(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 385 690**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08774596 .4**
(96) Fecha de presentación: **01.07.2008**
(97) Número de publicación de la solicitud: **2220883**
(97) Fecha de publicación de la solicitud: **25.08.2010**

(54) Título: **Métodos y aparatos que generan una clave para estación de base de radio en un sistema celular de radio**

(30) Prioridad:
11.12.2007 US 12814 P

(45) Fecha de publicación de la mención BOPI:
30.07.2012

(45) Fecha de la publicación del folleto de la patente:
30.07.2012

(73) Titular/es:
Telefonaktiebolaget L M Ericsson (publ)
164 83 Stockholm, SE

(72) Inventor/es:
BLOM, Rolf;
NORRMAN, Karl y
LINDSTRÖM, Magnus

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Métodos y aparatos que generan una clave para estación de base de radio en un sistema celular de radio

Campo técnico

La presente invención se refiere a un método y a un dispositivo para proporcionar una comunicación segura en un sistema celular de radio.

Antecedentes

El sistema evolucionado de paquetes (EPS, en sus siglas en inglés) es un estándar normalizado de telecomunicaciones celulares, normalizado en el Proyecto de Asociación de Tercera Generación (3GPP, en sus siglas en inglés). EPS es parte de la evolución a largo plazo (LTE, en sus siglas en inglés) de sistemas celulares de tercera generación diseñados para satisfacer los requisitos de mayores velocidades de transmisión de bits de usuarios más elevadas. Dentro del EPS, el tráfico del Estrato de Acceso (AS, en sus siglas en inglés) está protegido por medios criptográficos. En particular, el plano de usuario está protegido confidencialmente y la señalización del Control de Recursos de Radio (RRC, en sus siglas en inglés) está protegida tanto en la confidencialidad como en su integridad. Las claves utilizadas para proporcionar encriptado se derivan de una clave criptográfica llamada K_eNB.

En traspasos de estación móvil, también denominadas Equipos de Usuario (UE), desde una estación de base la K_eNB de una estación de base de origen se transforma en el Nodo B evolucionado (eNB, en sus siglas en inglés) de origen, es decir, la estación de base en una clave transformada llamada K_eNB* antes de que sea entregada al eNB objetivo. En la actualidad, el ENB objetivo transforma el K_eNB* junto con un Identificador Temporal de Red Celular de Radio (C-RNTI, en sus siglas en inglés) de eNB objetivo de usuario. Por este motivo, es posible proporcionar encriptación continuada entre el UE y la estación de base objetivo que usa la clave criptográfica transformada.

Además, se ha decidido que no solamente la célula objetivo destinada debe estar preparada para aceptar una estación móvil particular, sino también otras estaciones de base podrán hacer eso mismo. La razón subyacente es ayudar a recuperarse de un fallo del enlace de radio, y en particular de traspasos fallidos. Para facilitar la aceptación por parte de otras estaciones de base, además de la estación de base objetivo, la estación de base de origen eNB envía información clave y un Testigo de Identidad de Terminal (TeIT, en sus siglas en inglés) para el conjunto de estaciones de base que van a "estar-preparadas". Por lo general, la estación de base de origen eNB envía información clave y un Testigo de Identidad de Terminal (TeIT) a estaciones de base situadas cerca de la estación de base objetivo y/o cerca de la estación de base de origen. Sin embargo, si el mismo testigo de seguridad es compartido por todos los eNB en el conjunto que van a estar-preparados, cualquiera de aquellos podría hacerse pasar por la estación móvil, por lo menos hasta que la protección de AS está activada.

Un problema dentro del estándar propuesto existente es que la misma clave K_eNB* transformada no debería ser utilizada por todas las estaciones de base ya que esto permitiría a todas las estaciones de base en el conjunto que va a estar-preparados para generar la K_eNB finalmente utilizada por la estación de base después del traspaso, véase la contribución a SA3, Td S3a070975. Una solución propuesta es que el sistema genera datos iniciales que se utiliza en la transformación de K_eNB para una estación de base eNB dada en el conjunto para estar preparadas de estaciones de base. Estos datos iniciales se remitirá entonces junto con la clave K_eNB* de la estación de base correspondiente a la estación de base eNB.

También el documento “Key refresh in SAE/LTE, S3-070234”, XP-002445697 describe un método en el que los datos son enviados sobre la interfaz aérea para generar la entrada cuando se genera una nueva clave de estación de base.

Sin embargo, existe una demanda constante para reducir la complejidad y mejorar la seguridad en los sistemas de telecomunicaciones existentes. Por tanto, existe una necesidad de un método mejorado para proporcionar una comunicación segura en un sistema celular de radio.

Compendio

Es un objeto de la presente invención proporcionar un método mejorado para proporcionar una comunicación segura en un sistema celular de radio.

