(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 782 527**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/12 (2006.01)
H04W 8/04 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.07.2013 PCT/EP2013/064743**

(87) Fecha y número de publicación internacional: **16.01.2014 WO14009502**

(96) Fecha de presentación y número de la solicitud europea: **11.07.2013 E 13739384 (9)**

(97) Fecha y número de publicación de la concesión europea: **08.01.2020 EP 2873211**

(54) Título: **Procedimiento de registro de al menos una dirección pública en una red IMS y aplicación correspondiente**

(30) Prioridad:

12.07.2012 EP 12305841

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.09.2020

(73) Titular/es:

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

(72) Inventor/es:

BAUDOUIN, JULIEN y
FINE, JEAN-YVES

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de registro de al menos una dirección pública en una red IMS y aplicación correspondiente

La invención se engloba en el campo de las telecomunicaciones en redes de transmisión de datos. Más exactamente, la presente invención concierne al registro de al menos una dirección pública en una red IMS (IP Multimedia Subsystem).

Una red IMS es una red IP conectada a una red de acceso. La red IMS proporciona una combinación dinámica de transporte de voz, vídeo, mensajes, datos, etc. durante la misma sesión. El IMS utiliza el protocolo SIP (Session Initiation Protocol) para establecer y controlar comunicaciones o sesiones entre terminales de usuarios (denominados puntos terminales) o entre puntos terminales y servidores de aplicación. El protocolo SIP permite a un llamante establecer una sesión mediante conmutación de paquetes con una persona llamada (utilizando SIP User Agents, UAS, instalados en los puntos terminales), aun si el llamante no conoce la dirección IP actual del llamado antes de iniciar la llamada.

Las actuales especificaciones 3GPP IMS demandan la utilización de una operativa de autenticación de los usuarios hacia la red IMS. Esta operativa se encuentra descrita en 3GPP TS 24.229 y 33.203. Utilizando este planteamiento, son asignadas al usuario por el operador una identidad del usuario privado (IMPI) y una o varias identidades públicas de los usuarios (IMPU). Con objeto de participar en sesiones multimedia, el usuario debe registrar al menos un IMPU en la red. Las identidades son utilizadas a continuación por la red para identificar al usuario en el registro y la operativa de autenticación (el IMPI es utilizado para localizar las señas acerca de los abonados, como la información de autenticación de usuario, en tanto que el modelo de imputación requiere la identidad de usuario con la que desea interactuar el usuario, y a la que deben estar vinculados unos servicios específicos). El IMPI y los IMPU se almacenan en una aplicación denominada IMS Subscriber Identity Module (ISIM) convencionalmente almacenada en una tarjeta de circuito integrado (UICC) en el terminal del usuario.

Cada IMPU está asociado a un supuesto perfil de servicio. El perfil de servicio es un conjunto de servicios y de datos conexos, que comprende, entre otros, los criterios de filtrado inicial que proporcionan una lógica de servicio simple para el usuario (por ejemplo, define un conjunto de servicios IMS que la identidad pública IMPU podrá utilizar).

La red de acceso a la red IMS es, por ejemplo, una red UMTS, LTE, WLAN y/o Internet.

La figura 1 representa una red IMS de este tipo conectada a diferentes redes de acceso.

Una red IMS 10, de acuerdo con lo definido por 3GPP TS 23.228, se conecta a servidores de aplicación 11, 12 mediante enlaces SIP 13, 14. Los servidores 11 y 12 alojan aplicaciones IMS que representan servicios tales como mensajería instantánea, administración de presencia (usuario presente, ausente, en una reunión...), filtración de llamadas y sesiones en tiempo real tal como voz sobre IP (VoIP), videoconferencia, vídeo bajo demanda, compartir vídeos, juegos en red o televisión a través de IP.

Unos usuarios de puntos terminales 15 a 20 acceden a estos servicios de la red IMS por mediación de redes de acceso, tal como una red UMTS 21, una red LTE (Long Term Evolution) 22, una red 3GPP2 23, una red WLAN 24 o una red Internet 25. El terminal 17 se comunica mediante un enlace inalámbrico 26 con la red LTE 22 y un enlace EV-DO 27 con la red 3GPP2 23.

