(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 582 858**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.06.2013 E 13737345 (2)**

(97) Fecha y número de publicación de la concesión europea: **20.04.2016 EP 2868130**

(54) Título: **Implementación de una asociación de seguridad durante la adscripción de un terminal a una red de acceso**

(30) Prioridad:

02.07.2012 FR 1256330

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.09.2016

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

BOURNELLE, JULIEN y
MORAND, LIONEL

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Implementación de una asociación de seguridad durante la adscripción de un terminal a una red de acceso

El campo de la invención es el de las telecomunicaciones, y más particularmente las telecomunicaciones mediante redes móviles.

El organismo de normalización 3GPP ha definido una arquitectura denominada GBA ("Generic Bootstrapping Architecture") "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 11)", 3GPP STANDARD; 3GPP TS 33.220, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA-ANTIPOLIS CEDEX; FRANCIA, vol. SA WG3, n.º V11.2.0, 16 de marzo de 2012 (2012-03-16), páginas 1-91, XP050580312, cuyo objetivo es permitir la autentificación de un terminal móvil para crear una asociación de seguridad entre el terminal móvil y una aplicación. Esta arquitectura incluye un servidor de función de activación, denominado BSF ("Bootstrapping Function Server") que sirve de tercera parte de confianza que permite el establecimiento de una asociación de seguridad del terminal y la aplicación.

El proceso de autentificación utilizado en esta arquitectura se realiza por tanto en dos tiempos, con un primer proceso de autentificación del terminal móvil ante el servidor de activación BSF. Esta fase de autentificación permite establecer entre el terminal y el BSF una asociación de seguridad en base a una clave compartida generada en el curso de la autentificación. Esta clave compartida permite a continuación establecer una asociación de seguridad entre el terminal y una aplicación que tenga acceso al BSF para recuperar el material de seguridad necesario para autentificar el terminal.

En el caso en el que el terminal móvil busca conectarse a través de una red de acceso no 3GPP, se efectúa previamente una etapa suplementaria de adscripción del terminal a la red de acceso, típicamente utilizando el protocolo EAP (por Extensible Authentication Protocol), para autentificar el terminal con el fin de permitirle acceder a la red de acceso no 3GPP.

La figura 1 ilustra este proceso de autentificación cuando un terminal móvil busca conectarse a una aplicación a través de una red de acceso no 3GPP.

En un primer tiempo, el terminal móvil UE se adscribe a la red de acceso no 3GPP, dirigiéndose a un servidor de autentificación AAA/EAP por medio de un punto de acceso AP de esta red y procediendo a una primera autentificación utilizando el protocolo de autentificación EAP (etapa 105).

Una vez adscrito el terminal UE a la red de acceso no 3GPP, puede proceder a continuación a un segundo procedimiento de autentificación con la infraestructura GBA. De ese modo, el terminal UE, provisto de una tarjeta SIM, se autentifica inicialmente ante un servidor de función de activación BSF (etapa 110), utilizando una conexión basada en el protocolo http (etapa 111).

Esta autentificación tiene por resultado una clave de seguridad Ks, válida para una duración determinada, proporcionada por el servidor de activación BSF. El servidor de activación BSF proporciona igualmente al terminal un identificador de sesión B-TID asociado a la clave de seguridad Ks, así como la duración de validez de la clave (etapa 113).

Posteriormente, cuando el terminal desea acceder a una aplicación APP, se autentifica mutuamente con esta aplicación APP (etapa 120), abriendo una conexión con esta aplicación APP (etapa 121), indicando a esta aplicación que desea ser autentificado según la técnica GBA, y proporcionándole el identificador de sesión B-TID.

La aplicación APP contacta entonces con el servidor BSF para proporcionarle el identificador de sesión B-TID, y el servidor BSF le responde proporcionándole una nueva clave K' deducida a partir de la clave de seguridad y del nombre de la aplicación (etapa 123). El terminal efectúa las mismas operaciones por su lado (etapa 125).

De ese modo el terminal y la aplicación disponen de una misma clave K' que pueden utilizar para autentificarse mutuamente y asegurar la conexión IP entre ellos (etapa 127).

Este procedimiento de autentificación implica por tanto que el terminal abre su navegador http para poder a continuación abrir una conexión IP con la aplicación, mientras que esta conexión no está necesariamente basada en el protocolo http.

Por otro lado, el terminal móvil se ha autentificado previamente ante un servidor AAA de la red de acceso, durante su adscripción a la red, antes de autentificarse ante el servidor de activación BSF. Hay por tanto una autentificación doble del terminal móvil, una primera vez durante su adscripción a la red y posteriormente una segunda vez para

crear una asociación de seguridad con el servidor de activación BSF, lo que induce unos retardos durante el acceso del terminal a la aplicación APP, una complejidad creciente y aumenta los intercambios de mensajes en la red.

La presente invención tiene por objeto resolver los inconvenientes de la técnica anterior proporcionando un procedimiento de implementación de una asociación de seguridad, para un terminal que se adscribe a una red de acceso, en particular una red de acceso de tipo no 3GPP, que no necesite más que una única fase conjunta de adscripción a la red y de asociación de seguridad.

Según un primer aspecto de la invención, se propone un procedimiento de implementación de una asociación de seguridad para un terminal que se adscribe a una red de acceso, incluyendo las etapas siguientes, ejecutadas por un servidor de autentificación de la red de acceso, en respuesta a la recepción de una solicitud de adscripción a la red que procede del terminal:

recepción, desde un servidor de función de activación, de un primer mensaje que contiene al menos un parámetro de asociación de seguridad;
autentificación del terminal por medio de al menos un primer parámetro de autentificación proporcionado por el servidor de abonados residencial de este terminal; y
envío al terminal autentificado de un mensaje de asociación de seguridad que contiene el al menos un parámetro de asociación de seguridad.

De ese modo, una vez recibido este mensaje de asociación de seguridad, el terminal está no solamente adscrito a la red de acceso, sino que dispone igualmente de un parámetro de asociación de seguridad, utilizable para una autentificación mutua con una aplicación. Los procedimientos de adscripción a la red y de implementación de una asociación de seguridad se combinan por lo tanto en el seno de un único procedimiento, lo que reduce la señalización necesaria para estas dos operaciones.

En un primer modo de realización, el primer mensaje contiene el primer parámetro de autentificación, obtenido por el servidor de función de activación ante el servidor de abonados residencial, lo que permite al servidor de autentificación recuperar simultáneamente los parámetros de autentificación y de asociación de seguridad, minimizando el número de mensajes utilizados.

Según una característica ventajosa, al menos una parte del parámetro de asociación de seguridad se determina por el servidor de función de activación en función de al menos una parte del primer parámetro de autentificación recibido del servidor de abonados residencial, lo que permite utilizar los primeros parámetros de autentificación tanto para la autentificación del terminal propiamente dicho como para la implementación de la asociación de seguridad.

En otro modo de realización, el servidor de autentificación recibe un segundo mensaje que contiene el primer parámetro de autentificación del servidor de abonados residencial, en respuesta al envío por el servidor de autentificación de una solicitud de autentificación a este servidor de abonados residencial, lo que permite descorrelacionar los procesos de autentificación y de implementación de una asociación de seguridad.

