(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 709 663**

(51) Int. CI.:

H04W 4/14 (2009.01)
H04W 60/00 (2009.01)
H04W 4/60 (2008.01)
H04W 88/06 (2009.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.11.2015 PCT/FR2015/053046**

(87) Fecha y número de publicación internacional: **19.05.2016 WO16075407**

(96) Fecha de presentación y número de la solicitud europea: **10.11.2015 E 15804891 (8)**

(97) Fecha y número de publicación de la concesión europea: **31.10.2018 EP 3219157**

(54) Título: **Tarjeta EUICC que memoriza números cortos por perfil de abonado para notificar un servidor de gestión de suscripción**

(30) Prioridad:

14.11.2014 FR 1461031

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.04.2019

(73) Titular/es:

IDEMIA FRANCE (100.0%)
420, rue d'Estienne d'Orves
92700 Colombes, FR

(72) Inventor/es:

LARIGNON, GUILLAUME y
DUMOULIN, JÉRÔME

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Tarjeta EUICC que memoriza números cortos por perfil de abonado para notificar un servidor de gestión de suscripción

Campo de la invencion

La invención se refiere en general a las comunicaciones en una red de telefonía móvil y, en particular, las notificaciones de estado de tarjetas de seguridad, o cualquier otro elemento de seguridad, a una unidad de enrutamiento seguro de un servidor distante de gestión de suscripción, conocida bajo el acrónico SM-SR.

La presente invención se refiere más particularmente a un elemento de seguridad, por ejemplo, una tarjeta eUICC, a un sistema de infraestructura de red de telefonía móvil y a un método de comunicación en una red de telefonía móvil.

Estos diversos elementos pueden, en particular, realizar un servicio de mensajes cortos, tipo SMS (en inglés Short Message Service), para transmitir las notificaciones de estado de los elementos de seguridad de abonado.

Contexto de la invencion

Una tarjeta de circuito integrado universal convencional (UICC), tal como una tarjeta SIM, es un elemento de seguridad móvil definido en la norma ETSI TS 102 221 [102 221]. Está personalizada por un operador de telefonía antes de ser utilizada por un abonado. Las tarjetas eUICC (en inglés "embedded UICC"), o más en general los elementos de seguridad integrados eSE (en inglés "Embedded Secure Element"), están integradas en los terminales de telefonía móvil y pueden contener varias personalizaciones, denominadas perfiles, posiblemente para diferentes operadores.

Los propietarios de eUICC o eSE pueden gestionar a distancia las tarjetas eUICC o eSE de sus abonados a través de una unidad de enrutamiento seguro de un servidor de gestión de suscripción ("Subscription Manager-Secure Routing", también conocido con el acrónimo SM-SR, y posteriormente denominado servidor SM-SR) proporcionado en la infraestructura de la red móvil. Esta gestión a distancia permite, por ejemplo, cargar datos en la tarjeta o del elemento, o asegurar el cambio de la red móvil y, por lo tanto, del operador de telefonía móvil.

El documento EP 2 680 628 describe, por ejemplo, un método para cargar a distancia nuevos perfiles en una eUICC.

Según la norma GSMA 12FAST.15 en curso de establecimiento, esta gestión a distancia requiere que la eUICC o el eSE envíe notificaciones al servidor SM-SR. Estas notificaciones se pueden enviar por SMS (en inglés "Short Message Service"), por HTTPs (en inglés "HyperText Transfer Protocol Secure" más rápido) o posiblemente por CAT-TP (más rápido).

A título de ejemplo, estas notificaciones pueden confirmar que el terminal se ha conectado a la red móvil o indicar que, debido a una pérdida de cobertura, la eUICC o el eSE ha cambiado a otro perfil diferente al perfil actual, por ejemplo, a un perfil por defecto.

Según esta norma, un perfil de abonado en una eUICC o una eSE es la combinación de una estructura de ficheros, datos y aplicaciones que permiten a la eUICC o al eSE, cuando estos elementos están presentes, acceder a una infraestructura de red móvil particular, incluida la de un operador de telefonía móvil. Por lo tanto, un perfil de abonado es específico para un operador de telefonía móvil en la medida en que autoriza el acceso únicamente a la infraestructura particular correspondiente. A título de ejemplo, el perfil puede incluir información sobre las entidades de la infraestructura objeto de contacto, claves de conexión, etc. Por ejemplo, una eUICC o un eSE pueden tener dos perfiles asociados con dos operadores móviles diferentes, lo que permite el acceso a diferentes infraestructuras. Estos perfiles son gestionados por el campo raíz de seguridad emisor (ISD-R, en inglés "Issuer Security Domain - Root" de conformidad con la norma GlobalPlatform) de la tarjeta, controlada por el operador móvil (emisor, en inglés Issuer).

Para enviar una notificación como se mencionó anteriormente, la eUICC o eSE deben, en particular, recuperar los datos de estado recogidos en el perfil actual, los parámetros de conexión, así como una dirección destinataria de la notificación, es decir, la dirección del servidor SM-SR que recoge estas informaciones. En el caso de una notificación por SMS, la dirección del servidor SM-SR es un número de teléfono internacional único, es decir, constituido por un código de país que permite un acceso mundial al servidor SM-SR (del tipo +44 para el Reino Unido) y un número de teléfono en ese país.

Según siempre la misma norma, la dirección del servidor SM-SR se memoriza en la eUICC o en la eSE por el propietario del servidor SM-SR utilizando una orden particular emitida por el servidor SM-SR para las tarjetas eUICC o los elementos eSEs de los abonados. Esta orden, a saber, "UpdateSMSRAdressingParameters" y definida en la sección 4.1.1.10 de la versión actual de la norma, se envía al ISD-R de la eUICC o del eSE permitiendo la actualización de dicha dirección del servidor SM-SR.

Según la norma en su versión actual, el servidor SM-SR debería tener una dirección (número de teléfono internacional único) para todos los perfiles y, por lo tanto, accesible desde todos los operadores móviles.

Sin embargo, esta situación de la norma no es satisfactoria.

Por un lado, es relativamente difícil utilizar un único número de teléfono internacional para todos los operadores de todos los países. De hecho, en algunos casos, las redes filtran los SMS binarios procedentes de los terminales (SMS MO). Una solución en este caso es conectar el SM-SR al servidor de servicio de mensajes cortos (SMS-C) de cada operador. Sin embargo, el acceso al SM-SR ya no se realiza con el uso de un número de teléfono único.

Por otro lado, surge una dificultad cuando se cambia el servidor SM-SR y, por lo tanto, se asigna una nueva dirección. La actualización de la eUICCs o del eSEs es, por lo tanto, una carga de trabajo importante para el nuevo servidor SM-SR, habida cuenta del gran número de abonados afectados por este cambio.

