

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 954 628**

51 Int. Cl.:

H04W 12/06 (2011.01)

H04W 12/40 (2011.01)

H04W 8/18 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **03.11.2020 PCT/EP2020/080796**

87 Fecha y número de publicación internacional: **14.05.2021 WO21089533**

96 Fecha de presentación y número de la solicitud europea: **03.11.2020 E 20797518 (6)**

97 Fecha y número de publicación de la concesión europea: **05.07.2023 EP 4055854**

54 Título: **Método para permitir una solución multi-IMSI en redes 5G**

30 Prioridad:

05.11.2019 EP 19306430

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

23.11.2023

73 Titular/es:

**THALES DIS FRANCE SAS (100.0%)
6, rue de la Verrerie
92190 Meudon, FR**

72 Inventor/es:

**VOYER, JÉRÔME;
DANY, VINCENT y
GROS, JEAN-FRANÇOIS**

74 Agente/Representante:

DEL VALLE VALIENTE, Sonia

ES 2 954 628 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método para permitir una solución multi-IMSI en redes 5G

5 La presente invención se refiere a telecomunicaciones y, más precisamente, a la itinerancia en redes 5G. Se sabe que un terminal (un terminal móvil como un teléfono inteligente, una PDA o un ordenador, por ejemplo, o un equipo M2M) que coopera con un elemento de seguridad (una tarjeta SIM, una tarjeta UICC, una tarjeta eUICC [UICC embebida] o una tarjeta iUICC [UICC integrada], por ejemplo), puede estar en modo de itinerancia en distintos países. El elemento de seguridad también puede estar en forma de un software embebido comprendido en el terminal. El terminal normalmente está acoplado a su red doméstica, pero cuando entra en otro país, existen acuerdos de itinerancia entre el operador de la red doméstica y los operadores del país visitado. Esto permite al terminal recibir gestionar llamadas, correos electrónicos, SMS, ... en el país visitado.

15 También se conoce el uso de un elemento de seguridad que tiene almacenado en el mismo una pluralidad de IMSI (International Mobile Subscription Identifiers [Identidades internacionales de abonado móvil]). Una solución multiIMSI permite que un MNO tenga acuerdos de itinerancia limitados para sacar partido de los acuerdos de itinerancia de otros MNO (denominados “patrocinadores”). Cuando el dispositivo/usuario está en modo de itinerancia, un subprograma multiIMS en la SIM cambia la IMSI a la IMSI del patrocinador.

20 En el siguiente enlace puede obtenerse información más detallada: https://www.gemalto.com/brochures-site/download-site/Documents/linqUs_InstantRoamingMultiIMSI.pdf

25 Una IMSI está formada por un código MCC/MNC/MSIN, donde MCC significa Mobile Country Code (código móvil de país), MNC significa Mobile Network Code (código de red móvil), y MSIN significa Mobile Subscriber Identification Number (número de identificación de abonado móvil) del abonado del MNO.

30 La figura 1 representa este estado de la técnica. En esta figura, un usuario 100 está en un país visitado A 500 distinto de su país de origen 503. En una etapa 101, el usuario 100 enciende su teléfono móvil (terminal) en el país visitado A 500 o se conecta automáticamente a la PLMN del país visitado. A continuación, en una etapa 102, un subprograma multiIMSI que está presente en el elemento de seguridad que coopera con su teléfono móvil (una tarjeta SIM, una tarjeta UICC, una tarjeta eUICC, una tarjeta iUICC o una tarjeta SIM blanda) detecta, gracias a las señales recibidas de entre las mejores señales recibidas de la PLMN comprendida en la lista de PLMN incluidas en una lista de los MNO con los que su MNO doméstico tiene acuerdos de itinerancia. Se prevé que el teléfono móvil reciba señales del denominado MNO patrocinador 501. Esto tendrá lugar gracias a los códigos MCC/MNC recibidos de las estaciones base vecinas (BTS) del MNO patrocinador 501. Sobre esta base, el subprograma selecciona una IMSI correspondiente, denominada IMSI patrocinadora.

35 Por ejemplo, si el usuario 100 está en el país A 500, la IMSI seleccionada será la IMSI del MNO patrocinador 1 (501), si el usuario 100 está en el país B, la IMSI seleccionada será la IMSI del MNO patrocinador 2, y así sucesivamente. Por defecto, la IMSI usada por el elemento de seguridad es la del país de origen 503.