Este objeto y otros se obtienen mediante el método, nodo de sistema de radio y Equipo de Usuario y como se establece en las reivindicaciones adjuntas. Así, mediante la creación de una clave de estación de base de radio y/o un Testigo de Identidad de Terminal que utiliza datos conocidos tanto a la estación móvil como a la estación de base de radio, una comunicación segura se puede establecer y mejorar sin tener que proporcionar componentes adicionales de red de seguridad o de señalización adicional.

Según una realización, se genera clave de una estación de base de radio derivada. La clave de la estación de base de radio derivada se crea en respuesta a un conjunto determinado de bits de datos públicos y una clave criptográfica

existente utilizada para comunicación segura entre una estación de base de radio y un Equipo de Usuario. Los datos públicos pueden ser, por ejemplo, bits de datos asociados con la Tecnología de Acceso a la Radio, tales como los bits de datos que identifican la identidad de la célula física. Por este medio, una clave criptográfica de una estación de base, específica para cada estación de base de radio se deriva para cada estación de base de radio aumentando, de esa manera, la seguridad del sistema. Además, la clave (o claves) criptográfica específica se puede derivar sin señalización adicional ni/o sin necesidad de generar datos de entrada específicos cuando se deriva una clave criptográfica que es específica para cada estación de base de radio, lo que reduce la complejidad y proporciona un nivel elevado de seguridad.

De acuerdo con una realización, se crea un Testigo de Identidad de Terminales para la identificación de un Equipo de Usuario, UE, conectado a una estación de base de radio en un sistema de radio. El UE está destinado a comunicarse con el sistema de radio a través de una comunicación segura asociada con una clave de encriptación existente. Cuando se crea el Testigo de Identidad de Terminales, se determina un conjunto de bits de datos conocido tanto por el UE como por la estación de base de radio de origen. Luego, es generado el Testigo de Identidad de Terminales en respuesta al conjunto determinado de bits de datos, la identidad del terminal y la clave existente. Por esto, se deriva un Testigo de Identidad de Terminales que es específico para cada estación de base de radio, aumentando de ese modo la seguridad del sistema.

Según una realización, se proporciona un método de identificación de un Equipo de Usuario, UE, en un sistema de radio. El UE comunica con el sistema de radio a través de una comunicación segura asociada con una clave de encriptación existente. Un primer Testigo de Identidad de Terminales se genera en una estación de base de radio a la que está actualmente conectado el Equipo de Usuario.

El primer Testigo de Identidad de Terminales se distribuye luego a un número de otras estaciones de base de radio del sistema de radio. Un segundo Testigo de Identidad de Terminales también se genera en el Equipo de Usuario. El segundo testigo es transmitido a una de las otras estaciones de base de radio. Cuando el segundo testigo es recibido por una estación de radio, el UE es identificado mediante la comparación del primer y segundo Testigos de Identidad de Terminales. Ambos Testigos de Identidad de Terminales primero y segundo son creados en respuesta a la identidad del terminal y a la clave existente. Por lo tanto, un terminal que deja caer una conexión puede volver a conectarse al sistema a través de un procedimiento de identificación seguro.

La presente invención se extiende también a nodos y Equipos de Usuario destinados a ejecutar en la práctica los métodos que se han descrito más arriba.

Utilizar los métodos, los nodos y Equipos de Usuario según la invención proporcionará un procedimiento más eficiente y seguro para proporcionar comunicación segura en un sistema de radio. Esto se logra usando datos disponibles para la estación de base de radio y el Equipo de Usuario cuando se deriva una clave criptográfica o un Testigo de Identidad de Terminales.

Breve descripción de los dibujos

La presente invención se describirá ahora con más detalle por medio de ejemplos no limitativos y haciendo referencia a los dibujos adjuntos, en los cuales:

- La figura 1 es una vista que ilustra un sistema celular de radio,
- La figura 2 es un diagrama de flujo que ilustra las operaciones realizadas en un procedimiento para crear una clave de una estación de base de radio,
- La figura 3 es un diagrama de flujo que ilustra las operaciones realizadas en una estación de base de radio fuente cuando se preparan para verificar la autenticidad de una estación móvil en movimiento.
- La figura 4 es un diagrama de flujo que ilustra las operaciones realizadas en una estación de base de radio objetivo cuando se verifica la autenticidad de una estación móvil,
- La figura 5 es un diagrama de flujo que ilustra las operaciones realizadas en una estación móvil al verificar la autenticidad de la estación móvil para un sistema celular de radio,
- La figura 6 es una vista de una estación de base de radio, y
- La figura 7 es una vista de un Equipo de Usuario.

Descripción detallada

En lo que sigue, se hará referencia en las realizaciones ilustrativas descritas a un sistema LTE. Sin embargo, la invención no se limita a un sistema de LTE sino que es aplicable a cualquier sistema de radio que usa claves de estaciones de base de radio para proteger los datos transmitidos hacia o desde una estación móvil asociada con la estación de base de radio.

