(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 569 400**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 80/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.12.2006 E 06830684 (4)**

(97) Fecha y número de publicación de la concesión europea: **16.03.2016 EP 1985086**

(54) Título: **Procedimiento para transmitir datos en una red de comunicación**

(30) Prioridad:

13.02.2006 DE 102006006549

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.05.2016

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
WITTELSBACHERPLATZ 2
80333 MÜNCHEN, DE

(72) Inventor/es:

FALK, RAINER y
KOHLMAYER, FLORIAN

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO PARA TRANSMITIR DATOS EN UNA RED DE COMUNICACIÓN

DESCRIPCIÓN

La invención se refiere a un procedimiento y a un equipo para transmitir datos en una red de comunicación.

Para impulsar la compatibilidad e interoperabilidad de redes de comunicación de banda ancha, ligadas a línea física, se han reunido varios interesados en el llamado Foro WiMax (www.wimaxforum.org). Un objetivo de este foro es confeccionar una norma que posibilite que aparatos terminales de comunicación móviles puedan acceder a distintas redes de comunicación.

Al respecto está previsto que en una solicitud a la red para autentificar un abonado de comunicación en una red de comunicación se utilice el protocolo EAP (Extensible Authentication Protocol, protocolo de autentificación extensible). Al respecto se deduce en el protocolo EAP, además de la autentificación, también una clave criptográfica, que se incluye para proteger la comunicación en la red de comunicación. En particular se protege la comunicación sobre una sección de transmisión ligada a línea física. Una autentificación de abonado de comunicación basada en el protocolo EAP se utiliza hoy día entre otros también para un acceso seguro a la red a través de WLAN o en un acceso a la red basado en PANA (Protocol for carrying Authentication for Network Access, protocolo para realizar la autentificación para el acceso a red).

Además está previsto generar material adicional de claves sobre la base de la autentificación basada en EAP y con ello garantizar una comunicación segura del abonado de comunicación con otros servidores de servicios en la red de comunicación. Esto trae como consecuencia que un servidor de autentificación (AAA-Server) basado en el protocolo EAP se convierta en un servidor distribuidor de claves. En el caso de que por ejemplo un abonado de comunicación solicite un servicio a un servidor de servicios, utiliza el mismo una clave deducida de la solicitud EAP para proteger la solicitud de servicios. Para comprobar la solicitud de servicios pide el servidor de servicios al servidor de autentificación esta clave para el abonado de comunicación, que se genera en el servidor de autentificación en base a los datos memorizados durante la sesión de autentificación.

Al respecto es problemático que un abonado de comunicación tenga la posibilidad de realizar en paralelo varias autentificaciones EAP en el mismo servidor de autentificación o por ejemplo realizar en una re-autentificación varias autentificaciones EAP consecutivamente, sin que ya haya transcurrido el periodo de validez de la autentificación EAP precedente. Además existe la posibilidad de que un abonado de comunicación utilice a la vez varios aparatos, como por ejemplo PDA, teléfono móvil o notebook y para cada uno de estos aparatos realice una autentificación EAP. Además tiene el abonado de comunicación la posibilidad de anunciarse a través de distintos servidores proxy (intermediarios) de autentificación en distintas redes de comunicación a la vez, como por ejemplo WLAN, 3GPP y redes WiMax, que no obstante acceden todas al mismo servidor de autentificación de la red de origen del abonado de comunicación.

Todos estos escenarios descritos traen como consecuencia que para un mismo abonado de comunicación existan en el mismo servidor de autentificación varias claves válidas procedentes de distintas autentificaciones EPA. Al respecto es problemático en particular que un servidor de servicios no pueda determinar si una cierta cantidad de claves diferentes proceden de un abonado de comunicación o proceden en cada caso de un abonado de comunicación distinto. Esto da lugar en determinadas condiciones a que al no poder determinarse la clave se interrumpa la comunicación y/o se rechace una solicitud de servicio. Esto puede dar lugar también a que el servidor de servicios establezca otra sesión adicional de abonado cuando el abonado utiliza otra clave igualmente válida. Esto ocupa innecesariamente recursos en el servidor de servicios y al abonado no se le ofrece un servicio unificado.

Un objetivo de la presente invención es así indicar un procedimiento mediante el cual la clave obtenida de un servidor de autentificación pueda asociarse a abonados de comunicación individuales y con ello quede garantizada una comunicación estable en la red de comunicación.

Según la invención se logra este objetivo mediante un procedimiento, un equipo de autentificación, así como un equipo con las características de la reivindicación 1, de la reivindicación 13 y de la reivindicación 14. Ventajosos perfeccionamientos de la presente invención se describen en las reivindicaciones dependientes.