40 El subprograma multiIMSI envía entonces (etapa 103) una solicitud de acoplamiento al BSS de la red del país visitado que tiene acuerdos de itinerancia con el MNO patrocinador 501 (aquí, el patrocinador 1, ya que el usuario está en el país A). La solicitud de acoplamiento comprende la IMSI del MNO patrocinador 1 (501).

45 La red del MNO patrocinador 1 501 sabe que ha asignado esta IMSI al concentrador de itinerancia y redirige la solicitud de acoplamiento a un concentrador de itinerancia 502. El concentrador de itinerancia comprende una tabla que asocia la IMSI del MNO patrocinador 1 501 a la IMSI del MNO 503 del país de origen del abonado.

50 El MNO patrocinador 501 asigna una gama de IMSI al concentrador de itinerancia 502 para que éste pueda reconocer la IMSI utilizada por el elemento de seguridad cuando está en su país de origen 503 (y el concentrador de itinerancia 502 sabe qué MNO debe reenviar la solicitud de acoplamiento).

55 Por lo tanto, los códigos IMSI son conocidos por el concentrador de itinerancia 502, ya que están en un rango de códigos asignados por el MNO patrocinador 501.

El concentrador de itinerancia 502 conmuta la IMSI del patrocinador 1 a la IMSI del país de origen 503 del abonado.

60 En una etapa 105, el registro de ubicaciones locales (HLR) del país de origen realiza una autenticación del elemento de seguridad y autoriza al elemento de seguridad a conectarse a la red en el país visitado (que tiene un acuerdo de itinerancia con el MNO patrocinador del país A 500 [etapa 106]) a través de un mensaje enviado al elemento de seguridad a través del concentrador de itinerancia 502 y la red del MNO patrocinador 1 501.

65 La red del país de origen 503 es capaz de actualizar la lista de IMSI del elemento de seguridad a través de una plataforma OTA (over the air [inalámbrica]) (etapa 107) para, por ejemplo, para añadir un nuevo patrocinador. Esta solución funciona con redes 3G/4G.

El problema es que no funciona con redes 5G, puesto que la IMSI (denominada SUPI) está cifrada, y el MNO patrocinador 501 y el concentrador de itinerancia 502 no pueden encaminar la solicitud de acoplamiento del elemento de seguridad al MNO doméstico 503. No pueden encaminar la solicitud de acoplamiento porque el SUPI está cifrado en un SUCI con una clave del MNO doméstico y necesitan el valor completo del SUPI para encaminar la solicitud de acoplamiento al MNO doméstico 503.

En suma, en 5G, la solución multi-IMSI ya no funciona.

La especificación TS 33.501, v. 16.0.0, del 3GPP es técnica anterior relevante.

La presente invención propone una solución a este problema.

La invención propone un método para acoplar un terminal que coopera con un elemento de seguridad a la red de un MNO de un país visitado cuando se detecte que el terminal está en el país visitado, comprendiendo el método:

- Dar un nuevo valor a un conjunto de archivos del elemento de seguridad, que incluye un nuevo SUPI, llamado SUPI de apoyo de entidad, que corresponde a una entidad de apoyo, correspondiendo el nuevo valor a un SUPI reconocido por la entidad de apoyo;

- construir, a nivel del elemento de seguridad, un SUCI de apoyo de entidad con una clave pública correspondiente, denominada clave pública de apoyo de entidad, y un ID de encaminamiento, denominado ID de encaminamiento de apoyo de entidad;

- encaminar una solicitud de acoplamiento a la entidad de apoyo con el SUCI de apoyo de entidad;

- descifrar, en la entidad de apoyo, el SUCI de apoyo de entidad para obtener el SUPI de apoyo de entidad;

- cambiar, a nivel de la entidad de apoyo, el SUPI de entidad de apoyo en el SUPI correspondiente al MNO del país de origen del terminal;

- enviar la solicitud de acoplamiento de la entidad de apoyo a la red del MNO del país de origen;

- realizar una autenticación del elemento de seguridad a nivel del MNO del país de origen gracias al SUPI;

- si la autenticación es positiva a nivel del MNO del país de origen, enviar del MNO del país de origen al MNO del país visitado un mensaje de acuse de recibo de acoplamiento para que el terminal se conecte a la red del MNO del país visitado.