En la figura 1 se muestra una vista esquemática de un sistema celular de radio 100 que proporciona comunicación encriptada para una estación móvil, también denominada Equipo de Usuario (UE) 101. El UE 101 transmite y recibe datos hacia y desde una estación de base de radio 103. En el caso en el que el sistema celular de radio sea un sistema de LTE, la estación de base de radio 103 comúnmente se denomina NodoB evolucionado (eNB, en sus siglas en inglés). Cuando el UE 101 se desplaza por el área geográfica cubierta por el sistema celular de radio 100, algunas veces será necesario traspasar la conexión desde una estación de base de radio a otra estación de base de radio. También algunas veces el UE puede perder la conexión con el sistema celular de radio 100 y luego puede necesitar volver a conectarse al sistema celular de radio. En estos dos escenarios se desea mantener una conexión segura entre el sistema celular de radio 100 y el UE101.

En el caso de que el UE se desplace desde un área cubierta por la estación de base de radio 103 hacia un área cubierta por una estación de base de radio 105, el sistema celular de radio se prepara para el traspaso desde la estación de base de radio 103 de origen a la estación de base de radio 105 objetivo. También debido a que a veces puede ser difícil predecir a qué estación de base de radio será traspasada una estación móvil 101, varias otras estaciones de base de radio pueden también prepararse para el traspaso. Las estaciones de base de radio "que pueden prepararse" están representadas en la figura 1 por una única estación de base de radio 107.

Durante el traspaso, una nueva clave de estación de base de radio necesita ser derivada que se pueda utilizar para la comunicación continua segura entre la estación móvil 101 y la estación de base de radio 105, 107 a la que la conexión se transfiere después del traspaso. La nueva clave de la estación de base puede denominarse una clave de estación de base transformada o derivada. En el caso de que el sistema celular de radio sea un sistema de LTE, la clave transformada puede ser etiquetada K_eNB*.

Según un aspecto de la presente invención, la información para crear un clave única de la estación de base transformada K_eNB* en el conjunto que va a ser preparado se puede basar en los bits menos significativos de una identidad que se conoce (o se da a conocer a) por tanto la UE de la estación móvil como por eNB de la estación de base de radio. Por ejemplo, puede ser utilizada la identidad de la célula física de E-UTRAN de nueve bits, referida aquí como PhyCell_ID, o algunos otros datos específicos de células determinados por el contexto de la Tecnología de Acceso a la Radio (RAT, en sus siglas en inglés). La transformación puede, según una realización, hacer uso de una Función Pseudo Aleatoria (PRF, en sus siglas en inglés) o de una función de dispersión con la clave de la estación de base de origen K_eNB y los datos de las celdas, tales como los bits de PhyCell_ID, como entrada. También pueden ser incluidos otros parámetros de entrada. Ejemplos de otros parámetros pueden ser C-RNTI o cualquier otra información específica del usuario, datos que identifican cuando se puede utilizar la clave, etc.

La estación móvil conocerá los bits de PhyCell_ID a partir de su contexto de Tecnología de Acceso a la Radio (RAT). En la realización ilustrativa, por encima de la derivación de una clave K_eNB* de estación de base objetivo para una estación de base dada eNB con PhyCell_ID puede, en una realización ilustrativa, ser escrita como:

K_eNB* = PRF(K_eNB_Origen), bits de PhyCell_ID, Otros_parámetros)

De acuerdo con otro aspecto de la presente invención, un Testigo de Identidad de Terminales TeIT puede estar formado de una manera correspondiente y ser hecho único para cada estación de base eNB, es decir, también se puede derivar mediante la aplicación de una PRF en la identidad de la estación móvil, la clave de la estación de base K_eNB de origen y los bits de la PhyCell_ID de la estación de base receptora eNB. También pueden incluirse otros parámetros de entrada. Ejemplos de otros parámetros pueden ser la C-RNTI o cualquier otra información específica del usuario, datos que identifican cuándo puede utilizarse la clave, etc.

Además, cuando se requiere que una estación móvil pruebe su identidad, puede estar destinado a generar el correspondiente testigo de identidad. Normalmente, este puede ser el caso durante el traspaso cuando el Equipo de Usuario se conecta a una nueva estación de base de radio y el sistema necesita verificar la identidad del Equipo de Usuario o si la conexión a un Equipo de Usuario se ha caído y el Equipo de Usuario necesita volverse a conectar al sistema.