Por último, la utilización de una tal dirección de tipo de número de teléfono internacional único no permite efectuar fácilmente procesamientos de las notificaciones en función de los operadores. Además, no garantiza una confidencialidad de las notificaciones de servicio que un operador puede activar en las eUICC o en los eSEs de sus abonados, porque todos los operadores pueden manipular los mensajes destinados a una dirección universal.

En este contexto, la presente invención pretende resolver la totalidad o parte de estas desventajas.

Sumario de la invencion

La invención se define por las reivindicaciones. Un ejemplo proporciona en particular un elemento de seguridad, por ejemplo, una tarjeta segura, para la conexión a una red de telefonía móvil, que comprende, en la memoria local, al menos un identificador de dirección, por ejemplo, un número corto (en inglés "short code"), específico para un operador de telefonía móvil, estando dicho identificador de dirección asociado con un perfil de abonado en el operador dentro del elemento de seguridad y, el elemento de seguridad está configurado para recuperar, desde la memoria local, un identificador de dirección, por ejemplo un número corto, una dirección IP o también una dirección URL asociada con un perfil de abonado en curso de utilización y para enviar, usando dicho identificador recuperado, una notificación de estado del elemento seguro a un servidor distante de gestión de suscripción (SM-SR) en una infraestructura de telefonía móvil.

De forma correlativa, un ejemplo proporciona un método de comunicación en una red de telefonía móvil utilizando un elemento de seguridad, por ejemplo, una tarjeta segura, para la conexión a la red de telefonía móvil, comprendiendo el elemento de seguridad, en la memoria local, al menos un identificador de dirección, por ejemplo, un número corto, específico para un operador de telefonía móvil y asociado con un perfil de abonado al operador, comprendiendo el método, al recibir un evento de activación de notificación, las siguientes etapas:

recuperar, desde la memoria local, un identificador de dirección, por ejemplo, un número corto, asociado con un perfil de abonado en curso de utilización, y

enviar, usando el identificador recuperado, una notificación de estado de elemento de seguridad a un servidor distante de gestión de suscripción (SM-SR) en una infraestructura de telefonía móvil.

Un ejemplo también proporciona un sistema de infraestructura de red de red de telefonía móvil que comprende un servidor de gestión de suscripción (SM) (que incluye una unidad de enrutamiento seguro (SR)) y que comprende una pluralidad de terminales de abonados, cada uno equipado con un elemento de seguridad, por ejemplo, una tarjeta segura, de conexión como se definió anteriormente para enviar notificaciones al servidor de gestión de suscripción utilizando un identificador de dirección, por ejemplo, un número corto, específico para un operador de telefonía móvil.

Los inventores tuvieron la idea de usar identificadores de dirección, por ejemplo, los números cortos (o en inglés "short codes"), para superar las restricciones de actualizar una nueva dirección del servidor SM-SR y la posibilidad de identificar las notificaciones según los operadores a los que están suscritos los abonados, con el fin de permitir procesamientos específicos de estas notificaciones.

Gracias a dichos identificadores o números cortos, cada operador puede gestionar (por ejemplo, identificar, filtrar, tratar, etc.) fácilmente las notificaciones emitidas por sus propios abonados porque recibe estas notificaciones en equipos (por ejemplo, SMS-C), que le son propios (gracias al identificador o al número corto).

Otras características del elemento de seguridad, del sistema y del método según las formas de realización se describen en las reivindicaciones dependientes, usando esencialmente una terminología del dispositivo, que por lo tanto es transferible al método. Además, estas características se describen principalmente en relación con una tarjeta segura y uno o más números cortos. Por supuesto, estas características son igualmente aplicables a otros

tipos de elementos de seguridad y a otros identificadores de dirección. De hecho, el identificador de dirección puede incluir un número corto único para un operador de telefonía móvil (MNO) o una dirección IP específica para el operador o una URL específica para el operador.

En una forma de realización, la tarjeta segura comprende al menos dos números cortos, cada uno asociado con un perfil de abonado distinto, permitiendo cada número corto enviar una notificación al servidor de gestión de suscripción (SM-SR) cuando el perfil de abonado asociado está en curso de utilización. Por lo tanto, cada operador móvil (a través de sus perfiles de abonado) dispone de su propio número corto de acceso al servidor SM-SR.

En particular, los dos números cortos pueden designar (es decir, definir o identificar la dirección) del mismo servidor SM-SR accesible por dos o más perfiles de abonado, cada uno según una ruta de notificación diferente que corresponde a un servidor particular de servicio de mensajes cortos (a través de un primer SMS-C o un segundo SMS-C).

En una forma de realización particular, la tarjeta segura incluye, en la memoria local, una tabla de correspondencias que permite la asociación entre cada número corto y cada perfil de abonado. Esta tabla de correspondencias o, posiblemente, la tabla de enrutamiento, facilita, por un lado, la recuperación de los números cortos al minimizar la consulta de los perfiles y su modificación (para incluir dicho número) y, por otro lado, la actualización de los números cortos que designan el servidor SM-SR evitando modificar directamente los perfiles de abonado.

Según una característica particular, la tabla de correspondencias memoriza cada número corto en asociación con un identificador de número corto o "índice", cuyo índice se memoriza en un perfil de abonado correspondiente.

En una variante, la tabla de correspondencias memoriza cada número corto en asociación con un identificador de perfil de abonado. Esta variante minimiza las modificaciones que se aportarán a los perfiles tales como se define en la norma actual.

En una alternativa a la tabla de correspondencias, cada número corto se memoriza en el perfil de abonado asociado. Esta disposición reduce la ocupación de la memoria de la tarjeta segura.

En otra forma de realización, la tarjeta segura comprende, además, un único número de teléfono internacional del servidor distante de gestión de suscripción (SM-SR), estando configurada dicha tarjeta segura para recuperar, desde la memoria local, dicho número de teléfono internacional único cuando no hay un número corto asociado con un perfil de abonado en curso de utilización y para enviar, utilizando dicho número de teléfono internacional único recuperado, una notificación de estado de la tarjeta al servidor distante de gestión de suscripción (SM-SR). Esta disposición define la cohabitación del número de teléfono internacional único utilizado convencionalmente con los números cortos proporcionados según la invención. Por lo tanto, garantiza que el funcionamiento clásico de notificación del servidor SM-SR se utilice al menos cuando no hay un número corto disponible para el perfil de abonado en curso de utilización, especialmente cuando el operador móvil asociado no está definido.

