(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 467 666**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/08 (2009.01)
H04L 9/32 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.11.2008 E 08854914 (2)**

(97) Fecha y número de publicación de la concesión europea: **30.04.2014 EP 2215803**

(54) Título: **Autenticación del acceso a una red**

(30) Prioridad:

27.11.2007 FI 20075844

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.06.2014

(73) Titular/es:

TELIASONERA AB (100.0%)
Stureplan 8
10663 STOCKHOLM, SE

(72) Inventor/es:

KORHONEN, JOUNI

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Autenticación del acceso a una red

CAMPO DE LA INVENCIÓN

La presente invención se refiere a la tecnología de comunicaciones, y más en particular a la autenticación del acceso a una red.

ANTECEDENTES DE LA INVENCIÓN

Diferentes servicios multimedia de tercera generación 3G tienen la capacidad de utilizar la arquitectura genérica de arranque GBA (generic bootstrapping architecture) proporcionada por el proyecto de asociación de tercera generación 3GPP, y que se basa a en el protocolo de autenticación y gestión de claves AKA (authentication and key agreement) para distribuir certificados de abonado. Estos certificados son utilizados por los operadores móviles para autenticar a un abonado antes de que acceda a las aplicaciones y los servicios multimedia sobre un protocolo de transferencia de hipertexto HTTP. Los servicios y las aplicaciones incluyen presencia (tal como un sistema de mensajería instantánea), conferencia de video, mensajería, difusión de video, una aplicación de pulsar para hablar, etc., y son ofrecidos por operadores IMS (subsistema multimedia de protocolo de internet, IP). Una infraestructura de la arquitectura genérica de arranque permite asimismo una función de aplicación en la red y en el lado del usuario para utilizar claves compartidas. La arquitectura GBA ha sido mejorada mediante la implementación de una arquitectura genérica de autenticación GAA (generic authentication architecture) para proporcionar acceso seguro sobre HTTP utilizando la seguridad de la capa de transporte TLS (transport layer security). GAA describe una arquitectura genérica para autenticación de pares que puede servir a priori para cualquier aplicación presente y futura. GAA se puede describir asimismo como una infraestructura de autenticación con un modelo de referencia de autenticación que vincula entre sí GBA, mecanismos de seguridad, características basadas en secretos compartidos y en certificados, y características funcionales.

Sin embargo, actualmente no es posible tener autenticación de acceso para un usuario que utiliza un equipo de usuario que comunica en una primera red de comunicaciones que admite un primer tipo de identificación, en una segunda red de comunicaciones que admite un segundo tipo de identificación, con el primer tipo de identificación. Esto causa problemas, por ejemplo, en la gestión de la red.

El documento Huang C-M y otros: "Authentication mechanism over the integrated UMTS network and WLAN platform using the cross-layer bootstrap", 20071004, volumen 1, número 5, 4 de octubre de 2007 (04/10/2009), páginas 866-874, describe un mecanismo de autenticación sobre el mecanismo de integración de acoplamiento separado utilizando un arranque multicapa. El documento describe una descripción de protocolos, un análisis de seguridad y un análisis de costes del mismo.

El documento de Olkkonen, Timo: "Generic Authentication Procedure", 12 de diciembre de 2006 (12/12/2006, páginas 1 a 5, XP002610576) describe la arquitectura para el procedimiento de autenticación genérico, el soporte para certificados de abonado y las diferencias entre el arranque 3G y 2G.

BREVE DESCRIPCIÓN DE LA INVENCIÓN

Por lo tanto, un objetivo de la presente invención es dar a conocer un método y un aparato para implementar el método de manera que resuelvan el problema mencionado. Los objetivos de la invención se consiguen mediante un método y un dispositivo que están caracterizados por lo indicado en las reivindicaciones independientes. Se dan a conocer realizaciones preferidas de la invención en las reivindicaciones dependientes.

La invención está basada en la idea de proporcionar autenticación a un sistema que no utiliza un identificador con el que se ha identificado inicialmente el equipo de usuario. Por ejemplo, puede realizarse una autenticación SIM (módulo de autenticación de abonado) en un entorno que no utilice un identificador SIM.

Una ventaja del método y el dispositivo de la invención es que la gestión de la red de sistemas diferentes se hace más sencilla y más eficiente, por ejemplo, porque ahorra recursos del sistema y porque no requiere realizar modificaciones al sistema o sistemas actuales.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación, se describirá en detalle la invención mediante realizaciones preferidas y haciendo referencia a los dibujos adjuntos, en los cuales

la figura 1 muestra una arquitectura de autenticación y servicio, según la invención y sus realizaciones.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