Según una realización, un Testigo de Identidad de Terminales 1 (TeIT1) puede definirse como:

TeIT1 = PRF (K_eNB_Origen, Terminal_ID, PhyCell_ID bits, Otros_parámetros)

En la figura 2, se muestra un diagrama de flujo que ilustra las operaciones realizadas cuando se genera una clave de encriptación de estación de base para una conexión segura entre una estación móvil 101 y un sistema celular de radio 100 cuando la conexión segura es traspasada desde una estación de base de radio de origen 103 a una estación de base de radio de destino 105, 107. Primero, en la operación 201, el sistema detecta que puede haber un traspaso. Por ejemplo, el sistema puede determinar que la estación móvil 101 está cerca del extremo de la celda de la estación de base de radio de origen basándose en mediciones de radio. A continuación, en la operación 203, la estación de base la de radio de origen genera y transmite una clave de la estación de base transformada a la estación de base de destino 105. En la operación 203, la estación de base de origen 103 también puede enviar una clave de la estación de base transformada a un conjunto de estaciones de base de radio "que están preparadas" 107. La clave de la estación de base transformada puede ser derivada de acuerdo con lo anterior. De acuerdo con una realización, la estación de base de origen también transmite un Testigo de Identidad de Terminales en la

operación 205. El Testigo de Identidad de Terminales puede ser, por ejemplo, un testigo generado como el testigo TeIT1, como se ha descrito más arriba. Entonces, el traspaso puede realizarse de manera convencional, como se indica mediante la operación 207.

De acuerdo con otra realización de la presente invención, la estación de base de origen eNB puede estar destinada a distribuir un testigo común, TeIT3, a todas las estaciones de base del conjunto que va a estar preparado. Este testigo puede ser la salida de una PRF aplicada a la salida de una segunda PRF, que toma, por lo menos, la identidad del terminal y K_eNB como entrada. También pueden proporcionarse otros parámetros de entrada. Ejemplos de otros parámetros pueden ser la C-RNTI o cualquier otra información específica del usuario, datos que identifican cuándo se puede utilizar la clave, etc.

De acuerdo con una realización ilustrativa, cuando una estación móvil transmite información de testigo de identidad, TeIT2, transmite la PRF de la identidad del terminal y la clave de la estación de base K_eNB. La estación de base receptora puede aplicar la PRF externa sobre la TeIT2 recibida desde el terminal y comparar el resultado frente al testigo de identidad, es decir, la TeIT3 recibida desde la estación de base de origen. Si las dos entidades se corresponden, la identidad del terminal se determina para haber sido establecida. Dicho de otra manera, los Testigos de Identidad de Terminal 2 y 3 se pueden escribir:

TeIT2 = PRF (K_eENB_Origen, Terminal_ID, Otros_parámetros)

TeIT3 = PRF (TeIT2, Otros_parámetros2)

Una comparación de una estación de base de TeIT2 recibida desde la estación móvil y TeIT3 recibida desde el eNB de origen puede realizarse como sigue:

TeIT3 =?= PRF (TeIT2, Otros parámetos2),

donde =?= denota una operación de comparación.

En las descripciones anteriores, el Terminal_ID puede ser, por ejemplo, el C-RNTI asignado al terminal en la estación de base de origen eNB o cualquier otra información específica de usuario, datos que identifican cuándo se puede utilizar la clave, etc.

Así, si, por ejemplo, se ha caído una conexión para un UE 101 y el UE 101 necesita volver a conectarse al sistema celular de radio 100, todas las estaciones de base de radio que tienen acceso a la información del testigo de identidad TeIT3 pueden verificar la autenticidad de una estación móvil que transmite el testigo de identidad TeIT2.

De acuerdo con una realización, la clave de la estación de base transformada K_eNB* para la estación de base objetivo eNB puede ser derivada de la misma manera que para la estación de base de radio eNBs en el conjunto que va a estar preparado. La estación de base destino eNB puede recibir, luego, el mismo tipo de información que el resto de estaciones de base preparadas eNBs ya que el traspaso pueden fallar y la estación móvil intentará, luego, volverse a conectar a la estación de base objetivo prevista eNB.

En la figura 3, se muestra un diagrama de flujo que ilustra las operaciones realizadas en una estación de base de radio de origen cuando se preparan para verificar la autenticidad de una estación móvil en movimiento. En primer lugar, en una operación 301 una estación de base de radio de origen determina transmitir un testigo de identidad de terminal a otras estaciones de base de radio. La razón para transmitir el testigo de identidad de terminal puede ser, por ejemplo, que hay un procedimiento de traspaso en curso. El testigo de identidad de terminal puede ser generado, por ejemplo, como el testigo TeIT3 descrito más arriba en la operación 303. A continuación, el testigo se transmite a las otras estaciones de base de radio en la operación 305. Las otras estaciones de base de radio pueden ser, típicamente, estaciones de base de radio adyacentes, a las que la estación móvil es probable que se conecte en un futuro próximo.