En el procedimiento correspondiente a la invención para transmitir datos en una red de comunicación dispone un abonado de comunicación de al menos una identidad de abonado de comunicación. El abonado de comunicación transmite al menos un mensaje de autentificación que contiene la identidad del abonado de comunicación a un equipo de autentificación según el protocolo EAP (Extensible Authentication Protocol). Cuando la autentificación ha tenido éxito, se memorizan informaciones sobre el

abonado de comunicación en el equipo de autentificación. El equipo de autentificación proporciona en una transmisión de datos a los otros elementos de red de comunicación un identificador que puede asociarse al abonado de comunicación. Las informaciones del abonado de comunicación memorizadas en el equipo de autentificación pueden incluir una información de que el abonado de comunicación se ha autentificado con éxito ("session"), un identificador (siempre que no exista ya) que puede asociarse al abonado de comunicación y material de claves. Esto tiene la ventaja de que a otro elemento de red de comunicación, como por ejemplo un servidor de servicios, le resulta posible tratar a un abonado de comunicación que utilizando diversas sesiones de autentificación desearía utilizar un servicio suyo, también como el mismo abonado de comunicación. Esto funciona incluso cuando el abonado de comunicación no utiliza frente al servidor de servicios ningún identificador del abonado de comunicación asociado al mismo inequívocamente, como por ejemplo un NAI, Network Access Identifier (identificador de acceso a red). Así el material de claves proporcionado por un equipo de autentificación a partir de distintas sesiones de autentificación de un usuario puede asociarlo el servidor de servicios a un único usuario. De esta manera puede utilizar el usuario material de claves procedente de cualquier sesión de autentificación válida en ese momento para codificar con seguridad una solicitud de servicios a un servidor de servicios.

Además es posible que un abonado de comunicación utilice para distintas autentificaciones en cada caso un identificador de abonado de comunicación diferente. Igualmente puede utilizar aquél el mismo método de autentificación para establecer distintas autentificaciones o utilizar en cada caso un método de autentificación distinto. Por ello necesita el servidor de autentificación datos, que hacen posible una asociación al correspondiente abonado de comunicación independientemente del método de autentificación utilizado o del identificador del abonado de comunicación utilizado.

Según una configuración mejorada de la presente invención, transmite el equipo de autentificación, cuando hay una solicitud de datos del abonado de comunicación a través de otro elemento de comunicación, los datos solicitados juntamente con el identificador del abonado de comunicación. Esto tiene el efecto ventajoso de que para una solicitud de servicios para la que el servidor de servicios no conoce ninguna clave que encaje, transmite el servidor de autentificación la clave correspondiente junto con el identificador asociado al abonado de comunicación. Incluso cuando el abonado de comunicación utilice en consultas al servidor de servicios varios identificadores del abonado de comunicación o bien éstos no sean inequívocos frente al servidor de servicios, puede asociar el servidor de servicios mediante el identificador asociado al abonado de comunicación las consultas a un usuario. Puesto que el identificador que puede asociarse a un usuario se transmite a un servidor de servicios, queda mejor protegida la esfera privada del abonado; el servidor de servicios sólo puede detectar con ello que se han formulado varias consultas desde el mismo abonado, pero dicho servidor no conoce la identidad del abonado. El servidor de autentificación puede aportar de retorno también varias claves o enviar a la vez adicionalmente informaciones sobre la clave, como por ejemplo un Security Parameter Index (índice de seguridad de parámetros) asociado al mismo, una indicación sobre el procedimiento de seguridad que el mismo puede utilizar o valores de cómputo para utilizar esa clave. Este servidor de servicios compara los identificadores recibidos con los identificadores que ya conoce y asocia la solicitud de servicios al abonado de comunicación correspondiente al identificador. Si el identificador trasmitido le es aún desconocido al servidor de servicios, establece el mismo una nueva sesión. La solicitud de servicios puede decodificarse directamente con la clave transmitida o con una clave derivada de la misma. La clave o bien la clave derivada de la misma puede utilizarse a su vez para proteger la respuesta de servicios del servidor de servicios al abonado de comunicación.

Según otra variante ventajosa de la presente invención, transmite el equipo de autentificación un primer mensaje con el identificador del abonado de comunicación a otro elemento de red de comunicación o a un grupo de ellos. En base al mensaje finalizan procesos de comunicación predeterminados del abonado de comunicación identificado con estos otros elementos de comunicación y/o se borran informaciones predeterminadas del abonado de comunicación identificado de estos otros elementos de red de comunicación. Esto tiene el efecto ventajoso de que el equipo de autentificación puede finalizar las sesiones de autentificación asociadas al identificador, por ejemplo porque los importes de prepago del abonado de comunicación han expirado o porque la cuenta de usuario del abonado de comunicación se ha borrado o invalidado. Una ventaja adicional es que los recursos ocupados por las distintas sesiones de autentificación se liberan de nuevo con rapidez en el servidor de servicios. Otro efecto ventajoso es que de esta manera puede forzar el servidor de autentificación un rollover (extensión del plazo) de las sesiones de autentificación, es decir, que el correspondiente abonado de comunicación debe establecer nuevas sesiones de autentificación con el servidor de autentificación o los servidores de servicios. Mediante el correspondiente parámetro en el primer mensaje puede además darse a conocer que sólo deben finalizar las sesiones de autentificación, pero que el correspondiente identificador debe seguir siendo válido.