La red IMS incluye un servidor delegado, o proxy, 28 unido mediante enlaces SIP 29 a 31 a pasarelas de interconexión, tal como una pasarela GGSN (Gateway GPRS Support Node) 32, encargada especialmente de proporcionar una dirección IP al punto terminal 15 constituido por un terminal GPRS todo el tiempo que dure su conexión a la red IMS, una pasarela PDN GW (Packet Data Network Gateway) 33 que asume el mismo servicio para los terminales LTE 16 y 17, y una pasarela PDSN (Packet Data Serving Node) 34 que asume una conexión a través de la red 3GPP2 23 del terminal 18 de tipo CDMA 2000.

El acceso por parte de los usuarios de los puntos terminales 15 a 20 a los servicios de la red IMS 10 se obtiene después de que estos usuarios se hayan conectado a sus redes de acceso y hayan solicitado una conexión IP hacia esta red IMS 10. Asimismo, los puntos terminales pueden comunicarse sí por mediación de la red IMS, por ejemplo por VoIP.

La autenticación de los puntos terminales mediante la red IMS 10 se obtiene merced a sus identidades privadas IMPIs, comprendidas generalmente en una aplicación USIM o ISIM embarcada en cada uno de los puntos terminales 15 a 20. Por lo tanto, cada punto terminal posee su propia identidad privada IMPI. Durante el desarrollo de la solicitud de acceso a la red IMS 10, un punto terminal envía su IMPI a la red 10 y, si se autentica en ella (en un servidor de registro denominado HSS - Home Subscriber Subsystem), se le conceden derechos de acceso en función de su perfil y de su suscripción. La red IMS procede, en especial, a la facturación al usuario y al control de la sesión.

Cada punto terminal 15 a 20 alberga asimismo al menos una dirección pública IMPU (por lo tanto, no secreta) que permite a su usuario pedir y recibir comunicaciones con otros usuarios o acceder a un servicio. Los IMPUs se

materializan en forma de un SIP URI (Unified Resource Identifier) de acuerdo con lo definido en las recomendaciones IETF RFC 3261 e IETF RFC 2396. A título de ejemplo, una dirección IMPU podría materializarse en la forma de:

sip: jean-yves@gemalto.com

o si no, en forma de un número de teléfono:

sip: 0123456789e@qemalto.ims.com.

En cambio, el formato de una dirección privada IMPI es del tipo:

<xyz>@gemalto.com

siendo <xyz> una cadena de caracteres cualesquiera, llamándose al formato de un IMPI Network Access Identifier tal y como se describe en la recomendación IETF RFC 2486.

Los IMPU y el IMPI se almacenan convencionalmente en la aplicación ISIM de un punto terminal. El punto terminal puede incluir un equipo lógico que puede registrar IMPUs o, si no, se deja a su usuario el derecho de registrar IMPUs, es decir, de escoger el IMPU activo en un momento dado. Así, por ejemplo, el usuario puede decidir que su IMPU profesional esté activo durante sus horarios de oficina y que, fuera de estos horarios, esté activo su IMPU privado.

Si el punto terminal no incluye una aplicación ISIM o USIM, los IMPU y el IMPI se almacenan en una memoria del punto terminal. En una forma de realización convencional, la ISIM se almacena en un elemento seguro, por ejemplo en una tarjeta inteligente UICC extraíble del punto terminal. Una tarjeta UICC puede ser portadora de una o varias aplicaciones ISIM o USIM. Asimismo, el elemento seguro puede formar parte integrante del punto terminal.

Después de o durante la autenticación de un punto terminal mediante reconocimiento de su IMPI y de la verificación de los secretos de los que dispone, el punto terminal envía una de sus direcciones IMPU al HSS de la red IMS 10, con el fin de registrarse en ella y de beneficiarse de un servicio IMS.

El problema que la presente invención se propone solucionar es el siguiente: en la personalización de una UICC o de un terminal, no se conoce el usuario final. Por lo tanto, no hay IMPU en la UICC o en el terminal vendido al usuario final. En el mejor de los casos, hay almacenado un IMPU cualquiera (no personalizado) en la UICC (por ejemplo, martin1234@gemalto.com). Por lo tanto, el registro de IMPUs por parte del usuario de un terminal suele realizarse en el punto de venta del terminal, en una agencia comercial del operador. Un agente comercial del operador con el que el usuario contrata una suscripción registra, por mediación de un terminal de operador, uno o varios IMPUs escogidos por el usuario final. Este o estos IMPUs se cargan entonces por una vía *ad hoc* en la UICC o en el terminal (enlace alámbrico, OTA...) y, en paralelo, se informa de ello al HSS del operador.