En otra forma de realización, la tarjeta segura está configurada para:

recibir, desde el servidor distante de gestión de suscripción (SM-SR), una orden de actualización, en la memoria local de la tarjeta segura, de una dirección del servidor distante, incluyendo dicha orden de actualización un número de teléfono internacional único del servidor distante y/o al menos un número corto asociado con un perfil de abonado y que designe al servidor distante, y

actualizar (es decir, memorizar si no está ya memorizada ninguna información), en la memoria local de la tarjeta segura y en respuesta a la orden de actualización, el número de teléfono internacional único del servidor distante y/o el al menos un número corto en asociación con un perfil de abonado tal como se indica en la orden de actualización, para notificar al servidor de gestión de suscripción con la utilización de los números actualizados.

Conviene señalar que los números cortos son generalmente únicos en el interior de la red móvil de un mismo operador (MNO), a veces dentro de un mismo país, pero rara vez en todo el mundo. Estos números cortos válidos en varios países están especialmente disponibles a precios prohibitivos. En consecuencia, el mismo servidor SM-SR del que dependen varios operadores móviles está asociado, según la invención, a una pluralidad de números cortos, cada uno correspondiente a un operador móvil diferente. Ahora bien, la norma GSMA 12FAST.15 anterior no responde a tal situación, porque la dirección del servidor SM-SR debe ser única.

En este contexto, se proporciona, de conformidad con una forma de realización particular, que la orden de actualización sea similar a la orden "UpdateSMSRAdressingParameters" definida en la sección 4.1.1.10 de la norma GSMA 12FAST.15, aumentada en al menos un doble campo que asocia un número corto con un identificador de perfil de abonado. En particular, el doble campo puede ser reiterado una pluralidad de veces en la orden con el fin de definir una pluralidad de números cortos para una pluralidad correspondiente de perfiles de abonado.

En una forma de realización, el sistema de infraestructura comprende, además, un servidor de servicio de mensajes

cortos (SMS-C) adecuados para un operador de telefonía móvil, comprendiendo, en la memoria local el servidor de servicios de mensajes cortos a una tabla de correspondencias entre un número corto que es único para dicho operador de telefonía móvil y una dirección IP del servidor distante de gestión de suscripción (SM-SR). El servidor SMS-C se utiliza cuando las notificaciones de estado se envían por la tarjeta segura bajo la forma de mensajes SMS. La tabla de correspondencias proporcionada en este servidor, permite, entonces, al operador enrutar eficazmente estos mensajes hacia el servidor de SM-SR. De hecho, por lo general los servidores SMS-C y SM-SR se comunican a través de rutas IP, a diferencia de los equipos anteriores del servidor SMS-C.

En una forma de realización particular, el sistema de infraestructura comprende una pluralidad de servidores de servicios de mensajes cortos (SMS-C) asociados a una pluralidad de respectivos operadores de telefonía móvil, comprendiendo los servidores de servicio de mensajes cortos cada uno, en la memoria local, una tabla de correspondencias entre un número corto que es único para el operador asociado y el mismo servido distante de gestión de suscripción (SM-SR). De este modo, los operadores de telefonía móvil pueden compartir los costes de un mismo servidor de SM-SR, teniendo todos ellos una gran libertad de procesamiento de las notificaciones de estado emitidas por sus abonados. En hecho, mediante el uso de números cortos, los mensajes transmitidos son recibidos por un servidor SMS-C propio para el operador móvil correspondiente. Este último puede entonces realizar fácilmente cualquier procesamiento adecuado de los mensajes recibidos.

En una forma de realización, el servidor distante de gestión de suscripción (SM-SR) está configurado para enviar una orden de actualización para el control de una dirección del servidor distante, incluyendo la orden de actualización un número de teléfono internacional único del servidor distante y/o al menos un número corto asociado con un perfil de abonado y que designa el servidor distante, de modo que se actualice, en la memoria de las tarjetas seguras, el número de teléfono internacional único del servidor distante y/o al menos un número corto en asociación con un perfil de abonado, tal como se indica en la orden de actualización. La orden de actualización puede ser según se definió con anterioridad, en particular a partir de la orden "UpdateSMSRAdressingParameters" que se define en la sección 4.1.1.10 de la norma GSMA 12FAST.15.

Las ventajas, objetos y características particulares de este dispositivo, de este programa de ordenador y de este soporte de información, son similares a las del método objeto de la presente invención, y por ello no se repiten aquí de nuevo.

Breve descripción de las figuras

Otras ventajas, objetos y características particulares de la presente invención se derivan de la descripción dada a continuación, con un objeto explicativo y no limitativo en absoluto, con respecto a los dibujos adjuntos, en los que:

la Figura 1 ilustra, esquemáticamente, un ejemplo de red de telefonía móvil en donde pueden realizarse formas de realización de la presente invención;

la Figura 2 ilustra un ejemplo de arquitectura de hardware para el componente o el equipo del sistema 1 descrito con referencia a la Figura 1; y

la Figura 3 ilustra una puesta en práctica de la invención para la configuración de la tarjeta de abonado eUICC y comunicación de notificaciones desde estas tarjetas hacia el servidor de SM-SR de la Figura 1.

Descripción detallada de la invención

La Figura 1 ilustra, esquemáticamente, un ejemplo de red de telefonía móvil en donde se pueden poner en práctica formas de realización de la presente invención. En esta representación esquemática, sólo se muestra un terminal móvil ME que incluye una tarjeta segura eUICC. Por supuesto, una red de telefonía móvil incluye, en general, una pluralidad de dichos terminales móviles provistos de tarjetas eUICC (o SIM, USIM). La presente descripción se refiere a las tarjetas eUICC a título de ejemplo. De una forma general, la presente invención puede ponerse en práctica en cualquier tipo de elemento de seguridad (en inglés Secure Element según la norma anteriormente descrita), por ejemplo, elementos de seguridad integrados, o eSE.

El sistema 1 representado comprende, por lo tanto, un terminal móvil ME convencional, es decir, que dispone de medios de comunicación en la red móvil y que integra una tarjeta segura de abonado del tipo eUICC. La presente invención pone en práctica operaciones particulares en la tarjeta segura eUICC.

El sistema 1 también comprende una red móvil 10 que comprende, de forma convencional, estaciones base BS para conectar los terminales móviles ME, una pluralidad de entidades (tipo pasarela GMSC, servidores HLR, MSC, VLR, etc. no ilustrados) que incluye a servidores de servicio de mensajes cortos SMS-C1 y SMS-C2 y un servidor de gestión de suscripción SM provisto de una unidad de enrutamiento seguro SR y una unidad de preparación de datos DP.