Según una característica ventajosa, al menos una parte del parámetro de asociación de seguridad se determina por el servidor de función de activación en función de al menos una parte de un segundo parámetro de autentificación recibido del servidor de abonados residencial. La autentificación y la asociación de seguridad se realizan por tanto a partir de parámetros de autentificación distintos, lo que refuerza la seguridad del proceso.

Según una característica particular de la invención, el al menos un parámetro de asociación de seguridad es al menos un parámetro entre un identificador de sesión segura y una duración de validez de una clave de sesión segura. Según otra característica particular de la invención, el al menos un primer parámetro de autentificación es al menos un parámetro entre un valor aleatorio, un parámetro de identificación de la red y un valor de respuesta esperada cuando el terminal utiliza este valor aleatorio para autentificarse.

En un modo de realización ventajoso, el mensaje de asociación de seguridad es un mensaje según el protocolo EAP que comprende un campo de datos que contiene el al menos un parámetro de asociación de seguridad, con el fin de proteger este parámetro de asociación de seguridad. En particular, el mensaje de asociación de seguridad es un mensaje según el protocolo EAP-AKA que puede comprender un encabezado según el protocolo de autentificación AKA antes del campo de datos que contiene los parámetros de asociación de seguridad.

Según otro modo de realización particular, la asociación de seguridad es una asociación de seguridad según la arquitectura GBA. Según otro modo de realización particular, la red de acceso es una red de acceso de tipo no 3GPP.

Según otro objeto de la invención, se propone un servidor de autentificación adaptado para implementar una asociación de seguridad para un terminal que se adscribe a una red de acceso, que incluye un módulo de emisión-recepción adecuado para recibir una petición de adscripción a esta red de acceso emitida por el terminal, estando configurado este módulo de emisión-recepción además para:

recibir, desde un servidor de función de activación, un primer mensaje que contiene al menos un parámetro de asociación de seguridad;
enviar al terminal un mensaje de asociación de seguridad conteniendo este al menos un parámetro de asociación de seguridad, en respuesta a la autentificación del terminal por el servidor de autentificación por medio de al menos un primer parámetro de autentificación proporcionado por un servidor de abonados residencial de este terminal.

Este servidor presenta unas ventajas análogas a las del procedimiento anteriormente presentado.

Según otro objeto de la invención, se propone un terminal, adecuado para desencadenar la implementación de una asociación de seguridad durante su adscripción a una red de acceso, que incluye un módulo de emisión-recepción adaptado para:

enviar una petición de adscripción a la red de acceso hacia un punto de acceso de la red de acceso;
recibir, desde este punto de acceso, un mensaje que contiene al menos un primer parámetro de autentificación proporcionado por un servidor de abonados residencial del terminal;
enviar, hacia el punto de acceso, una respuesta que contiene un valor calculado por el terminal a partir del al menos un primer parámetro de autentificación;
recibir, desde el punto de acceso, un mensaje de asociación de seguridad que contiene al menos un parámetro de asociación de seguridad adecuado para ser utilizado por el terminal para autentificarse durante una conexión con una aplicación.

En un modo particular de realización, las diferentes etapas del procedimiento según la invención se determinan mediante unas instrucciones de programas informáticos. En consecuencia, la invención se dirige también a un programa informático sobre un soporte de informaciones, siendo este programa susceptible de ser implementado en un ordenador, incluyendo este programa unas instrucciones adaptadas para la implementación de las etapas del procedimiento tal como se ha descrito en el presente documento anteriormente. Este programa puede utilizar no importa qué lenguaje de programación, y estar en la forma de código fuente, código objeto, o de código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada, o en no importa qué otra forma deseable.

La invención se dirige también a un soporte de informaciones legible por un ordenador, y que incluye unas instrucciones de programas informáticos tales como los mencionados en el presente documento anteriormente. El soporte de informaciones puede ser no importa qué entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD ROM, o una ROM de circuito microelectrónico, o incluso un medio de grabación magnética, por ejemplo un disquete (floppy disc) o un disco duro. Por otro lado, el soporte de informaciones puede ser un soporte que puede transmitirse tal como una señal eléctrica u óptica, que puede encaminarse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede en particular descargarse desde una red de tipo Internet. Alternativamente, el soporte de informaciones puede ser un circuito integrado en el que se incorpora el programa, estando adaptado el circuito para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

Surgirán otras características y ventajas con la lectura de modos de realización preferidos descritos en referencia a las figuras en las que, además de la figura 1 ya explicada anteriormente:

- la figura 2 representa de manera esquemática los equipos de una red de telecomunicación móvil implicados en la presente invención;
- la figura 3A representa las etapas del procedimiento de implementación de una asociación de seguridad para un terminal, según un primer modo de realización de la invención;
- la figura 3B representa las etapas del procedimiento de implementación de una asociación de seguridad para un terminal, según un segundo modo de realización de la invención; y
- las figuras 4A a 4C ilustran la utilización de paquetes de datos según el protocolo EAP en un modo de realización ventajoso de la invención.

Se hace referencia de entrada a la figura 2 que representa de manera esquemática los equipos de una red de telecomunicación móvil implicados en la presente invención.

Los equipos que implementan la invención son un terminal móvil UE, un punto de acceso a la red AP y un servidor de autentificación AAA, perteneciendo ambos dos a una red de acceso ACC_NET, un servidor de función de activación BSF y un servidor de abonados HSS.

La invención se implementa ventajosamente para un acceso a través de una red de acceso de tipo no 3GPP, siendo este acceso de tipo Wi-Fi (es decir según una norma IEEE 802.11x), WiMax (es decir según una norma IEEE 802.16x) o según un modo de conexión VPN (por Virtual Private Network), que utiliza por ejemplo el protocolo IKEv2.

De ese modo, en un modo de realización en el que el acceso a la red de acceso ACC_NET se realiza según la norma Wi-Fi, el punto de acceso a la red AP es una pasarela de acceso o un enrutador Wi-Fi. En un modo de realización en el que este acceso se realiza según la norma WiMax, el punto de acceso a la red AP es una estación de base WiMax. Finalmente, en un modo de realización en el que el acceso se realiza según un modo de conexión VPN, el punto de acceso a la red AP es un servidor VPN.

El terminal móvil UE puede ser, por ejemplo, un terminal de telefonía móvil, un ordenador portátil, un asistente personal digital, u otro. En el ejemplo representado el terminal móvil UE es un terminal de telefonía móvil que pertenece a un usuario.

Como representa a éste la figura 2, el terminal móvil UE incluye un módulo de emisión-recepción 10 configurado para emitir y recibir unos datos principalmente hacia y desde el punto de acceso de red AP. Incluye igualmente un procesador 11, una memoria volátil 12 y una memoria no volátil 13.

El punto de acceso a la red AP de la red de acceso ACC_NET es una unidad que incluye un procesador 21, una memoria volátil 22 y una memoria no volátil 23, así como un módulo de emisión-recepción 20 (típicamente una o varias antena(s)) configurado para comunicar con el terminal móvil UE y el servidor de autentificación AAA.

El servidor de autentificación AAA de la red de acceso ACC_NET presenta la estructura convencional de un ordenador. Incluye un procesador 31, una memoria volátil 32 y una memoria no volátil 33. Incluye un módulo de emisión-recepción 30 configurado para comunicar con el punto de acceso de red AP, el servidor de función de activación BSF y el servidor de abonado HSS.