En una realización, la entidad de apoyo es un MNO patrocinador que tiene la clave privada para descifrar el SUCI, enviando el MNO patrocinador el SUPI a un concentrador de itinerancia, haciendo el concentrador de itinerancia el cambio de SUPI de apoyo de entidad a SUPI doméstico y enviando el SUPI doméstico al MNO del país de origen.

En este caso, el ID de encaminamiento de apoyo es preferiblemente el del MNO patrocinador.

En otra realización, la entidad de apoyo es un concentrador de itinerancia que tiene la clave privada para descifrar el SUCI, recibiendo el concentrador de itinerancia el SUCI procedente de un MNO patrocinador que recibe el SUCI de un MNO patrocinador al que el terminal ha enviado el SUCI, pasando el concentrador de itinerancia del SUPI de apoyo de entidad al SUPI doméstico y enviando el SUPI doméstico al MNO del país doméstico.

En este caso, el ID de encaminamiento de apoyo es el necesario para que el MNO patrocinador encamine la solicitud de acoplamiento al concentrador de itinerancia.

El elemento de seguridad se encuentra preferiblemente entre lo siguiente:

- Una tarjeta SIM

- Una tarjeta UICC

- Una tarjeta eUICC

- Una tarjeta iUICC

- Un software embebido en el terminal.

La invención también se refiere a un elemento de seguridad que coopera con un terminal, comprendiendo el elemento de seguridad instrucciones para implementar las siguientes etapas:

- 5 - cambiar un conjunto de archivos a un nuevo valor, que incluye un nuevo SUPI, llamado SUPI de apoyo de entidad, correspondiente a una entidad de apoyo, correspondiendo el nuevo valor a un SUPI reconocido por la entidad de apoyo;
- 10 - construir un SUCI de apoyo de entidad con una clave pública correspondiente, denominada clave pública de apoyo de entidad, y un ID de encaminamiento, denominado ID de encaminamiento de apoyo de entidad;
- enviar una solicitud de acoplamiento a esta entidad de apoyo con el SUCI de apoyo de entidad;
- conectar el terminal a la red del MNO del país visitado si el MNO de su país de origen lo ha autenticado.

15 La invención se entenderá mejor con la siguiente descripción de las figuras, que representan lo siguiente:

- figura 1 el estado de la técnica para redes 3G/4G;
- 20 - figura 2 el cifrado de una IMSI, denominada SUPI en un entorno 5G, donde el SUPI cifrado se denomina SUCI;
- figura 3 archivos en el elemento de seguridad que permiten implementar la presente invención;
- 25 - figura 4 el método según la invención.

En la figura 2, se ha representado un elemento de seguridad 200 que coopera con un terminal 201. El terminal 201 envía un SUCI 202 (que significa un SUPI cifrado, siendo el SUPI el equivalente de una IMSI en una red 5G) al MNO patrocinador 203 cuando está en el extranjero (ya no hay más cobertura del MNO doméstico).

30 El SUCI 202 comprende:

- El código MCC del MNO patrocinador;
- 35 - El código MNC del MNO patrocinador;
- una instancia de UDM que corresponde a un ID de encaminamiento (para contactar con un cierto UDM del MNO patrocinador o del concentrador de itinerancia);
- 40 - un ID de esquema, que es un algoritmo para cifrar los datos enviados. Este ID de esquema se pone a cero (ningún algoritmo);
- un identificador de clave (ID de clave), que es un identificador de una clave. Este identificador también se pone a cero;
- 45 - un MSIN cifrado del elemento de seguridad, correspondiendo este MSIN a un MSIN anejado al elemento de seguridad en el país de itinerancia, sin los códigos MCC y MNC (solo está cifrado el MSIN). A efectos de privacidad, el cifrado se realiza preferiblemente por medio de criptografía de curva elíptica (ECC).

50 Por lo tanto, en resumen, el MCC, el MNC, la instancia de UDM (RID), el ID de esquema y el ID de clave se envían limpiamente al MNO patrocinador 501. El MSIN correspondiente al correspondiente al país visitado 500 se cifra y se envía con ellos. El MSIN es el correspondiente al MNO patrocinador 501 (país A -> MSIN del MNO patrocinador del país A).

