(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 381 803**

(51) Int. CI.:
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08835476 .6**
(96) Fecha de presentación: **25.09.2008**
(97) Número de publicación de la solicitud: **2208375**
(97) Fecha de publicación de la solicitud: **21.07.2010**

(54) Título: **Procedimiento para autenticar unidades móviles unidas a una femtocélula en comunicación con una red central segura, tal como un IMS**

(30) Prioridad:
04.10.2007 US 997639 P
25.01.2008 US 19903

(45) Fecha de publicación de la mención BOPI:
31.05.2012

(45) Fecha de la publicación del folleto de la patente:
31.05.2012

(73) Titular/es:
Alcatel Lucent
3, avenue Octave Gréard
75007 Paris, FR

(72) Inventor/es:
MORGAN, Todd, Cartwright;
PATEL, Sarvar y
THOMPSON, Robin, Jeffrey

(74) Agente/Representante:
Carpintero López, Mario

DESCRIPCIÓN

Procedimiento para autenticar unidades móviles unidas a una femtocélula en comunicación con una red central segura, tal como un IMS

Antecedentes de la invención

1. Campo de la invención

La presente invención versa en general acerca de sistemas de comunicaciones y, más en particular, acerca de sistemas de comunicaciones inalámbricas.

2. Descripción de la técnica relacionada

Los sistemas convencionales de comunicaciones inalámbricas usan una red de estaciones base para proporcionar una conectividad inalámbrica con una o más unidades móviles. En algunos casos, las unidades clave pueden iniciar una comunicación inalámbrica con una o más estaciones base en la red; por ejemplo, cuando el usuario de la unidad móvil desease iniciar una llamada de voz o datos. Alternativamente, la red puede iniciar el enlace de comunicaciones inalámbricas con la unidad móvil. Por ejemplo, en comunicaciones inalámbricas jerárquicas convencionales, un servidor transmite voz y/o datos destinados para una unidad móvil diana a un elemento central tal como un controlador de red de radio (RNC). El RNC puede transmitir entonces mensajes de notificación a la unidad móvil diana a través de una o más estaciones base. La unidad móvil diana puede establecer un enlace inalámbrico a una o más de las estaciones base en respuesta a la recepción de la notificación del sistema de comunicaciones inalámbricas. Una función de gestión de recursos de radio dentro del RNC recibe la voz y/o los datos y coordina los recursos de radio y tiempo usados por el conjunto de estaciones base para transmitir la información a la unidad móvil diana. La función de gestión de recursos de radio puede llevar a cabo un control de alta resolución para asignar y liberar recursos para la transmisión de radiodifusión en un conjunto de estaciones base.

Se establecen comunicaciones seguras en un sistema jerárquico convencional, tal como un sistema CDMA, con base en información secreta (por ejemplo, una clave de autenticación) conocida únicamente a la unidad móvil y una entidad segura en la red. El HLR/AuC y la unidad móvil pueden derivar datos secretos compartidos (SSD) de la clave de autenticación (AK), por ejemplo usando el algoritmo CAVE. La AK es una clave secreta primaria de 64 bits conocida únicamente por la estación móvil y el HLR/AuC. Esta clave nunca es compartida con socios de itinerancia. La AK puede usarse para generar los SSD, que son una clave secundaria de 128 bits que puede ser calculada usando el algoritmo CAVE y que puede ser compartida con socios de itinerancia. Durante la autenticación, tanto el HLR/AuC como la unidad móvil calculan una respuesta de autenticación por separado e independientemente usando entradas compartidas, tales como los SSD, el número de serie electrónico (ESN), el número de identidad móvil (MIN) y un número aleatorio compartido (RAND). Si los resultados calculados independientemente coinciden, se aprueba la autenticación y se permite que la unidad móvil se dé de alta en la red.

La AK o los SSD pueden ser usados para autenticar unidades móviles que están dadas de alta en la red. Por ejemplo, una estación base puede generar periódicamente un número aleatorio (RAND) y transmitir el RAND. Las unidades móviles que reciben el RAND transmitido calculan una salida de algoritmo de autenticación (AUT) usando las entradas, incluyendo el RAND y la AK o los SSD. A veces se denomina par a la AUT y al RAND asociado (o a porciones seleccionadas del RAND). La estación móvil puede transmitir entonces el par AUT/RAND a la estación base, que puede pasar a continuación esta información, por medio de la red, al HLR/AuC. El HLR/AuC usa el algoritmo de autenticación, el valor almacenado de la AK o los SSD, otros datos correspondientes a cada unidad móvil y el RAND para calcular el valor esperado de AUT. Si este valor coincide con el valor transmitido por la unidad móvil, la unidad móvil es autenticada. La estación base cambia frecuentemente el valor de RAND para garantizar que el valor AUT sea reciente y reducir la posibilidad de que resultados AUT/RAND generados previamente puedan ser capturados monitorizando la interfaz aérea y reproducidos por una unidad móvil fraudulenta o un emulador de unidad móvil. Se considera que esta técnica es razonablemente fiable, al menos en parte, debido a que las estaciones base son típicamente dispositivos seguros que están bajo el control de proveedores de comunicaciones inalámbricas.

También puede usarse un reto único para retar a la unidad móvil. En un reto único, un centro de autenticación genera un número aleatorio único, que puede ser transmitido a la unidad móvil. La unidad móvil usa un algoritmo de seguridad para calcular una respuesta única al reto único y luego transmite información que indica al centro de autenticación el valor de la respuesta única. El centro de autenticación también ejecuta el algoritmo de seguridad para generar un valor esperado de la respuesta única. Si el centro de autenticación determina que el valor esperado de la respuesta única es igual que el valor proporcionado por la unidad móvil, la unidad móvil es autenticada entonces. Si no, se ha producido una posible violación de seguridad. Típicamente, los retos únicos son usados por sistemas que no son capaces de autenticar en el acceso al sistema, por ejemplo, usando retos globales. Los retos únicos también pueden usarse como procedimiento de autenticación de respaldo si no se produjo un intercambio válido en el acceso al sistema.

Una alternativa a la arquitectura de red jerárquica convencional es una arquitectura distribuida que incluya una red de puntos de acceso, tales como dispositivos de encaminamiento de estaciones base, que implementen una funcionalidad de red de comunicaciones distribuida. Por ejemplo, cada dispositivo de encaminamiento estación base puede combinar funciones de RNC y/o PDSN en una sola entidad que gestiones radioenlaces entre una o más unidades móviles y una red exterior, tal como Internet. En comparación con las redes jerárquicas, las arquitecturas distribuidas tienen el potencial de reducir los costes y/o la complejidad del despliegue de la red, así como el coste y/o la complejidad de añadir puntos adicionales de acceso inalámbrico, por ejemplo dispositivos de encaminamiento de estaciones base, para expandir la cobertura de una red existente. Las redes distribuidas también puede reducir (con respecto a las redes jerárquicas) los retardos experimentados por los usuarios, porque pueden reducirse o eliminarse los retardos debidos a la puesta en memoria temporal de paquetes en el RNC y el PDSN de las redes jerárquicas.

Al menos en parte, debido al coste y la complejidad reducidos del despliegue de un dispositivo de encaminamiento de estación base, los dispositivos de encaminamiento de estaciones base pueden ser desplegados en emplazamientos que son poco prácticos para estaciones base convencionales. Por ejemplo, puede desplegarse un dispositivo de encaminamiento de estación base en una vivienda o un edificio para proporcionar conectividad inalámbrica a los ocupantes o los residentes del edificio. Típicamente, los dispositivos de encaminamiento de estaciones base desplegados en una residencia son denominados dispositivos propios de encaminamiento de estaciones base o femtocélulas, porque están concebidos para proporcionar conectividad inalámbrica a una zona mucho más pequeña (por ejemplo, una femtocélula) que abarca una vivienda. Sin embargo, típicamente, la funcionalidad en una femtocélula es muy similar a la funcionalidad implementada en un dispositivo de encaminamiento convencional de estación base que esté concebido para proporcionar conectividad inalámbrica a una macrocélula que pueda abarcar un área de aproximadamente algunos kilómetros cuadrados. Una diferencia importante entre una femtocélula y un dispositivo de encaminamiento convencional de estación base es que los dispositivos propios de encaminamiento de estaciones base están diseñados para ser dispositivos económicos de conexión y uso inmediato que puedan ser comprados en puntos de venta al público e instalados con facilidad por una persona sin experiencia.

Típicamente, las femtocélulas no incluyen caros chips de seguridad para almacenar información que puedan ser usados para establecer comunicaciones seguras entre la femtocélula y las unidades móviles. Además, las femtocélulas están pensadas para ser desplegadas en emplazamientos no seguros, tales como el hogar o el negocio de una persona. En consecuencia, no se considera que las femtocélulas sean emplazamientos de confianza para almacenar claves secretas u otra información que pueda ser usada para autenticar unidades móviles. Por lo tanto, una femtocélula puede ser modificada para representar de manera fraudulenta a una unidad móvil si las femtocélulas están configuradas para generar los números aleatorios RAND usados para autenticar unidades móviles. Por ejemplo, una femtocélula ilegítima puede interceptar un par AUT/RAND válido transmitido entre una unidad móvil legítima y una estación base legítima. La femtocélula ilegítima puede emular entonces a la unidad móvil legítima usando el par AUT/RAND interceptado. Dado que la femtocélula es responsable de generar valores RAND, la red no puede determinar si el par AUT/RAND transmitido por la femtocélula ilegítima corresponde o no con un valor reciente de RAND.

El documento US 6.167.279 da a conocer un procedimiento para permitir la integración de un sistema de comunicaciones de acceso personal (PACS = sistema de comunicaciones de acceso personal) que soporta dispositivos de comunicaciones inalámbricas de radio de bajo nivel de conexión con una red GSM usada para soportar dispositivos celulares de alto nivel de conexión para permitir conexiones del sistema PACS a redes telefónicas públicas conmutadas que no tengan prestaciones avanzadas de red inteligente.

El documento “IMS security framework”, 3GPP2 S.S0086-B, versión 1.0, de 8 de diciembre de 2005, especifica características y mecanismos de seguridad para el acceso seguro al subsistema IM para el sistema 3G de telecomunicaciones móviles. El documento aborda la forma en que la señalización SIP está protegida entre el abonado y el IMS, la forma en que el abonado es autenticado y la forma en que el abonado autentica al IMS.

El documento “Text and Requirements proposed to be added to S.P0126”, 3GPP2 S 10-20070913-002rl da a conocer requisitos de seguridad para proteger a los usuarios y a la red de acceso/central de un acceso no autorizado y para proporcionar integridad y confidencialidad de comunicaciones en un sistema de pico células y femtocélulas.

Resumen de la invención

La presente invención está dirigida a abordar los efectos de uno o más de los problemas presentados en lo que antecede. Lo que sigue presenta un resumen simplificado de la invención para proporcionar una comprensión básica de algunos aspectos de la invención. Este resumen no es una visión general exhaustiva de la invención. Su único propósito es presentar algunos conceptos de forma simplificada como preludio de la descripción más detallada que se expone después.