Concretamente y a título de ejemplo, el agente del operador introduce un código administrativo ADM utilizando el comando “Verify Pin” y actualiza el fichero EF_IMPU de la UICC con el concurso de un comando “Update”, insertándose la UICC en un lector de tarjetas.

El inconveniente de esta solución está en que el usuario final necesita personarse en una agencia del operador para la personalización de su terminal/UICC para registrar en él uno o varios IMPUs de su elección. Esto vale también si el usuario, a lo largo de la utilización de su terminal, desea añadir, suprimir o modificar uno de sus IMPUs.

Además, el estándar 3GPP TS 31.103 no permite a un usuario actualizar la ISIM de su terminal: el acceso al fichero EF_IMPU precisa de un comando de tipo administrativo (“ADM command” en inglés) que solo el operador conoce. Por lo tanto, el usuario final no tiene la posibilidad de modificar o de actualizar por sí mismo el contenido de este fichero que alberga uno o varios IMPUs. Nos remitiremos ventajosamente a la versión 10 del estándar publicada en abril de 2011, donde el párrafo 4.2.4 titulado EF_IMPU (IMS public user identity) muestra que los comandos “Update”, “Deactivate” y “Activate” de IMPUs están protegidos por códigos administrativos.

El documento EP-2.355.455 propone un terminal que incluye un equipo lógico que puede registrar IMPUs. También se propone dejar al usuario el derecho de registrar IMPUs. Pero, entre otras cosas, este equipo lógico se almacena en el punto terminal, y no en un elemento de seguridad del punto terminal.

El documento 3GPP TS SA WG Security - S3#20 de 27 a 30 de noviembre de 2001 propone la misma solución.

Sin embargo, el usuario no puede, según los estándares, introducir en la ISIM un identificador público de su elección, ya que la ISIM pertenece a y está gestionada por el operador.

El propósito principal de la presente invención es el de subsanar este inconveniente.

Más exactamente, uno de los propósitos de la invención es el de proporcionar un procedimiento y una aplicación que permiten al usuario de un terminal que comprende un elemento de seguridad crear, modificar, activar o desactivar

personalmente una dirección pública IMPU a partir de su terminal, sin tener que personarse en una agencia comercial de su operador de radiotelefonía.

Este propósito, así como otros que en lo sucesivo se irán poniendo de manifiesto, se logra gracias a un procedimiento según la reivindicación 1, es decir, un procedimiento de registro de al menos una dirección pública en una red IMS que comprende un terminal cooperante con un elemento de seguridad, comprendiendo el elemento de seguridad una aplicación que invita al usuario del terminal, al producirse un evento, a introducir una dirección pública de su elección por mediación de la interfaz hombre-máquina del terminal, transmitiendo la aplicación la dirección pública, acompañada de al menos un identificador del elemento de seguridad, a una red remota por mediación del terminal, con el fin de que la red remota asocie la dirección pública al identificador, devolviendo la red remota a dicho elemento de seguridad un mensaje de confirmación de asociación si dicha dirección pública está disponible y una vez que se ha asociado dicha dirección pública al identificador recibido, con el fin de que dicha aplicación registre dicha dirección pública en dicho elemento de seguridad, comprendiendo la red remota una plataforma OTA que hace las funciones de punto de entrada hacia un HSS de una red IMS.

En una forma ventajosa de puesta en práctica, la invención consiste en actualizar el terminal con la dirección pública, previa recepción, por el elemento de seguridad, del mensaje de confirmación de asociación.

Preferiblemente, el identificador del elemento de seguridad comprende al menos uno de los siguientes identificadores:

- el IMSI;

- la ICCID;

- el IMPI.

El evento es, por ejemplo, el primer encendido del terminal.

Asimismo, la invención concierne a una aplicación según la reivindicación 5, es decir, a una aplicación para el registro de al menos una dirección pública en una red IMS que comprende un terminal cooperante con un elemento de seguridad, albergando el elemento de seguridad dicha aplicación, aplicación esta que invita al usuario del terminal, al producirse un evento, a introducir una dirección pública de su elección por mediación de la interfaz hombre-máquina del terminal, transmitiendo la aplicación la dirección pública, acompañada de al menos un identificador del elemento de seguridad, a una red remota por mediación del terminal, con el fin de que la red remota asocie la dirección pública al identificador, registrando dicha aplicación dicha dirección pública en dicho elemento de seguridad a la recepción de un mensaje de confirmación de asociación que, enviado por dicha red remota, indica que dicha dirección pública está disponible y que se ha asociado dicha dirección pública al identificador recibido, comprendiendo dicha red remota una plataforma OTA que hace las funciones de punto de entrada hacia un HSS de una red IMS.