Ambos servidores SMS-C1 y SMS-C2 son gestionados por dos operadores de telefonía móvil diferentes,

respectivamente MNO1 y MNO2. Por supuesto, la presente invención se aplica cuando el sistema 1 comprende un número mayor de servidores de servicio de mensajes cortos, gestionados por dos o más operadores.

De manera similar, el servidor SM-SR, en este ejemplo, se comparte entre los dos operadores MNO1 y MNO2 con el fin de reducir los costes de instalación, de desarrollo, de funcionamiento y de mantenimiento. Por supuesto, se pueden proporcionar otros servidores SM-SR, que se comparten entre varios operadores de MNO.

Tal como se muestra en la figura y según se da a conocer por la norma GlobalPlatform, la tarjeta segura eUICC comprende, en la memoria, un campo de seguridad del transmisor (en este caso, un operador MNO) que gestiona una pluralidad de perfiles de abonado 21, 22, una tabla de correspondencias 23 y una dirección universal 24 del servidor SM-SR, que incluye un número de teléfono internacional único de este servidor.

Los perfiles de abonado pueden ser diferentes perfiles de operador (por ejemplo, MNO1 y MNO2) que dan acceso a sus infraestructuras correspondientes, o perfiles que dan acceso a diferentes infraestructuras de un mismo operador MNO (por ejemplo, la infraestructura 3G y la infraestructura 4G). De manera conocida, solo un perfil está activo a la vez, es decir, en curso de utilización. La selección de un perfil o el cambio de un perfil a otro, puede activarse automáticamente, de forma controlada por los operadores de MNO utilizando mensajes de servicio, o también, de forma manual por el usuario (cambiando, por ejemplo, de operador o de tecnología, 3G o 4G).

Además de la información memorizada convencionalmente en un perfil (consultar la norma GSMA 12FAST.15), cada perfil 21, 22 memoriza la dirección de un servidor SMS-C correspondiente (en el ejemplo, los dos perfiles memorizan las direcciones @ 1 y @ 2 respectivamente de SMS-C1 y SMS-C2) y memoriza un índice, SC1 para el perfil 21 y SC2 para el perfil 22.

La tabla de correspondencias 23 asocia, en cuanto a ella misma, cada índice aquí utilizado para un identificador de dirección. Este identificador de dirección puede comprender o estar constituido por un número corto efectivo único para un operador de telefonía móvil. De manera conocida, un número corto es un número de teléfono especial de un tamaño sustancialmente más pequeño que los números de teléfono tradicionales. Normalmente, un número corto incluye entre 4 y 8 dígitos.

En el ejemplo, el índice SC1 está asociado con el número corto 568, mientras que el índice SC2 está asociado con el número corto 345. De forma alternativa, el identificador de dirección puede estar constituido por una dirección IP específica del operador, formada normalmente por 15 caracteres como máximo (por ejemplo, SC1 = 78.123.2.23). En otra variante, el identificador de la dirección puede consistir en una dirección URL específica para el operador, por ejemplo, con un máximo de 256 caracteres (por ejemplo, SC1 = www.smsr1.com).

Por lo tanto, la tabla de correspondencias 23 hace posible asociar cada identificador de dirección, por ejemplo, cada número corto, con un perfil de abonado.

En la siguiente descripción, se hace referencia principalmente a los números cortos para simplificar las explicaciones. Por supuesto, la invención se aplica a cualquier tipo de identificador de dirección formado con caracteres alfanuméricos, incluidos caracteres especiales. Así, dependiendo del caso, por ejemplo, se usa SC1 = 568 o SC1 = 78.123.2.23 o SC1 = www.smsr1.com.

En la forma de realización de la figura, la tarjeta eUICC memoriza varios números que identifican el servidor SM-SR y le permiten enviar notificaciones de estado de la tarjeta.

A este respecto, la tarjeta es capaz de recuperar, desde la memoria local, uno de los números cortos, el que está asociado al perfil de abonado en curso de utilización si este número corto existe. De no ser así, la tarjeta recupera de manera convencional la dirección universal 24 correspondiente al servidor SM-SR.

A continuación, utilizando dicho número corto o el número de teléfono internacional único recuperado, la tarjeta envía una notificación de estado de la tarjeta al servidor SM-SR.

Como se deducirá de los ejemplos descritos a continuación, esta notificación puede tomar la forma de un mensaje SMS transmitido al servidor SMS-C correspondiente al perfil activo (es decir, al servidor SMS-C indicado en dicho perfil activo).

Tal como se ilustra en la figura, cada servidor SMS-C comprende, en la memoria, una tabla de correspondencias (11, 12) entre un número corto (o cualquier identificador de dirección) que sea único para el operador asociado al servidor SMS-C considerado (MNO1 para SMS-C1 y MNO2 para SMS-C2) y el mismo servidor SM-SR, en particular una dirección IP (Protocolo de Internet) de este servidor SM-SR.

El servidor SMS-C que recibe un mensaje SMS de la tarjeta eUICC, cuyo mensaje comprende los datos de estado que deben transmitirse y el número corto que designa al servidor SM-SR, convierte así el mensaje recibido en un mensaje IP. El destino de la dirección del servidor SM-SR se asocia con el número corto recibido en la tabla 11 o 12.

Conviene señalar que en el caso en donde el identificador de la dirección sea una dirección IP, puede ser directamente la dirección IP del servidor SM-SR o ser una dirección IP cualquiera que esté asociada, en la tabla de correspondencias, con la dirección IP del servidor SM-SR.

El servidor SM-SR procesa, de forma convencional, los mensajes (notificaciones) así recibidos.

La Figura 2 ilustra un ejemplo de una arquitectura de hardware para los dispositivos constituyentes del sistema 1 descrito con referencia a la Figura 1.