En una realización de la presente invención, se proporciona un procedimiento que implica una femtocélula en comunicación con una red de subsistemas multimedia con protocolo de Internet (IMS). En una realización, la

femtocélula opera según los estándares de acceso múltiple por división de código (CDMA). El procedimiento incluye recibir de la femtocélula y en una primera entidad segura en la red IMS una primera información de autenticación generada por una unidad móvil usando un primer número aleatorio transmitido por la femtocélula en un reto global. El procedimiento también incluye recibir de una segunda entidad segura en la red segura al menos una clave de seguridad formada con base en el reto global y una segunda información de autenticación para retar de forma única a la unidad móvil. En una realización, la segunda entidad segura es un servidor de autenticación con base en CDMA. El procedimiento incluye, además, proporcionar la o las claves de seguridad a la femtocélula en respuesta a la autenticación de la unidad móvil con base en la segunda información de autenticación.

Breve descripción de los dibujos

La invención puede ser entendida con referencia a la siguiente descripción tomada en conjunto con los dibujos adjuntos, en los que número de referencia similares identifican elementos similares, y en los que:

la Figura 1 ilustra conceptualmente una realización ejemplar de un sistema de comunicaciones inalámbricas según la presente invención;

la Figura 2 ilustra conceptualmente una realización ejemplar de un procedimiento de autenticación de una unidad móvil proporcionando un reto único cuando la unidad móvil se da de alta según la presente invención;

la Figura 3 ilustra conceptualmente una realización ejemplar de un procedimiento de autenticación de una unidad móvil con base en un reto único durante el alta de una unidad móvil según la presente invención;

la Figura 4 ilustra conceptualmente una realización ejemplar de un procedimiento de autenticación de una unidad móvil proporcionando un reto único en respuesta a la iniciativa de la unidad móvil según la presente invención;

la Figura 5 ilustra conceptualmente una realización ejemplar de un procedimiento de autenticación de una unidad móvil con base en un reto único durante la expedición del mensaje de la unidad móvil según la presente invención; y

las Figuras 6A y 6B ilustran conceptualmente una realización ejemplar alternativa de un procedimiento de autenticación de una unidad móvil con base en un reto único según la presente invención.

Aunque la invención es susceptible de diversas modificaciones y de formas alternativas, se muestran realizaciones específicas de la misma a título de ejemplo en los dibujos y son descritas en detalle en el presente documento. Sin embargo, debería entenderse que no se pretende que la descripción del presente documento de realizaciones específicas limite la invención a las formas particulares dadas a conocer, sino que, al contrario, la intención es abarcar todas las modificaciones, los equivalentes y las alternativas que se encuentren dentro del alcance de la invención tal como es definida en las reivindicaciones adjuntas.

Descripción detallada de realizaciones específicas

En lo que sigue se describen realizaciones ilustrativas de la invención. En aras de la claridad, no se describen en esta memoria todas las características de una implementación real. Se apreciará, por supuesto, que en el desarrollo de cualquier realización real tal, deberían adoptarse numerosas decisiones específicas a la implementación para lograr las metas específicas de los diseñadores, tales como conformidad con limitaciones relativas al sistema y relativas al negocio, que variarán de una implementación a otra. Además, se apreciará que tal esfuerzo de desarrollo podría ser complejo y llevar mucho tiempo, pero sería, no obstante, una empresa rutinaria para las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación.

La presente invención será descrita ahora con referencia a las figuras adjuntas. en los dibujos se representan esquemáticamente diversas estructuras, diversos sistemas y dispositivos con fines de explicación únicamente y para no embrollar la presente invención con detalles que son bien conocidos para los expertos en la técnica. No obstante, los dibujos adjuntos se incluyen para describir y explicar ejemplos ilustrativos de la presente invención. Debería entenderse e interpretarse que las palabras y las frases usadas en el presente documento tienen un significado coherente con la comprensión de esas palabras y esas frases por parte de los expertos en la técnica relevante. No se pretende que haya implicada ninguna definición especial de un término o una frase, es decir, una definición que sea diferente del significado ordinario y habitual según entienden los expertos en la técnica, por el uso coherente del término o de la frase en el presente documento. Cuando se pretenda que un término o una frase tenga un significado especial, es decir, un significado distinto del entendido por expertos en la técnica, tal definición especial será formulada expresamente en la memoria de una manera definitoria que proporcione de manera directa e inequívoca la definición especial para el término o la frase.

La Figura 1 ilustra conceptualmente una realización ejemplar de un sistema 100 de comunicaciones inalámbricas. En la realización ilustrada, el sistema 100 de comunicaciones inalámbricas incluye una o más femtocélulas 105 para proporcionar conectividad inalámbrica. Las femtocélulas 105 pueden proporcionar conectividad inalámbrica según

estándares y/o protocolos que incluyen, sin limitación, estándares y/o protocolos de acceso múltiple por división de código (CDMA), estándares y/o protocolos del servicio universal de telecomunicaciones móviles (UMTS), estándares y/o protocolos del sistema global para comunicaciones móviles (GSM), estándares y/o protocolos WiMAX, estándares y/o protocolos IEEE y similares. Además, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación deberían apreciar que la presente invención no está limitada al uso de femtocélulas 105 para proporcionar conectividad inalámbrica. En realizaciones alternativas, pueden usarse dispositivos tales como estaciones base, dispositivos de encaminamiento de estaciones base, puntos de acceso, redes de acceso y similares para proporcionar conectividad inalámbrica en el sistema 100 de comunicaciones inalámbricas.

La femtocélula 105 está concebida para proporcionar cobertura inalámbrica a una zona que abarque aproximadamente un edificio que incluya una o más unidades móviles 110 a las que se garantice acceso a la femtocélula 105. Las unidades móviles 110 pueden ser dadas de alta en la femtocélula 105 usando una variedad de técnicas, incluyendo hacer que un usuario introduzca, a través de una página electrónica, una identidad internacional de abonado móvil (IMSI) para las unidades móviles 110 dadas de alta, usando un protocolo de enlace entre las unidades móviles 110 y la femtocélula 105 y similares. A continuación, se pone a disposición de la femtocélula 105 una lista de las unidades móviles 110 dadas de alta. En una realización, la femtocélula 105 contiene una base de datos que incluye los valores IMSI de las unidades móviles 110 dadas de alta. En la realización ilustrada, la unidad móvil 110 es una unidad móvil 110 inalámbrica basada en el acceso múltiple por división de código (CDMA). Sin embargo, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación deberían apreciar que la presente invención no está limitada a unidades móviles 110 basadas en CDMA.

La femtocélula 105 proporciona acceso al sistema 100 de comunicaciones inalámbricas por medio de una red 115 de subsistemas multimedia con protocolo de internet (IMS) (indicada por la caja de trazo discontinua). En diversas realizaciones alternativas la femtocélula 105 puede estar acoplada a la red IMS 115 mediante varios elementos funcionales. Por ejemplo, en la Figura 1 la femtocélula 105 está acoplada a una línea digital de abonado (DSL) o una red 120 de módem de cable, que está acoplada a una pasarela 125 de femtorred. Puede acoplarse un servidor 130 de administración y mantenimiento de operaciones (OA & M) a la pasarela 125 de femtorred y puede usarse para establecer comunicaciones entre la femtocélula 105 y una red 135 de protocolo de Internet (IP) por medio de una pasarela 125 de femtorred (FNG). Por ejemplo, puede formarse un túnel IPSec entre la femtocélula 105 y la pasarela 125 de femtorred. Sin embargo, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación deberían apreciar que no se pretende que esta realización ejemplar limite la presente invención a esta arquitectura particular de red.

La red IMS 115 es una red basada en el protocolo de inicio de sesión (SIP), que soporta la comunicación a través de Internet por parte de muchos tipos de microteléfonos. Por ejemplo, estos microteléfonos (tales como la unidad móvil 110 combinada con la femtocélula 105) pueden usar el protocolo de voz sobre Internet (VoIP) y otros procedimientos para transferir datos y voz en aplicaciones de tiempo real en la red IP 135. La red IMS 115 incluye un servidor local 140 de abonados (HSS), que es una base de datos maestra de usuarios que da soporte a las entidades de la red IMS que pueden gestionar llamadas. El HSS 140 puede contener información relacionada con abonos (perfiles de usuarios), llevar a cabo una autenticación y la autenticación del usuario, y pueden proporcionar información sobre la ubicación física del usuario. La red IMS 115 puede incluir también una o más entidades 145 de función de control de una sesión de llamadas (CSCF) que se usan para procesar paquetes de señalización SIP en la red IMS 115. Aunque en la Figura 1 las entidades 145 de CSCF son mostradas como un solo bloque funcional, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación deberían apreciar que las entidades 145 de CSCF pueden incluir múltiples entidades, tales como una CSCF servidora, una CSCF representante, una CSCF interrogadora y similares, que pueden ser implementadas en una o más entidades funcionales y/o físicas distintas. Se usa un servidor 150 de aplicaciones de gestión de la movilidad (MMAS) para coordinar y gestionar las funciones relativas a la movilidad de las unidades móviles 110.

La femtocélula 105 puede transmitir retos globales a la unidad móvil 110 por un canal suplementario. En una realización, el reto global se basa en un número aleatorio global que se genera en la femtocélula 105. En cada acceso al sistema, se requiere de las unidades móviles que calculen una respuesta usando datos secretos (SSD o AK) y que devuelvan al sistema la respuesta y al menos una porción del número aleatorio para su verificación. La femtocélula 105 usa el número aleatorio global y la respuesta para autenticar la unidad móvil 110 y para establecer un enlace seguro de comunicaciones por la interfaz aérea con la unidad móvil 110. Sin embargo, la femtocélula 105 puede no ser un elemento de confianza del sistema 100 de comunicaciones inalámbricas. Por ejemplo, la femtocélula 105 puede no ser físicamente segura, porque puede estar situada en la vivienda o el negocio de un usuario. En consecuencia, el proveedor del servicio puede ser incapaz de garantizar que la femtocélula 105 no pueda ser objeto de acceso por un usuario no autorizado que pueda intentar modificar o piratear la femtocélula 105. Además, la femtocélula 105 puede ser susceptible de piratería informática en una red. Por ejemplo, el usuario de la femtocélula 105 puede no proporcionar suficiente protección de cortafuegos, protección antivirus y similar, lo que puede permitir que usuarios no autorizados pirateen informáticamente la femtocélula 105. Dado que la femtocélula 105 no es un elemento de confianza del sistema 100, los retos globales emitidos por la femtocélula 105 (así como las autenticaciones basadas en estos retos globales) también pueden resultar sospechosos.