En la figura 4, un diagrama de flujo que ilustra las operaciones realizadas en una estación de base de radio objetivo cuando se verifica la autenticidad de una estación móvil. Primero, en la operación 401 la estación de base de radio objetivo recibe una identidad de testigo TeIT3 desde una estación de base de radio de origen. A continuación, en la operación 403, la estación de base de radio de destino recibe un testigo de identidad de terminal TeIT2 desde una estación móvil. Entonces, en la operación 405 la estación de base objetivo compara la identidad del testigo TeIT3 con la identidad del testigo terminal TeTI2. Finalmente, en la operación 407 la estación de base de radio objetivo verifica la autenticidad de la estación móvil sobre la base de la comparación de la operación 405.

En la figura 5, un diagrama de flujo que ilustra las operaciones realizadas en una estación móvil cuando se verifica la autenticidad de la estación móvil a un sistema celular de radio. En primer lugar, en la operación 501, la estación móvil se activa para enviar un mensaje de autenticación. Por ejemplo, durante el traspaso o cuando se interrumpe una conexión, la estación móvil puede necesitar (volver a) autentificarse a una estación de base de radio del sistema celular de radio. A continuación, en la operación 503, la estación móvil genera un testigo de identidad de terminal. El testigo de identidad de terminal puede ser generado como el testigo de terminal de identidad TeIT2 descrito más arriba. Finalmente, la estación móvil transmite un mensaje de autentificación a una estación de base de radio de la

red de radio celular en la operación 505, basándose en el cual el sistema celular de radio puede autentificar a la estación móvil.

En la figura 6 se ilustra una estación de base de radio ilustrativa 103 destinada a generar una clave de estación de base de radio criptográfica transformada de acuerdo con lo anterior. La estación de base de radio comprende un módulo 601 de seleccionar datos que van a ser utilizados cuando se crea una clave criptográfica o un Testigo de identidad de Terminales según lo anterior. El módulo 601 está conectado a un módulo 603 destinado a generar una clave criptográfica o un Testigo de identidad de Terminal según lo anterior. La estación de base de radio ilustrativa 103 puede comprender también un módulo identificador 605 destinado a identificar un UE que se conecta con la estación de base de radio que utiliza un Testigo de Identidad de Terminal como se ha descrito más arriba.

En la figura 7, se ilustra un Equipo de Usuario ilustrativo (UE) 101 destinado a generar un Testigo de Identidad de Terminal según lo anterior. El UE comprende un módulo 701 para seleccionar datos que se van a utilizar cuando se crea un Testigo de identidad de Terminal según lo anterior. El módulo 701 está conectado a un módulo 703 destinado a generar un Testigo de identidad de Terminal según lo anterior. Un Testigo de identidad de Terminal generado en el módulo 703 puede ser transmitido por un transmisor de testigos 705 conectado al módulo 703.

Usar el método y el sistema como se ha descrito en este documento proporcionará un procedimiento más eficaz para proporcionar comunicación segura en un sistema celular de radio, tanto en una situación de traspaso como en situaciones que requieren la autentificación de una estación móvil.

REIVINDICACIONES

1. Un método de crear una clave de estación de base de radio derivada en una estación de base de radio de origen de un sistema celular de radio en una conexión con un Equipo de Usuario, UE, que es susceptible de ser conectado al sistema celular de radio, caracterizado por las operaciones de:

- crear (203) la clave de la estación de base de radio en respuesta a un conjunto determinado de datos y una clave criptográfica existente utilizada para la comunicación entre el Equipo de Usuario, UE, y la estación de base de radio de origen, en el que el conjunto determinado de datos son bits de identidad de célula física derivada de la identidad de células de la célula asociada con una estación de base de radio objetivo, conocida tanto por el Equipo de Usuario como por la estación de base de radio de origen.

2. El método según la reivindicación 1, caracterizado por la operación de usar parámetros de entrada adicionales como datos de entrada cuando se crea la clave de la estación de base de radio derivada.

3. El método según cualquiera de las reivindicaciones 1-2, caracterizado por la operación de crear la clave de la estación de base de radio derivada utilizando una Función Pseudo Aleatoria.

4. Un nodo (103) para su uso en un sistema celular de radio, estando el nodo destinado a crear una clave de estación de base de radio derivada, estando el nodo caracterizado, adicionalmente, por:

- Medios (601) para determinar un conjunto de datos que son bits de identidad de células físicas derivados de la identidad de la célula de la célula asociada con una estación de base de radio objetivo, conocida tanto por un Equipo de Usuario, UE, que se comunica con el sistema de radio celular vía una comunicación segura asociada con una clave criptográfica existente, como por una estación de base de radio del sistema celular de radio, y

- Medios (603) para la creación de la clave de la estación de base de radio en respuesta al conjunto determinado de datos y la clave criptográfica existente.

5. El nodo según la reivindicación 4, caracterizado por medios para usar parámetros de entrada adicionales como datos de entrada cuando se crea la clave de la estación de base de radio derivada.

6. El nodo según cualquiera de las reivindicaciones 4-5, caracterizado por medios para la creación de la clave de la estación de base de radio derivada usando una Función Pseudo Aleatoria.