A continuación, la invención y sus realizaciones se describirán principalmente en relación con dos sistemas de comunicaciones y con dos redes de acceso. Se describirán asimismo en relación con dos diferentes maneras de acceder a una red central. Sin embargo, la invención y sus realizaciones no están limitadas al número de sistemas de comunicaciones, o de redes de acceso, o de maneras de realizar el acceso. Asimismo, en relación con la invención, el funcionamiento y la estructura de los sistemas de comunicaciones y de las redes de acceso se describen solamente de la medida en que ayudan a la comprensión de la invención y de sus realizaciones. La invención y sus realizaciones no son específicas de los sistemas de comunicaciones y redes de acceso particulares, sino que se apreciará que la invención y sus realizaciones tienen aplicación en muchos tipos de sistemas y pueden aplicarse, por ejemplo, a un dominio de conmutación de circuitos, por ejemplo, en un sistema de comunicación celular digital GSM (Global System for Mobile Communications, sistema global de comunicaciones móviles), en un dominio de conmutación de paquetes, por ejemplo en el sistema UMTS (Universal Mobile Telecommunications System, sistema universal de telecomunicaciones móviles), y, por ejemplo, en redes según los estándares IEEE 802.11: WLAN (Wireless Local Area networks, redes inalámbricas de área local), HomeRF (Radio Frequency, radiofrecuencia) o especificaciones (HIPERLAN1 y 2, HIPERACCESS) de BRAN (Broadband Radio Access Networks, redes de acceso radio de banda ancha). La invención y sus realizaciones pueden aplicarse asimismo a un sistema de red heredado, que describe una red que no está basada en el protocolo IP (protocolo de internet) o el protocolo TCP/IP (protocolo de control de transmisión/protocolo de internet). Ejemplos de redes heredadas incluyen cualquier red de acceso IP que no sea capaz de proporcionar autenticación de acceso de red basado en (U)SIM (UMTS Subscriber Identity Module, módulo de identidad de abonado UMTS), como parte de un procedimiento natural de autenticación de acceso. Éstas incluyen las redes IPX (Internet Packet Exchange, intercambio de paquetes de internet), SNA, Appletalk y DECnet. Una realización es una red de acceso WLAN sin ninguna clase de soporte de EAP (Extensible Authentication Protocol, protocolo de autenticación extensible), tal como un punto de acceso basado en acceso web. La invención y sus realizaciones se pueden aplicar asimismo a sistemas de comunicaciones ad hoc que proporcionan acceso IP, tales como una red IrDA (Infrared Data Association, asociación de datos por infrarrojos) o una red Bluetooth. En otras palabras, los principios básicos de la invención se pueden utilizar para permitir autenticación entre y/o dentro de cualesquiera sistemas de comunicaciones móviles de la segunda, 2,5-ésima, tercera y cuarta generaciones, tales como GSM, GPRS (General Packet Radio Service, servicio general de radiocomunicaciones por paquetes), TETRA (Terrestrial Trunked Radio, sistema radioeléctrico terrestre con concentración de enlaces), sistemas UMTS y sistemas HSPA (High Speed Packet Access, acceso a paquetes de alta velocidad), por ejemplo en tecnología WCDMA (Wideband Code Division Multiple Access, acceso múltiple por división de código de banda ancha). La presente invención es aplicable a cualquier terminal, servidor, componente correspondiente y/o a cualquier sistema de comunicaciones o cualquier combinación de diferentes sistemas de comunicaciones.

Los protocolos utilizados, las especificaciones de sistemas de comunicaciones, los servidores y los terminales de usuario, especialmente en comunicaciones inalámbricas, se desarrollan rápidamente. Dicho desarrollo puede requerir cambios extra en una realización. Por lo tanto, todas las palabras y expresiones utilizadas deberán interpretarse en sentido amplio y están previstas para ilustrar, no para limitar, la invención.

La figura 1 muestra una arquitectura de autenticación y servicio, según la invención y sus realizaciones. El elemento, un aparato 1-2, puede ser un terminal de usuario que es una pieza de un equipo o un dispositivo que asocia, o está dispuesto para asociar, el terminal de usuario y su usuario con un abono, y que permite al usuario interactuar con un sistema de comunicaciones. El terminal de usuario presenta información al usuario y permite a éste introducir información. En otras palabras, el terminal de usuario puede ser cualquier terminal capaz de recibir información de la red y/o capaz de transmitir información a la red, y se puede conectar a la red de diferentes maneras, por ejemplo de manera inalámbrica o a través de una conexión fija. Ejemplos de un terminal de usuario incluyen un ordenador personal, una consola de juegos, un portátil (un cuaderno electrónico), un asistente digital personal, una estación móvil (un teléfono móvil), un comunicador y un teléfono de línea.

El elemento 1-2, que puede ser apto para la GAA, puede comprender medios de procesamiento o medios para aplicar, por ejemplo, por lo menos uno de los servicios siguientes, aplicaciones o mensajes: presencia, videoconferencia, mensajería, difusión de video, pulsar para hablar, mensajes cortos, mensajes instantáneos, mensajes de correo electrónico, mensajes multimedia, mensajes de mensajería unificada, mensajes WAP (Wireless Application Protocol, protocolo de aplicación inalámbrica) o mensajes SIP (Session Initiation Protocol, protocolo de inicio de sesiones). La estación móvil, o el dispositivo, pueden ser asimismo una estación móvil o un dispositivo equipados, por ejemplo, con un servicio o una aplicación de presencia, de videoconferencia, de mensajería, de difusión de video, de pulsar para hablar, de mensajes instantáneos, de mensajes de correo electrónico, de mensajes multimedia, de mensajes de mensajería unificada, de mensajes WAP o de mensajes SIP, y servicios y aplicaciones tales como llamadas de voz, navegación inalámbrica por internet y difusión web.