55 La figura 3 representa archivos en el elemento de seguridad que permiten implementar la invención. Estos archivos son archivos estándar según la especificación técnica TS 131 102 v. 15.5.0, del ETSI (2019-04).

60 Un primer archivo EFSuci_calc_info '4F07' comprende una clave pública para cada MNO patrocinador o para el concentrador de itinerancia (el MNO patrocinador tiene la clave privada correspondiente). Tal y como se explicará más adelante, también se puede usar una clave pública para la cual el concentrador de itinerancia tiene una clave privada correspondiente.

65 Un segundo archivo EFrouting_indicator '4FOA' identifica a qué UDM del MNO patrocinador hay que enviar el SUCI (la solicitud de acoplamiento va a una BTS del MNO patrocinador y se reenvía a un registro de ubicaciones de visitante [AMF] vinculado a una pluralidad de UDM). El AMF busca los primeros dígitos del MSIN para encaminar la solicitud a un cierto HLR. También se puede seleccionar un RID del concentrador de itinerancia.

La invención propone almacenar en estos archivos las claves públicas y los ID de encaminamiento. Esta información también se puede almacenar en una memoria intermedia del elemento de seguridad o del terminal.

Según la invención, que se describe en la figura 4, cuando el elemento de seguridad detecta que está en modo de itinerancia, por ejemplo, después de que el abonado haya encendido su teléfono móvil en el país visitado 500 (etapa 300), el subprograma multi-IMSI cambia su IMSI (2G, 3G o 4G) o SUPÍ (5G) a un SUPÍ del MNO patrocinador 501 (etapa 301) y selecciona una clave pública correspondiente (todos los elementos seguros que están en modo de itinerancia en un país determinado seleccionan la misma clave pública). El SUPÍ se cifra según la figura 2 en un SUCI. La primera parte del SUCI no está cifrada, solo se cifra con la clave pública el MSIN del elemento de seguridad para el MNO patrocinador 501.

En esta figura, el ID de encaminamiento (RID) elegido por el elemento de seguridad es un ID de encaminamiento del concentrador de itinerancia 502, pero, tal y como se verá más adelante, el RID puede ser un RID del MNO patrocinador 501 o el RID del concentrador de itinerancia 502. Por lo tanto, en términos generales, el MNO patrocinador 501 y el concentrador de itinerancia 502 constituyen las llamadas “entidades de apoyo”, y el elemento de seguridad, cuando detecta que está en el extranjero, cambia el valor de un conjunto de archivos, que incluye un nuevo SUPÍ, llamado SUPÍ de apoyo de entidad, que corresponde a una entidad de apoyo (el SUPÍ del MNO patrocinador), y construye un SUCI de apoyo de entidad con una clave pública correspondiente, denominada clave pública de apoyo de entidad, y un ID de encaminamiento, denominado ID de encaminamiento de apoyo de entidad. La clave privada de apoyo que es capaz de descifrar la solicitud de acoplamiento se encuentra al nivel de la entidad de apoyo (el UDM del MNO patrocinador 501 o del concentrador de itinerancia 502).

El elemento de seguridad envía la solicitud de acoplamiento a la entidad de apoyo a través de la red MNO del país visitado A 500 con el SUCI de apoyo de entidad. Gracias a su clave privada, la entidad de apoyo descifra el SUCI de apoyo de entidad para obtener el SUPÍ de apoyo de entidad.

El elemento de seguridad envía entonces este SUCI a la red 5G del MNO patrocinador 501.

Tal y como ya se ha mencionado, hay dos alternativas posibles:

La primera alternativa es cuando la clave pública usada para cifrar el MSIN es una clave pública del MNO patrocinador 501. Un UDM del MNO patrocinador 501 (identificado por un RID de patrocinador) recibe el SUCI y emplea su clave privada para descifrar el MSIN del elemento de seguridad. El UDM puede reenviar el SUPÍ al concentrador de itinerancia 502, que cambia el SUPÍ recibido que tiene el MCC/MNC de MNO patrocinador al MCC/MNC del MNO del país de origen 503.