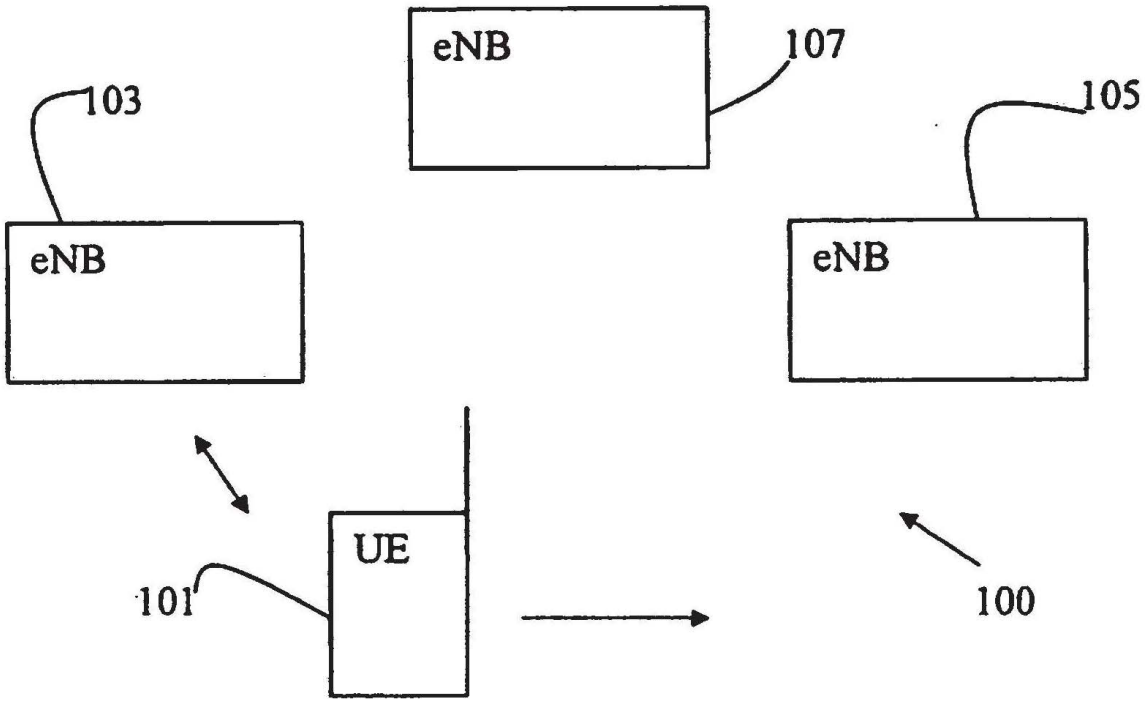

Fig. 1

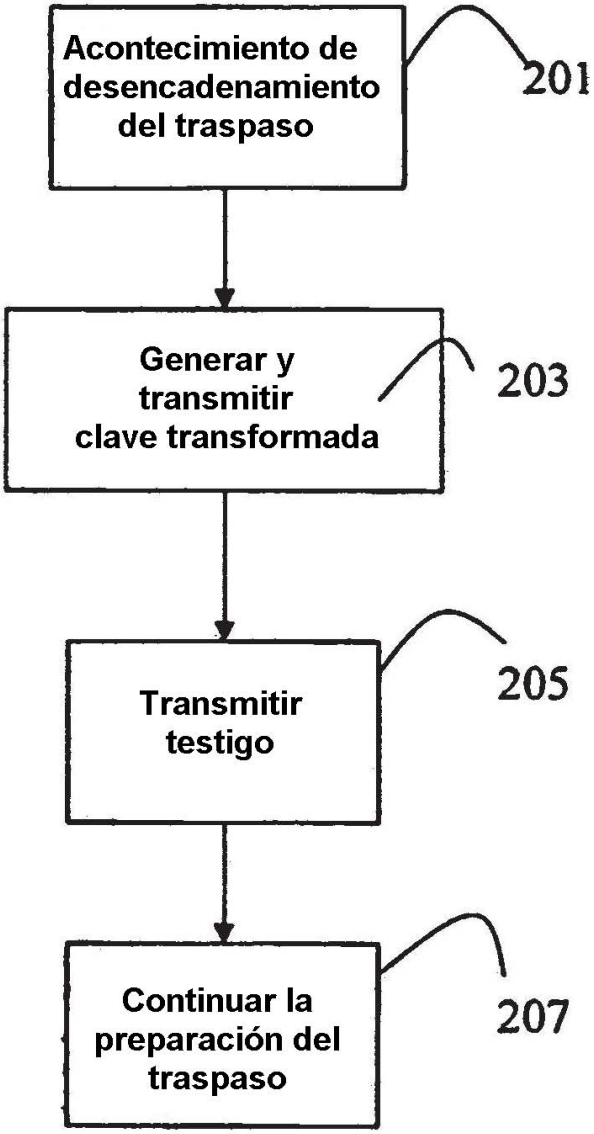
Acontecimiento de desencadenamiento del traspaso
201
Generar y transmitir clave transformada
203
Transmitir testigo
205
Continuar la preparación del traspaso
207