Los aparatos, tales como servidores, o componentes de servidores correspondientes, terminales de usuario y/u otros dispositivos o aparatos correspondientes que implementan la funcionalidad de un aparato correspondiente descrito con una realización, comprenden no solamente medios de la técnica anterior, sino asimismo medios para autenticar el equipo. De manera más precisa, estos comprenden medios para implementar una funcionalidad de un aparato correspondiente descrito con una realización, y pueden comprender medios separables para cada función independiente, o medios que se pueden configurar para llevar a cabo dos o más funciones. Los presentes aparatos comprenden procesadores y memoria que se pueden utilizar en una realización. Por ejemplo, una unidad de servidor AAA (autenticación, autorización y contabilización) 1-4 y/o las unidades de servidor intermediario 1-10 y 1-12 pueden ser una aplicación de soporte lógico, un módulo, o una unidad configurada como una operación aritmética, o como un programa, ejecutado mediante un procesador de operaciones. Todas las modificaciones y configuraciones necesarias para implementar una funcionalidad de una realización se pueden llevar a cabo como rutinas, que se pueden implementar como rutinas de soporte lógico añadidas o actualizadas, circuitos de aplicación (ASIC, circuito integrado de aplicación específica) y/o circuitos programables. Las rutinas de soporte lógico, denominadas asimismo productos de programa, que incluyen miniaplicaciones y macros, se pueden almacenar en cualquier medio de almacenamiento de datos legible por un aparato, e incluyen instrucciones de programa para llevar a cabo tareas particulares. Las rutinas de soporte lógico se pueden descargar a un aparato. El aparato, tal como un servidor, un componente de servidor correspondiente, o un terminal de usuario se pueden configurar como un ordenador que incluye por lo menos una memoria para proporcionar un área de almacenamiento utilizada para operaciones aritméticas, y un procesador de operaciones para ejecutar la operación aritmética. Un ejemplo del procesador de operaciones incluye una unidad central de procesamiento. La memoria puede ser memoria extraíble acoplada de manera desmontable al aparato.

Las etapas/puntos, mensajes de señalización y funciones relacionadas descritas en la figura 1 no están en modo alguno en orden cronológico, y algunas de las etapas/puntos se pueden realizar de manera simultánea o en cualquier orden que difiera del proporcionado. Se pueden ejecutar asimismo otras funciones entre las etapas/puntos o dentro de las etapas/puntos, y se pueden enviar otros mensajes de señalización entre los mensajes mostrados. Algunas de las etapas/puntos o parte de las etapas/puntos pueden asimismo descartarse o sustituirse por una etapa/punto correspondiente, o por parte de la etapa/punto. Las operaciones del servidor muestran un procedimiento que se puede implementar en una o varias entidades físicas o lógicas. Los mensajes de señalización son solamente a modo de ejemplo y pueden comprender asimismo varios mensajes independientes para transmitir la misma información. Además, los mensajes pueden contener otra información.

Según la figura 1, el equipo de usuario puede comunicar 1 con el servidor 1-4 AAA (autenticación, autorización y contabilización), que tiene una función de servidor de arranque BSF (bootstrapping server function). El servidor 1-4 puede estar en comunicación 2 con una base de datos HSS 1-6 (home subscriber server, servidor de abonados propio), que está dispuesta para que el equipo de usuario mantenga información asociada con el equipo de usuario. Un elemento 1-8 describe un elemento de control de acceso AC y un servidor web, por ejemplo, un servidor de internet. El elemento AC se puede describir como una pasarela 3, 10 entre una red IP, tal como internet, y el equipo de usuario inalámbrico 1-2, que puede estar acoplado, por ejemplo, a una red inalámbrica de área local.

El servidor 1-8 está en comunicación con un servidor intermediario de itinerancia AAA visitado 1-10. El servidor intermediario transporta mensajes de comunicaciones desde un operador visitado, tal como un operador WLAN visitado, a un operador propio, tal como un operador WLAN propio, y viceversa. El servidor intermediario de itinerancia AAA visitado 1-10 está en comunicación con un servidor intermediario de itinerancia AAA propio 1-12. El servidor intermediario propio proporciona un punto de tráfico controlado hacia y desde una red propia 1-30.

El servidor intermediario de itinerancia AAA propio 1-12 puede funcionar asimismo como un elemento de función de aplicación de red NAF (network application function) de una arquitectura general de arranque GBA. El elemento NAF 1-14 puede recibir desde, y comunicar 6, 7 de manera segura con la función BSF del abonado.

Los servidores intermediarios y la función BSF pueden estar adaptados a la capacidad NAF. Esto significa que pueden comunicar con una funcionalidad y protocolo NAF. Diferentes elementos de la figura 1 pueden tener asimismo capacidades para sistemas de comunicaciones diferentes, tal como se ha descrito anteriormente.

Un área 1-16 que cubre el servidor 1-8 y el servidor intermediario 1-10 describe una red visitada. Debe observarse que, de acuerdo con la invención y sus realizaciones, ésta no tienen que ser alterada o modificada. Ésta puede ser accedida de acuerdo con una lógica de acceso basada en web, de la red visitada.

El elemento 1-18 describe una función de aplicación de red en relación con una red de comunicaciones 1-20. El usuario puede acceder a diferentes servicios, proveedores de servicio, pasarelas, redes de acceso u otras redes, a través y/o mediante la red 1-20. El número de referencia puede describir asimismo servicios a los que el usuario desea acceder.

Los elementos HSS, BSF y NAF pueden formar parte de la arquitectura GAA y/o GBA. Estos pueden definirse perteneciendo a la red propia. La red propia puede incluir asimismo otros elementos no mostrados en la figura 1. Algunos elementos de la red propia de la figura 1 pueden estar situados asimismo fuera de la red propia. Por ejemplo, la función NAF puede ser cualquier elemento de servicio que proporcione la función NAF. Ésta puede estar situada en la red propia, en la red visitada o incluso fuera de la red del operador. Puede decirse que la red propia es la red central de un operador.