Este servidor de autentificación AAA está adaptado en particular para implementar una asociación de seguridad, por ejemplo de tipo GBA, para un terminal que busca adscribirse a la red de acceso ACC_NET.

Para hacer esto, su módulo de emisión-recepción 30 puede recibir una petición de adscripción a la red que procede del terminal, emitir una solicitud de asociación de seguridad al servidor de función de activación BSF, en respuesta a la recepción de una petición de ese tipo de adscripción a la red, recibir un primer mensaje, denominado de respuesta de asociación de seguridad, que incluye unos parámetros de asociación de seguridad y eventualmente unos parámetros de autentificación, desde el servidor de función de activación, y enviar al terminal un mensaje de asociación de seguridad que incluye los parámetros de asociación de seguridad al terminal, si este último se autentifica con éxito, con el fin de indicar a este terminal que está bien adscrito a la red y autentificado por el servidor de función de activación BSF.

El servidor de función de activación BSF presenta igualmente la estructura convencional de un ordenador. Incluye un procesador 41, una memoria volátil 42 y una memoria no volátil 43. Incluye un módulo de emisión-recepción 40 configurado para comunicar con el servidor de autentificación AAA y el servidor de abonado HSS.

El servidor de abonado HSS presenta también la estructura convencional de un ordenador. Incluye un procesador 51, una memoria volátil 52 y una memoria no volátil 53. Incluye un módulo de emisión-recepción 50 configurado para comunicar con el servidor de autentificación AAA y el servidor de función de activación BSF, principalmente con el fin de enviarle unos parámetros de autentificación tras la solicitud de su parte. Este servidor de abonados HSS puede ser principalmente una base de datos centralizada que aloja los datos del perfil de usuario asociado al terminal móvil UE. Cuando este perfil de usuario soporta una asociación de seguridad (por ejemplo de tipo GBA), mientras que el servidor HSS almacena igualmente una indicación de esta característica.

Se hace referencia ahora a la figura 3A, que ilustra un procedimiento de implementación de una asociación de seguridad para un terminal móvil UE que se adscribe a una red de acceso ACC_NET, según un primer modo de realización de la presente invención.

El procedimiento ilustrado en esta figura 3A incluye una primera fase 210 combinada de autentificación y de implementación de una asociación de seguridad, durante la adscripción del terminal UE a la red ACC_NET, seguida de una segunda fase 220 de conexión del terminal móvil UE a una aplicación APP por medio de parámetros de asociación de seguridad definidos durante esta asociación de seguridad.

La asociación de seguridad empleada en este procedimiento es típicamente una asociación de seguridad de tipo GBA (por Generic Bootstrapping Architecture) entre el terminal móvil UE y cualquier aplicación APP que se base en esta técnica GBA para autentificar este terminal móvil.

En el curso de la primera fase 210, el terminal móvil UE pide inicialmente su adscripción ante la red de acceso ACC_NET (por ejemplo por medio de un módulo de cliente instalado en este terminal UE), enviando una solicitud de adscripción al punto de acceso de red AP de esta red de acceso (etapa 211).

Esta solicitud de adscripción puede contener particularmente un identificador único Id(UE), por ejemplo la identidad de abonado móvil internacional IMSI (por “International Mobile Subscriber Identity”) del usuario del terminal móvil UE.

Esta solicitud de adscripción se redirige, por el punto de acceso AP, al servidor de autentificación AAA de esta red de acceso (etapa 211), con el fin de que éste pueda procesar esta petición.

En respuesta a la recepción de esta solicitud de adscripción trasmitida por el punto de acceso AP, el servidor AAA desencadena entonces el proceso de autentificación del terminal UE, enviando una solicitud de asociación de seguridad al servidor de función de activación BSF (etapa 212), conteniendo esta solicitud el identificador Id(UE) del terminal UE. Esta solicitud de asociación de seguridad se puede formatear según el protocolo Diameter o el protocolo MAP.

En respuesta a la recepción de esta solicitud de asociación de seguridad que procede del servidor de autentificación AAA, el servidor de función de activación BSF puede verificar que el identificador único Id(UE) del usuario del terminal móvil UE existe y tiene derecho al servicio de asociación de seguridad. Interroga entonces al servidor de abonados residencial HSS de este terminal UE, con el fin de recuperar unos parámetros de autentificación asociados con el usuario de este terminal.

Para hacer esto, el servidor de función de activación BSF envía (etapa 213) una solicitud de autentificación que contiene el identificador Id(UE) del usuario abonado del terminal UE.

En respuesta a la recepción de esta solicitud de autentificación, el servidor de abonados residencial HSS reenvía uno, o varios, parámetro(s) de autentificación, así como eventualmente unas informaciones GUSS (“Generic User Security Settings”) al servidor de función de activación BSF que los almacena.

En particular, estos parámetros de autentificación pueden tomar la forma de un vector de autentificación AV que incluye un valor aleatorio RAND generado por el servidor de abonados HSS, una ficha de autentificación de la red AUTN que permite autentificar la red, un valor XRES de respuesta esperada cuando el terminal utiliza el valor aleatorio RAND para autentificarse, una clave de cifrado Ck calculada a partir de este valor aleatorio RAND y una clave de integridad Ik calculada igualmente a partir de este valor aleatorio RAND. En otros términos, el vector de autentificación AV = (RAND, AUTN, XRES, Ck, Ik) es devuelto por el servidor de abonados residencial HSS al servidor de función de activación BSF.

El servidor de función de activación BSF genera a continuación al menos un parámetro de asociación de sesión, principalmente un identificador de sesión B-TID y una duración de sesión Tks asociada una clave de sesión Ks (etapa 215). En particular, esta clave de sesión Ks puede generarse a partir de ciertos de los parámetros de autentificación recibidos desde el servidor de abonados residencial HSS, por ejemplo, concatenando las claves Ik y Ck del vector de autentificación AV anteriormente introducido.

El servidor de función de activación BSF envía a continuación un primer mensaje, denominado de respuesta de asociación de seguridad, al servidor de autentificación AAA que contiene el (los) parámetro(s) de asociación de sesión (por ejemplo el identificador de sesión B-TID y la duración de validez Tks de la clave de sesión Ks) generados por el servidor BSF (etapa 216).

En el modo de realización de la figura 3A, este mensaje de respuesta de asociación de seguridad contiene igualmente, entre el conjunto de los parámetros de autentificación recibidos desde el servidor HSS, al menos los parámetros de autentificación que sirven para autentificar el terminal UE ante el servidor de autentificación AAA, es decir el valor aleatorio RAND, la ficha AUTN y el valor XRES.

Este mensaje de respuesta de asociación de seguridad puede contener de ese modo el conjunto del vector de autentificación AV = (RAND, AUTN, XRES, Ck, Ik), pudiendo utilizarse las claves Ck e Ik por el servidor de autentificación AAA para asegurar la sesión de acceso tras la autentificación así como para deducir otras claves transmitidas en el acceso.

A continuación de la recepción de este primer mensaje, el servidor de autentificación AAA puede proceder a la autentificación del terminal UE (etapa 217), gracias particularmente al valor aleatorio RAND, a la ficha de autentificación AUTN y al valor XRES. El servidor de autentificación AAA efectúa este procedimiento de autentificación del terminal UE enviándole el RAND y la ficha AUTN en un primer tiempo. El terminal UE autentifica la red gracias a la ficha AUTN. Si la autentificación de la red se concluye con éxito, el terminal UE calcula a continuación un valor de respuesta de autentificación RES a partir del valor aleatorio RAND recibido desde el servidor de autentificación AAA, y reenvía este valor RES al servidor de autentificación AAA. Comparando los valores RES y XRES, el servidor de autentificación AAA puede entonces autentificar la respuesta del terminal UE.