Fig. 2

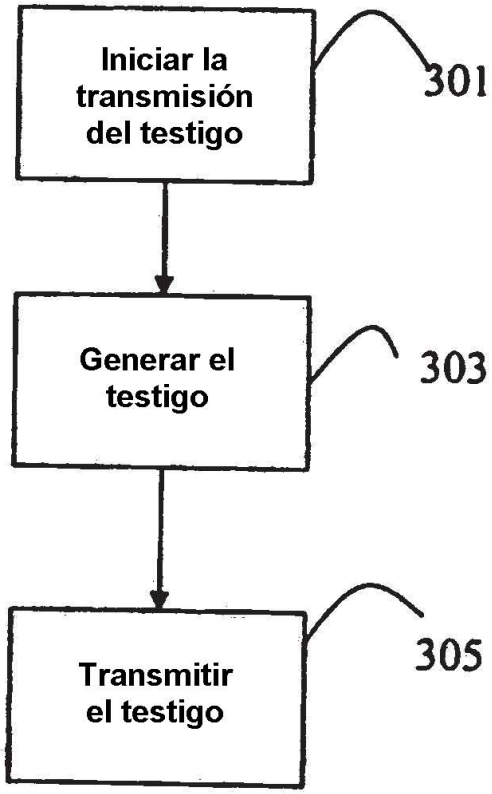
Iniciar la transmisión del testigo
301
Generar el testigo
303
Transmitir el testigo
305

Fig. 3

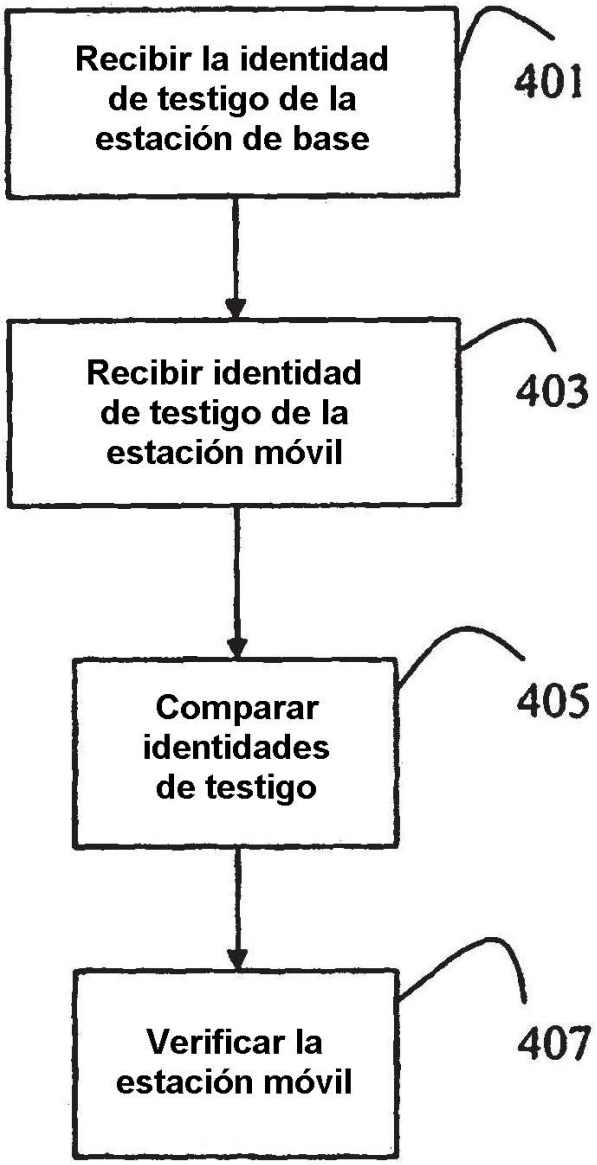
Recibir la identidad de testigo de la estación de base
401
Recibir identidad de testigo de la estación móvil
403
Comparar identidades de testigo
405
Verificar la estación móvil
407