En la figura 1 se muestra una posibilidad de funcionamiento de la arquitectura de autenticación y servicio. En la etapa 1, el equipo de usuario puede llevar a cabo señalización de arranque GBA utilizando una función de servidor de arranque. Esta función puede ser, por ejemplo, una función de autenticación y gestión de claves AKA o una autenticación de módulo de identidad de abonado SIM, tal como HTTP-Digest-AKA (HTTP, protocolo de transferencia de hipertexto) o UMTS-AKA. Esta función se puede llevar a cabo periódicamente y/o en respuesta a un evento de activación y/o a petición. El periodo puede ser, por ejemplo, de uno o varios minutos, horas, días o meses. La petición puede realizarse en el lado GPRS de la red, mediante una interfaz Ub. En la etapa 2, el elemento BSF puede comprobar el perfil de un usuario de un UE en comunicación con el elemento de base de datos 1-6. Asimismo, puede llevar a cabo la autenticación con la base de datos HSS a través de una interfaz Zh.

A continuación, la función BSF tiene conocimiento de la existencia del equipo de usuario, y la BSF puede proporcionar una identificación temporal o fija, y/o un numero aleatorio para la identificación del usuario. Si este material de claves es para uso temporal, puede tener una cierta vida útil después de la cual la clave ya no se puede utilizar más. El identificador señalizado al equipo de usuario puede comprender una o varias partes, por ejemplo, una primera parte y una segunda parte.

Tal como se describe a continuación, la primera parte del identificador puede ser un secreto compartido que sirve como una contraseña conocida para el equipo de usuario 1-2 y para la base de datos 1-6. La segunda parte del identificador se puede utilizar para designar e indexar la primera parte del identificador. Además, el valor de la primera parte y/o de la segunda parte del identificador pueden ser local o globalmente únicos.

Después de las etapas 1 y 2, el equipo de usuario y la red de comunicaciones son autenticados. El equipo de usuario conoce un identificador B-TID y alguna información que ha sido utilizada cuando se ha obtenido el B-TID en la BSF. Esto tiene como resultado un secreto compartido KS, una cadena de texto que puede servir como una contraseña que es conocida por el equipo de usuario y por la BSF de la red. Además, el equipo de usuario y la red saben que el identificador, tal como B-TID, se puede utilizar posteriormente para designar e indexar el secreto compartido.

El identificador o parte del mismo pueden obtenerse mediante diferentes métodos criptográficos, y el identificador o parte del mismo pueden además modificarse, por ejemplo, de tal modo que no sean legibles. El valor del identificador puede ser local y/o globalmente único y su forma puede ser, por ejemplo, "BASE64_Encoded(RAND)@FQDN", donde RAND puede ser un numero aleatorio generado mediante el elemento HSS. FQDN es un nombre DNS (domain name server, servidor de nombres de dominio) de la función BSF que ha llevado a cabo la autenticación. El identificador B-TID puede ser un identificador NAI. Se puede decir que la arquitectura GPA genera la autenticación y/o el reconocimiento entre la red propia 1-30 y el equipo de usuario 1-2.

En la etapa 3, que es la siguiente, en relación con la autenticación para la red visitada, el equipo de usuario transfiere un nombre de usuario y una contraseña que ha recibido desde el servidor AAA propio al elemento AC y al servidor web. La autenticación puede ser, por ejemplo, una autenticación basada en internet o una autenticación de acceso de red heredada. El nombre de usuario puede ser el identificador B-TID y la contraseña puede obtenerse a partir del secreto compartido KS. A continuación, la contraseña se puede denominar una KS-Legacy-PWD.

Después de esto, en la etapa 4, un sistema de autenticación de la red visitada 1-16 puede encaminar la autenticación de acuerdo con un encaminamiento AAA a su servidor intermediario de itinerancia AAA. En este proceso, una parte REALM, es decir @FQDN, del identificador B-TID se puede utilizar para direccionar el mensaje.

En la etapa 5, el servidor intermediario de itinerancia de la red visitada pueden caminar un mensaje AAA al servidor intermediario AAA de la red propia. El REALM del identificador B-TID se puede utilizar en este encaminamiento. En esta etapa, se puede utilizar una itinerancia AAA existente, que puede ser la misma que la que existe para una itinerancia WLAN (red inalámbrica local). El identificador B-TID puede estar en un atributo Username (nombre de usuario) en el protocolo AAA y en un atributo Password (contraseña) en la KS-Legacy-PWD.

El servidor intermediario de itinerancia AAA de la red propia puede ser el mismo que la función NAF del elemento GBA, y el servidor intermediario puede comparar y/o comprobar y/o conocer que el mensaje es conforme con la itinerancia AAA.

El servidor intermediario propio 1-12 sabe a continuación que la función de arranque existe, y el servidor intermediario transmite un mensaje al elemento BSF en base a la funcionalidad GBA, indicando si el equipo de usuario existe.

En la etapa 6, el servidor intermediario de itinerancia AAA y el elemento NAF realizan una pregunta a la función BSF del servidor AAA. Esta pregunta puede ser conforme al elemento GBA, y puede realizarse sobre la interfaz Zn. El valor del identificador B-TID se puede utilizar para indexación KS en la función BSF. La función BSF puede comprobar en el perfil del usuario si se permite itinerancia desde un operador o servidor intermediario a otro operador o servidor intermediario, por ejemplo itinerancia heredada. Ésta puede comprobar asimismo otras funciones. La función BSF puede asumir entonces que la autenticación en cuestión es autenticación heredada sobre la itinerancia AAA. Esto puede realizarse, por ejemplo, de tal modo que el elemento NAF transporta la información en uno o varios atributos añadidos a la interfaz Zn.