Según otro perfeccionamiento ventajoso de la presente invención modifica el equipo de autentificación el identificador del abonado de comunicación y se comunica el identificador modificado a los otros elementos de red de comunicación en otro segundo mensaje. Esto tiene el efecto ventajoso de que a iniciativa del servidor de autentificación el identificador de un abonado de comunicación frente a los

servidores de servicios se sustituye por un nuevo identificador y de esta manera mejora aún más la privacy (esfera privada) del abonado de comunicación frente a la red de comunicación, ya que un ente externo no puede asociar al mismo abonado de comunicación dos identificadores diferentes de un abonado de comunicación. También puede estar previsto para un grupo de servidores de menos confianza hacer borrar los identificadores en un primer mensaje y para servidores de servicios de confianza hacer sustituir los identificadores antiguos en un segundo mensaje por nuevos identificadores. Esto tiene además la ventaja de que se logra una gran flexibilidad en la gestión de los identificadores de abonados de comunicación mediante el equipo de autentificación.

Según un perfeccionamiento de la presente invención, está previsto como equipo de autentificación al menos un servidor proxy de autentificación de una red intermedia, que retransmite mensajes de autentificación a un servidor de autentificación de una red de origen del abonado de comunicación. La identidad del abonado de comunicación y el identificador del abonado de comunicación se memorizan en el servidor proxy de autentificación y el servidor de autentificación de la red de origen. Esto tiene la ventaja de que incluso cuando un abonado de comunicación se anuncie en distintas redes de comunicación con un servidor proxy de autentificación distinto en cada caso, sigue pudiendo determinarse la identidad del abonado de comunicación frente a los correspondientes servidores de servicios.

El equipo de autentificación correspondiente a la invención en una red de comunicación memoriza en la red de comunicación, cuando la autentificación de un abonado de comunicación ha tenido éxito, informaciones sobre el abonado de comunicación y al menos un identificador que puede asociarse al abonado de comunicación. En una transmisión de datos proporciona el equipo de autentificación el identificador que puede asociarse a los abonados de comunicación a otros elementos de la red de comunicación.

La presente invención se describirá a continuación más en detalle con ejemplos de ejecución en base a los dibujos. Se muestra en

figura 1 en una representación esquemática una estructura de la red de comunicación con distintas redes de acceso,
figura 2 en una representación esquemática una secuencia del procedimiento con dos autentificaciones distintas de un abonado de comunicación,
figura 3 en una representación esquemática una posible asociación de diversos parámetros del procedimiento a un abonado de comunicación.

La figura 1 muestra una representación esquemática de una red con tres abonados de comunicación 101, 102, 103, que tienen en cada caso acceso a una red núcleo 107 a través de una de tres redes de acceso diferentes 104, 105, 106. La red núcleo 107 incluye cuatro servidores de servicios distintos 108, 109, 110, 111, que proporcionan cada uno distintos servicios. Además incluye la red núcleo 107 un servidor de autentificación 112. Usualmente comienza una solicitud de red de un abonado de comunicación con una autentificación. Aquí enviaría por ejemplo el abonado de comunicación 101 a través del servidor proxy de autentificación de la red de acceso 106 un mensaje de autentificación al servidor de autentificación 112 de su red de origen. Cuando la autentificación ha tenido éxito, se deduce para el abonado de comunicación 101 en el servidor de autentificación una primera clave, que incluye el abonado de comunicación 101 para otras comunicaciones con la red de acceso 106. A la vez se anuncia el abonado de comunicación 101 a través de la red de acceso 104 con otro aparato terminal de comunicación en el servidor de autentificación 112 de la red núcleo, a continuación de lo cual deduce el equipo de autentificación una segunda clave para el abonado de comunicación 101. Si ahora formula el abonado de comunicación 101 una solicitud de servicios a través de la red de acceso 106 al servidor de servicios 108, que el mismo ha codificado con la primera clave, entonces solicita el servidor de servicios 108 al servidor de autentificación 112 la clave correspondiente y recibe el material de claves junto con un identificador, que da a conocer al primer abonado de comunicación 101. Además solicita el abonado de comunicación 101 a través de la red de acceso 104 al mismo servidor de servicios 108 otro servicio, estando codificada la solicitud de servicios con la segunda clave. A continuación recibe el servidor de servicios 108 a demanda del servidor de autentificación 112 la segunda clave junto con un identificador del primer abonado de comunicación 101. De esta manera sabe el servidor de servicios 108 que ambas solicitudes de servicios las ha realizado el mismo abonado de comunicación 101.