Otras características y ventajas de la invención se irán poniendo de manifiesto con la lectura de la siguiente descripción de una forma preferente de puesta en práctica, dada a título ilustrativo y no limitativo, y de las figuras que se acompañan, en las cuales:

- la figura 1 representa una red IMS conectada a diferentes redes de acceso; y

- la figura 2 representa un ejemplo de puesta en práctica del procedimiento según la invención.

La figura 1 se ha descrito con referencia al estado de la técnica.

La figura 2 representa un ejemplo de puesta en práctica del procedimiento según la invención.

La invención propone aprovechar una aplicación (applet) instalada en una ISIM en el seno de una UICC 100. La UICC 100 está comprendida en un terminal 101, representado en el caso presente en forma de un teléfono móvil. Asimismo, la aplicación puede estar instalada en un chip (eUICC) solidario del terminal 101, siendo en este caso la UICC 100 no extraíble del terminal 101 como puede serlo una tarjeta SIM.

Asimismo, la UICC 100 o la eUICC puede comunicarse vía radio (Bluetooth o Wifi, por ejemplo) con el terminal 101, es decir, que no necesita estar comprendida en el terminal 101. Puede estar comprendida, por ejemplo, en un elemento trasladado tal como un reloj de pulsera, siendo lo esencial que ésta se comunique con el terminal 101.

El terminal 101 es apto para comunicarse con una red remota que, en el caso presente, comprende una plataforma OTA 102 y un elemento HSS 103 de una red de operador. El terminal 101 puede comunicarse con el HSS 103 por mediación de la plataforma OTA 102.

El HSS 103 tiene por principal función el almacenar, para cada usuario de la red, información referente a su UICC 100. En tal sentido, a cada UICC se le asocia un IMSI/ICCID, un IMPI, uno o varios IMPUs, su dominio IMS (el dominio IMS permite a los abonados comunicarse entre sí a través de los servicios IMS o acceder a servicios IMS

alojados en plataformas de servicio) y un perfil de servicios. Antes de la ejecución de la aplicación según la invención, el HSS 103 conoce al usuario 104 por su IMSI, su ICCID y/o su IMPI, el dominio al que pertenece, así como su perfil de servicios. Sabe, asimismo, que no hay asociado ningún IMPU a estos identificadores (IMPU NOK). Igualmente, la UICC 100 contiene los ficheros EF_IMPI, EF_Domain y EF_PCSCF (fichero de dirección IP del proxy de acceso al operador). La UICC 100 contiene asimismo el fichero vacío EF_IMPU (EF_IMPU NOK).

Al producirse un evento, por ejemplo en el primer encendido del terminal 101, en el encendido del terminal 101 tras la descarga de la aplicación según la invención o, si no, por activación de una función de un menú, o de manera más general por demanda, un mensaje de bienvenida 105 invita al usuario 104 del terminal 101 a introducir uno o varios perfiles IMS, correspondiéndose un perfil IMS con una dirección IMPU.

El usuario 104 introduce entonces, por mediación de la interfaz hombre-máquina del terminal 101, por ejemplo, el teclado, uno o varios IMPUs de su elección. En el ejemplo representado, en una etapa 106, escoge las siguientes direcciones:

Sip:James.bond@mno.com

Sip:Bob.thebest@mno.com

Sip:little.Louise@mno.com

La aplicación transmite estas direcciones públicas a la ISIM, en una etapa 107, mediante un comando STK. La ISIM almacena provisionalmente estos IMPUs en un directorio *ad hoc*.

En una etapa 108, la aplicación transmite los IMPUs escogidos por el usuario 104 a la plataforma OTA 102, acompañados de al menos un identificador de la UICC. En el ejemplo dado, con los IMPUs se transmiten tres identificadores de la UICC a la plataforma OTA 102: el IMSI, la ICCID y el IMPI. La plataforma OTA retransmite estos identificadores (IMSI / ICCID / IMPI / IMPUs) al HSS, en una etapa 109. El HSS 103 procede entonces a un control de los IMPUs escogidos por el usuario 104. Este control consiste especialmente en verificar que los IMPUs no se han asignado ya a otro usuario, abonado de la misma red de operador o de otra red de operador. Asimismo, el HSS 103 asocia los IMPUs recibidos al identificador de la UICC.