La BSF puede generar una nueva clave para la función NAF. La función NAF no tiene por qué saber de dónde procede la clave o el identificador, y cómo se ha realizado la clave o el identificador.

En otras palabras, el servidor intermediario propio y la función NAF reciben el identificador que comprende una primera parte y una segunda parte, recuperan, utilizando la primera parte, una segunda parte correspondiente a partir de la base de datos HSS, comparan la segunda parte recibida con la segunda parte correspondiente recuperada, y si son iguales, proporcionan al equipo de usuario 1-2 autenticación de acceso a la segunda red de comunicaciones 1-16, 1-20.

En la etapa 7, el elemento BSF devuelve la información de perfil sobre el usuario. Éste puede devolver asimismo el secreto compartido. La NAF y los servidores intermediarios de itinerancia AAA pueden comprobar si coinciden la contraseña obtenida a partir de la itinerancia AAA entre los operadores o los servidores intermediarios, y la contraseña devuelta por el elemento BSF. Si coinciden, se transfiere una aceptación, por ejemplo, a un servicio, a un proveedor de servicio o a una red siguiente 1-20. Por otra parte, si no coinciden, se deniega el acceso.

En la etapa 8, se transmite una respuesta AAA sobre una conexión de itinerancia, de vuelta a la red visitada, sobre la conexión de itinerancia AAA. En la etapa 9, la respuesta AAA y otra posible información son transmitidas a un controlador de acceso. En la etapa 10, pueden ser transmitidas una respuesta y otra información posible al equipo de usuario y, en la etapa 11, puede abrirse una conexión a la red de comunicaciones si ha sido aceptada la autenticación del equipo de usuario.

El estándar GAA, TS33.220 arquitectura de autenticación genérica de 3GPP, permite establecer el secreto compartido entre el equipo de usuario, el terminal de usuario y el servidor de función de arranque BSF de la red. Esto puede llevarse a cabo, por ejemplo, utilizando el algoritmo AKA o SIM TS33.920. Después del establecimiento, el equipo de usuario y diferentes servicios pueden utilizar este secreto compartido para sus propias necesidades de autenticación. El secreto compartido se puede denominar la información B-TID conocida por la red y/o por terminal. Esta información puede ser, por ejemplo, una cadena, tal como la identificación NAI, que puede ser, por ejemplo, única globalmente.

Si un terminal multi-radio equipado con información o una tarjeta (U)SIM se utiliza asimismo para otros servicios de la red móvil, el problema de la autenticación de red está ahora solucionado. Se proporcionan, a modo de ejemplo, métodos de autenticación basados en web para redes WLAN o para redes xDSL (línea de abonado digital), tales como redes basadas en TiSPAN (Telecoms & Internet converged Services & Protocols for Advanced Networks, servicios y protocolos convergentes de telecomunicaciones e internet para redes avanzadas). Este tipo de sistemas heredados pueden tener conexiones de itinerancia entre proveedores de servicios diferentes. Este encaminamiento puede producirse con algún protocolo AAA, tal como un protocolo RADIUS, basado en REALM.

La solución acorde con la invención y sus realizaciones se puede utilizar para autenticación para redes heredadas y asimismo para permitir autenticación de usuario basada en (U)SIM, por ejemplo, al mismo tiempo. La autenticación para la red heredada puede utilizar, por ejemplo, credenciales (U)SIM. Tal como se describirá a continuación, no se requieren modificaciones en las redes heredadas. La invención y sus realizaciones permiten unir autenticación heredada y autenticación basada en (U)SIM, según soluciones de tipo estándar. Las conexiones de itinerancia AAA se utilizan sin ninguna modificación, por ejemplo, para la red visitada.

La KS-Legacy-PWD se puede obtener según el estándar 3GPP TS33.220, pero asimismo utilizando el identificador genérico NAF-ID. Alternativamente, se puede definir la función de derivación para la autenticación heredada. Esta función puede ser, por ejemplo, la KS-Legacy-NAF = KDF (KS, "gba-me-legacy", RAND, IMPI, generic_NAF_Id).

Es posible, asimismo, que la red visitada sea la red propia, es decir, no es obligatoria ninguna conexión de itinerancia.

La invención y sus realizaciones pueden conectar o mapear juntos por lo menos dos sistemas diferentes, por ejemplo la itinerancia RADIUS basada en web y la itinerancia WLAN basada en (U)SIM, de manera que las itinerancias GPA y (U)SIM pueden funcionar conjuntamente.

La invención y sus realizaciones pueden conectar o mapear juntas una red de comunicación basada en operador y una red de comunicación no basada en operador. Después de esto, la red no basada en operador puede verse desde el punto de vista de la red central basado en operador, como si fuera también una red basada en operador, tal como la red GPRS. Después de esto, en la autenticación basada en web, se puede usar y utilizar autenticación basada en (U)SIM. Esto se puede llevar a cabo con la ayuda del sistema GPA, cuando el equipo de usuario y el elemento de BSF han creado y modificado el material de identificación. Asimismo, después de esto, la itinerancia WLAN se puede mapear en el servidor intermediario de la red propia.

Una ventaja de la invención y sus realizaciones es que la solución permite autenticación basada en (U)SIM en la red, utilizando arquitectura GAA, de manera que no es necesario realizar modificaciones a la red de acceso o a la red de acceso visitada. Tampoco se requiere ningún soporte EAP (protocolo de autenticación extensible) desde la red de acceso.