Si el terminal UE es autentificado con éxito por el servidor de autentificación AAA (es decir cuando el valor RES es igual al valor XRES), el servidor de autentificación AAA trasmite a continuación (etapa 218) al terminal UE un

mensaje de asociación de seguridad que contiene el (los) parámetro(s) de asociación de seguridad (por ejemplo el identificador de sesión B-TID así como la duración de validez Tks de la clave de sesión Ks).
Este mensaje de asociación de seguridad puede contener ventajosamente además ciertos de los parámetros de autentificación, en particular el valor aleatorio RAND, utilizado para recuperar la clave de sesión Ks en el terminal UE (etapa 219). En este caso, este valor aleatorio RAND se utiliza para calcular las claves Ck e Ik según el mismo procedimiento que a nivel del servidor HSS, y la clave de sesión Ks se deduce de estas claves Ck e Ik de la misma manera que a nivel del servidor BSF.

Este mensaje de asociación de seguridad puede igualmente contener ventajosamente la ficha AUTN, lo que permite poder interrogar a la tarjeta SIM del terminal UE cuando la implementación de este terminal lo exige.

En esta situación, el terminal UE está adscrito a la red de acceso ACC_NET con la que está autentificado y dispone además de una asociación de seguridad que puede utilizar para conectarse a unas aplicaciones que se basan en esta asociación de seguridad.

El usuario del terminal UE puede entonces conectarse a la aplicación APP, gracias al identificador de sesión B-TID, durante una fase de conexión 221 similar a la fase 120 descrita anteriormente en relación con la figura 1. En particular, las etapas 221 a 227 de esta fase de conexión 221 son respectivamente similares a las 121 a 127 de la fase de conexión ilustrada en la figura 1.

De ese modo, el procedimiento de adscripción del terminal UE a la red de acceso ACC_NET y el procedimiento de asociación de seguridad entre este terminal UE y unas aplicaciones que permiten una autentificación mutua por medio del identificador de sesión B-TID se combinan en el seno de un solo y único procedimiento, con el fin de disminuir la señalización entre las diferentes entidades de la red descrita en la figura 2 y simplificar la utilización del procedimiento de asociación de seguridad.

Se hace referencia ahora a la figura 3B, que ilustra otro modo de realización del procedimiento de implementación de una asociación de seguridad para un terminal móvil UE que se adscribe a la red de acceso ACC_NET.

En este otro modo de realización, el procedimiento implementa una primera fase 210' combinada de autentificación y de implementación de un asociación de seguridad que se distingue de la primera fase 210, descrita anteriormente en relación con la figura 3A, en que la autentificación del terminal para el acceso a la red ACC_NET se descorrelaciona del procedimiento de asociación de seguridad.

Esta primera fase 210' arranca así mediante el envío (etapa 211') de una solicitud de adscripción del terminal UE al punto de acceso de red AP de la red ACC_NET, que es redirigida por este punto de acceso AP hacia el servidor de autentificación AAA de esta red ACC_NET con el fin de que éste pueda tratar esta petición, de modo similar a la etapa 211 anteriormente descrita.

En respuesta a la recepción de esta solicitud de adscripción transmitida por el punto de acceso AP, el servidor AAA desencadena entonces el proceso de autentificación del terminal UE, enviando una solicitud de autentificación al servidor de abonados residencial HSS del terminal UE (etapa 212'), conteniendo esta solicitud el identificador Id(UE) del terminal UE lo que permite recuperar a cambio (etapa 213') uno, o varios, primer(os) parámetro(s) de autentificación que el servidor de autentificación almacena en memoria y utiliza a continuación para proceder a la autentificación del terminal UE por la red ACC_NET. En particular, estos primeros parámetros de autentificación pueden estar en la forma de un primer vector de autentificación AV = (RAND, AUTN, XRES, Ck, Ik) tal como se ha introducido anteriormente.

Paralelamente a este proceso de autentificación (es decir antes, después o simultáneamente con, este proceso de autentificación), el servidor de autentificación AAA desencadena el proceso de asociación de seguridad enviando una solicitud de asociación de seguridad al servidor de función de activación BSF (etapa 214'), que contiene igualmente el identificador Id(UE) de este usuario abonado.

En respuesta a la recepción de esta solicitud, el servidor de función de activación BSF interroga al servidor de abonados residencial HSS del terminal UE (etapa 215'), enviándole una solicitud de interrogación que contiene el identificador Id(UE), con el fin de que este último le devuelva (etapa 216') un mensaje de respuesta que contiene uno, o varios, segundo(s) parámetro(s) de autentificación.

Estos parámetros de autentificación comprenden en particular un segundo valor aleatorio RAND' generado por el servidor HSS, una clave de cifrado Ck' calculada a partir de este valor aleatorio RAND' y una clave de integridad Ik' igualmente calculada a partir de este valor aleatorio RAND', con el fin de permitir tanto la generación de una clave de sesión Ks por el servidor BSF como la recuperación de esta clave de sesión Ks por el terminal UE. Se puede transmitir también una ficha AUTN' con el fin de poder interrogar a la tarjeta SIM del terminal UE cuando la implementación de este terminal lo exige.

En un modo de realización particular, el servidor de abonados residencial HSS reenvía un mensaje que contiene un segundo vector de autentificación AV' que comprende el conjunto de estos diferentes parámetros de autentificación, así como un valor XRES' del resultado esperado cuando el terminal UE se autentifica con el valor aleatorio RAND', en cuyo caso AV' = (RAND', AUTN', XRES', Ck', Ik').

El servidor de función de activación BSF almacena estos segundos parámetros de autentificación después de haberlos recibido y puede generar al menos un parámetro de asociación de seguridad, particularmente un identificador de sesión B-TID y una clave de sesión Ks, así como una duración de validez Tks asociada a esta clave de sesión Ks, de modo similar a lo que se hace en el primer modo de realización (etapa 217'). En particular, la clave de sesión Ks puede generarse a partir de las claves Ik' y Ck' del segundo vector de autentificación AV', concatenándolas por ejemplo.

De ese modo, en este segundo modo de realización, la clave de sesión Ks se obtiene a partir de parámetros de autentificación diferentes a los utilizados por el proceso de autentificación del terminal, lo que es ventajoso en términos de seguridad.

El servidor de función de activación BSF envía (etapa 218') a continuación un mensaje al servidor de autentificación AAA que contiene el (los) parámetro(s) de asociación de seguridad (por ejemplo el identificador de sesión B-TID y la duración Tks de validez de la clave de sesión Ks).

Una vez recibido este mensaje, el servidor de autentificación AAA puede iniciar el proceso de autentificación del terminal UE con la ayuda de los primeros parámetros de autentificación RAND, AUTN y XRES almacenados durante la etapa 213', de modo similar al proceso de autentificación 217 ya descrito.