El HSS 103, si comprueba que los IMPUs recibidos están disponibles, informa de ello a la UICC mediante un mensaje ACK (etapa 110) de confirmación de asociación, una vez que la o las direcciones públicas están asociadas al identificador o a los identificadores recibidos. Este mensaje se retransmite de la plataforma OTA 102 a la UICC 100.

La ISIM procede entonces a una actualización de su fichero EF_IMPU 6F04 que comprende los IMPUs del usuario 104. Esta actualización consiste en registrar en él los IMPUs almacenados provisionalmente con anterioridad en el directorio *ad hoc* antedicho.

Si uno de los IMPUs no está disponible, informa de ello igualmente a la UICC, con el fin de que no tenga en cuenta el IMPU no disponible. Entonces se presenta al usuario un mensaje para informarle de la no disponibilidad de ese IMPU, eventualmente con una invitación a escoger otro.

La aplicación transmite entonces un comando “Refresh ISIM” al terminal 101 (etapa 111), con el fin de que el mismo tenga en cuenta los nuevos IMPUs. El terminal, entonces, acusa recibo de estos IMPUs en la etapa 112. Se puede realizar entonces una validación del registro de los IMPUs (realizada después de la etapa 110).

Facultativamente, se puede invitar entonces al usuario 104 a contratar servicios (etapa 113), ya que ahora dispone de al menos una dirección IMPU. Si el usuario acepta, se le puede proponer una lista de servicios (etapa 114). En el caso presente, se proponen al usuario cuatro servicios:

- Vídeo bajo demanda

- Mensajería

- Juegos en línea

- Descarga de música

Si el usuario, por ejemplo, elige “Juegos en línea”, el HSS 103 recibe un comando de servicio de juegos en línea (etapa 115), acompañado de al menos un identificador de la UICC (en el caso presente, el IMSI, el ICCID y el IMPI), por mediación de la plataforma OTA 102. El HSS 103, con el concurso del identificador recibido, puede remitirse entonces a la UICC 100 con el concurso de los IMPUs asociados al identificador recibido.

Aunque la invención anteriormente descrita se ha llevado a cabo en el ámbito de la creación de IMPUs, puede ser de aplicación, asimismo, en la modificación de IMPUs existentes, así como en la activación o la desactivación de IMPUs, como también en la supresión de IMPUs.

La aplicación de la ISIM que permite poner en práctica la presente invención puede ser grabada en esta ISIM bajo control del operador, por ejemplo a través de la plataforma OTA 102. Su instalación en la ISIM se realiza bajo control del operador y la aplicación comprende los derechos PIN y administrativos (ADM). El operador dispone de los derechos de instalación de la aplicación en la ISIM de la UICC (eUICC) del usuario. Por lo tanto, la aplicación conoce el código administrativo (ADM) que permite acceder al HSS y registrar en él uno o varios IMPUs.

La invención radica, por tanto, en una aplicación de confianza que es una applet instalada en una UICC. Esta applet es la que inicia el diálogo con la plataforma OTA 102 y el HSS 103 para enviar los IMPUs escogidos por el usuario 104. Como consecuencia del consentimiento del HSS 103, esta applet escribe (por intermedio de una interfaz interna del SO y porque ha sido instalada con el derecho administrativo ADM) los IMPUs escogidos en el fichero EF_IMPU.

Por lo tanto, la invención permite a un usuario crear, modificar, activar o desactivar uno o varios IMPUs en una red IMS.

En un ejemplo que no queda cubierto por las reivindicaciones, la plataforma OTA 102 que, en la descripción precedente, hace las funciones de punto de entrada hacia un HSS de una red IMS puede sustituirse por un servidor de aplicaciones unido al HSS del operador.

Aunque las comunicaciones representadas en la figura 2 son preferiblemente de tipo http (red IP integral tal como LTE), se pueden utilizar asimismo comunicaciones de tipo SMS o SIP entre el terminal 101 y la plataforma OTA 102, e incluso entre esta plataforma 102 y el HSS 103. Estas comunicaciones son cifradas mediante mecanismos bien conocidos para evitar todo fraude y asegurar la seguridad del usuario 104 y del operador de la red.