En este ejemplo, el equipo, el elemento de seguridad, la tarjeta eUICC, el terminal ME, el servidor SMS-C o SM-SR, comprenden un bus de comunicación al que están conectados:

- una unidad de procesamiento, o microprocesador, denominada CPU (acrónimo de Central Processing Unit en terminología inglesa);

- una o más memorias no volátiles, por ejemplo, memoria ROM (acrónimo de Read Only Memory en terminología inglesa) que puede constituir un soporte en sentido de la idea inventiva, es decir, que puede incluir un programa informático que comprende instrucciones para la puesta en práctica de un método según una forma de realización de la invención; esta memoria no volátil también puede ser una memoria EEPROM (acrónimo de Electrically Erasable Read Only Memory) o también una memoria instantánea (Flash);

- una memoria de acceso aleatorio o memoria caché o memoria volátil, por ejemplo RAM (acrónimo de Random Access Memory en terminología inglesa) que comprende registros adaptados para la grabación de las variables y parámetros creados y modificados durante la ejecución del programa mencionado anteriormente; durante la puesta en práctica de la invención, los códigos de instrucciones del programa almacenado en memoria de solamente lectura ROM se cargan en memoria RAM con el fin de ponerse en práctica por la unidad de procesamiento de la CPU;

- una interfaz de comunicación adaptada para transmitir y recibir datos, por ejemplo, a través de una red de telecomunicaciones o una interfaz de lectura/escritura de un elemento de seguridad;

- una interfaz de entrada/salida I/O (por ser Input/Output en terminología inglesa), por ejemplo, una pantalla, un teclado, un ratón u otro dispositivo de señalización, tal como una pantalla táctil o un mando a distancia; esta interfaz de I/O permite al usuario interactuar con el sistema durante la puesta en práctica del método a través de una interfaz gráfica.

El bus de comunicación permite la comunicación y la interoperabilidad entre los diversos elementos incluidos en el equipo o conectados al mismo. La representación del bus no es limitativa y, en particular, la unidad de procesamiento es susceptible de comunicar instrucciones a cualquier elemento del equipo directamente o por intermedio de otro elemento de este equipo.

La Figura 3 ilustra una puesta en práctica de la invención para la configuración de las tarjetas eUICC de abonado y la comunicación de notificaciones desde estas tarjetas hacia el servidor SM-SR. Las entidades eUICC están representadas en la parte derecha de la figura, dentro de un cuadro discontinuo rematado por las letras "eUICC". Los elementos enumerados en la parte izquierda de la figura se refieren a los elementos de la red móvil 10.

La primera fase de configuración o actualización de las tarjetas eUICC, o más en general de cualquier elemento de seguridad según la invención, se ilustra en la parte superior de la figura (por encima del trazo grueso). Permite memorizar los números cortos, o más en general los identificadores de dirección, en las tarjetas eUICC en asociación con los perfiles de abonados.

En las etapas 300 y 302, un operador móvil MNO añade información relacionada con los números cortos SC a las unidades DP (preparación de datos) y SR (enrutamiento seguro) del servidor de gestión de suscripción SM.

En la etapa 300, envía una orden Add (SC, tipo de perfil) a la unidad DP del servidor SM (es decir, SM-DP) para asociar el número corto SC, o más en general, el identificador de dirección SC, a los perfiles identificados por el "tipo de perfil". A modo de ejemplo, el nuevo número corto SC está asociado a los perfiles pertinentes con la tecnología 4G. La unidad SM-DP se encarga de crear y mantener los diferentes perfiles creados por los operadores que comparten el servidor SM.

En la etapa 302, envía (etapa 306) una orden Add (SC, SMS-C) a la unidad SR del servidor SM (es decir, SM-SR) que mantiene actualizada toda la información de direccionamiento y enrutamiento en la red. Por lo tanto, la unidad SM-SR puede difundir (sincronización entre los servidores en la etapa 304) el nuevo número corto SC al servidor SMS-C apropiado, con el fin de que este último lo asocie con la dirección IP del servidor SM (o de la unidad SM-SR emisora del mensaje que permite esta difusión).

De este modo, todos los nuevos números cortos creados por un operador de MNO son conocidos por el servidor SM y se transmiten a los diversos servidores de la red 10.

A continuación, con el fin de difundir los nuevos números cortos a las tarjetas de abonado eUICC, la unidad SM-SR envía una orden para actualizar una dirección de la unidad de enrutamiento seguro, en este caso de un nuevo número corto.

La orden de actualización incluye un número de teléfono internacional único de la unidad de enrutamiento seguro en el caso clásico de la orden "UpdateSMSRAdressingParameters" definido en la sección 4.1.1.10 de la norma GSMA 12FAST.15 (ver el campo "SMS parameter Value" en el siguiente ejemplo).

La orden también puede incluir (ocasionalmente, la sección relativa con el número de teléfono internacional único puede estar vacía si este número permanece sin cambios) al menos un número corto asociado con un perfil de abonado y que designa la unidad de enrutamiento seguro.

Esta orden se puede realizar a partir de la orden denominada "UpdateSMSRAdressingParameters" mencionada anteriormente, en donde al menos un doble campo que asocia un número corto, o más en general un identificador de dirección SC, se agrega a un identificador de perfil de abonado. Por supuesto, el doble campo se repite tantas veces como sea necesario para definir el conjunto de las asociaciones (número corto - identificador de perfil) que es necesario transmitir a las tarjetas eUICC.

En una forma de realización, la orden denominada "UpdateSMSRAdressingParameters" definida en la sección 4.1.1.10 de la norma GSMA 12FAST.15 se modifica como sigue (los campos en negrita subrayados se añaden con respecto a la norma):

Código	Valor	Significado	Presencia
DGI	'DF6D'	DGI propietaria para la tarjeta	Obligatoria
Length	xx	Longitud de los datos que siguen	Obligatoria
Command	10	Orden de actualización de los parámetros de dirección SM-SR	Obligatoria
SMS Parameter Tag	'A3	Etiqueta de los parámetros SMS	Condicional
SMS Parameter Length	X	Longitud de los parámetros SMS	Condicional
SMS parameter Value	xx...xx	Dirección de destino del SM-SR	Condicional
CAT-TP Parameter Tag	'A4'	Etiqueta del parámetro CAT_TP	Condicional
CAT-TP Parameter Length	Y	Longitud de los parámetros CAT_TP	Condicional
CAT-TP Parameter Value	xx...xx	Valor de los parámetros de enlace CAT_TP	Condicional
SC Parameter Tag	'E3'	Etiqueta del parámetro SC	Condicional
SC Parameter Length	X +Y +4	Longitud de los parámetros SC	Condicional
SC Value Tag	91	Etiqueta del SC	Condicional
SC Value Length	X	Longitud del SC	Condicional
SC Value value	xx ..xx	Valor del SC	Condicional
Profile ID Tag	"01"	Etiqueta del perfil	Condicional
Profile ID Length	Y	Longitud del identificador de perfil	Condicional
Profile ID Length	xx ..xx	Valor del identificador de perfil	Condicional

Orden "UpdateSMSRAdressingParameters" modificada según una forma de realización de la invención

Los campos "SC Value Length" y "SC Value value" permiten gestionar los números cortos que son de magnitud variable de un país a otro, o más en general los identificadores de dirección cuyo número de caracteres puede fluctuar.