Cuando el terminal UE es autentificado con éxito por el servidor de autentificación AAA (es decir cuando el terminal UE devuelve un valor RES igual al valor XRES del resultado esperado), el servidor de autentificación AAA transmite entonces (etapa 220') al terminal UE un mensaje de asociación de seguridad que contiene los parámetros de asociación de seguridad, por ejemplo el identificador de sesión B-TID y la duración Tks de validez de la clave Ks.

Este mensaje de asociación de seguridad contiene además ventajosamente ciertos de los segundos parámetros de autentificación, en particular el valor aleatorio RAND' que permite recuperar la clave de sesión Ks en el terminal UE (etapa 219). De ese modo, este valor aleatorio RAND' se utiliza para calcular las claves Ck' e Ik' según el mismo procedimiento que al nivel del servidor HSS, siendo deducida la clave de sesión Ks de estas claves Ck' e Ik' de la misma manera que al nivel del servidor BSF.

En un modo de realización ventajoso, se utiliza el protocolo EAP en los mensajes intercambiados entre las entidades implementadas en este procedimiento, y particularmente entre el terminal de usuario UE, el punto de acceso AP y el servidor de autentificación AAA, con el fin de asegurar que los datos intercambiados en estos mensajes están protegidos.

Como se especifica en la norma RFC 3748, los paquetes de datos según el protocolo EAP comienzan por un encabezado formado por varios campos: campo "Code", campo identificación "Identifiers", campo de longitud "Length", campo "Type", seguidos de otro campo "Type-Data" que contiene unas informaciones específicas del protocolo de autentificación. Un encabezado de ese tipo, específico del protocolo EAP, se ilustra en la figura 4A.

En el caso particular de un protocolo EAP-AKA, el campo "Type-Data" comienza por un encabezado específico que comprende un byte que indica que el subtipo, y posteriormente un byte reservado. La continuación del mensaje contiene unos atributos bajo la forma Tipo-Longitud-Valor (TLV). Un encabezado de ese tipo, específico del protocolo EAP-AKA, se ilustra en la figura 4B.

Este formato de paquetes puede emplearse ventajosamente, en la presente invención, para definir nuevos atributos específicos que permitan transmitir los parámetros siguientes al terminal UE:

- El valor aleatorio RAND proporcionado por el servidor de abonados HSS;
- El parámetro AUTN que permite autentificar la red, igualmente proporcionado por el servidor de abonados residencial HSS;
- El identificador de sesión B-TID generado por el servidor de activación BSF;
- La duración Tks de validez de la clave de sesión Ks, igualmente calculada por el servidor de activación BSF.

Los atributos x a z siguientes pueden definirse así como en el presente documento a continuación, con el fin de transmitir cada uno de los parámetros respectivamente indicados en el presente documento anteriormente:

- *Attribute Type: x /Length: n / Value: GBA RAND value*
- *Attribute Type: y /Length: m /Value: GBA AUTN value*
- *Attribute Type: z /Length: p /Value: B-TID value*
- *Attribute Type: w /Length: q /Value: session keylifetime value*

En función del modo de realización, los parámetros RAND y AUTN son opcionales.

La figura 4C ilustra de ese modo un paquete conformado según el protocolo EAP-AKA en el caso particular del transporte de un parámetro de asociación de seguridad B-TID, utilizando un atributo de tipo z, de longitud p, teniendo como valor el parámetro B-TID.

De ese modo, en este modo de realización, un módulo cliente según el protocolo EAP se instala en el terminal móvil UE, con el fin de que éste pueda, por un lado, formatear su solicitud de adscripción a la red ACC_NET según este protocolo EAP, insertando su identidad Id(UE) en un campo de datos de un paquete formateado según este protocolo EAP, tal como se ilustra en las figuras 4A o 4B.

Además, este módulo cliente EAP se configura para interpretar un mensaje de adscripción formateado según el protocolo EAP cuando es recibido por el terminal móvil UE procedente del servidor de autentificación AAA, con el fin de recuperar uno de los parámetros de asociación mencionados anteriormente, para utilización posterior durante la conexión de una aplicación APP.

Este módulo cliente EAP puede tomar la forma de un módulo de software memorizado en una de las memorias 12 o 13 del terminal UE e implementado por el procesador 11 de este terminal UE.

En este modo de realización, un módulo servidor según el protocolo EAP se instala igualmente en el servidor de autentificación AAA, con el fin de que este pueda, por un lado, interpretar la solicitud de adscripción que emana del terminal UE y, por otro lado, formatear el mensaje de asociación de seguridad que contiene el (los) parámetro(s) de asociación de seguridad según este protocolo EAP, tal como se ha ilustrado en las figuras 4A o 4B. Este módulo servidor EAP puede tomar la forma de un módulo de software memorizado en una de las memorias 32 o 33 del servidor de autentificación AAA e implementado por el procesador 31 de este servidor.

Por supuesto, le invención no está limitada a los ejemplos de realización descritos y representados en el presente documento anteriormente, a partir de los que se podrán prever otros modos y otras formas de realización, sin por ello salirse del marco de la invención.

Así, los protocolos EAP y EAP-AKA se han mencionado específicamente para formatear las solicitudes de adscripción y el mensaje de asociación de seguridad, intercambiados entre el terminal UE y el servidor de autentificación AAA. Sin embargo, pueden emplearse otros protocolos que permitan proteger los parámetros de asociación de seguridad intercambiados entre estas entidades, como por ejemplo los protocolos EAP-SIM, EAP-TTLS o EAP-AKA'.

Además, se ha indicado anteriormente que la invención es particularmente ventajosa cuando la red de acceso ACC_NET es una red de tipo no 3GPP. La invención no se limita sin embargo a este único tipo de red de acceso.

Finalmente, se ha evocado anteriormente una asociación de seguridad de tipo GBA en el marco de la autentificación de un terminal UE con un servidor de función de activación BSF, soportando ambos dos este tipo de asociación. Sin embargo, la invención no se limita por tanto a este único tipo de asociación de seguridad y puede aplicarse a otras formas de asociación de seguridad soportadas por un terminal y un servidor de función de activación, como por ejemplo una asociación de seguridad según el protocolo Digest.

REIVINDICACIONES

1. Procedimiento de implementación de una asociación de seguridad para un terminal (UE) que se adscribe a una red de acceso (ACC_NET), caracterizado por que incluye las etapas siguientes, ejecutadas por un servidor de autentificación (AAA) de la red de acceso, en respuesta a la recepción (211) de una solicitud de adscripción a la red que procede del terminal:

recepción (216, 218'), desde un servidor de función de activación (BSF), de un primer mensaje que contiene al menos un parámetro de asociación de seguridad (B-TID, Tks);
autentificación (217, 219') del terminal por medio de al menos un primer parámetro de autentificación (RAND, AUTN, XRES) proporcionado por un servidor de abonados residencial (HSS) de dicho terminal; y
envío (218, 220') al terminal autentificado de un mensaje de asociación de seguridad que contiene dicho al menos un parámetro de asociación de seguridad.

2. Procedimiento según la reivindicación 1, caracterizado por que el primer mensaje contiene dicho primer parámetro de autentificación, obtenido (214) por el servidor de función de activación ante el servidor de abonados residencial.

3. Procedimiento según la reivindicación 2, caracterizado por que al menos una parte (Tks) de dicho parámetro de asociación de seguridad es determinado por el servidor de función de activación en función de al menos una parte (Ck, Ik) de dicho primer parámetro de autentificación (AV) recibido del servidor de abonados residencial.

