de nova autenticação, os elementos de rede AAA (servidores AAA ou o proxy ou o dispositivo de serviço) examinam a identidade de nova autenticação incluída no pedido para determinar para onde encaminhar o pedido, e encaminhar o pedido de modo a chegar ao servidor AAA indicado pela identidade de nova autenticação.
16
O servidor AAA que efetuou a autenticação completa responde ao pedido de nova autenticação através do protocolo estabelecido.
17
As comunicações subsequentes relacionadas com a nova autenticação são efetuadas entre o terminal e o servidor AAA que efetuou a autenticação completa (a comunicação sendo possivelmente através dos elementos AAA intermédios), segundo os protocolos AAA estabelecidos.

FIG. 1

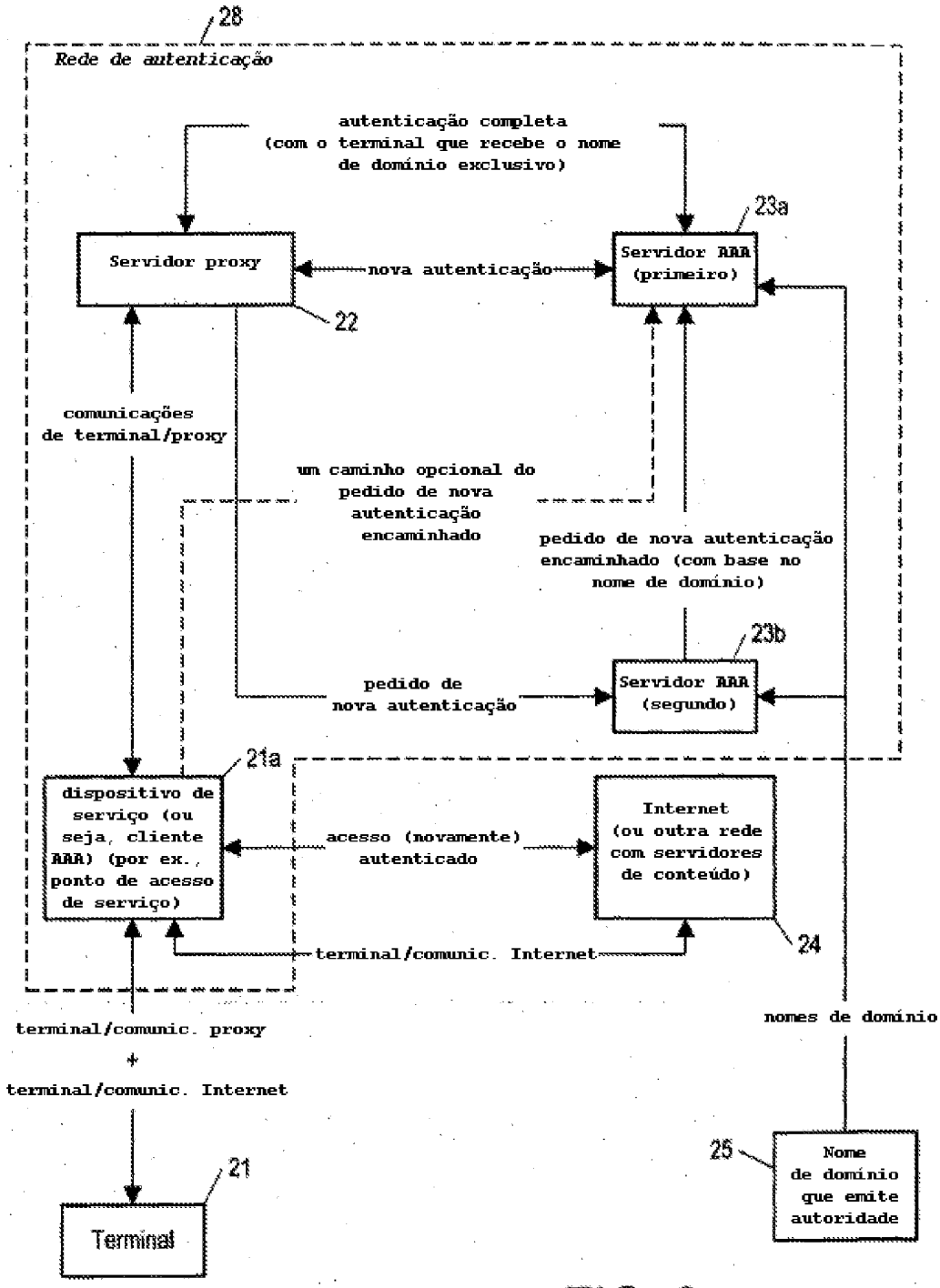
28
Rede de autenticação
autenticação completa
(com o terminal que recebe o nome
de domínio exclusivo)
23a
Servidor proxy
nova autenticação
Servidor AAA
(primeiro)
22
comunicações
de terminal/proxy
um caminho opcional do
pedido de nova
autenticação
encaminhado
pedido de nova autenticação
encaminhado (com base no
nome de domínio)
23b
pedido de
nova autenticação
Servidor AAA
(segundo)
21a
dispositivo de
serviço (ou
seja, cliente
AAA) (por ex.,
ponto de acesso
de serviço)
acesso (novamente)
autenticado
Internet
(ou outra rede
com servidores
de conteúdo)
terminal/comunic. Internet
24
terminal/comunic. proxy
+
terminal/comunic. Internet
nomes de domínio
25
Nome
de domínio
que emite
autoridade
21
Terminal

FIG. 2