La invención permite encontrar una vía paralela al estándar existente, permitiendo al usuario de un terminal definir direcciones IMPUs de su elección, sin tener que personarse en una agencia de su operador.

Asimismo, la invención concierne a una aplicación para el registro de al menos una dirección pública en una red IMS que comprende un terminal cooperante con un elemento de seguridad, invitando el elemento de seguridad que alberga esta aplicación al usuario del terminal, al producirse un evento, a introducir una dirección pública de su elección por mediación de la interfaz hombre-máquina del terminal, transmitiendo esta aplicación la dirección pública, acompañada de al menos un identificador del elemento de seguridad, a una red remota por mediación de este terminal, con el fin de que la red remota asocie la dirección pública al identificador recibido, registrando dicha aplicación dicha dirección pública en dicho elemento de seguridad a la recepción de un mensaje de confirmación de asociación que, enviado por dicha red remota, indica que dicha dirección pública está disponible y que se ha asociado dicha dirección pública al identificador recibido, comprendiendo dicha red remota una plataforma OTA que hace las funciones de punto de entrada hacia un HSS de una red IMS.

La invención permite evitar a un usuario de un terminal tener que personarse en una agencia de su operador de telefonía o conectarse a un servicio de Internet después de haber comprado su terminal con su UICC (eUICC) con el fin de configurarlo con su(s) IMPU(s).

El HSS del operador es actualizado dinámicamente por el usuario final, y la invención responde a los estándares de la IMS, del 3GPP sobre la ISIM y de los intercambios OTA (“OTA messaging” en inglés) y del aprovisionamiento del HSS del operador.

REIVINDICACIONES

1. Procedimiento de registro de al menos una dirección pública en una red IMS que comprende un terminal (101) cooperante con un elemento de seguridad (100), comprendiendo dicho elemento de seguridad (100) una aplicación que invita al usuario (104) de dicho terminal (101), al producirse un evento, a introducir una dirección pública de su elección por mediación de la interfaz hombre-máquina de dicho terminal (101), transmitiendo dicha aplicación dicha dirección pública, acompañada de al menos un identificador de dicho elemento de seguridad (100), a una red remota (102, 103) por mediación de dicho terminal (101), con el fin de que dicha red remota (102, 103) asocie dicha dirección pública a dicho identificador, devolviendo dicha red remota (102, 103) a dicho elemento de seguridad (100) un mensaje de confirmación de asociación si dicha dirección pública está disponible y una vez que se ha asociado dicha dirección pública al identificador recibido, con el fin de que dicha aplicación registre dicha dirección pública en dicho elemento de seguridad (100), comprendiendo dicha red remota (102, 103) una plataforma OTA (102) que hace las funciones de punto de entrada hacia un HSS (103) de una red IMS.

2. Procedimiento según la reivindicación 1, caracterizado por que consiste en actualizar dicho terminal (101) con dicha dirección pública, previa recepción, por dicho elemento de seguridad (100), de dicho mensaje de confirmación de asociación (110).

3. Procedimiento según una de las reivindicaciones 1 y 2, caracterizado por que dicho identificador de dicho elemento de seguridad (100) comprende al menos uno de los siguientes identificadores:

- el IMSI;

- el ICCID;

- el IMPI.

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado por que dicho evento es el primer encendido de dicho terminal (101).

5. Aplicación para el registro de al menos una dirección pública en una red IMS que comprende un terminal (101) cooperante con un elemento de seguridad (100), albergando dicho elemento de seguridad (100) dicha aplicación, invitando dicha aplicación al usuario (104) de dicho terminal (101), al producirse un evento, a introducir una dirección pública de su elección por mediación de la interfaz hombre-máquina de dicho terminal (101), transmitiendo dicha aplicación dicha dirección pública, acompañada de al menos un identificador de dicho elemento de seguridad (100), a una red remota (102, 103) por mediación de dicho terminal (101), con el fin de que dicha red remota (102, 103) asocie dicha dirección pública a dicho identificador, registrando dicha aplicación dicha dirección pública en dicho elemento de seguridad (100) a la recepción de un mensaje de confirmación de asociación que, enviado por dicha red remota (102, 103), indica que dicha dirección pública está disponible y que se ha asociado dicha dirección pública al identificador recibido, comprendiendo dicha red remota (102, 103) una plataforma OTA (102) que hace las funciones de punto de entrada hacia un HSS (103) de una red IMS.