La segunda alternativa es cuando la clave pública utilizada para cifrar el MSIN es, tal y como se muestra en la figura 4, una clave pública del concentrador de itinerancia 502. El concentrador de itinerancia 502 (identificado por un RID de concentrador de itinerancia) recibe el SUCI cuando la clave pública usada para cifrar el MSIN es una clave pública del concentrador de itinerancia 502. El concentrador de itinerancia 502 utiliza su clave privada para descifrar el MSIN del elemento de seguridad concernido en el país visitado. Cuando recibe una solicitud de acoplamiento procedente del elemento de seguridad que comprende un MSIN cifrado por medio de una clave pública del concentrador de itinerancia, el UDM de MNO patrocinador no puede descifrar el SUCI y lo reenvía directamente al concentrador de itinerancia 502 (etapa 303). El concentrador de itinerancia 502 cambia el SUPÍ reconstruido al SUPÍ del MNO del país de origen.

En suma, cuando el MNO patrocinador descifra el SUCI, el SUCI se cifra con una clave PKpatrocinador (PK significa “Public Key”, o “clave pública”) y comprende un RIDpatrocinador. Cuando el concentrador de itinerancia 502 descifra el SUCI, el SUCI se cifra con una clave PKconcentrador y comprende un RIDconcentrador. Por lo tanto, cada una de estas entidades es capaz de descifrar el SUCI recibido.

Así pues, en términos generales, el SUPÍ puede denominarse SUPÍ de apoyo de entidad, siendo la entidad el MNO patrocinador o el concentrador de itinerancia 502.

La entidad de apoyo (aquí, el concentrador de itinerancia 502) entonces cambia (etapa 304) el SUPÍ de entidad de apoyo al SUPÍ correspondiente al MNO del país de origen del terminal. De nuevo, esto se puede hacer a nivel del MNO patrocinador o a nivel del concentrador de itinerancia 502.

El concentrador de itinerancia 502 envía entonces la solicitud de acoplamiento al UDM de la red del MNO del país de origen 503 (etapa 305).

La red doméstica del país de origen 503 realiza entonces una autenticación (etapa 306) del elemento de seguridad gracias al SUPÍ y, si la autenticación es positiva, el MNO del país de origen 503 envía al MNO del país visitado 500 un mensaje de acuse de recibo de acoplamiento (etapa 307) para que el terminal se conecte a la red del MNO del país visitado 500 (etapa 308). Esto se hace a través del concentrador de itinerancia 502 y del MNO patrocinador 501.

Por lo tanto, la entidad de apoyo puede ser un MNO patrocinador 501 que tenga la clave privada para descifrar el SUCI, enviando este MNO patrocinador 501 el SUPI a un concentrador de itinerancia 502, haciendo el concentrador de itinerancia 502 el cambio del SUPI de apoyo de entidad al SUPI doméstico y enviando el SUPI doméstico al MNO del país de origen 503.

5

En este caso, el ID de encaminamiento de apoyo es el del MNO patrocinador 501.

En otro caso, la entidad de apoyo es un concentrador de itinerancia 502 que tiene la clave privada para descifrar el SUCI, recibiendo el concentrador de itinerancia 502 el SUCI procedente de un MNO patrocinador 501 al que el terminal ha enviado el SUCI, cambiando el concentrador de itinerancia 502 el SUPI de apoyo de entidad al SUPI doméstico y enviando el SUPI doméstico al MNO del país de origen 503.

10

En este caso, el ID de encaminamiento de apoyo es el necesario para que el MNO patrocinador 501 encamine la solicitud de acoplamiento al concentrador de itinerancia 502.

15

De nuevo, el RID utilizado por el elemento de seguridad es el RID del MNO patrocinador 501 cuando el MNO patrocinador 501 descifra el SUCI.

También puede ser un RID especial (decidido por el MNO patrocinador 501) que indique al MNO patrocinador 501 que el SUCI recibido ha de enviarse al concentrador de itinerancia 502 cuando el concentrador de itinerancia 502 descifre el SUCI, tal y como se describe en la figura 4.

20

El método aplica a todo tipo de elementos de seguridad. El elemento de seguridad puede ser una tarjeta SIM, una tarjeta UICC, una tarjeta eUICC, una tarjeta iUICC o un software embebido en el terminal.