La figura 2 muestra en una representación esquemática una secuencia del procedimiento en dos autentificaciones diferentes de un abonado de comunicación. En una primera autentificación 204 realiza el abonado de comunicación 201, según el método de autentificación EAP-TLS, una autentificación en el servidor de autentificación 203. A continuación envía el abonado de comunicación 201 una solicitud de servicios protegida por una primera clave 205 deducida durante la autentificación al servidor de servicios 102. Si la primera clave utilizada no es conocida por el servidor de servicios 202, solicita el mismo esta clave al servidor de autentificación 203 en 206 y recibe la primera clave 207 junto con un identificador del abonado de comunicación 201, que en este ejemplo se denomina FASI (Federated Authentication Session Identifier, identificador de sesión de autentificación federada). A continuación contesta el servidor

de servicios 202 con una respuesta de servicio 208 al abonado de comunicación 201, protegiéndose la respuesta de servicio opcionalmente mediante la primera clave. En otra solicitud de servicio 209 por parte del abonado de comunicación 201, que está codificada mediante la primera clave, responde el servidor de servicios 202 sin consulta de retorno al servidor de identificación 203, ya que ahora conoce la primera clave 210.

En una segunda autentificación 211 se autentifica el abonado de comunicación 201 según el método de autentificación EAP-AKA en el servidor de autentificación 203, a continuación de lo cual se deduce una segunda clave de la segunda autentificación 211. Si ahora envía el abonado de comunicación 201 una solicitud de servicio 212 al servidor de servicios 202, que ahora está codificada con la segunda clave, envía el servidor de servicios 202 una solicitud para esta clave 213 al servidor de autentificación 203, ya que el mismo no conoce la segunda clave. A continuación conserva el servidor de servicios 202 mediante el servidor de autentificación 203 la segunda clave junto con el identificador FASI 214 del abonado de comunicación 201. En base al identificador FASI reconoce el servidor de servicios 202 que la solicitud de servicio codificada con la segunda clave corresponde al mismo abonado de comunicación que en la solicitud de servicios codificada con la primera clave. En base a ello, añade el servidor de servicios 202 la segunda clave a la sesión de usuario ya existente con el abonado de comunicación 201 y envía una respuesta de servicio 215 al abonado de comunicación 201, que está codificada opcionalmente con la segunda clave.

La figura 3 muestra a modo de ejemplo posibles relaciones entre identificadores 310 y 311 utilizados para un abonado de comunicación 301 e identificadores de abonado de comunicación 302 a 304 utilizadas por el abonado de comunicación 301, sesiones de autentificación 305 a 309 y servidores de servicios 312 a 314. Así es posible según la presente invención que un abonado de comunicación 301 posea tres identificadores de abonado de comunicación 302, 303, 304 distintos y utilice el primer identificador del abonado de comunicación 302 para dos sesiones de autentificación distintas 305 y 300 y el tercer identificador del abonado de comunicación 304 para tres sesiones de autentificación distintas 307, 308 y 309. El equipo de autentificación ha asociado ahora las distintas sesiones de autentificación del abonado de comunicación 301 tal que para los dos primeros servidores de servicios 312 y 313 las sesiones de autentificación 306, 307 y 308, caracterizadas por el identificador FASI 310, retornan al mismo abonado de comunicación y para el servidor de servicios 304 han de atribuirse las sesiones de autentificación 308 y 309 identificadas por el identificador FASI 311 al mismo abonado de comunicación.

Las ventajas de la invención se compendiarán de nuevo a continuación.

La presente invención hace posible utilizar un servidor de autentificación basado en EAP como servidor distribuidor de claves para servidores de servicios.

El servidor de servicios funciona con la invención incluso cuando un usuario realiza varias autentificaciones EAP y como consecuencia ya no está establecida sólo una única clave de sesión para un determinado usuario. Otras ventajas son que ya no se llega a Race-Conditions (condiciones de carrera) con las que se dependa de la secuencia en el tiempo de las autentificaciones realizadas, cuya clave se proporciona a un servidor de servicios. Esto traería como consecuencia que con una clave falsa el servicio ya no podría utilizarse. Cuando en algunos casos la clave proporcionada o utilizada proceda de otra autentificación, puede a pesar de ello el servidor de servicios asociar está clave al usuario actual, aun cuando el mismo previamente ha utilizado una clave diferente procedente de otra autentificación anterior. Esto es esencial para Macro-Mobility-Management (gestión de macro-movilidad) o Vertical Handovers (transferencias verticales) cuando se realiza en los mismos una nueva autentificación o re-autentificación para el acceso a la red, en la que se establece nuevo material de claves.

Otro efecto ventajoso resulta cuando el servidor de autentificación (servidor AAA) desea finalizar una sesión FASI y el mismo informa de ello a todos los servidores de servicios. De esta manera finalizan todas las sesiones de autentificación asociadas a FASI. Esto ahorra recursos en los servidores de servicios y se evita que cuando finaliza la sesión se mantengan sesiones de autentificación que aún pueden utilizarse en servidores de servicios.

La invención facilita además utilizar el servidor de autentificación para otros servicios, ya que el mismo no tiene que entender la semántica de los identificadores de un servicio especial. Así pueden utilizarse seudónimos cambiantes o identificadores de usuario anónimos frente al servidor de servicios. El servidor de servicios no aprende necesariamente un ID de usuario permanentemente válido, ya que la sesión de autentificación virtual FASI puede ser cualquier identificador.