Fig. 4

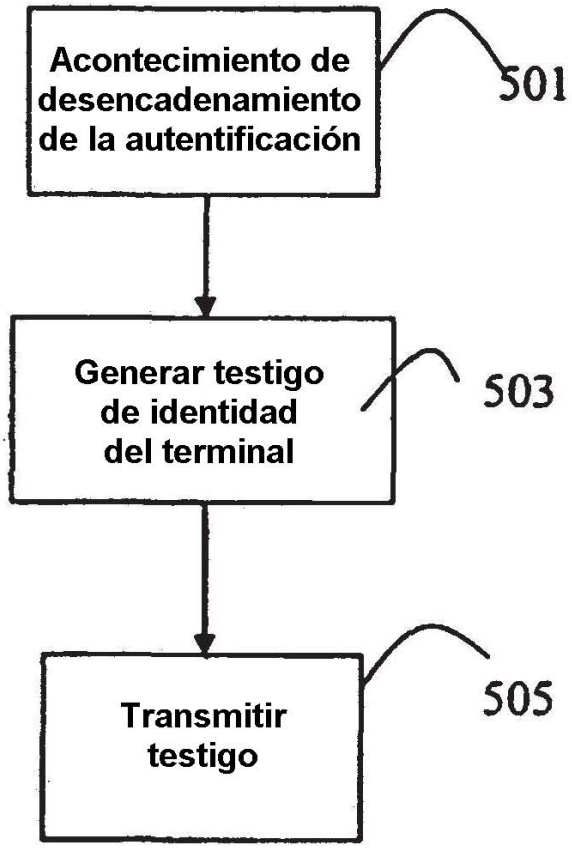
Acontecimiento de desencadenamiento de la autentificación
501
Generar testigo de identidad del terminal
503
Transmitir testigo
505

Fig. 5

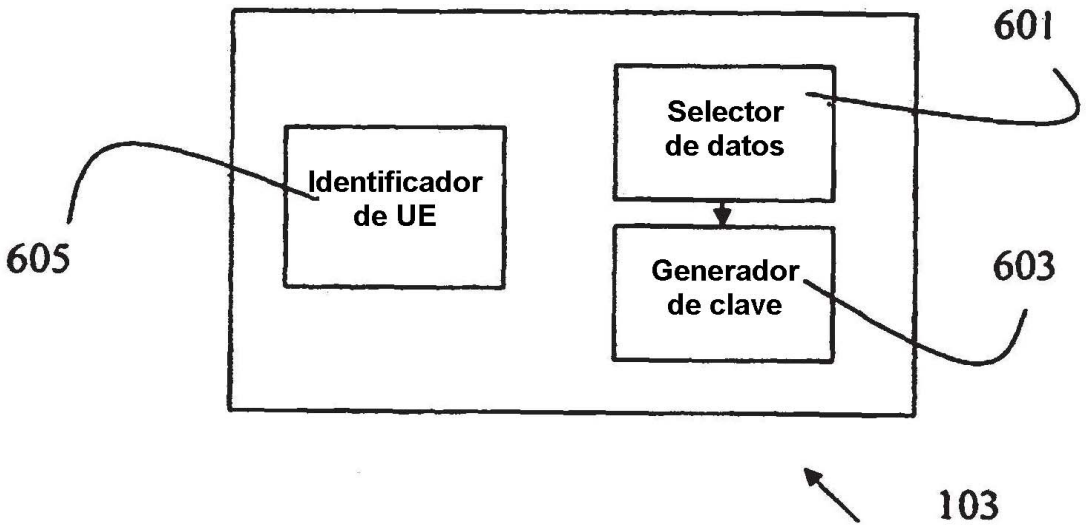
601
Selector de datos
Identificador de UE
605
Generador de clave
603
103

Fig. 6

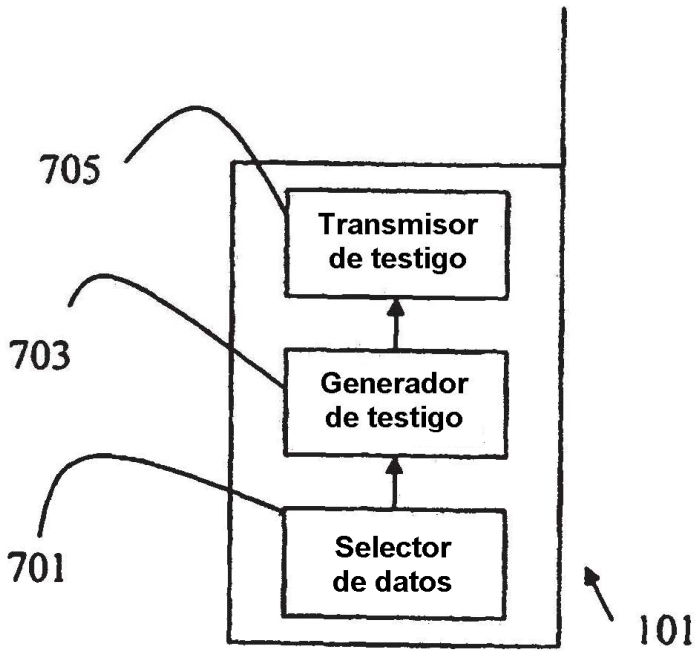
705
Transmisor de testigo
703
Generador de testigo
701
Selector de datos
101

Fig. 7