En cambio, las entidades de la red IMS 115 son entidades de confianza o seguras. Por ejemplo, el MMAS 150 puede ser físicamente seguro porque esté situado en un edificio que esté bajo el control del proveedor del servicio. En consecuencia, el proveedor del servicio puede ser capaz de garantizar que el MMAS 150 no pueda ser objeto de acceso por un usuario no autorizado que pueda intentar modificar o piratear informáticamente la femtocélula 105. Además, el MMAS 150 puede ser protegido del pirateo informático usando una protección de cortafuegos, una protección antivirus y similares, lo que puede evitar el acceso no autorizado al MMAS 150. También puede considerarse que otras entidades de la red, tales como un registro propio de localización/centro de autenticación (HLR/AuC) 160, que se usa para generar y proporcionar una o más claves a la femtocélula 105 y/o a la unidad móvil 110, son de confianza relativa y/o seguros porque estén bajo el control de un proveedor de servicios.

Por lo tanto, las entidades de confianza y/o seguras dentro de la red IMS 115 (o acopladas de forma segura a la misma) pueden ser usadas para autenticar a la unidad móvil 110 usando un reto único que pueda ser emitido después de un reto global sospechoso. En una realización, la unidad móvil 110 puede responder a un reto global (potencialmente sospechoso) emitido por la femtocélula 105 remitiendo una respuesta de autenticación global a la red IMS 115, que puede verificar la respuesta de autenticación global y generar información segura, tal como claves de sesión, en cooperación con el HLR/AuC 160. La red IMS 115 puede entonces crear y enviar un reto único a la unidad móvil 110 por medio de la femtocélula 105. Tras la recepción del reto único, la unidad móvil 110 genera una respuesta de autenticación única que es remitida a la red IMS 115 para su verificación. Una vez que la unidad móvil 110 ha sido autenticada por la entidad de confianza y/o segura, la red IMS 115 puede proporcionar a la femtocélula 105 servicios de procesamiento de llamadas o información de seguridad, tal como una o más claves generadas en el registro propio de localización/centro de autenticación (HLR/AuC) 160.

La Figura 2 ilustra conceptualmente una realización ejemplar de un procedimiento 200 de autenticación de una unidad móvil (EU) proporcionando un reto único cuando la unidad móvil se da de alta en la red. En la realización ilustrada, se usa una femtocélula o dispositivo de encaminamiento de estación base (BSR) para proporcionar conectividad inalámbrica a la unidad móvil. La femtocélula está acoplada en comunicación con una red IMS que incluye una CSCF servidora (S-CSCF), una CSCF representante (P-CSCF), una CSCF interrogadora (I-CSCF), un servidor local de abonados (HSS) y un servidor de aplicaciones de gestión de la movilidad (MMAS). La red IMS también está en comunicación con un registro propio de localización/centro de autenticación (HLR/AuC). Las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación deberían apreciar que los elementos mostrados en la Figura 2 son ilustrativos y que no se pretende que limiten la presente invención. En realizaciones alternativas pueden incluirse más o menos elementos que lleven a cabo más o menos funciones.

En la realización ilustrada, la femtocélula crea un número aleatorio global (RAND) y transmite este número aleatorio global (RAND) en la cadena de mensajes administrativos, tal como se indica por medio de la flecha 205. La unidad móvil calcula una respuesta de autenticación global (AUTR) usando el número aleatorio global y una clave tal como una clave SSD que sea conocida únicamente para la unidad móvil y el HLR/AuC. La unidad móvil puede enviar entonces un mensaje de alta a la femtocélula, tal como se indica por medio de la flecha 210. El mensaje de alta enviado por la unidad móvil puede ser un mensaje SIP de alta que incluya el número aleatorio global, la respuesta de autenticación global, un identificador de unidad móvil y un número electrónico de abonado. La femtocélula remite el mensaje de alta a la P-CSCF, que puede entonces remitir el mensaje de alta a la I-CSCF, tal como se indica por medio de las flechas 215, 220. La I-CSCF puede enviar un mensaje de interrogación al servidor local de abonados para determinar la S-CSCF apropiada para la unidad móvil, tal como se indica por medio de la flecha 225. El servidor local de abonados responde con información que indica la S-CSCF seleccionada, tal como se indica por medio de la flecha 230. El mensaje de alta es remitido entonces a la S-CSCF seleccionada, tal como se indica por medio de la flecha 240.

La S-CSCF envía un mensaje al servidor local de abonados para preguntar si es preciso llevar a cabo una autenticación IMS para la unidad móvil, tal como se indica por medio de la flecha 245. Por ejemplo, la S-CSCF puede enviar (en 245) una solicitud de autenticación móvil (MAR) al servidor local de abonados. El servidor local de abonados devuelve entonces información que indica si es o no preciso llevar a cabo una autenticación IMS para la unidad móvil, tal como se indica por medio de la flecha 250. Si el mensaje procedente del servidor local de abonados indica que no es necesario autenticar la unidad móvil, entonces puede saltarse la autenticación IMS (en 255). Si el mensaje procedente del servidor local de abonados indica que es necesario autenticar la unidad móvil, entonces puede llevarse a cabo la autenticación con un agente de usuario en la femtocélula (en 255). En cualquiera de los dos casos, la S-CSCF transmite una solicitud de un perfil de servicio de la unidad móvil al servidor local de abonados, tal como se indica por medio de la flecha 260, y el servidor local de abonados devuelve a la SCSCF el perfil de servicio para la unidad móvil, tal como se indica por medio de la flecha 265. Si se saltó la etapa de autenticación IMS, entonces la S-CSCF dice a la femtocélula que el alta está completa (por ejemplo, transmitiendo un mensaje 200-OK) y la femtocélula puede responder con un mensaje de acuse de recibo, tal como se indica por medio de las flechas dobles 270.

En una realización, la femtocélula puede abonarse entonces (en 275) a su estado de alta en el IMS, por ejemplo transmitiendo un mensaje de ABONO a la S-CSCF, que puede devolver un mensaje (tal como un mensaje 200-OK) confirmando el abono. Si la autenticación de la unidad móvil falla más tarde en la secuencia reto/respuesta,

entonces el servidor de aplicaciones de gestión de la movilidad puede informar a la S-CSCF de que el abono en el IMS ha fallado, por ejemplo proporcionando un mensaje 4xx de fallo en vez de un mensaje 200-OK. Dado que el servidor de aplicaciones de gestión de la movilidad recibe el mensaje de alta como un mensaje de abono de tercero con base en unos criterios de filtro inicial en el perfil de usuario almacenado en la S-CSCF, el mensaje de fallo de alta puede hacer que la S-CSCF dé de baja la unidad móvil. La baja de la unidad móvil puede significar que se anularía el alta en el IMS completada previamente. Un agente de usuario en la femtocélula debería recibir una notificación cuando el alta sea anulada, puesto que la femtocélula objeto de abono cambia en su estado de alta en el IMS. Así, el agente de usuario en la femtocélula está en situación de limpiar lo que necesite ser limpiado. En una realización, el agente de usuario puede cometer suicidio.

La S-CSCF puede enviar un mensaje de abono al servidor de aplicaciones de gestión de la movilidad, tal como se indica por medio de la flecha 280. En una realización, la S-CSCF envía (en 280) un mensaje SIP de alta de tercero que incluye información que indica el identificador de unidad móvil, el número electrónico de serie, la respuesta de autenticación y el número aleatorio global. En respuesta a la recepción del mensaje de alta, el servidor de aplicaciones de gestión de la movilidad autentica (en 285) la unidad móvil usando un par único de reto/respuesta proporcionado por el HLR/AuC. Los resultados del procedimiento de autenticación son transmitidos entonces a la S-CSCF en un mensaje, tal como un mensaje 200-OK de alta, según se indica por medio de la flecha 290.

La Figura 3 ilustra conceptualmente una realización ejemplar de un procedimiento 300 de autenticación de una unidad móvil con base en un reto único durante el alta de una unidad móvil. Parte o la totalidad del procedimiento 300 puede ser implementada como parte de la etapa 285 representada en la Figura 2. En la realización ilustrada, la S-CSCF envía un mensaje de alta, tal como un mensaje SIP de alta de tercero al servidor de aplicaciones de gestión de la movilidad, tal como se indica por medio de la flecha 305. En respuesta a la recepción del mensaje de alta, el servidor de aplicaciones de gestión de la movilidad solicita un par único de reto/respuesta que pueda ser usado para autenticar la unidad móvil. Por ejemplo, el servidor de aplicaciones de gestión de la movilidad puede funcionar como un registro de localización de visitantes (VLR) y enviar una solicitud de autenticación para el par único de reto/respuesta al HLR/AuC, tal como se indica por medio de la flecha 310. El HLR/AuC puede entonces devolver el par único solicitado de reto/respuesta, tal como un número aleatorio único (RANDU) y una respuesta de autenticación única (AUTU).

El servidor de aplicaciones de gestión de la movilidad puede retar a la unidad móvil usando el par proporcionado único de reto/respuesta. En la realización ilustrada, el servidor de aplicaciones de gestión de la movilidad remite un mensaje, tal como un mensaje SIP, a la S-CSCF, que remite el mensaje a la femtocélula, tal como se indica por medio de las flechas 320, 325. El mensaje incluye el reto único representado por el número aleatorio único generado por el HLR/AuC para la unidad móvil. La femtocélula forma entonces un mensaje de reto único usando el número aleatorio de reto único y lo transmite a la unidad móvil, según se indica por medio de la flecha 330. Tras la recepción del reto único, la unidad móvil genera una respuesta de autenticación única (AUTU) usando el número aleatorio único proporcionado y una clave de seguridad conocida para la unidad móvil. La unidad móvil devuelve a la femtocélula un mensaje de respuesta al reto que incluye el número aleatorio único y la respuesta de autenticación calculada (RANDU/AUTU), tal como se indica por medio de la flecha 335. La femtocélula puede transmitir entonces la respuesta de autenticación calculada (AUTU) a la S-CSCF, que puede remitir esta respuesta al servidor de aplicaciones de gestión de la movilidad, tal como se indica por medio de las flechas 340, 345. Por ejemplo, la respuesta de autenticación calculada puede ser transmitida en un mensaje 200-OK de respuesta.

El servidor de aplicaciones de gestión de la movilidad puede autenticar (en 350) la unidad móvil usando los valores de respuesta de autenticación proporcionados por la unidad móvil y el HLR/AuC. En una realización, el servidor de aplicaciones de gestión de la movilidad compara (en 350) los valores de respuesta de autenticación proporcionados por la unidad móvil y el HLR/AuC y autentica (en 350) la unidad móvil si estos dos valores coinciden. Si la unidad móvil es autenticada con éxito (en 350), el servidor de aplicaciones de gestión de la movilidad transmite entonces una notificación de alta al HLR/AuC, tal como se indica por medio de la flecha 355. El HLR/AuC puede transmitir una confirmación en respuesta a la recepción de la notificación de alta, tal como se indica por medio de la flecha 360. En una realización, la confirmación 360 puede incluir un perfil de registro de localización de visitantes asociado con la unidad móvil.