Al recibir dicha orden, cada tarjeta eUICC puede así actualizarse (es decir, memorizar si alguna información no está ya memorizada), en su memoria local y en respuesta a la orden de actualización, el número de teléfono internacional único de la unidad de enrutamiento seguro y/o al menos un número corto en asociación con un perfil de abonado tal como se indica en la orden de actualización. De esta manera, la tarjeta eUICC puede notificar a la unidad de enrutamiento seguro del servidor de gestión de suscripción utilizando los números actualizados.

Esta actualización efectiva se ilustra en la figura por las etapas 308 y 310.

En la etapa 308, el campo raíz de seguridad del emisor (ISD-R) de la tarjeta recibe y ejecuta la orden de actualización. De hecho, solo este campo ISD-R es conocido por el servidor SM, tal como puerto de entrada en la tarjeta eUICC. Por lo tanto, la unidad SM-SR envía la orden de actualización al ISD-R.

Aún en la etapa 308, en respuesta a la ejecución de esta orden, el ISD-R envía una orden para actualizar la tabla de correspondencias 23 con uno o varios nuevos números cortos indicados en la orden, por ejemplo, con la ayuda de la orden STORE en donde los números cortos se transmiten en parámetros (con un identificador de perfil o un índice SC).

A modo de ejemplo, puede tratarse de almacenar el número corto '345', al que la tabla de correspondencias asocia al índice SC2 (primer índice disponible, por ejemplo).

En la etapa 310, en donde la tabla de correspondencias 23 asocie un índice de SC con cada nuevo número corto, el ISD-R vincula los nuevos números cortos a los perfiles del abonado tal como se especifica en la orden recibida, en particular a los perfiles ya existentes. A modo de ejemplo, el ISD-R puede modificar cada perfil de abonado implicado para memorizar el índice SC asociado con el número corto correspondiente (tal como se memoriza en la tabla 23), usando una orden Link SC. En nuestro ejemplo, el perfil 2 (22 en la Figura 1) se modifica para memorizar el índice SC2.

Conviene señalar que, si un número corto ya hubiera sido proporcionado para un perfil dado, la orden que indica un número corto nuevo para el mismo perfil conduce a la eliminación y sustitución del número corto anterior, a favor del nuevo.

Asimismo, conviene señalar que en una variante de la invención que no utiliza una tabla de correspondencias 23, cada número corto, o más en general cada identificador de dirección, se memoriza en el perfil de abonado asociado. A este respecto, el ISD-R genera una orden que modifica directamente el perfil, por ejemplo, STORE SC en el perfil (etapa 312).

Una vez que esté configurada la tarjeta eUICC, el ISD-R envía un acuse de recibo al SM-SR (etapa 314) que a su vez informa al operador del MNO (etapa 316).

Posteriormente, la tarjeta eUICC, o más en general el elemento de seguridad, desea enviar una notificación al servidor SM-SR. Esto se describe a continuación en la etapa 350, en una forma de realización de la invención. En este momento, la tarjeta eUICC está conectada a una red de telefonía móvil utilizando uno de los perfiles disponibles en la tarjeta (este perfil está activo, es decir, en curso de utilización, y se indica como "Enabled" en los registros del ISD-R). A modo de ejemplo, el perfil activo es el perfil 2 (22 en la Figura 1).

Se pueden producir varios eventos de activación con el fin de activar la etapa 350.

Esto se refiere principalmente a eventos internos de la tarjeta eUICC, tal como una conexión a una red móvil, un cambio de localización (por ejemplo, cambio de célula de radio), una primera activación de la tarjeta de abonado, un error (por ejemplo, imposible una conexión a la red) lo que lleva a cambiar hacia un perfil predeterminado o "de repli".

Por supuesto, se pueden tener en cuenta los eventos relacionados con las herramientas del SIM Toolkit, por ejemplo, los eventos que se originan cuando el usuario interactúa con las interfaces del SIM Toolkit (menús).

Como variante, tal evento podría ser la recepción de una orden en particular desde el servidor SM-SR.

Tras la detección de dicho evento iniciador, el ISD-R emite una orden para recuperar una dirección del servidor SM-SR. Esta es la etapa 350 durante la cual el ISD-R emite, por ejemplo, la orden GET para recuperar, en el perfil activo, el índice de un número corto, o más en general de un identificador de dirección, asociado al perfil de abonado activo, si existe un tal número (caso **a** de la figura). De esta manera, se prefiere el uso del número corto en lugar del número de teléfono internacional único 24.

En respuesta a esta orden, el índice SC se recupera durante la etapa 352. En el ejemplo considerado, el índice 'SC2' se recupera porque el perfil 2 está activo.

Durante estas etapas 350 y 352, el ISD-R también recupera la dirección del servidor SMS-C asociado al perfil activo, la dirección @ 2 del SMS-C2, en nuestro ejemplo.

El ISD-R recupera, entonces, el número corto asociado con este índice en la tabla de correspondencias 23: orden GET SC durante la etapa 354 y respuesta a la etapa 356. En el ejemplo de la Figura 1, el índice 'SC2' recupera el

número corto '345'.

Conviene señalar que cuando la tabla de correspondencias 23 asocia directamente el número corto del SM-SR con un identificador de perfil de abonado, las etapas 350 a 356 pueden consistir en recuperar la dirección del servidor de SMS-C al nivel del perfil activo, y en recuperar un número corto asociado con el identificador de perfil activo (conocido del ISD-R) solamente a nivel de la tabla de correspondencias 23.

Teniendo conocimiento del número corto (si existe uno), el ISD-R prepara y envía un mensaje de notificación de estado de la tarjeta a la etapa 358.

Este mensaje adopta, por ejemplo, la forma de un mensaje SMS al destino del servidor SMS-C (cuya dirección @ 1 o @ 2 se recuperó en la etapa 352), cuyo mensaje comprende:

- los datos de estado de la tarjeta eUICC; y
- la dirección del servidor SM-SR, es decir, el número corto recuperado '345', en particular indicado en el campo TP-DA (Destination Address) de la notificación por SMS.

A modo de ejemplo, la norma GSMA mencionada anteriormente define diferentes tipos de notificaciones:

- valor ‘01' en caso de primera conexión a la red;
- valor '02' en caso si el perfil ha cambiado con éxito;
- el valor '03' en caso de que no se cambie el perfil y el retorno hacia atrás (Rollback);
- el valor '04' en el caso de un error de cambio de perfil y conmutación por error en un perfil de reserva;
- valor '05' en caso de cambio de perfil después de la recuperación local a un perfil de reserva.