25

La invención también se refiere a un elemento de seguridad que comprende instrucciones para implementar las etapas de la figura 4, en donde este:

- da un nuevo valor a un conjunto de archivos, que incluye un nuevo SUPI, denominado SUPI de apoyo de entidad, que corresponde a una entidad de apoyo (501 o 502), correspondiendo dicho nuevo valor a un SUPI reconocido por dicha entidad de apoyo (501 o 502);
- construye un SUCI de apoyo de entidad con una clave pública correspondiente, denominada clave pública de apoyo de entidad, y un ID de encaminamiento, denominado ID de encaminamiento de apoyo de entidad;
- envía una solicitud de acoplamiento a esta entidad de apoyo (501 o 502) con la SUCI de apoyo de entidad SUCI;
- conecta el terminal a la red del MNO del país visitado 500 si el MNO de su país de origen 503 lo ha autenticado.

30

35

40

La invención permite capacitar elementos de seguridad multi-IMSI para que trabajen en 5G y aprovecha las características de privacidad.

45

REIVINDICACIONES

1. Un método para acoplar un terminal que coopera con un elemento de seguridad a la red de un MNO de un país visitado (500) cuando se detecta que dicho terminal está en dicho país visitado (500), comprendiendo dicho método:
- Dar un nuevo valor a un conjunto de archivos de dicho elemento de seguridad, que incluye un nuevo SUPI, denominado SUPI de apoyo de entidad, que corresponde a una entidad de apoyo (501, 502), correspondiendo dicho nuevo valor a un SUPI reconocido por dicha entidad de apoyo (501, 502);
 - Construir, a nivel de dicho elemento de seguridad, un SUCI de apoyo de entidad con una clave pública correspondiente, denominada clave pública de apoyo de entidad, y un ID de encaminamiento, denominado ID de encaminamiento de apoyo de entidad;
 - Encaminar una solicitud de acoplamiento a dicha entidad de apoyo (501, 502) con dicha SUCI de apoyo de entidad;
 - Descifrar, en dicha entidad de apoyo (501, 502) dicha SUCI de apoyo de estándar para obtener dicho SUPI de apoyo de entidad;
 - Cambiar a nivel de dicha entidad de apoyo (501, 502) dicha SUCI de entidad de apoyo al SUPI correspondiente al MNO del país doméstico (503) de dicho terminal;
 - Enviar dicha solicitud de acoplamiento de dicha entidad de apoyo (501, 502) a la red de dicho MNO de dicho país doméstico (503);
 - Realizar una autenticación de dicho elemento de seguridad a nivel de dicho MNO de dicho país doméstico (503) gracias a dicha SUPI;
 - Si dicha autenticación es positiva a nivel de dicho MNO de dicho país doméstico (503), enviar de dicho MNO de dicho país doméstico (503) al MNO de dicho país visitado (500) un mensaje de acuse de recibo de acoplamiento para que dicho terminal se conecte a dicha red de dicho MNO de dicho país visitado (500).
2. El método según la reivindicación 1, en donde dicha entidad de apoyo es un MNO patrocinador (501) que tiene la clave privada para descifrar dicho SUCI, enviando dicho MNO patrocinador (501) dicho SUPI a un concentrador de itinerancia (502), haciendo dicho concentrador de itinerancia (502) el cambio del SUPI de apoyo de entidad al SUPI doméstico y enviando dicho SUPI doméstico a dicho MNO de dicho país doméstico (503).
3. El método según la reivindicación 2, en donde dicho ID de encaminamiento de apoyo es el de dicho MNO patrocinador (501).
4. El método según la reivindicación 1, en donde dicha entidad de apoyo es un concentrador de itinerancia (502) que tiene la clave privada para descifrar dicho SUCI, recibiendo dicho concentrador de itinerancia (502) dicho SUCI procedente de un MNO patrocinador (501) al que dicho terminal ha enviado dicho SUCI, cambiando dicho concentrador de itinerancia (502) el SUPI de apoyo de entidad al SUPI doméstico y enviando dicho SUPI doméstico a dicho MNO de dicho país doméstico (503).
5. El método según la reivindicación 4, en donde dicho ID de encaminamiento de apoyo es el necesario para que el MNO patrocinador (501) encamine la solicitud de acoplamiento a dicho concentrador de itinerancia (502).
6. El método según cualquiera de las reivindicaciones 1 a 3, en donde dicho elemento de seguridad se encuentra entre lo siguiente:
- Una tarjeta SIM
 - Una UICC
 - Una eUICC
 - Una iUICC
 - Un software embebido en dicho terminal.