Si la unidad móvil ha sido autenticada con éxito (en 350) y dada de alta (en 355, 360), el servidor de aplicaciones de gestión de la movilidad puede transmitir entonces a la S-CSCF un mensaje de acuse del alta, tal como se indica por medio de la flecha 365. Por ejemplo, el servidor de aplicaciones de gestión de la movilidad puede transmitir (en 365) un mensaje 200-OK que indique que el alta y la autenticación de la unidad móvil han tenido éxito. En una realización, la S-CSCF puede proseguir llevando a cabo tareas tales como usar su lista de reglas para determinar si se supone o no que cualquier otro servidor de aplicaciones deba ser notificado en caso de que la unidad móvil se dé de alta con éxito. Sin embargo, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación deberían apreciar que determinar si debe notificarse a otros servidores de aplicaciones es solo un ejemplo de un “disparador” de red inteligente y que la lista de reglas en la S-CSCF son ejemplos de instrucciones que pueden usarse para determinar cuándo activar estos disparadores. En una realización, los disparadores proporcionan a los servidores de aplicaciones la oportunidad de procesar uno o más mensajes SIP.

La Figura 4 ilustra conceptualmente una realización ejemplar de un procedimiento 400 de autenticación de una unidad móvil (EU) proporcionando un reto único en respuesta a la iniciativa de la unidad móvil. En la realización ilustrada, se usa una femtocélula o dispositivo de encaminamiento de estación base (BSR) para proporcionar conectividad inalámbrica a la unidad móvil. La femtocélula está acoplada en comunicación con una red IMS que incluye una CSCF servidora (S-CSCF), una CSCF representante (P-CSCF), una CSCF interrogadora (I-CSCF) y un servidor de aplicaciones de gestión de la movilidad (MMAS). La red IMS también está en comunicación con un registro propio de localización/centro de autenticación (HLR/AuC) y con otro usuario final (FIN), tal como otra unidad móvil u otros dispositivos de comunicaciones. Las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación deberían apreciar que los elementos mostrados en la Figura 4 son ilustrativos y que no se pretende que limiten la presente invención. En realizaciones alternativas pueden incluirse más o menos elementos que lleven a cabo más o menos funciones.

En la realización ilustrada, la femtocélula crea un número aleatorio global (RAND) y transmite este número aleatorio global (RAND) en la cadena de mensajes administrativos, tal como se indica por medio de la flecha 405. La unidad móvil calcula una respuesta de autenticación global (AUTR) usando el número aleatorio global y una clave tal como una clave SSD que sea conocida únicamente para la unidad móvil y al centro de autenticación (AuC). Si la unidad móvil quiere originar el servicio, la unidad móvil puede enviar un mensaje de origen a la femtocélula, tal como se indica por medio de la flecha 410. Por ejemplo, la unidad móvil puede transmitir (en 410) un mensaje CDMA de origen que incluya el número aleatorio global, la respuesta de autenticación, un identificador de unidad móvil y un número electrónico de abonado. La unidad móvil también puede transmitir los dígitos marcados del otro usuario final. La femtocélula forma un mensaje de invitación y remite el mensaje de invitación a la P-CSCF, que puede entonces remitir el mensaje de invitación a la I-CSCF, tal como se indica por medio de las flechas 415, 420. En una realización, el mensaje de invitación es un mensaje SIP de INVITACIÓN que incluye el número aleatorio global, la respuesta de autenticación, un identificador de unidad móvil y un número electrónico de abonado. La I-CSCF puede remitir entonces el mensaje de invitación al servidor de aplicaciones de gestión de la movilidad, tal como se indica por medio de la flecha 430.

A la recepción del mensaje de invitación, el servidor de aplicaciones de gestión de la movilidad intenta (en 435) autenticar la unidad móvil y puede también crear una o más claves de seguridad, tal como una SMEKEY y/o una clave PLCM que puedan ser usadas para cifrar mensajes o tráfico de voz. En una realización, las etapas que se usan para autenticar la unidad móvil y crear las claves de cifrado de CDMA pueden ser llevadas a cabo de manera concurrente y/o síncrona. Sin embargo, las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación deberían apreciar que las etapas pueden estar distribuidas, de manera alternativa, dentro del flujo de los mensajes de establecimiento de llamada para intentar optimizar el procedimiento. Por ejemplo, podría derivarse un reto único antes de la llamada y ser almacenado por el servidor de aplicaciones de gestión de la movilidad para su uso inmediato en el momento de la llamada. Si la unidad móvil es autenticada con éxito (en 435), el servidor de aplicaciones de gestión de la movilidad puede transmitir un mensaje de invitación al usuario final (FIN), tal como se indica por medio de la flecha 440. Por ejemplo, el servidor de aplicaciones de gestión de la movilidad puede transmitir (en 440) un mensaje de INVITACIÓN al usuario final. Entonces puede ser devuelto un mensaje de respuesta, tal como un mensaje 180-Llamando, al servidor de aplicaciones de gestión de la movilidad, que puede remitir este mensaje a la unidad móvil a través de la femtocélula, tal como se indica por medio de las flechas 445, 450. También puede proporcionarse un mensaje audible de llamada a la unidad móvil, tal como se indica por medio de la flecha 455. Puede transmitirse a la femtocélula un mensaje que indique que el usuario ha contestado la llamada, tal como un mensaje 200-OK-Responder, a través del servidor de aplicaciones de gestión de la movilidad si el usuario final acepta la llamada, tal como se indica por medio de las flechas 460, 465.

La Figura 5 ilustra conceptualmente una realización ejemplar de un procedimiento 500 de autenticación de una unidad móvil con base en un reto único durante la expedición del mensaje de la unidad móvil. Parte o la totalidad del procedimiento 500 puede ser implementada como parte de la etapa 435 representada en la Figura 4. En respuesta a la recepción de una solicitud de origen, tal como un mensaje SIP de INVITACIÓN, el servidor de aplicaciones de gestión de la movilidad envía una solicitud de autenticación al HLR/AuC, tal como se indica por medio de la flecha 505. En una realización, la solicitud de autenticación incluye el número aleatorio global, la respuesta de autenticación global calculada por la unidad móvil, parte o la totalidad de los dígitos marcados correspondientes al otro usuario final, un identificador de unidad móvil, el número electrónico de serie y cualquier otra información. El HLR/AuC puede entonces proporcionar información de seguridad tal como la SMEKEY y/o una clave PLCM asociadas con la llamada originada, según se indica por medio de la flecha 510. El servidor de aplicaciones de gestión de la movilidad también puede transmitir una solicitud de autenticación al HLR/AuC, tal como se indica por medio de la flecha 515. La solicitud de autenticación incluye una solicitud de un par único de reto/respuesta asociado con la unidad móvil de origen. El HLR/AuC puede entonces devolver (en 520) el par único solicitado de reto/respuesta, que puede ser un número aleatorio único (RANDU) y una correspondiente respuesta de autenticación única (AUTU).

El servidor de aplicaciones de gestión de la movilidad puede entonces remitir un reto único que incluya el número aleatorio único a la S-CSCF, que puede remitir el reto único a la femtocélula, tal como se indica por medio de las flechas 525, 530. La femtocélula puede usar el número aleatorio único proporcionado para emitir un reto único a la unidad móvil, tal como se indica por medio de la flecha 535. En respuesta al reto único, la unidad móvil puede

calcular una respuesta de autenticación usando el número aleatorio único proporcionado y una clave de seguridad almacenada en la unidad móvil. La respuesta de autenticación única puede ser entonces transmitida de nuevo a la femtocélula, tal como se indica por medio de la flecha 540. La femtocélula puede entonces transmitir la respuesta de autenticación calculada (AUTU) a la S-CSCF, que puede remitir esta respuesta al servidor de aplicaciones de gestión de la movilidad, tal como se indica por medio de las flechas 545, 550. Por ejemplo, la respuesta de autenticación calculada y el número aleatorio único pueden ser transmitidos en un mensaje 200-OK de respuesta.

El servidor de aplicaciones de gestión de la movilidad puede autenticar (en 555) la unidad móvil usando los valores de respuesta de autenticación única proporcionados por la unidad móvil y el centro de autenticación. En una realización, el servidor de aplicaciones de gestión de la movilidad compara (en 555) los valores de respuesta de autenticación proporcionados por la unidad móvil y el centro de autenticación y autentica (en 555) la unidad móvil si estos dos valores coinciden. Si la unidad móvil es autenticada con éxito (en 555), el servidor de aplicaciones de gestión de la movilidad puede transmitir entonces una notificación de seguridad para la llamada a través de la S-CSCF, según se indica por medio de las flechas 560, 565. Por ejemplo, el servidor de aplicaciones de gestión de la movilidad puede transmitir (en 560, 565) un mensaje 200-OK que indique que el alta y la autenticación de la unidad móvil han tenido éxito y que incluya la SMEKEY y/o la clave PLCM determinadas previamente. En este punto la femtocélula tiene las claves de cifrado que pueden ser usadas para cifrar el canal de tráfico para la llamada. La femtocélula puede confirmar la recepción de la información de seguridad volviendo a transmitir un mensaje al servidor de aplicaciones de gestión de la movilidad, tal como se indica por medio de las flechas 570, 575. Por ejemplo, la femtocélula puede transmitir (en 570, 575) un mensaje 200-OK al servidor de aplicaciones de gestión de la movilidad.

Las Figuras 6A y 6B ilustran conceptualmente una realización ejemplar alternativa de un procedimiento 600 de autenticación de una unidad móvil con base en un reto único. En la realización ilustrada, se usa una femtocélula o dispositivo de encaminamiento de estación base (BSR) para proporcionar conectividad inalámbrica al equipo móvil de usuario (EU). La femtocélula está acoplada en comunicación con una red IMS que incluye una CSCF servidora (S-CSCF), una CSCF representante (P-CSCF), una CSCF interrogadora (I-CSCF) y un servidor de aplicaciones de gestión de la movilidad (MMAS). La red IMS también está en comunicación con un registro propio de localización/centro de autenticación (HLR/AuC) y con otro usuario final (FIN), tal como otra unidad móvil u otros dispositivos de comunicaciones. Las personas con un dominio normal de la técnica que cuenten con el beneficio de la presente revelación deberían apreciar que los elementos mostrados en las Figuras 6A y 6B son ilustrativos y que no se pretende que limiten la presente invención. En realizaciones alternativas pueden incluirse más o menos elementos que lleven a cabo más o menos funciones.

El servidor de aplicaciones de gestión de la movilidad envía una solicitud de autenticación al centro de autenticación, tal como se indica por medio de la flecha 601. En una realización, la solicitud de autenticación puede incluir un identificador de unidad móvil, el número electrónico de serie y cualquier otra información. El HLR/AuC puede responder entonces con un mensaje que incluya información que pueda ser usada para formar después un reto único a la unidad móvil. En la realización ilustrada, la solicitud (en 601) y la respuesta (en 602) se efectúan antes de que la unidad móvil solicite acceso al sistema; por ejemplo, durante una solicitud de alta o una solicitud de origen. Por ejemplo, la solicitud (en 601) y la respuesta (en 602) pueden efectuarse durante un acceso previo al sistema por parte de la unidad móvil y la información de autenticación única (por ejemplo, el par RANDU/AUTU) puede ser almacenada en el MMAS hasta que la unidad móvil solicite acceso al sistema.