4. Procedimiento según la reivindicación 1, caracterizado por que el servidor de autentificación recibe (213') un segundo mensaje que contiene el primer parámetro de autentificación del servidor de abonados residencial, en respuesta al envío (212') por el servidor de autentificación de una solicitud de autentificación a dicho servidor de abonados residencial.

5. Procedimiento según la reivindicación 4, caracterizado por que al menos una parte (Tks) de dicho parámetro de asociación de seguridad se determina (217') por el servidor de función de activación en función de al menos una parte (Ck', Ik') de un segundo parámetro de autentificación (AV') recibido (216') del servidor de abonados residencial.

6. Procedimiento según una de las reivindicaciones 1 a 5, caracterizado por que el al menos un parámetro de asociación de seguridad es al menos un parámetro entre un identificador de sesión segura (B-TID) y una duración de validez (Tks) de una clave de sesión segura (Ks).

7. Procedimiento según una de las reivindicaciones 1 a 6, caracterizado por que el al menos un primer parámetro de autentificación es al menos un parámetro entre un valor aleatorio (RAND), un parámetro de identificación de la red (AUTN) y un valor de respuesta esperada cuando el terminal utiliza dicho valor aleatorio para autentificarse (XRES).

8. Procedimiento según una de las reivindicaciones 1 a 7, caracterizado por que el mensaje de asociación de seguridad es un mensaje según el protocolo EAP que comprende un campo de datos que contiene dicho al menos un parámetro de asociación de seguridad.

9. Procedimiento según la reivindicación 8, caracterizado por que el mensaje de asociación de seguridad es un mensaje según el protocolo EAP-AKA que comprende un encabezado según el protocolo de autentificación AKA antes del campo de datos que contiene el al menos un parámetro de asociación de seguridad.

10. Procedimiento según una cualquiera de las reivindicaciones 1 a 9, caracterizado por que la asociación de seguridad es una asociación de seguridad según la arquitectura GBA.

11. Procedimiento según una cualquiera de las reivindicaciones 1 a 10, caracterizado por que la red de acceso es una red de acceso de tipo no 3GPP.

12. Servidor de autentificación (AAA) adaptado para implementar una asociación de seguridad para un terminal (UE) que se adscribe a una red de acceso (ACC_NET), que incluye un módulo de emisión-recepción (30) adecuado para recibir una petición de adscripción a dicha red de acceso emitida por el terminal, caracterizado por que el módulo de emisión-recepción está configurado además para:

recibir (216, 218'), desde un servidor de función de activación (BSF), un primer mensaje que contiene al menos un parámetro de asociación de seguridad (B-TID, Tks); y
enviar (218, 220') al terminal un mensaje de asociación de seguridad que contiene dicho al menos un parámetro de asociación de seguridad (B-TID), en respuesta a la autentificación (217, 219') de dicho terminal por el servidor de autentificación, por medio de al menos un primer parámetro de autentificación (RAND, AUTN, XRES) proporcionado por un servidor de abonados residencial (HSS) de dicho terminal.

13. Terminal (UE) adecuado para desencadenar la implementación de una asociación de seguridad durante su adscripción a una red de acceso (ACC_NET), que incluye un módulo de emisión-recepción (10) adaptado para:

enviar (211) una petición de adscripción a dicha red de acceso hacia un punto de acceso (AP) de dicha red de acceso;
recibir (217), desde dicho punto de acceso, un mensaje que contiene al menos un primer parámetro de autentificación (RAND, AUTN) proporcionado por un servidor de abonados residencial (HSS) del terminal;
enviar (217), hacia dicho punto de acceso, una respuesta que contiene un valor (RES) calculado por el terminal a partir del al menos un primer parámetro de autentificación;
recibir (217), desde dicho punto de acceso, un mensaje de asociación de seguridad que contiene al menos un parámetro de asociación de seguridad (B-TID, Tks) adecuado para ser utilizado por el terminal para autentificarse durante una conexión con una aplicación.

14. Programa informático que incluye unas instrucciones para la ejecución de las etapas del procedimiento según una cualquiera de las reivindicaciones 1 a 11 cuando dicho programa se ejecuta por un ordenador.

15. Soporte de registro, legible por un ordenador, sobre el que se registra un programa informático que comprende unas instrucciones para la ejecución de las etapas del procedimiento según una cualquiera de las reivindicaciones 1 a 11.

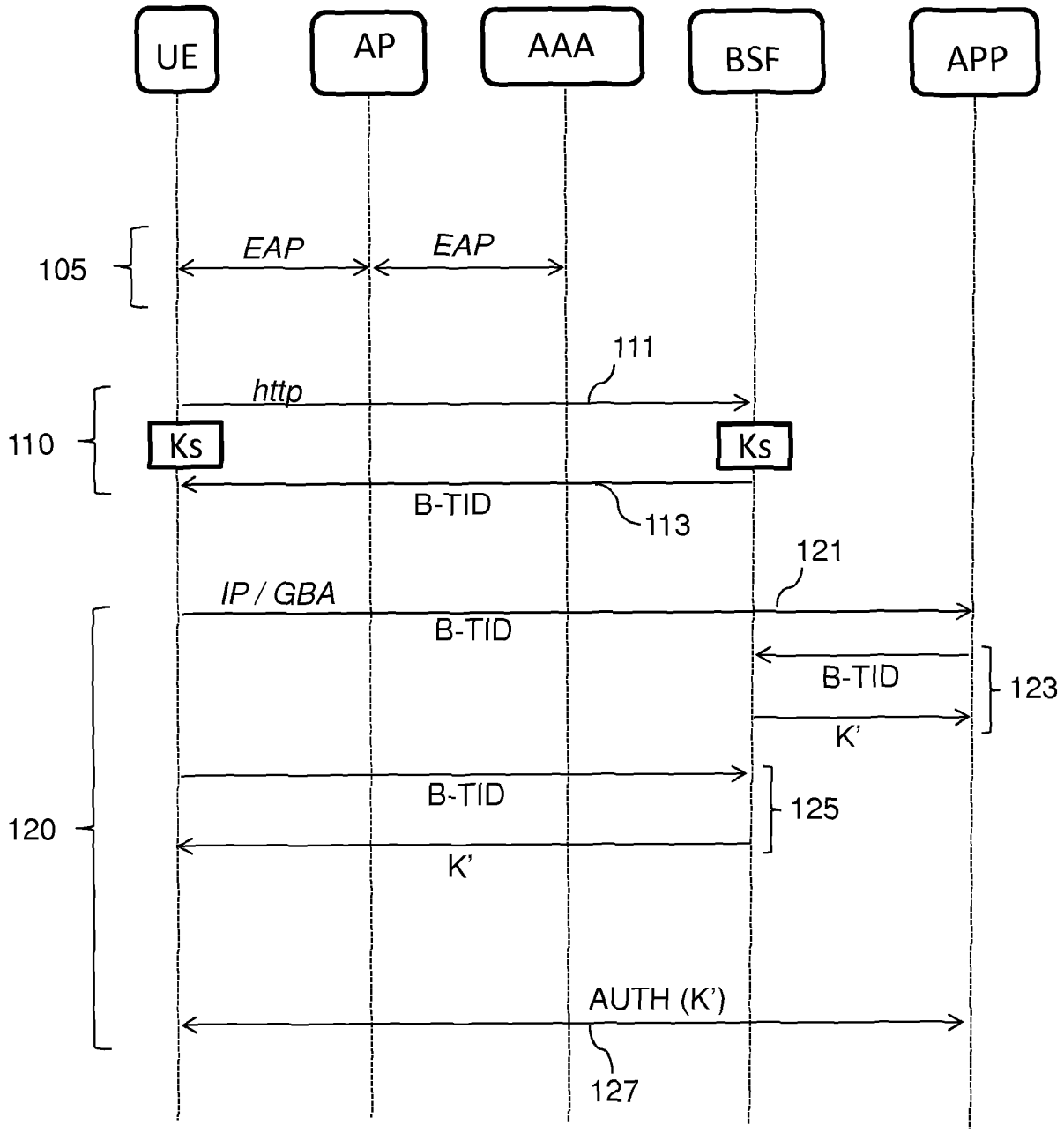
UE
AP
AAA
BSF
APP
105
EAP
EAP
111
http
110
Ks
Ks
B-TID
113
121
IP / GBA
B-TID
B-TID
123
K'
B-TID
125
120
K'
AUTH (K')
127