La invención y sus realizaciones permiten a los operadores facturar en base a la utilización de una tarjeta SIM. Las rutinas de facturación y la administración en redes sin licencia se hace más sencilla, más eficiente y se ahorra capacidad del sistema. En las redes basadas en web, la gestión de la red y la itinerancia entre redes diferentes se hace más sencilla, más eficiente y se ahorra capacidad del sistema.

Existen, asimismo, muchas otras ventajas de la invención y sus realizaciones. La solución permite la autenticación basada en (U)SIM para redes heredadas tales como WLAN, acceso web TiSPAN sin soporte EAP SIM/AKA y/o sin modificaciones en la red de acceso. Permite asimismo la autenticación basada en (U)SIM y la itinerancia basada en AAA y REALM, sin modificaciones en la conexión o conexiones de itinerancia existentes. Además, permite, después de la autenticación de red, una autenticación de servicio de tipo entidad federada entre servicios y el equipo de usuario. Esta autenticación puede ser automática, o en respuesta a un evento de activación. La autenticación puede producirse tal como se muestra mediante el elemento GAA. Si el dispositivo está capacitado para GAA, la utilización de GAA para autenticar uno o varios servicios es posible e incluso deseable. En tal caso, se supone que los servicios soportan asimismo GAA.

No obstante, cabe señalar que la autenticación requiere soporte según la arquitectura GAA/GBA, desde la red propia.

La invención y sus realizaciones tienen asimismo la ventaja de que no se requiere ninguna participación del usuario en el proceso de autenticación, por ejemplo, en accesos web basados en HTTP, que normalmente son incompatibles. Debido a que la utilización de la arquitectura EAP-SIM/AKA fuera del estándar 802.x se implementa normalmente en relación con accesos web, ahora se pueden superar los problemas con incompatibilidades provocadas mediante las tecnologías de acceso web. Asimismo, si el equipo de usuario negocia con la AAA de la red propia mediante la utilización de algún otro protocolo diferente de HTTP o HTTPS (hypertext transfer protocol secure, protocolo seguro de transferencia de hipertexto), la comunicación será satisfactoria. Un ejemplo de dicha negociación es la utilización de un protocolo RADIUS directamente desde el equipo de usuario. Además, las diferentes soluciones propietarias soportan un posible cambio de la infraestructura AAA, por ejemplo, en la dirección de EAP-SIM/AKA. En cualquier caso, esto ocurrirá mediante UMA (unlicensed mobile access, acceso móvil sin licencia) y mediante VCC (Voice Call Continuity, continuidad de llamadas de voz) 3GPP. Además, no se requieren modificaciones en redes de acceso ni soluciones no estándar.

Resultará obvio para un experto en la materia que, a medida que la tecnología avanza, el concepto inventivo se puede implementar de diversas maneras. La invención y sus realizaciones no están limitadas a los ejemplos descritos anteriormente, sino solamente mediante las reivindicaciones.

REIVINDICACIONES

1. Un método de provisión de autenticación de acceso para un usuario que utiliza un equipo de usuario (1-2) que comunica (1) en una primera red de comunicaciones (1-30) que admite un primer tipo de identificación, a una segunda red de comunicaciones (1-16, 1-20) que admite un segundo tipo de identificación, comprendiendo el método:

autenticar el equipo de usuario (1-2) en la primera red de comunicaciones (1-30) mediante el primer tipo de identificación;

crear, mediante una función de servidor de arranque en la primera red de comunicaciones, para el equipo de usuario autenticado en la primera red de comunicaciones, un identificador B-TID en la primera red de comunicaciones (1-30), estando previsto el identificador B-TID para ser utilizado en el segundo tipo de identificación en respuesta a la autenticación del equipo de usuario (1-2) en la primera red de comunicaciones (1-30);

enviar el identificador B-TID creado al equipo de usuario sobre la primera red de comunicaciones;

recibir (5) en la primera red de comunicaciones, el identificador B-TID creado enviado desde el equipo de usuario a un elemento de control de acceso para la segunda red de comunicaciones, **caracterizado porque** el identificador B-TID comprende una primera parte y una segunda parte;

recuperar (7), utilizando la primera parte, una segunda parte correspondiente a partir de una base de datos de la primera red de comunicaciones (1-30) mediante la función de servidor de arranque;

comparar la segunda parte recibida con la correspondiente segunda parte recuperada, y son iguales, proporcionar al equipo de usuario (1-2) autenticación de acceso para la segunda red de comunicaciones (1-16, 1-20).

2. Un método acorde con la reivindicación 1, **caracterizado por**, antes de recibir (5) el identificador B-TID, autenticar el equipo de usuario (1-2) y la segunda red de comunicaciones (1-16, 1-20).

3. Un método acorde con la reivindicación 1 ó 2, **caracterizado por** proporcionar un secreto compartido como la primera parte del identificador B-TID, sirviendo dicho secreto compartido como una contraseña conocida por el equipo de usuario (1-2) y por la base de datos (1-6).

4. Un método acorde con cualquiera de las reivindicaciones 1 a 3, **caracterizado por** utilizar la segunda parte del identificador B-TID para designar e indexar la primera parte del identificador B-TID.

5. Un método acorde con cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** el valor de la primera parte y/o la segunda parte del identificador B-TID es local o globalmente único.

6. Un método acorde con cualquiera de las reivindicaciones 1 a 5, **caracterizado porque** el valor del identificador B-TID comprende un numero aleatorio codificado y un nombre de servidor de dominio de la función que lleva a cabo la autenticación.