En la realización ilustrada, la femtocélula crea periódicamente un número aleatorio global (RAND) y transmite este número aleatorio global (RAND) en la cadena de mensajes administrativos, tal como se indica por medio de la flecha 603. Si la unidad móvil quiere originar el servicio, la unidad móvil puede enviar un mensaje de origen a la femtocélula, tal como se indica por medio de la flecha 604. Por ejemplo, la unidad móvil puede transmitir (en 604) un mensaje de origen CDMA que incluya el número aleatorio global, la respuesta de autenticación, un identificador de unidad móvil y un número electrónico de abonado. La unidad móvil también puede transmitir los dígitos marcados del otro usuario final. La femtocélula forma un mensaje de invitación y remite el mensaje de invitación a la P-CSCF, que puede entonces remitir el mensaje de invitación a la S-CSCF, tal como se indica por medio de las flechas 605, 606. En una realización, el mensaje de invitación es un mensaje SIP de INVITACIÓN que incluye el número aleatorio global, la respuesta de autenticación, un identificador de unidad móvil y un número electrónico de abonado. La S-CSCF puede remitir entonces el mensaje de invitación al servidor de aplicaciones de gestión de la movilidad, tal como se indica por medio de la flecha 607.

El servidor de aplicaciones de gestión de la movilidad puede entonces remitir un reto que incluya el número aleatorio único a la S-CSCF, que puede remitir el reto a la femtocélula, según se indica por medio de las flechas 608, 609. Dado que la información de autenticación única ya ha sido calculada y almacenada, el MMAS puede transmitir (en 608) el reto único directamente en respuesta a la recepción del mensaje de invitación, en lugar de tener que solicitar al AuC en primer lugar la información de reto único. La femtocélula puede usar el número aleatorio único proporcionado (RANDU) para emitir un reto único a la unidad móvil, tal como se indica por medio de la flecha 610. El servidor de aplicaciones de gestión de la movilidad también puede enviar una solicitud de autenticación al centro de autenticación, tal como se muestra por medio de la flecha 611. En una realización, la solicitud de autenticación puede incluir el número aleatorio global, la respuesta de autenticación global calculada por la unidad móvil, un

identificador de unidad móvil, el número electrónico de serie y cualquier otra información. El centro de autenticación puede entonces proporcionar información de seguridad, tal como la SMEKEY y/o la clave PLCM asociadas con la llamada de origen, según se indica por medio de la flecha 612. La solicitud de la información de seguridad (en 611) y la respuesta que incluye la información de seguridad (en 612) pueden efectuarse de forma concurrente con parte o la totalidad de las etapas 608, 609, 610.

En respuesta al reto único (en 610), la unidad móvil puede calcular una respuesta de autenticación usando el número aleatorio único proporcionado y la clave secreta almacenada en la unidad móvil. La respuesta de autenticación única puede volver a transmitirse a la femtocélula, tal como se indica por medio de la flecha 613. La femtocélula puede transmitir entonces la respuesta de autenticación calculada (AUTU) a la S-CSCF, que puede remitir esta respuesta al servidor de aplicaciones de gestión de la movilidad, tal como se indica por medio de las flechas 614, 615. Por ejemplo, la respuesta de autenticación calculada y el número aleatorio único pueden ser transmitidos en un mensaje 200-OK de respuesta.

El servidor de aplicaciones de gestión de la movilidad puede autenticar (en 616) la unidad móvil usando los valores de respuesta de autenticación (AUTU) proporcionados por la unidad móvil y el centro de autenticación. En una realización, el servidor de aplicaciones de gestión de la movilidad compara (en 616) los valores de respuesta de autenticación proporcionados por la unidad móvil y el centro de autenticación y autentica (en 616) la unidad móvil si estos dos valores coinciden. Si la unidad móvil es autenticada con éxito (en 616), el servidor de aplicaciones de gestión de la movilidad puede transmitir entonces a la femtocélula información de seguridad para la llamada a través de la S-CSCF, según se indica por medio de las flechas 617, 618. Por ejemplo, el servidor de aplicaciones de gestión de la movilidad puede transmitir (en 617, 618) un mensaje 200-OK que indique que el alta y la autenticación de la unidad móvil han tenido éxito y que incluya la SMEKEY y/o la clave PLCM determinadas previamente. En este punto la femtocélula tiene las claves de cifrado que pueden ser usadas para cifrar el canal de tráfico para la llamada. La femtocélula puede confirmar la recepción de la información de seguridad volviendo a transmitir un mensaje al servidor de aplicaciones de gestión de la movilidad, tal como se indica por medio de las flechas 619, 620. Por ejemplo, la femtocélula puede transmitir (en 619, 620) un mensaje 200-OK al servidor de aplicaciones de gestión de la movilidad.

En algunos casos, es posible que pueda haber ocurrido una actualización de los SSD entre la creación de la información de autenticación (en 601, 602) y la autenticación (en 616) de la unidad móvil. Si este ocurre y no se recupera del HLR/AuC un conjunto reciente de AUTU/RANDU, la unidad móvil no será autenticada, aunque devuelva el debido AUTU. Sin embargo, las actualizaciones de SSD ocurren en todo el sistema servidor de la femtocélula, que en este caso es el MMAS. Así, el MMAS estaría involucrado y sabría que tiene que obtener un par reciente de RANDU/AUTU. Cuando ocurre la actualización en toda macrocélula (por ejemplo, porque el microteléfono se haya desplazado de la femtocélula a la macrocélula), la actualización debería provocar un alta en el HLR/AuC y debería enviarse un aviso de baja al VLR anterior, que es el MMAS. Por lo tanto, el MMAS sabría que su par actual no es reciente, de modo que, cuando el microteléfono vuelva a darse de alta en la femtocélula, el MMAS pueda obtener un RANDU/AUTU reciente que se usaría durante la siguiente llamada de acceso al sistema.

Una vez que la unidad móvil ha sido autenticada con éxito (en 616), el servidor de aplicaciones de gestión de la movilidad puede transmitir un mensaje de invitación al usuario final (FIN), tal como se indica por medio de la flecha 621. Por ejemplo, el servidor de aplicaciones de gestión de la movilidad puede transmitir (en 621) un mensaje de INVITACIÓN al usuario final. Entonces puede ser devuelto un mensaje de respuesta, tal como un mensaje 180-Llamando, al servidor de aplicaciones de gestión de la movilidad, que puede remitir este mensaje a la unidad móvil a través de la femtocélula, tal como se indica por medio de las flechas 622, 623. También puede proporcionarse un mensaje audible de llamada a la unidad móvil, tal como se indica por medio de la flecha 624. Puede transmitirse a la femtocélula un mensaje que indique que el usuario ha contestado la llamada, tal como un mensaje 200-OK-Responder, a través del servidor de aplicaciones de gestión de la movilidad si el usuario final acepta la llamada, tal como se indica por medio de las flechas 625, 626.

Se presentan porciones de la presente invención y de la correspondiente descripción detallada en términos de soporte lógico o de algoritmos y representaciones simbólicas de operaciones en bits de datos dentro de la memoria de un ordenador. Estas descripciones y representaciones son aquellas mediante las cuales las personas con un dominio normal de la técnica transmiten de manera efectiva la sustancia de sus labores a otras personas con un dominio normal de la técnica. Se concibe que un algoritmo, según se usa el término aquí, y según se usa en general, es una secuencia internamente coherente de etapas que conducen a un resultado deseado. Las etapas son aquellas que requieren manipulaciones físicas de cantidades físicas. Normalmente, aunque no necesariamente, estas cantidades adoptan la forma de señales ópticas, eléctricas o magnéticas capaces de ser almacenadas, transferidas, combinadas, comparadas o manipuladas de otra forma. Se ha demostrado conveniente a veces, principalmente por razones de uso común, referirse a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares.

Sin embargo, debería tenerse en cuenta que todos estos términos y similares han de estar asociados con las cantidades físicas apropiadas y son meramente etiquetas convenientes aplicadas a estas cantidades. A no ser que se indique específicamente otra cosa, o como resulte evidente por la exposición, términos tales como

“procesamiento” o “cálculo” o “calculando”, o “determinando” o “mostrando” o similares se refieren a la acción y los procesos de un sistema de ordenador o un dispositivo informático electrónico similar que manipule y transforme datos representados como cantidades físicas electrónicas dentro de los registros y las memorias del sistema de ordenador en otros datos similarmente representados como cantidades físicas dentro de las memorias o los registros del sistema de ordenador o de otros dispositivos tales de almacenamiento, transmisión o presentación de la información.

Obsérvese también que los aspectos de la invención implementados mediante soporte lógico se codifican típicamente en alguna forma de medio de almacenamiento de programas o se implementan en algún tipo de medio de transmisión. El medio de almacenamiento de programas puede ser magnético (por ejemplo, un disquete o un disco duro) u óptico (por ejemplo, una memoria de solo lectura en disco compacto o “CD-ROM”) y puede ser de solo lectura o de acceso aleatorio. De forma similar, el medio de transmisión pueden ser pares trenzados de hilo, cable coaxial, fibra óptica o algún otro medio de transmisión adecuado conocido en la técnica. La invención no está limitada por estos aspectos de ninguna implementación dada.

Las realizaciones particulares dadas a conocer en lo que antecede son únicamente ilustrativas, ya que la invención puede ser modificada y puesta en práctica de maneras diferentes, aunque equivalentes, evidentes a los expertos en la técnica que cuenten con el beneficio de las enseñanzas del presente documento. Además, no se contempla ninguna limitación a los detalles de construcción o de diseño mostrados en el presente documento que los descritos en las reivindicaciones que siguen. Por lo tanto, resulta evidente que las realizaciones particulares dadas a conocer en lo que antecede pueden ser alteradas o modificadas y se considera que todas las variaciones de ese tipos están dentro del alcance de la invención. En consecuencia, la protección buscada en el presente documento es según se expone en las reivindicaciones que siguen.

REIVINDICACIONES

1. Un procedimiento (200, 300, 400, 500, 600) que implica una femtocélula (105) en comunicación con una red segura (115) **caracterizado porque** el procedimiento comprende:

recibir (415, 420, 430, 605, 606, 607) de la femtocélula (105) en la primera entidad segura (150) de la red segura (115) una primera información de autenticación generada por una unidad móvil (110) usando un número aleatorio transmitido por la femtocélula (105) en un reto global;
recibir (510) de una segunda entidad segura (160) en la red segura (115) al menos una clave de seguridad formada con base en el reto global;
recibir (285, 520, 602) de la segunda entidad segura (160) en la red segura (115) una segunda información de autenticación para retar de forma única a la unidad móvil (110), y
proporcionar (560, 565, 617, 618) dicha al menos una clave de seguridad a la femtocélula (105) en respuesta a la autenticación de la unidad móvil (110) con base en la segunda información de autenticación.

2. El procedimiento (400, 600) de la reivindicación 1 en el que la recepción de la primera información de autenticación comprende recibir información que indica un identificador que identifique de forma única a la unidad móvil (110), el número aleatorio y una respuesta de autenticación calculada por la unidad móvil (110) con base en el número aleatorio y a una clave conocida por la unidad móvil (110) y no conocida por la femtocélula (105).