Fig. 1

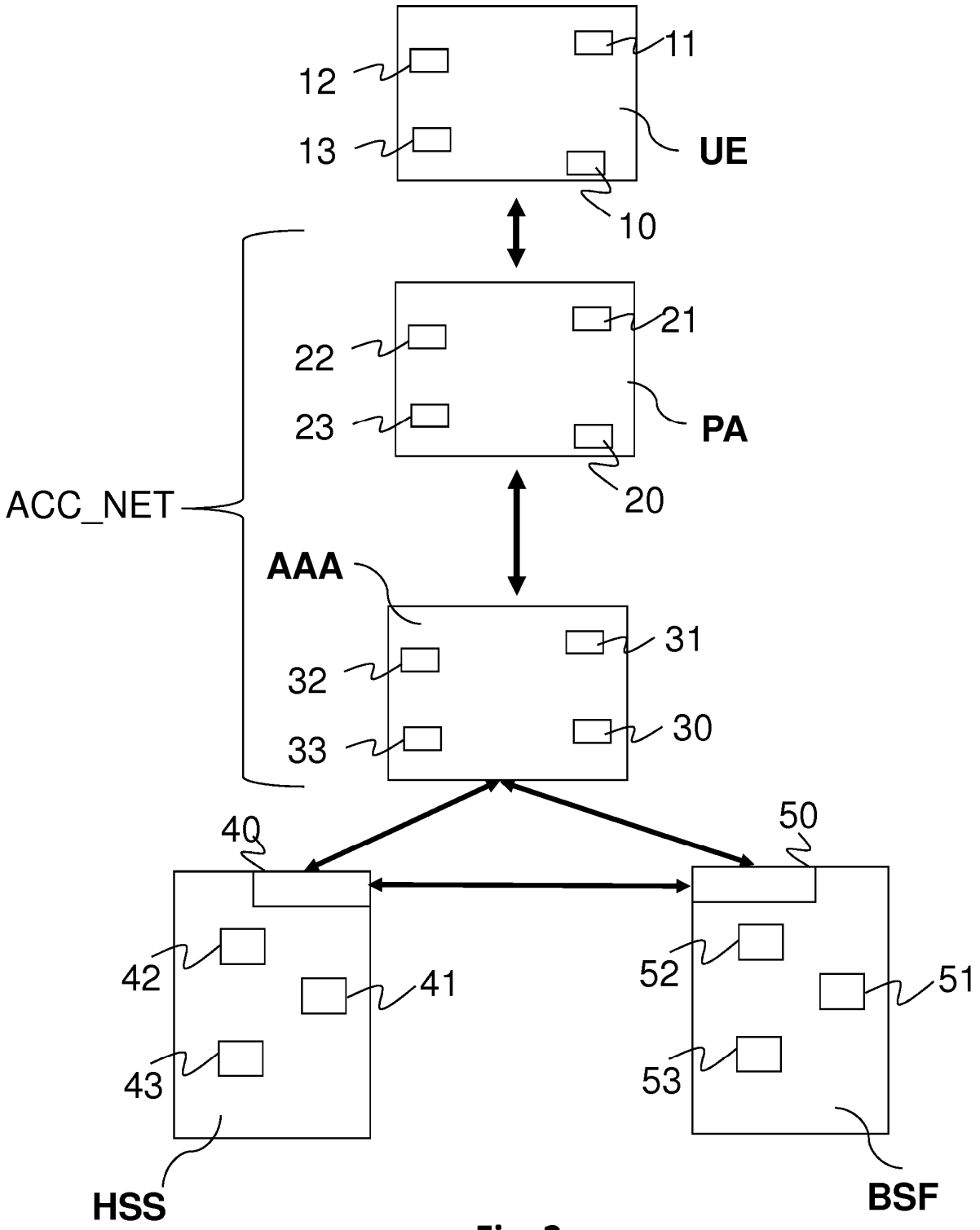
12
13
11
UE
10
22
23
21
PA
20
ACC_NET
AAA
32
33
31
30
40
50
42
41
43
52
51
53
HSS
BSF