7. Un método acorde con cualquiera de las reivindicaciones 1 a 6, **caracterizado porque** la segunda parte del identificador B-TID es un identificador NAI.

8. Un método acorde con cualquiera de las reivindicaciones 1 a 7, **caracterizado por** la autenticación del equipo de usuario (1-2) para la segunda red de comunicaciones (1-16, 1-20) de acuerdo con un nombre de usuario y una contraseña, en el que el identificador B-TID es un nombre de usuario y la contraseña puede obtenerse a partir del secreto compartido.

9. Un método acorde con cualquiera de las reivindicaciones 1 a 8, **caracterizado porque** la autenticación de acceso para la segunda red de comunicaciones (116, 1-20) es una autenticación basada en internet o una autenticación heredada.

10. Un método acorde con cualquiera de las reivindicaciones 1 a 9, **caracterizado por** recibir (5) el identificador B-TID que comprende la primera parte y la segunda parte como un mensaje AAA (autenticación, autorización y contabilización), mensaje AAA que es el mismo mensaje que el de la autenticación del equipo de usuario (1-2) para la primera red de comunicaciones (1-30).

11. Un servidor intermediario (1-12) de provisión de autenticación de acceso para un usuario que utiliza un equipo de usuario (1-2) que comunica (1) en una primera red de comunicaciones (1-30) que admite un primer tipo de

identificación, a una segunda red de comunicaciones (1-16, 1-20) que admite un segundo tipo de identificación, que comprende:

medios para recibir (5) desde otro servidor intermediario un identificador B-TID enviado por el equipo de usuario mediante un elemento de control de acceso, **caracterizado porque**

el identificador B-TID comprende una primera parte y una segunda parte, y está previsto para ser utilizado en el segundo tipo de identificación;

medios para enviar (7) una pregunta que comprende la primera parte, a un servidor de autenticación, autorización y contabilización que comprende una función de servidor de arranque y que se utiliza en la autenticación del equipo de usuario en la primera red de comunicaciones;

medios para recibir, como una respuesta a la pregunta, una segunda parte correspondiente;

medios para comparar la segunda parte recibida con la segunda parte correspondiente recibida, y si son iguales, medios para proporcionar mediante el otro servidor intermediario y el elemento de control de acceso, al equipo de usuario (1-2), la autenticación de acceso para la segunda red de comunicaciones (1-16, 1-20).

12. Un elemento de servidor (1-4) de provisión de autenticación de acceso para un usuario que utiliza un equipo de usuario (1-2) que comunica (1) en una primera red de comunicaciones (1-30) que admite un primer tipo de identificación, a una segunda red de comunicaciones (1-16, 1-20) que admite un segundo tipo de identificación, comprendiendo el elemento de servidor:

una función de servidor de arranque (BSF); y

medios para autenticar (BSF) el equipo de usuario (1-2) en la primera red de comunicaciones (1-30) mediante el primer tipo de identificación;

comprendiendo además el elemento de servidor medios para crear, en respuesta a la autenticación del equipo de usuario (1-2) en la primera red de comunicaciones, un identificador B-TID para el equipo de usuario, estando previsto el identificador para su utilización en el segundo tipo de identificación, dichos medios para crear estando configurados para utilizar la función de servidor de arranque a efectos de crear el identificador B-TID;

medios para transmitir (5) el identificador B-TID creado al equipo de usuario

caracterizado por:

que el identificador B-TID comprende una primera parte y una segunda parte;

medios para recibir (6), desde un servidor intermediario de autenticación, autorización y contabilización una pregunta que comprende la primera parte;

medios para recuperar (7), utilizando la primera parte, una correspondiente segunda parte a partir de una base de datos (BSF) de la primera red de comunicaciones (1-30);

medios para comunicar la segunda parte recuperada al servidor intermediario de autenticación, autorización y contabilización.

13. Un sistema para proporcionar autenticación de acceso para un usuario que utiliza un equipo de usuario (1-2) que comunica (1) en una primera red de comunicaciones (1-30) que admite un primer tipo de identificación, a una segunda red de comunicaciones (1-16, 1-20) que admite un segundo tipo de identificación

comprendiendo el sistema la primera red de comunicaciones y la segunda red de comunicaciones, en el que

la primera red de comunicaciones (1-30) comprende un servidor de autenticación, autorización y contabilización AAA (1-4) que tiene una función de servidor de arranque BSF para autenticar el equipo de usuario (1-2) en la primera red de comunicaciones (1-30) mediante el primer tipo de identificación, y una base de datos de servidor de abonados propio HSS (1-6) que comprende información asociada con el equipo de usuario, y un servidor intermediario de itinerancia AAA propio, estando configurado el servidor AAA (1-4) para estar en comunicación con la base de datos del servidor de abonados propio y el servidor intermediario de itinerancia AAA propio,

la segunda red de comunicaciones comprende por lo menos un elemento de control de acceso y un servidor intermediario de itinerancia AAA visitado, el servidor intermediario de itinerancia AAA visitado está configurado para estar en comunicación con el elemento de control de acceso y el servidor intermediario de itinerancia AAA propio;

la función de servidor de arranque en el servidor AAA está configurada para crear un identificador B-TID para el segundo tipo de identificación, en respuesta al autenticación del equipo de usuario (1-2) en la primera red de comunicaciones (1-30) y para enviar el identificador B-TID creado al equipo de usuario sobre la primera red de comunicación;

caracterizado porque

el equipo de usuario está configurado para recibir el identificador B-TID creado procedente de la primera red de comunicaciones y para enviar el identificador B-TID creado, que comprende una primera parte y una segunda parte, al elemento de control de acceso en la segunda red de comunicaciones;

el elemento de control de acceso está configurado para transferir el identificador B-TID creado al servidor intermediario AAA de itinerancia visitado;