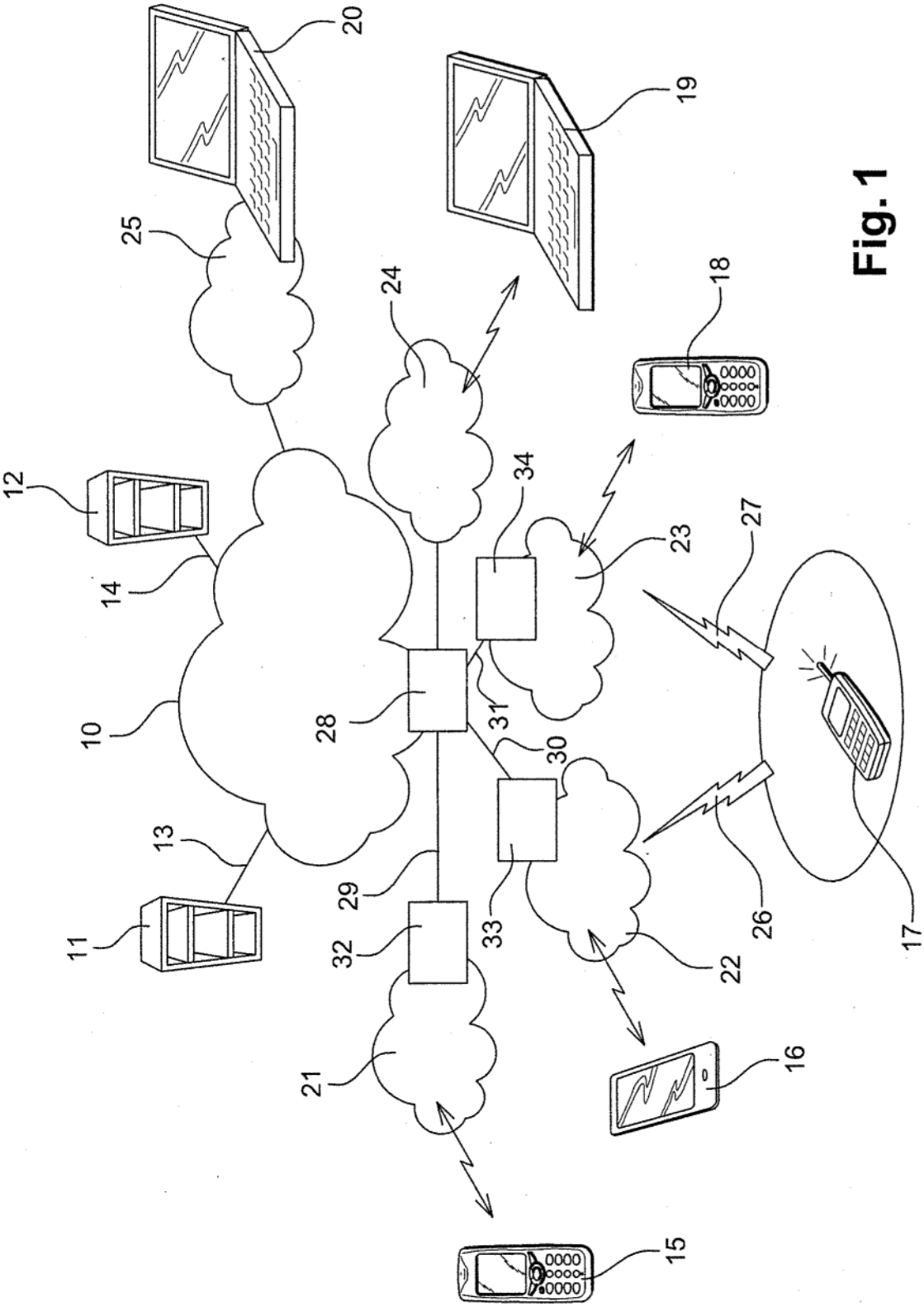
20
19
25
24
18
12
34
23
27
14
10
28
31
30
13
29
33
26
11
32
22
21
16
15
17