Fig. 2

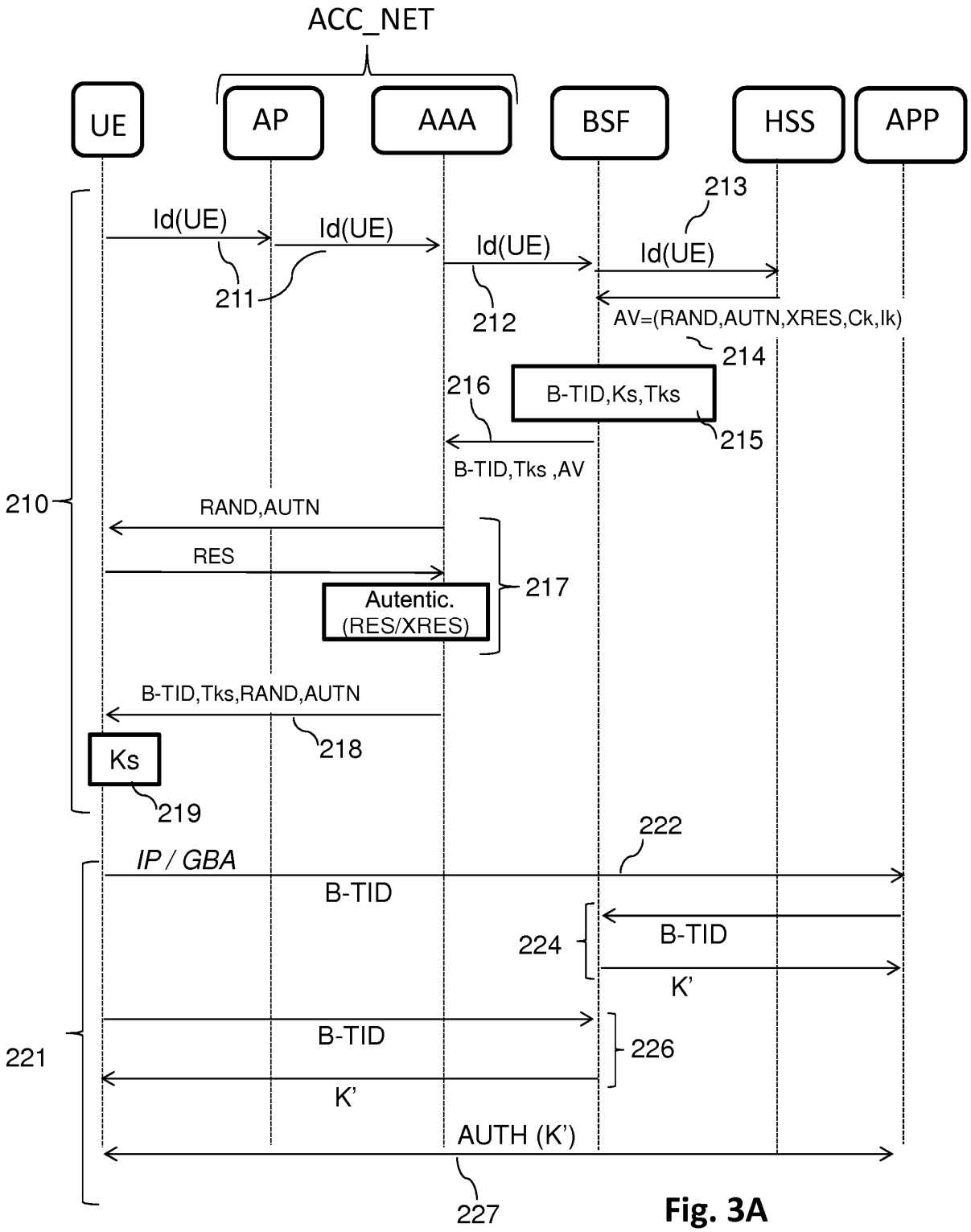
ACC_NET
UE
AP
AAA
BSF
HSS
APP
213
Id(UE)
Id(UE)
Id(UE)
Id(UE)
211
212
AV=(RAND,AUTN,XRES,Ck,Ik)
214
216
B-TID,Ks,Tks
215
B-TID,Tks ,AV
210
RAND,AUTN
RES
Autentic.
(RES/XRES)
217
B-TID,Tks,RAND,AUTN
218
Ks
219
222
IP / GBA
B-TID
224
B-TID
K'
221
B-TID
226
K'
AUTH (K')
227

Fig. 3A

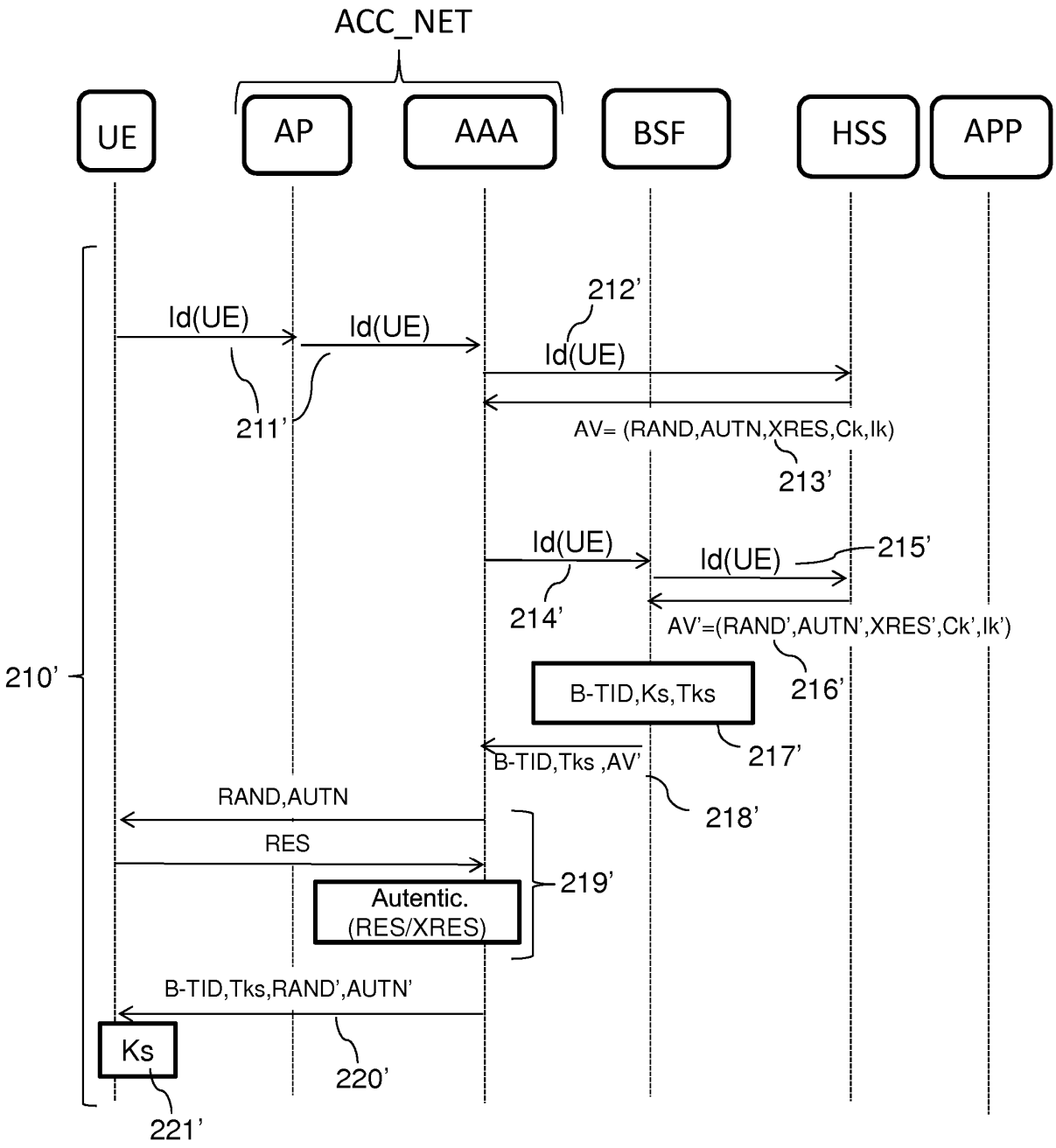
ACC_NET
UE
AP
AAA
BSF
HSS
APP
Id(UE)
Id(UE)
212'
Id(UE)
211'
AV= (RAND,AUTN,XRES,Ck,Ik)
213'
Id(UE)
Id(UE)
215'
214'
AV'=(RAND',AUTN',XRES',Ck',Ik')
210'
B-TID,Ks,Tks
216'
217'
B-TID,Tks ,AV'
218'
RAND,AUTN
RES
219'
Autentic.
(RES/XRES)
B-TID,Tks,RAND',AUTN'
Ks
220'
221'

Fig. 3B

1	2	3	4
01234567	01234567	01234567	01234567
Código	Identificador	Longitud	
Tipo	Tipo-Datos...		

Fig. 4A

1	2	3	4
01234567	01234567	01234567	01234567
Código	Identificador	Longitud	
Tipo	Subtipo	Reservado	
Tipo atributo	Longitud	Valor...	

Fig. 4B

1	2	3	4
01234567	01234567	01234567	01234567
Código	Identificador	Longitud	
Tipo	Subtipo	Reservado	
z	p	B-TID	

Fig. 4C