Este mensaje de notificación es recibido por el servidor SMS-C (SMS-C2 en el ejemplo) que (1) determina en su tabla local 11/12 la dirección IP del servidor SM-SR correspondiente al número corto indicado en el SMS recibido (por ejemplo, la dirección IP 78.123.2.23 asociada con '345' en esta tabla), y (2) retransmite los datos de estado (notificación) al servidor SM-SR bajo la forma del mensaje IP a la dirección IP obtenida 78.123.2.23. Se trata de la etapa 360.

Las etapas 362 a 366 ilustran la situación en la que no se asocia ningún número corto al perfil de abonado activo (caso **b** de la figura). En este caso, en respuesta a la orden 350, solo el número de teléfono internacional único 24 se devuelve al ISD-R. Este número se especifica en el mensaje SMS transmitido en la etapa 364 (similar a la etapa 358) que permite al servidor SMS-C determinar la dirección IP del servidor SM-SR para retransmitir los datos de estado (notificación) bajo la forma del paquete IP (etapa 366).

Los ejemplos anteriores son solamente formas de realización de la invención que no se limitan por ello y se definen por las reivindicaciones.

REIVINDICACIONES

1. Un elemento de seguridad de conexión a una red telefonía móvil (10), que comprende, en la memoria local, dos números cortos que designan el mismo servidor distante de gestión de suscripción en una infraestructura de telefonía móvil para dos operadores de telefonía móvil respectivos, siendo cada número corto propio de uno de los operadores de telefonía móvil y que está asociado a un perfil diferente de abonado (21, 22) al operador dentro del elemento de seguridad, y dicho elemento de seguridad está configurado para recuperar, a partir de la memoria local, el número corto asociado al perfil del abonado en curso de utilización y para enviar un mensaje SMS a dicho número corto recuperado, incluyendo dicho mensaje SMS una notificación de estado de elemento de seguridad, lo que permite la transmisión de dicha notificación de estado al servidor distante de gestión de suscripción a través de un servidor de servicio de mensajes cortos SMS-C específico para el operador de telefonía móvil asociado al número corto recuperado.

2. Un elemento de seguridad según la reivindicación 1, que comprende, en la memoria local, una tabla de correspondencias (23) que permite la asociación entre cada número corto y cada perfil de abonado.

3. Un elemento de seguridad según la reivindicación 2, en donde la tabla de correspondencias (23) memoriza cada número corto en asociación con un identificador de perfil de abonado.

4. Un elemento de seguridad según la reivindicación 1, en donde cada número corto se memoriza en el perfil de abonado asociado.

5. Un elemento de seguridad según una cualquiera de las reivindicaciones 1 a 4, que comprende, además, un número de teléfono internacional único (24) del servidor distante de gestión de suscripción, cuyo elemento de seguridad está configurado para recuperar, desde la memoria local, dicho número de teléfono internacional único cuando no hay un número corto asociado con un perfil de abonado en curso de utilización y para enviar, utilizando dicho número de teléfono internacional único recuperado, una notificación de estado del elemento de seguridad al servidor distante de gestión de suscripción.

6. Un elemento de seguridad según una cualquiera de las reivindicaciones 1 a 5, configurado para:

recibir, desde el servidor distante de gestión de suscripción, una orden de actualización, en la memoria local del elemento de seguridad, de una dirección del servidor distante, incluyendo la orden de actualización un número de teléfono internacional único (24) de la unidad de enrutamiento seguro y/o al menos un número corto asociado con un perfil de abonado (21, 22) y que designa el servidor distante, y

actualizar, en la memoria local del elemento de seguridad y en respuesta a la orden de actualización, el número de teléfono internacional único del servidor distante y/o el al menos un número corto en asociación con un perfil de abonado tal como se indica en la orden de actualización, con el fin de notificar al servidor de gestión de suscripción con el uso de los números actualizados.

7. Un método de comunicación en una red de telefonía móvil (10) ejecutado por un elemento de seguridad de conexión a la red de telefonía móvil, que comprende, en memoria local, dos números cortos que designan el mismo servidor distante de gestión de suscripción en una infraestructura de telefonía móvil para dos operadores de telefonía móvil respectivos, cada número corto es exclusivo de uno de los operadores de telefonía móvil y está asociado con un perfil de abonado diferente (21, 22) para el operador, comprendiendo el método la recepción de un evento de activación de notificación, las etapas siguientes:

recuperar (350, 352), desde la memoria local el número corto asociado al perfil de abonado en curso de utilización, y

enviar (358) un mensaje SMS a dicho número corto recuperado, incluyendo dicho mensaje SMS una notificación de estado del elemento de seguridad, permitiendo así la transmisión de dicha notificación de estado al servidor distante de gestión de suscripción a través de un servidor de servicios de mensajes cortos SMS-C específico para el operador de telefonía móvil asociado al número corto recuperado.

8. El método según la reivindicación 7, en donde el elemento de seguridad

recibe (306), desde el servidor distante de gestión de suscripción, una orden de actualización, de una dirección del servidor distante, la orden de actualización que incluye un número de teléfono internacional único (24) del servidor distante y/o al menos un número corto asociado a un perfil de abonado (21, 22) y que designa el servidor distante, y

la actualización (308, 310, 312), en su memoria local en respuesta a la orden de actualización, del número de teléfono internacional único del servidor distante y/o del al menos un número corto en asociación con un perfil de abonado del servidor distante tal como se indica en la orden de actualización, para notificar al servidor de gestión de suscripción utilizando los números actualizados.

9. Un sistema de infraestructura de red de telefonía móvil que comprende un servidor de gestión de suscripciones y que incluye una pluralidad de terminales de abonado, cada uno equipado con un elemento de seguridad de conexión según una cualquiera de las reivindicaciones 1 a 6 para enviar notificaciones al servidor de gestión de suscripción utilizando un número corto, siendo el número corto específico para un operador de telefonía móvil.

10. Un sistema según la reivindicación 9, en donde el servidor distante de gestión de suscripción está configurado para enviar una orden para actualizar una dirección del servidor distante, incluyendo dicha orden de actualización un número de teléfono internacional único del servidor distante y/o al menos un número corto asociado con un perfil de abonado y que designa al servidor distante, para actualizar, en la memoria de los elementos de seguridad, el número de teléfono internacional único del servidor distante y/o el al menos un número corto en asociación con un perfil de abonado tal como se indica en la orden de actualización.

11. Un sistema según la reivindicación 9 o 10, que comprende, además, dos servidores de servicio de mensajes cortos SMS-C específicos para los dos operadores de telefonía móvil, respectivamente, comprendiendo cada servidor de servicios de mensajes cortos, en la memoria local, una tabla de correspondencias (11, 12) entre un número corto específico para dicho operador de telefonía móvil y una dirección IP del mismo servidor distante de gestión de suscripción.