3. El procedimiento (500, 600) de la reivindicación 2 en el que la solicitud de la segunda información de autenticación comprende solicitar información que indica un segundo número aleatorio y una respuesta de autenticación que sea única a la unidad móvil (110), determinando la segunda entidad segura (160) la respuesta de autenticación con base en el identificador que identifica de forma única a la unidad móvil (110).

4. El procedimiento (500, 600) de la reivindicación 3 en el que la autenticación de la unidad móvil (110) comprende:

proporcionar (525, 530, 608, 609) el segundo número aleatorio a la femtocélula (105) para que la femtocélula (105) pueda transmitir a la unidad móvil (110) un reto único que incluya el segundo número aleatorio;
recibir (550, 615) en la primera entidad segura (150), y en respuesta a proporcionar el segundo número aleatorio, información que indica el segundo número aleatorio y una respuesta de autenticación calculada por la unidad móvil (110) con base en el segundo número aleatorio; y
autenticar (555, 616) la unidad móvil (110) si la respuesta de autenticación calculada por la unidad móvil (110) con base en el segundo número aleatorio corresponde a la respuesta de autenticación recibida de la segunda entidad segura (160).

5. El procedimiento (400, 500, 600) de la reivindicación 1 en el que la solicitud de al menos una clave de seguridad de la segunda entidad segura (160) comprende solicitar claves de sesión para el cifrado de la señalización y del tráfico portador y ene el que la recepción de la primera información de autenticación generada por la unidad móvil (110) comprende recibir la primera información de autenticación en respuesta a al menos uno de un mensaje de alta transmitido desde la unidad móvil (110) a la femtocélula (105) o un mensaje de origen transmitido desde la unidad móvil (110) a la femtocélula (105).

6. El procedimiento (200, 300, 400, 500, 600) de la reivindicación 1 en el que la femtocélula (105) opera según estándares de acceso múltiple por división de código (CDMA) en el que la red segura (115) es una red de subsistemas multimedia con protocolo de Internet (IMS), en el que la segunda entidad segura (160) es un servidor de autenticación basado en CDMA conectado a la red IMS y en el que la al menos una clave de seguridad es al menos una clave de cifrado.

7. El procedimiento (400, 600) de la reivindicación 2 en el que el identificador es un número de serie electrónico.

8. El procedimiento (500, 600) de la reivindicación 6 en el que la solicitud de al menos una clave de cifrado del servidor de autenticación basado en CDMA comprende solicitar al menos una de una SMEKEY o una clave de máscara larga pública de código, y en el que la recepción de la primera información de autenticación generada por la unidad móvil (110) comprende recibir la primera información de autenticación en respuesta a al menos uno de un mensaje de alta transmitido desde la unidad móvil (110) a la femtocélula (105) o un mensaje de origen transmitido desde la unidad móvil (110) a la femtocélula (105).

9. Una entidad segura (150) para su uso en una red segura (115) **caracterizada porque** la entidad segura está adaptada para
recibir de una femtocélula (105) que proporciona conectividad inalámbrica en un sistema (100) de comunicaciones inalámbricas una primera información de autenticación generada por una unidad móvil (110) usando la transmisión de un primer número aleatorio por la femtocélula (105) en un reto global;

recibir de una segunda entidad segura (160) en la red segura (115) al menos una clave de seguridad formada con base en el reto global;
recibir de la segunda entidad segura (160) una segunda información de autenticación para retar de forma única a la unidad móvil (110); y
proporcionar dicha al menos una clave de seguridad a la femtocélula (105) en respuesta a la autenticación de la unidad móvil (110) con base en la segunda información de autenticación.

10. La entidad segura (150) según la reivindicación 10 en la que la entidad segura (150) es un servidor de aplicaciones de gestión de la movilidad usado para coordinar y gestionar funciones relativas a la movilidad de la unidad móvil (110).

11. La entidad segura (150) según la reivindicación 10 en la que la entidad segura (150) está protegida de la piratería informática usando una protección de cortafuegos y protección antivirus para evitar el acceso no autorizado a la entidad segura (150).

12. Una femtocélula (105) **caracterizada porque** la femtocélula (105) está adaptada para:

comunicarse con una red segura (115);
transmitir un primer número aleatorio en un reto global;
proporcionar a una entidad segura (150) una primera información de autenticación generada por una unidad móvil (110) usando el primer número aleatorio; y
recibir de la primera entidad segura (150) al menos una clave de seguridad recibida de una segunda entidad segura (160) en la red segura (115) en respuesta a la autenticación de la unidad móvil (110) con base en la segunda información de autenticación.

13. Un sistema (100) de comunicaciones inalámbricas que comprende:

al menos una unidad móvil (110);
al menos una femtocélula (105) según la reivindicación 12;
una primera entidad segura (150) según una de las reivindicaciones 9, 10 u 11; y
una segunda entidad segura (160).

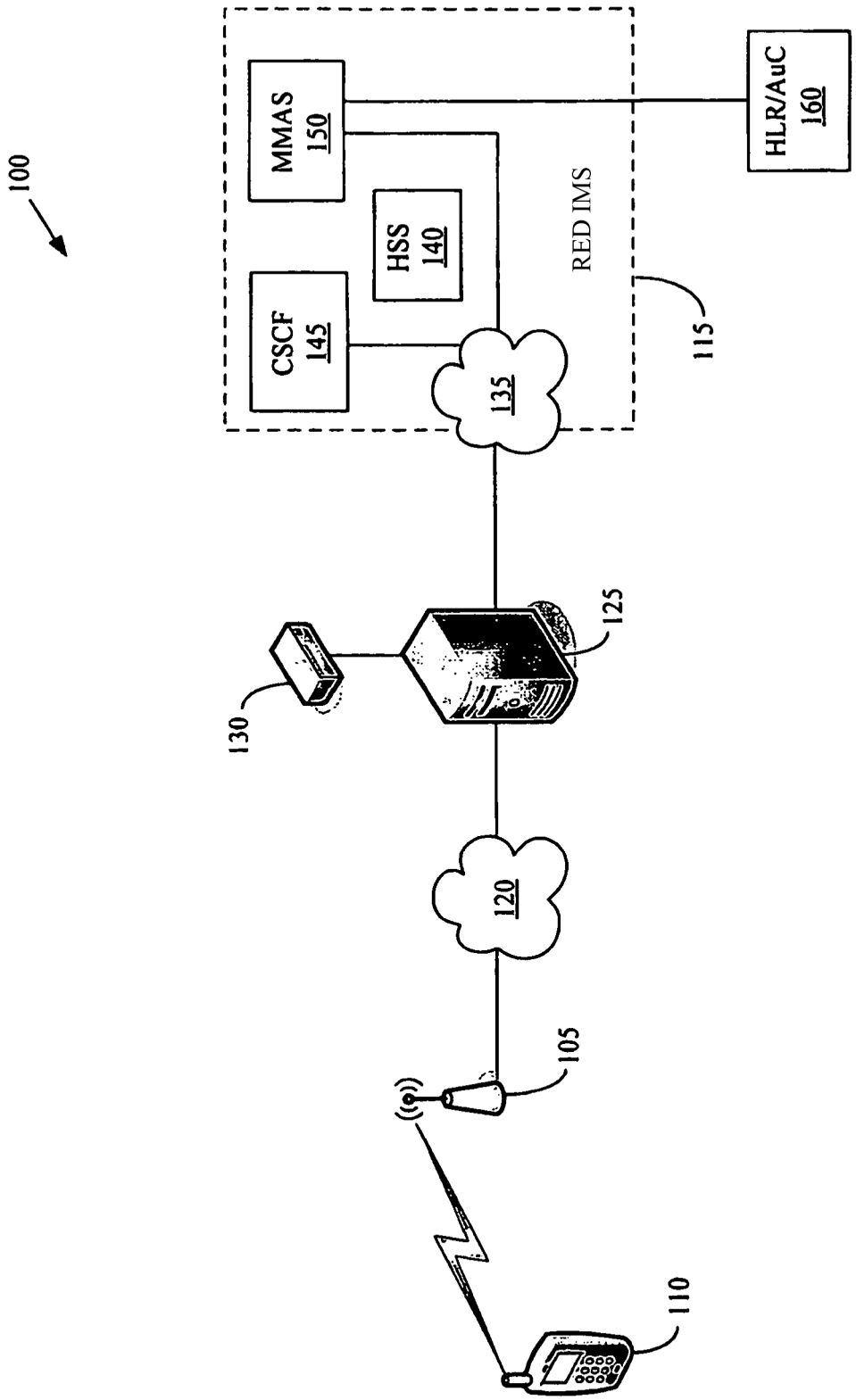
100
MMAS 150
HLR/AuC 160
HSS 140
CSCF 145
RED IMS
115
135
125
130
120
105
110

Figura 1

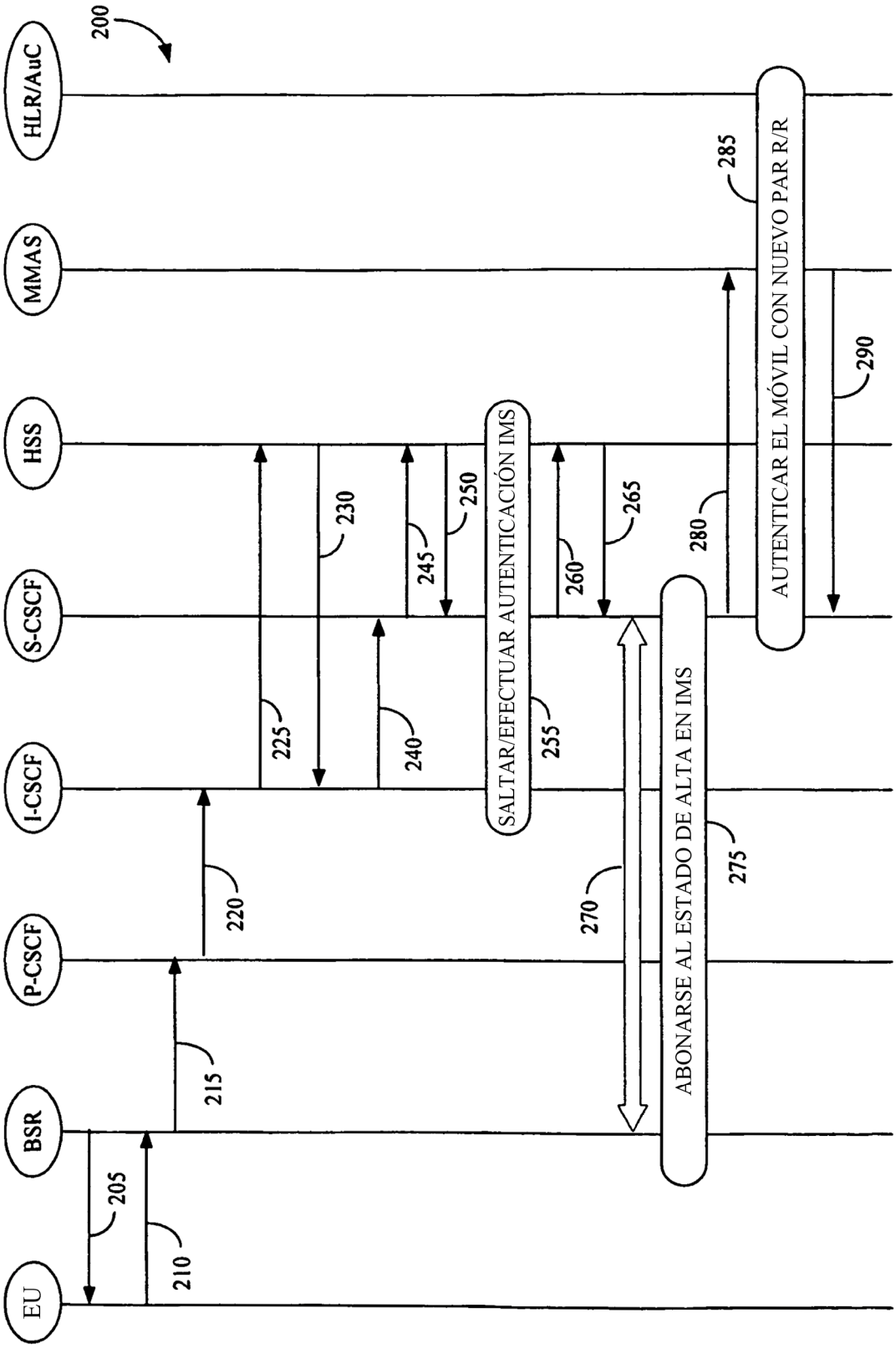
200
HLR/AuC
MMAS
HSS
S-CSCF
I-CSCF
P-CSCF
BSR
EU
205
210
215
220
225
230
240
245
250
255
260
265
270
275
280
285
290
SALTAR/EFECTUAR AUTENTICACIÓN IMS
ABONARSE AL ESTADO DE ALTA EN IMS
AUTENTICAR EL MÓVIL CON NUEVO PAR R/R