La presente invención no queda limitada a los ejemplos de ejecución aquí descritos.

REIVINDICACIONES

1. Procedimiento para transmitir datos en una red de comunicación, en el que
   - un abonado de comunicación dispone de al menos una identidad de abonado de comunicación,
   - el abonado de comunicación transmite al menos un mensaje de autentificación, que contiene la identidad del abonado de comunicación, a un equipo de autentificación según el protocolo EAP Extensible Authentication Protocol,
   - cuando la autentificación ha tenido éxito, se memorizan informaciones sobre el abonado de comunicación en el equipo de autentificación,

   caracterizado porque
   - el equipo de autentificación proporciona en una transmisión de datos a otros elementos de red de comunicación un identificador que puede asociarse al abonado de comunicación,
   - el equipo de autentificación transmite un primer mensaje con el identificador del abonado de comunicación que puede asociarse a otro elemento de red de comunicación o a un grupo de ellos,
   - en base al primer mensaje finalizan procesos de comunicación predeterminados del abonado de comunicación identificado con estos otros elementos de comunicación y/o se borran informaciones predeterminadas del abonado de comunicación identificado de estos otros elementos de red de comunicación.

2. Procedimiento según la reivindicación 1,
en el que otros elementos de red de comunicación son servidores de servicios en la red de comunicación.

3. Procedimiento según la reivindicación 2,
en el que el servidor de servicios es un servidor de movilidad, en particular un Mobil-IP-Home-Agent (agente propio de IP móvil).

4. Procedimiento según la reivindicación 1,
en el que las redes de comunicación están configuradas como red WiMax, red WLAN y/o redes de telefonía móvil 3GPP.

5. Procedimiento según la reivindicación 1,
en el que el equipo de autentificación, cuando hay una solicitud de datos del abonado de comunicación por parte de otro elemento de red de comunicación, transmite los datos solicitados junto con los identificadores del abonado de comunicación que pueden asociarse.

6. Procedimiento según la reivindicación 5,
en el que los datos solicitados incluyen una clave criptográfica.

7. Procedimiento según la reivindicación 6,
en el que la clave criptográfica se ha deducido de la autentificación del abonado de comunicación frente al equipo de autentificación.

8. Procedimiento según la reivindicación 1,
en el que el equipo de autentificación prevé en cada caso para otro elemento de red de comunicación o un grupo de otros elementos de red de comunicación un identificador del abonado de comunicación unificado que puede asociarse.

9. Procedimiento según la reivindicación 1,
en el que
   - el equipo de autentificación modifica el identificador del abonado de comunicación que puede asociarse,
   - el identificador modificado se comunica a los otros elementos de red de comunicación en un segundo mensaje.

10. Procedimiento según la reivindicación 1,
en el que
   - como equipo de autentificación está previsto al menos un servidor proxy de autentificación de una red intermedia, que retransmite mensajes de autentificación a un servidor de autentificación de una red de origen del abonado de comunicación,
   - la identidad del abonado de comunicación y el identificador del abonado de comunicación que puede asociarse se memorizan en el servidor proxy de autentificación y el servidor de autentificación de la red de origen.

11. Procedimiento según la reivindicación 1,

en el que el mensaje de autentificación se transmite según un protocolo de transmisión de datos RADIUS.

12. Procedimiento según la reivindicación 1,
en el que los mensajes de autentificación se transmiten según un protocolo de transmisión de datos Diameter.

13. Equipo de autentificación en una red de comunicación,
en el que
- cuando la autentificación de un abonado de comunicación ha tenido éxito en la red de comunicación, se memoriza al menos un identificador que puede asociarse al abonado de comunicación,

caracterizado porque
- el equipo de autentificación proporciona en una transmisión de datos a otros elementos de red de comunicación un identificador que puede asociarse al abonado de comunicación,
- el equipo de autentificación transmite un primer mensaje con el identificador del abonado de comunicación que puede asociarse a otro elemento de red de comunicación o a un grupo de ellos,
- en base al primer mensaje finalizan procesos de comunicación predeterminados del abonado de comunicación identificado con estos otros elementos de comunicación y/o se borran informaciones predeterminadas del abonado de comunicación identificado de estos otros elementos de red de comunicación.

14. Equipo en una red de comunicación,
en el que
- el identificador que puede asociarse según la reivindicación 13 está incluido en una transmisión de datos del equipo de autentificación según la reivindicación 13,
- en base al identificador incluido se ha realizado una asociación de los datos transmitidos a un abonado de comunicación.