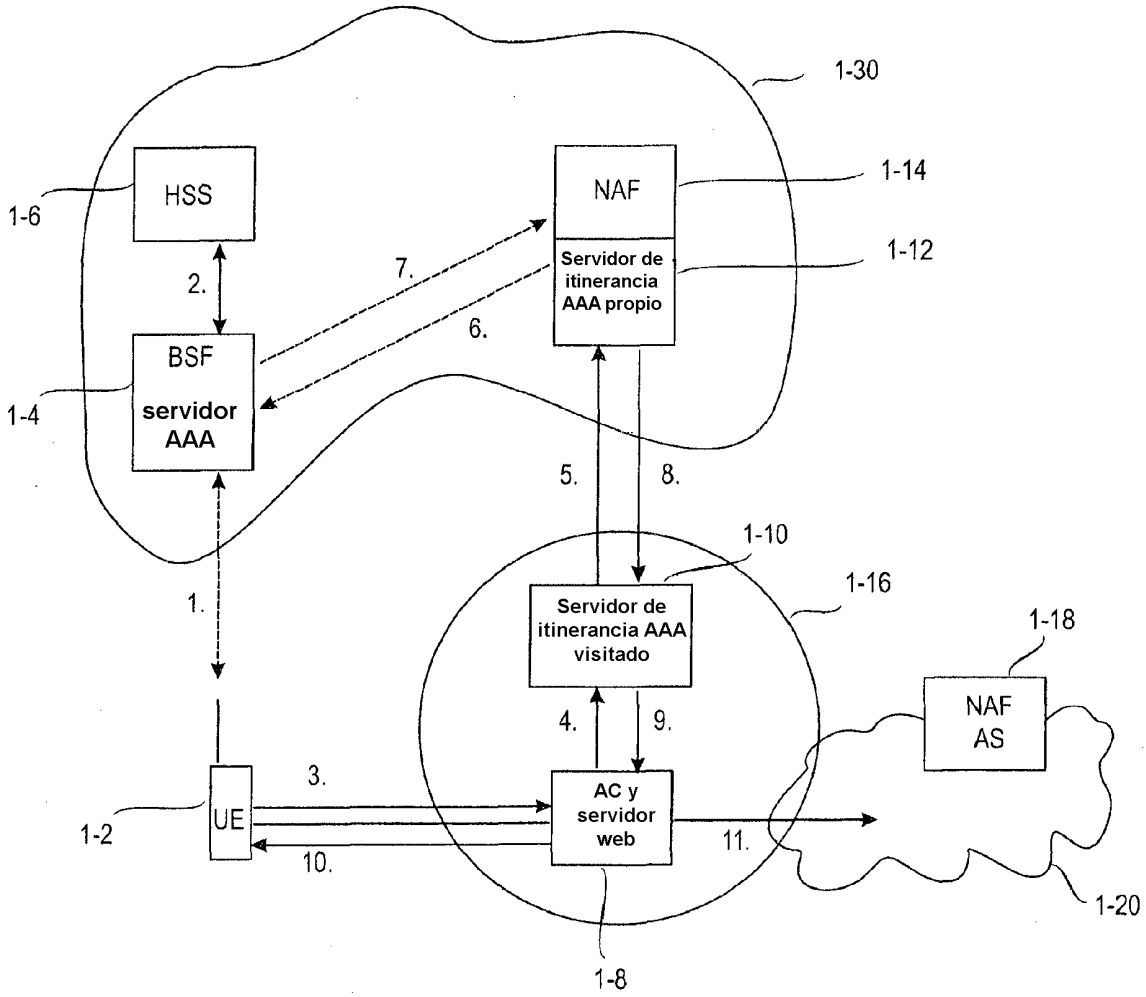
el servidor intermediario AAA de itinerancia visitado está configurado para transferir el identificador B-TID creado al servidor intermediario AAA de itinerancia propio;

el servidor intermediario AAA de itinerancia propio está configurado para recibir el identificador B-TID creado, solicitar una correspondiente segunda parte mediante enviar la primera parte en una pregunta al servidor AAA, recibir la correspondiente segunda parte desde el servidor AAA y comparar la segunda parte recibida con la segunda parte correspondiente, y si son iguales proporcionar al equipo de usuario (1-2) autenticación de acceso a la segunda red de comunicaciones (1-16, 1-20) mediante el servidor intermediario AAA de itinerancia visitado y el elemento de control de acceso; y

el servidor AAA está configurado para recibir la pregunta, recuperar, por medio de la función de arranque, utilizando la primera parte, la segunda parte correspondiente a partir de la base de datos del servidor de abonados propio, y transmitir la correspondiente segunda parte al servidor intermediario AAA de itinerancia propio.

14. Un programa informático, **caracterizado porque** comprende medios de código informático adaptados para realizar cualquiera de las etapas de cualquiera de las reivindicaciones 1 a 10, cuando el programa se ejecuta en un ordenador o en un procesador.

Fig. 1


1-30
HSS
1-6
NAF
1-14
Servidor de itinerancia AAA propio
1-12
2.
7.
6.
BSF
servidor AAA
1-4
5.
8.
1-10
1-16
Servidor de itinerancia AAA visitado
1-18
NAF AS
1.
4.
9.
3.
UE
1-2
AC y servidor web
11.
10.
1-20
1-8