Figura 2

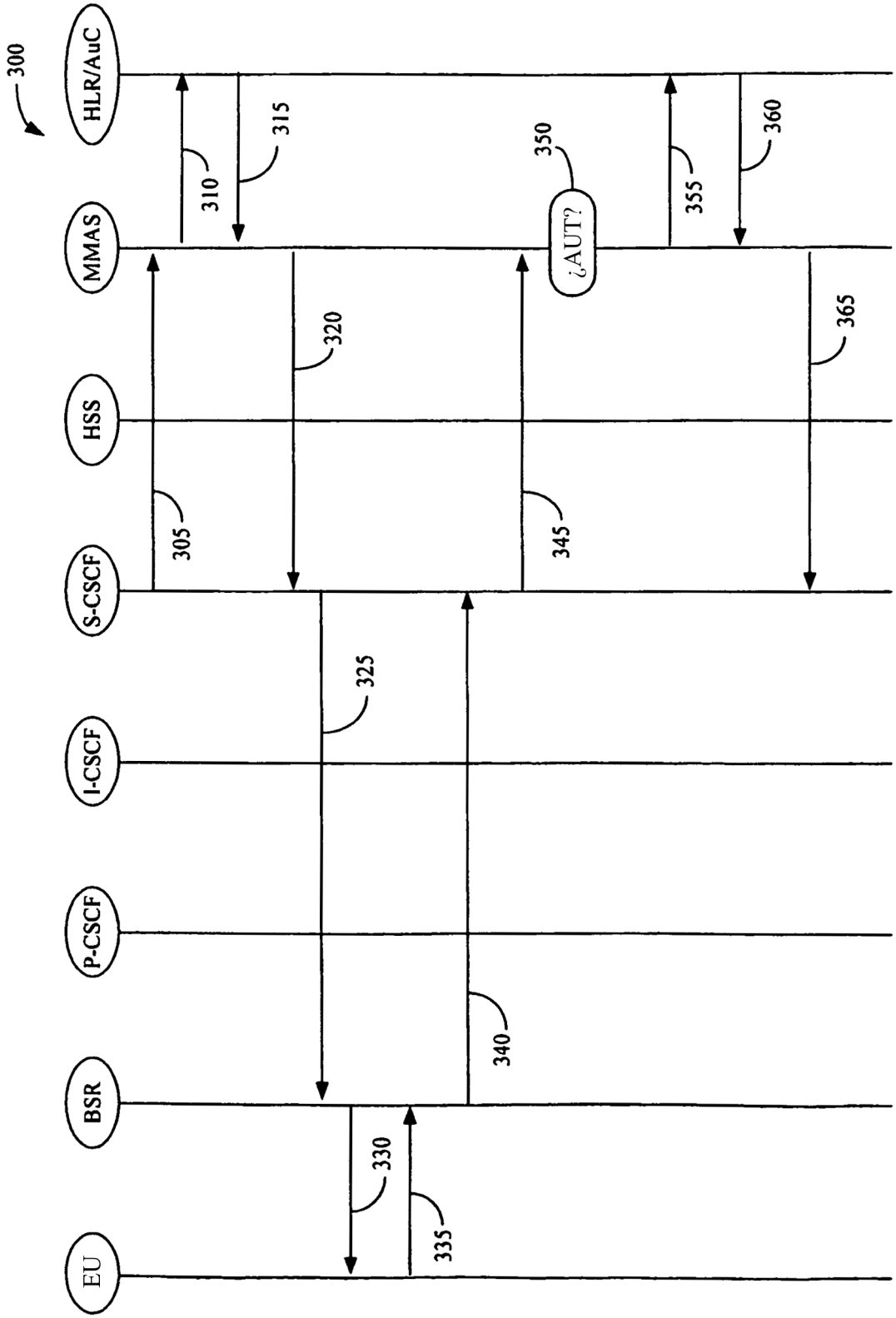
300
HLR/AuC
MMAS
HSS
S-CSCF
I-CSCF
P-CSCF
BSR
EU
310
315
350
¿AUT?
355
360
320
365
305
345
325
340
330
335

Figura 3

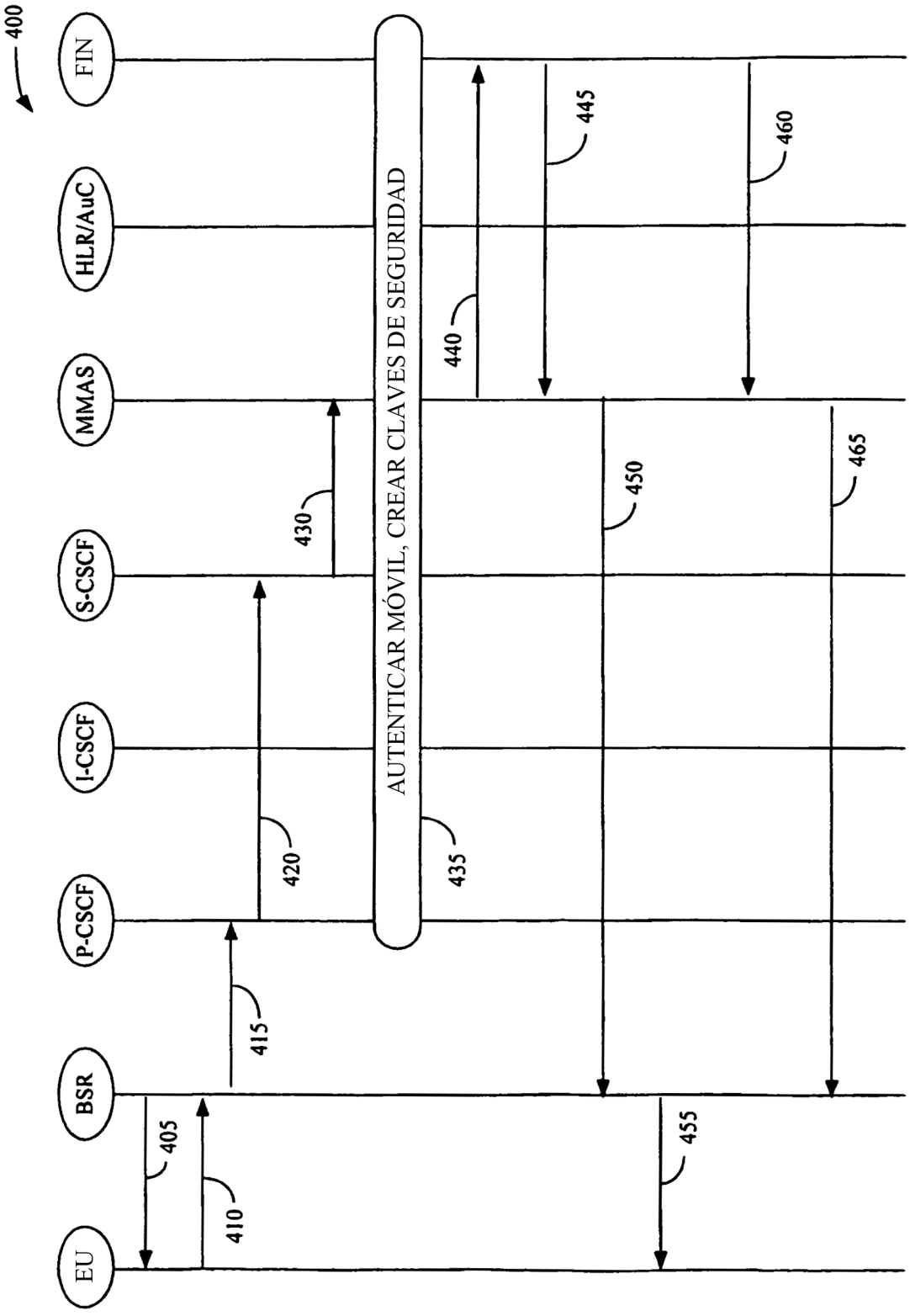
400
EU
BSR
P-CSCF
I-CSCF
S-CSCF
MMAS
HLR/AuC
FIN
AUTENTICAR MÓVIL, CREAR CLAVES DE SEGURIDAD
405
410
415
420
430
435
440
445
450
455
460
465