FIG 1

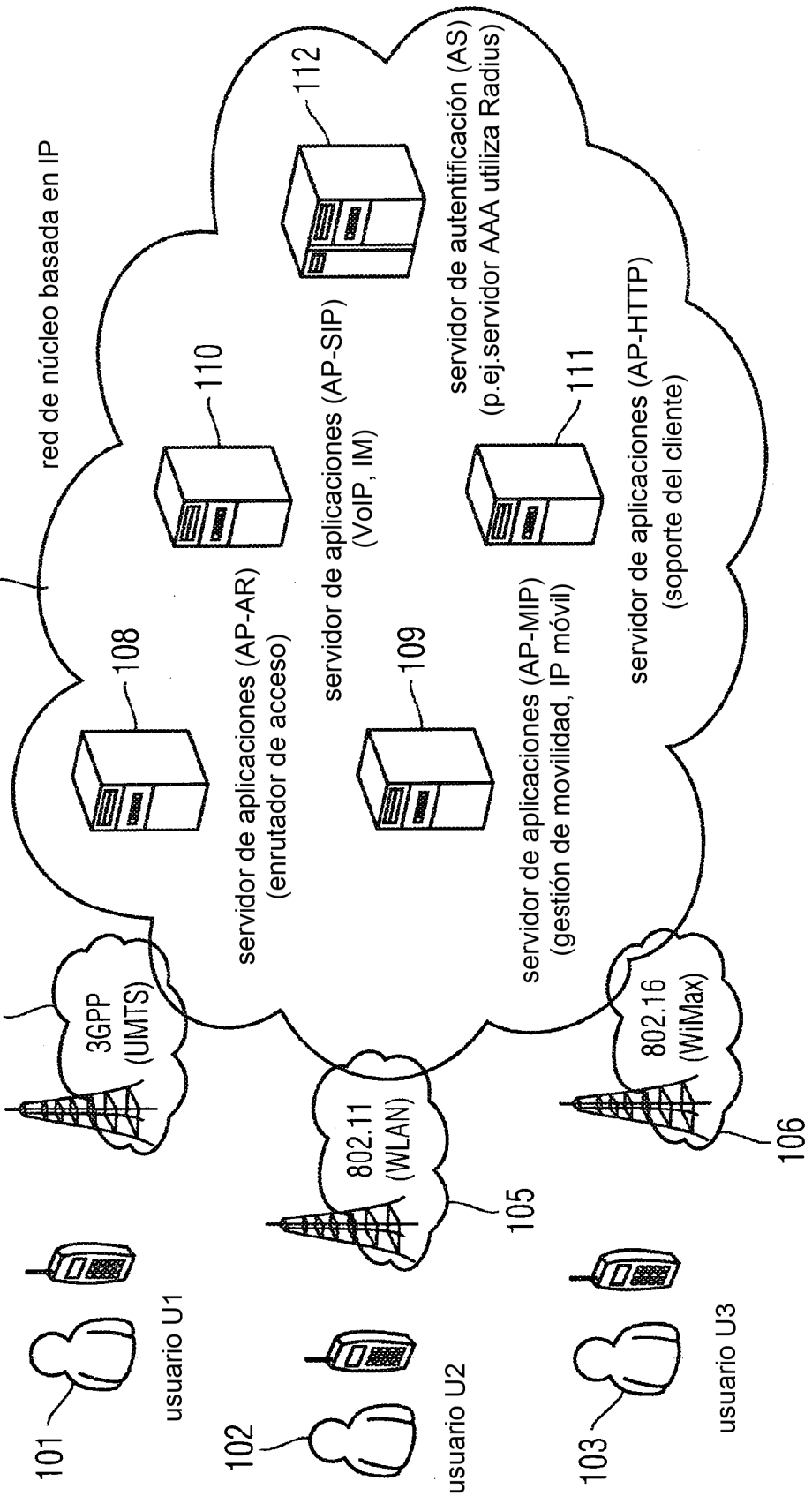

red de núcleo basada en IP
107
servidor de aplicaciones (AP-AR)
(enrutador de acceso)
108
servidor de aplicaciones (AP-SIP)
(VoIP, IM)
110
servidor de autentificación (AS)
(p.ej.servidor AAA utiliza Radius)
112
servidor de aplicaciones (AP-MIP)
(gestión de movilidad, IP móvil)
109
servidor de aplicaciones (AP-HTTP)
(soporte del cliente)
111
3GPP
(UMTS)
104
802.11
(WLAN)
105
802.16
(WiMax)
106
usuario U1
101
usuario U2
102
usuario U3
103

FIG 2

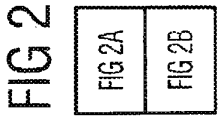


FIG 2A
FIG 2B

FIG 2A

usuario (U)
201
servidor de aplicaciones (AP)
(p.ej. MIP HA)
202
servidor de autentificación (AS)
(p.ej. servidor AAA utiliza Radius)
203
204
autentificación 1 (por ejemplo EAP con EAP-TLS) por ejemplo para autentificar un acceso WLAN a una red de empresa con un acceso de la empresa
205
solicitud de servicio (SR) protegida con clave 1 derivada de la sesión de autentificación 1
206
comprobación SR (por ejemplo ¿se conoce la clave del usuario?)
solicitud clave (comprobación implícita de si el usuario está autentificado frente a AS)
logra autentificación sesión 1 conectado con usuario U (incluyendo clave 1, FASI)
aporta clave 1 y FASI
207
logra usuario AS sesión para usuario U incluyendo clave 1 y FASI
208
respuesta servicio (opcionalmente protegido con clave 1)
209
solicitud servicio (SR) protegido con clave 1 derivada de la sesión de autentificación 1