Figura 1

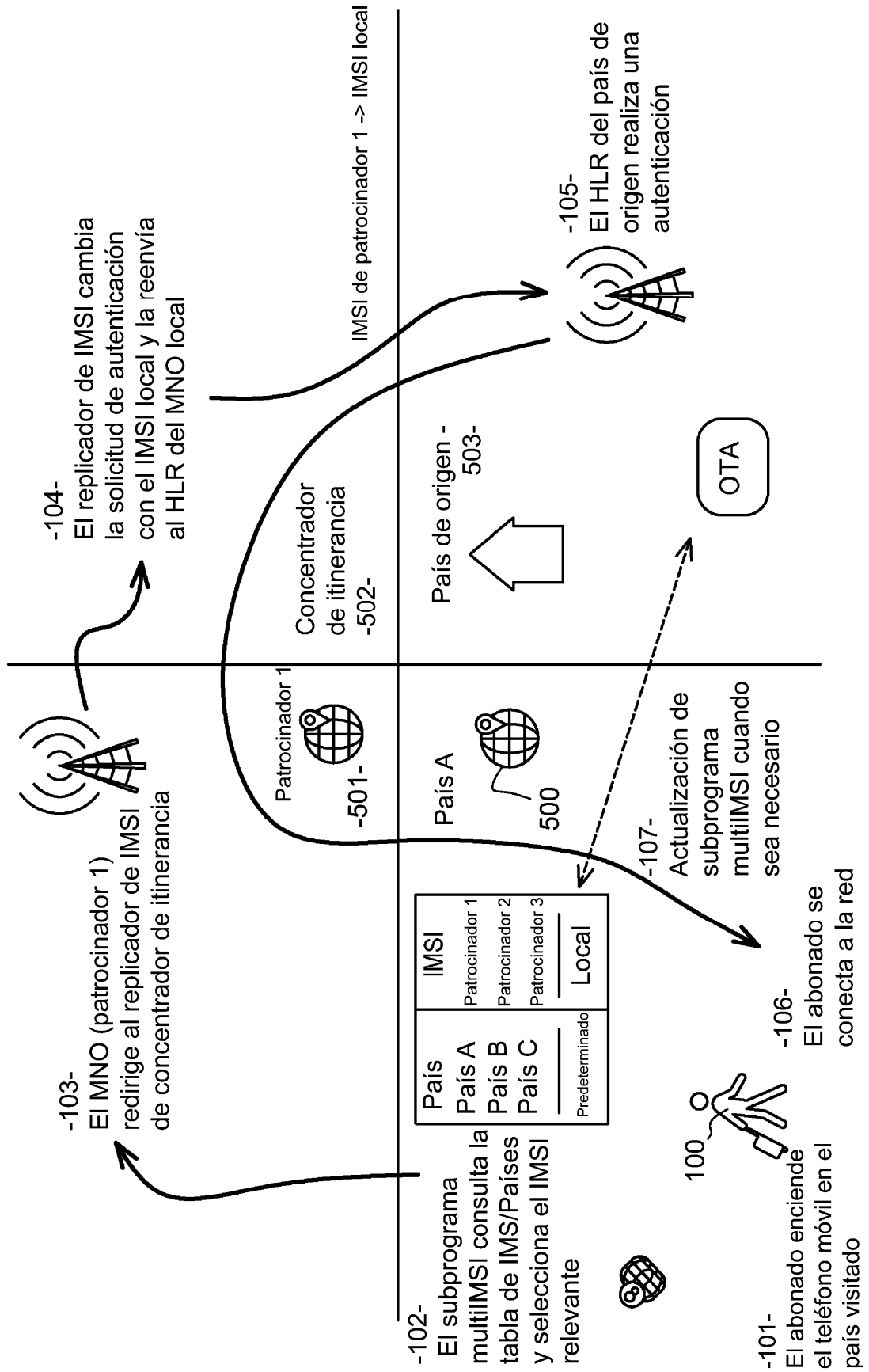


Figura 2

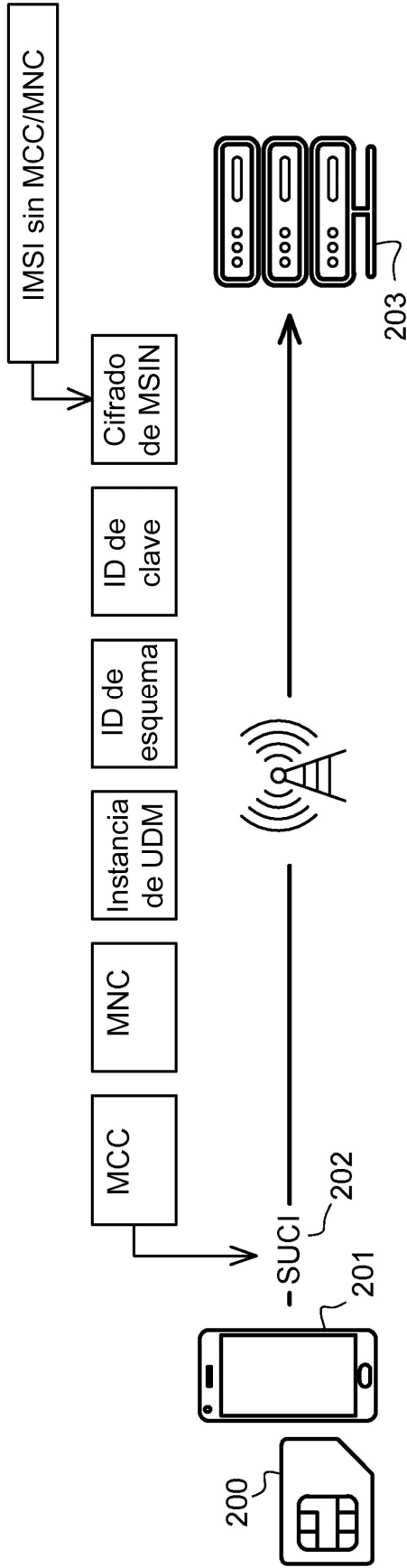