Fig. 1

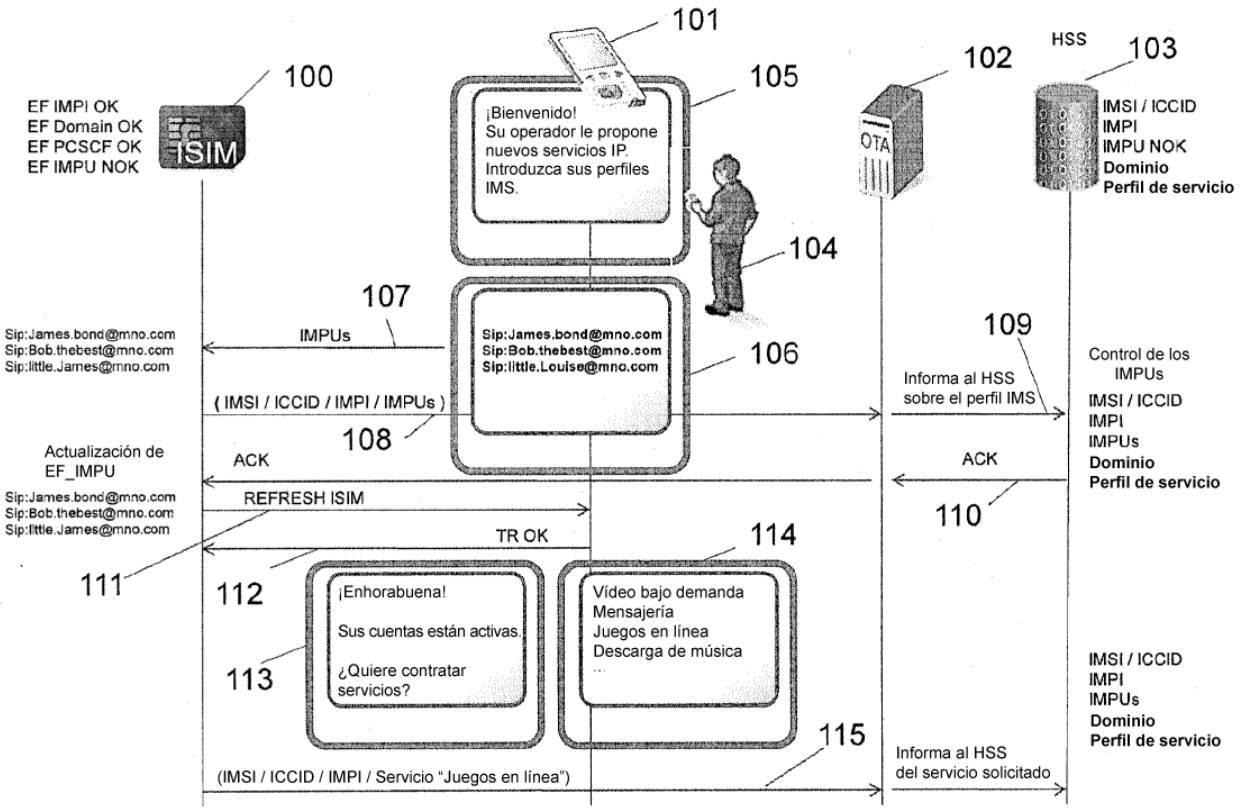
101
100
EF IMPI OK
EF Domain OK
EF PCSCF OK
EF IMPU NOK
ISIM
105
¡Bienvenido!
Su operador le propone nuevos servicios IP.
Introduzca sus perfiles IMS.
102
OTA
HSS
103
IMSI / ICCID
IMPI
IMPU NOK
Dominio
Perfil de servicio
104
107
Sip:James.bond@mno.com
Sip:Bob.thebest@mno.com
Sip:little.James@mno.com
IMPUs
Sip:James.bond@mno.com
Sip:Bob.thebest@mno.com
Sip:little.Louise@mno.com
106
109
Control de los IMPUs
IMSI / ICCID
IMPI
IMPUs
Dominio
Perfil de servicio
Informa al HSS sobre el perfil IMS
(IMSI / ICCID / IMPI / IMPUs)
108
Actualización de EF_IMPU
ACK
ACK
110
Sip:James.bond@mno.com
Sip:Bob.thebest@mno.com
Sip:little.James@mno.com
REFRESH ISIM
TR OK
111
112
114
¡Enhorabuena!
Sus cuentas están activas.
¿Quiere contratar servicios?
113
Vídeo bajo demanda
Mensajería
Juegos en línea
Descarga de música
...
IMSI / ICCID
IMPI
IMPUs
Dominio
Perfil de servicio
115
(IMSI / ICCID / IMPI / Servicio "Juegos en línea")
Informa al HSS del servicio solicitado

FIG.2