FIG 2B

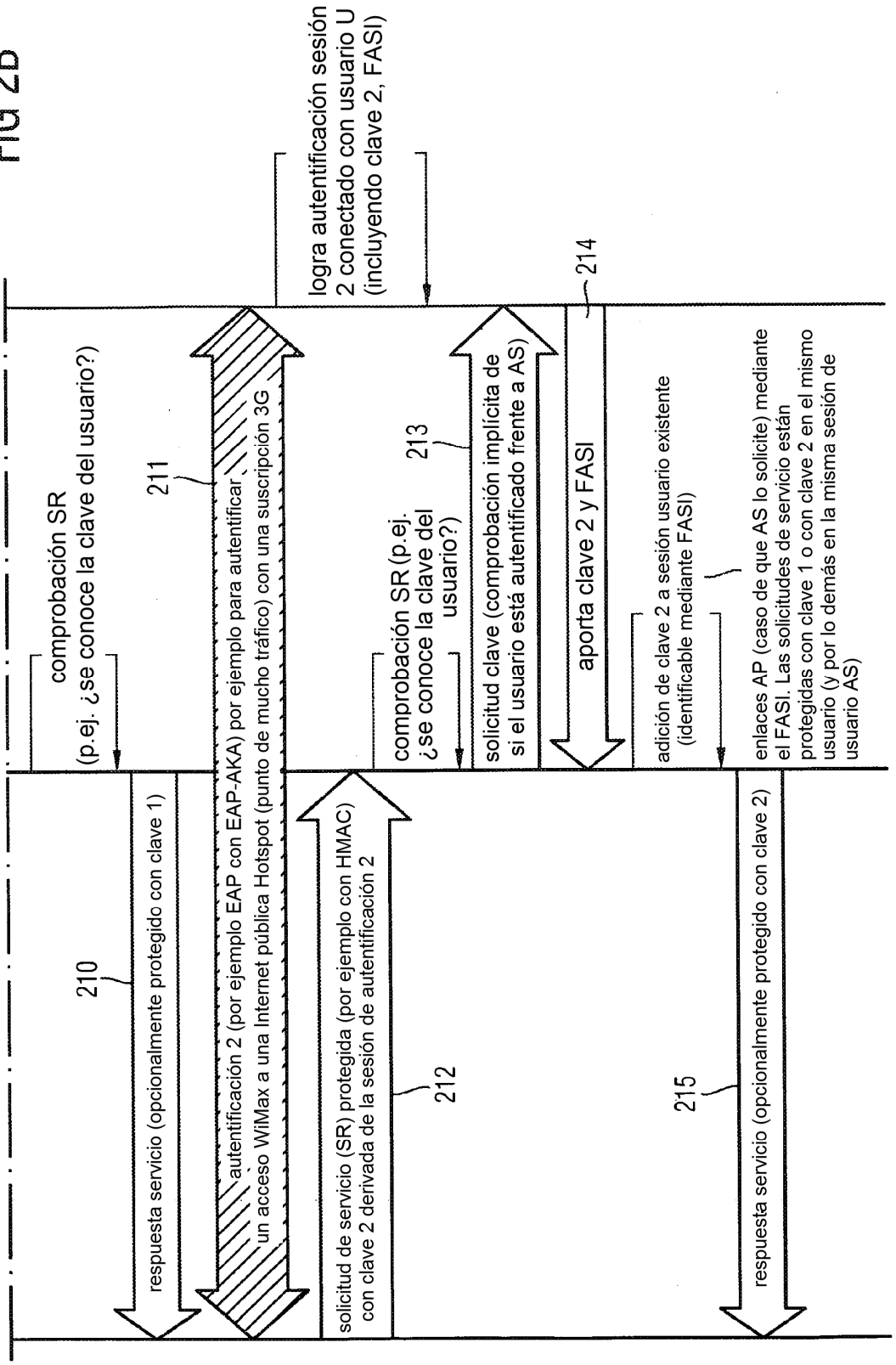
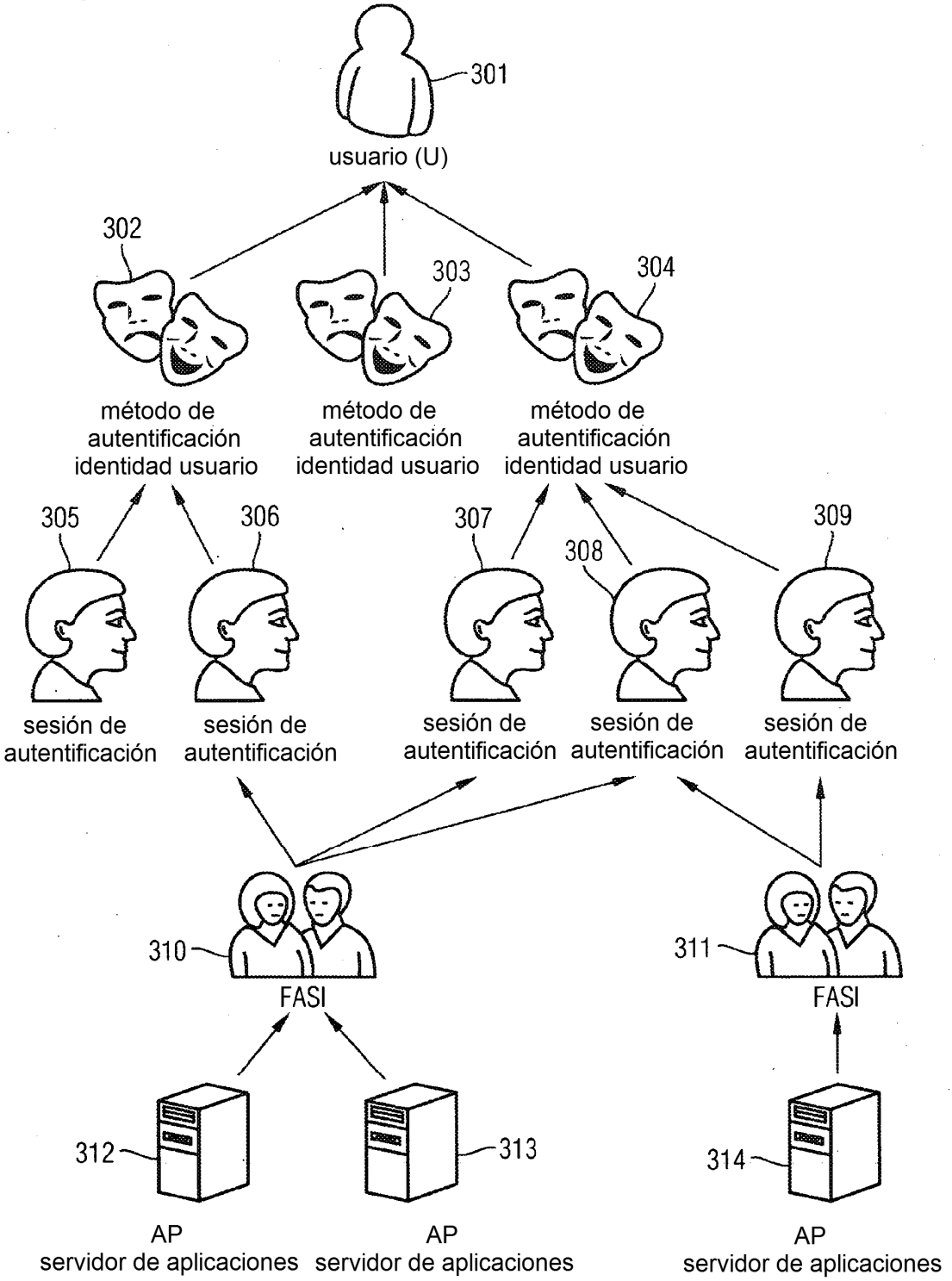