Figura 3

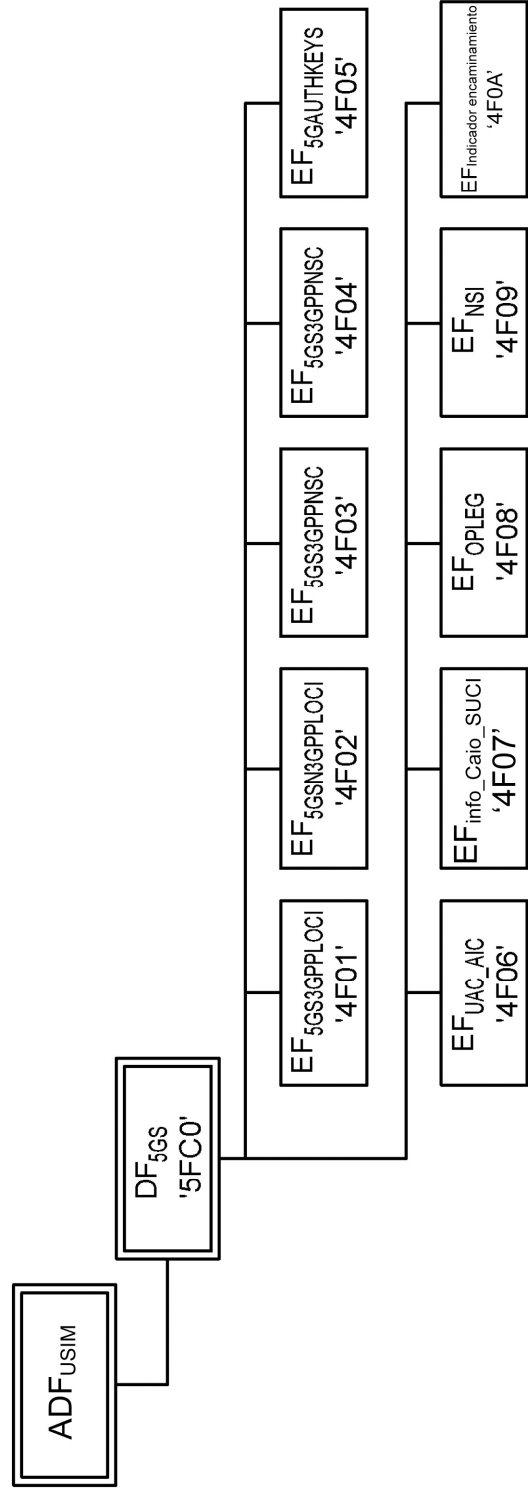


Figura 4