Figura 4

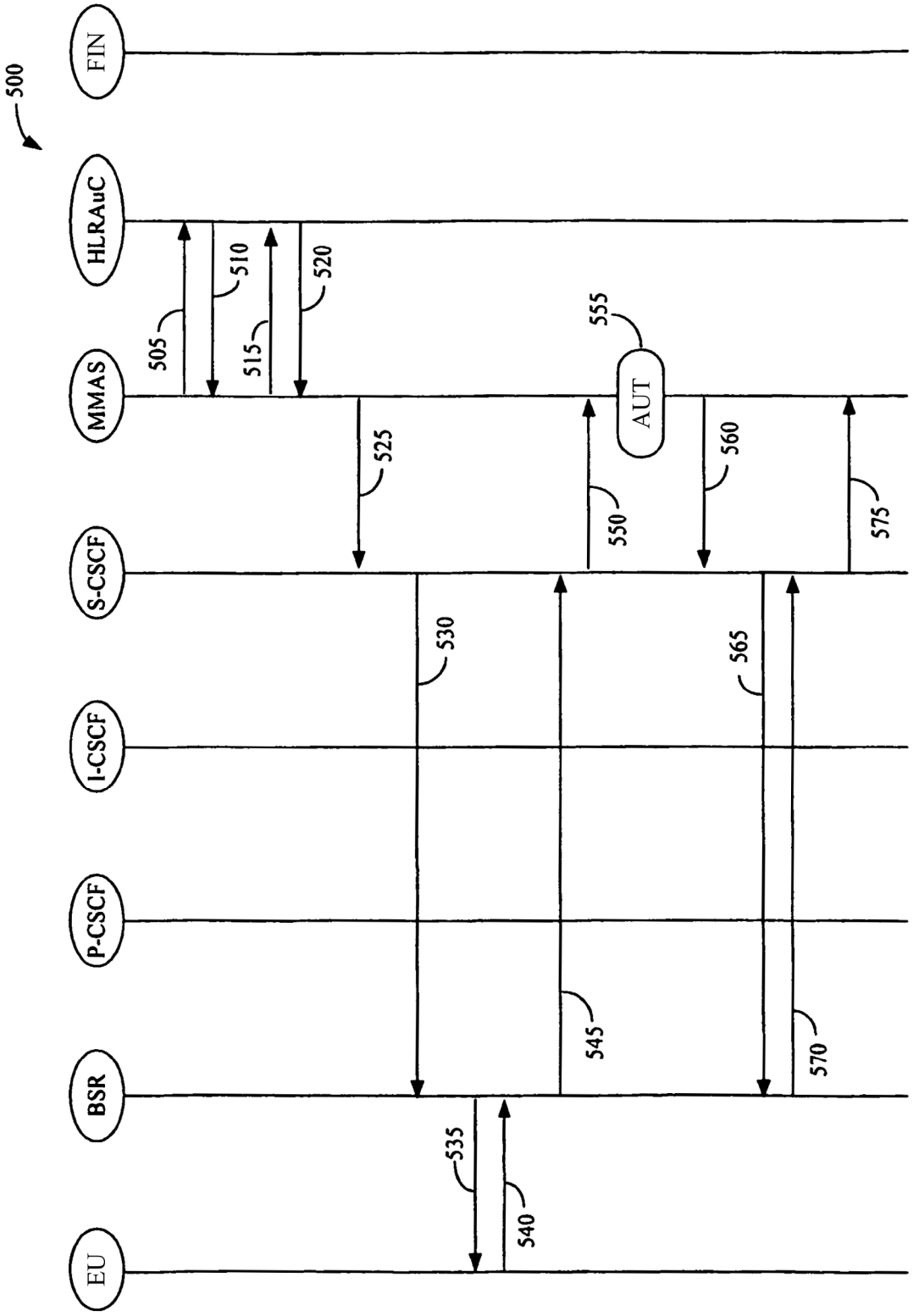
500
EU
BSR
P-CSCF
I-CSCF
S-CSCF
MMAS
HLRAuC
FIN
AUT
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575

Figura 5

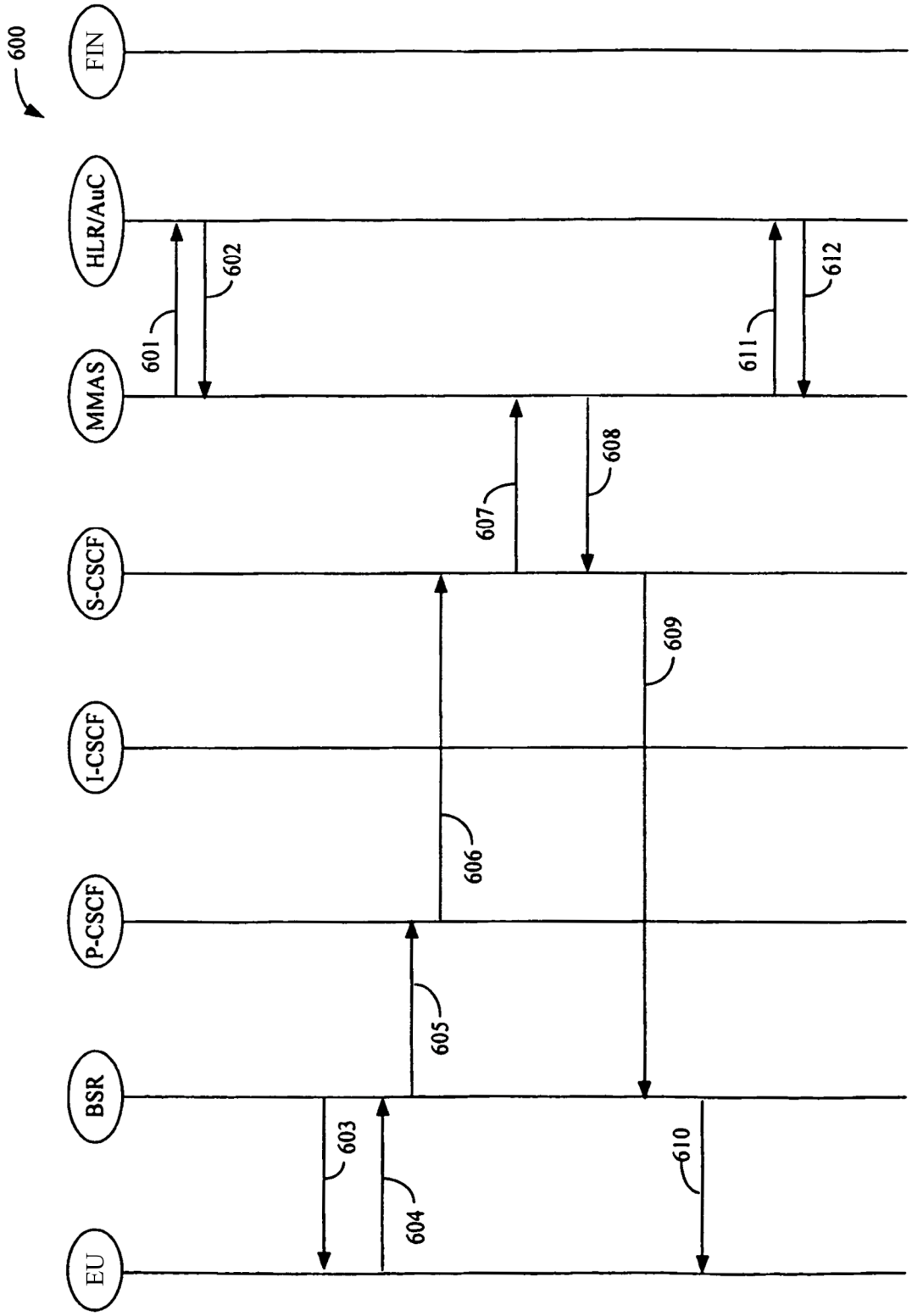
600
FIN
HLR/AuC
MMAS
S-CSCF
I-CSCF
P-CSCF
BSR
EU
601
602
603
604
605
606
607
608
609
610
611
612

Figura 6A

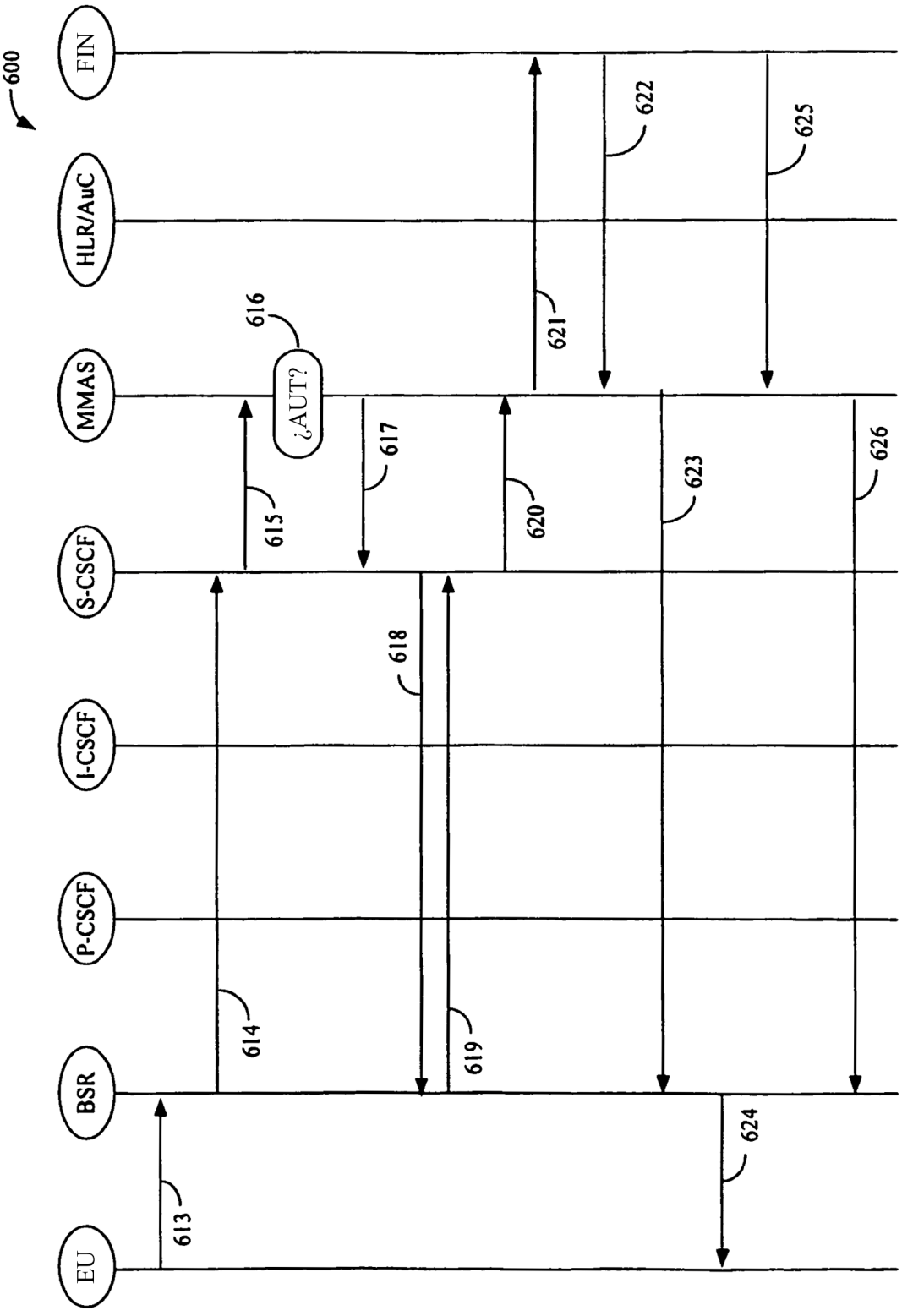
600
EU
BSR
P-CSCF
I-CSCF
S-CSCF
MMAS
HLR/AuC
FIN
¿AUT?
613
614
615
616
617
618
619
620
621
622
623
624
625
626

Figura 6B