logra autentificación sesión 2 conectado con usuario U (incluyendo clave 2, FASI)
214
comprobación SR (p.ej. ¿se conoce la clave del usuario?)
211
213
comprobación SR (p.ej. ¿se conoce la clave del usuario?)
solicitud clave (comprobación implícita de si el usuario está autentificado frente a AS)
aporta clave 2 y FASI
adición de clave 2 a sesión usuario existente (identificable mediante FASI)
enlaces AP (caso de que AS lo solicite) mediante el FASI. Las solicitudes de servicio están protegidas con clave 1 o con clave 2 en el mismo usuario (y por lo demás en la misma sesión de usuario AS)
210
respuesta servicio (opcionalmente protegido con clave 1)
autentificación 2 (por ejemplo EAP con EAP-AKA) por ejemplo para autentificar un acceso WiMax a una Internet pública Hotspot (punto de mucho tráfico) con una suscripción 3G
212
solicitud de servicio (SR) protegida (por ejemplo con HMAC) con clave 2 derivada de la sesión de autentificación 2
215
respuesta servicio (opcionalmente protegido con clave 2)

FIG 3


301
usuario (U)
302
303
304
método de autentificación identidad usuario
método de autentificación identidad usuario
método de autentificación identidad usuario
305
306
307
308
309
sesión de autentificación
sesión de autentificación
sesión de autentificación
sesión de autentificación
sesión de autentificación
310
FASI
311
FASI
312
313
314
AP servidor de aplicaciones
AP servidor de aplicaciones
AP servidor de aplicaciones