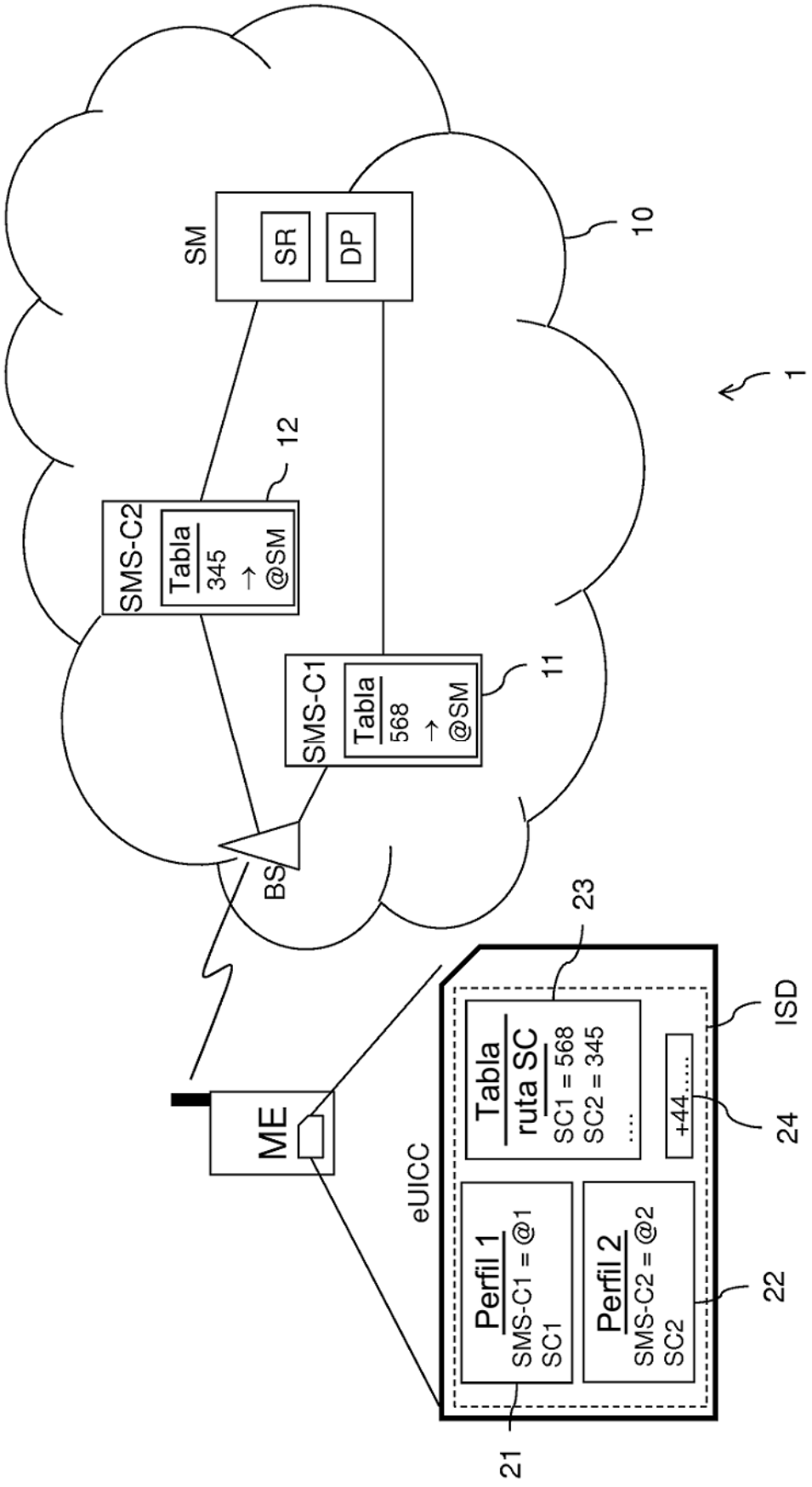
SM
SR
DP
10
1
12
SMS-C2
Tabla
345 → @SM
SMS-C1
Tabla
568 → @SM
11
BS
23
ME
eUICC
Tabla
ruta SC
SC1 = 568
SC2 = 345
....
+44.....
ISD
24
Perfil 1
SMS-C1 = @1
SC1
Perfil 2
SMS-C2 = @2
SC2
22
21

Fig. 1

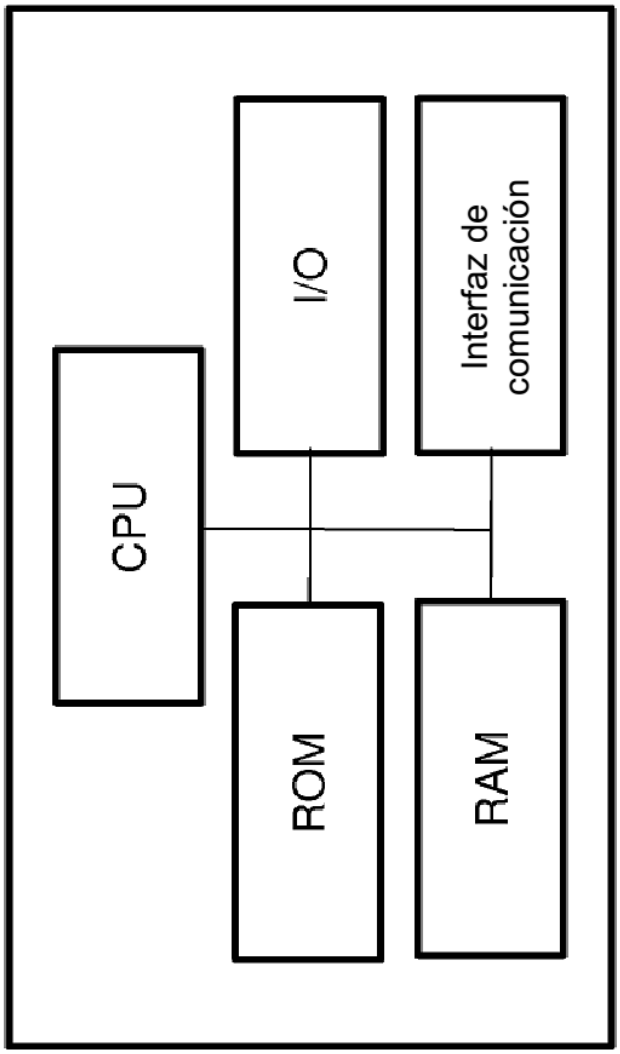

Fig. 2

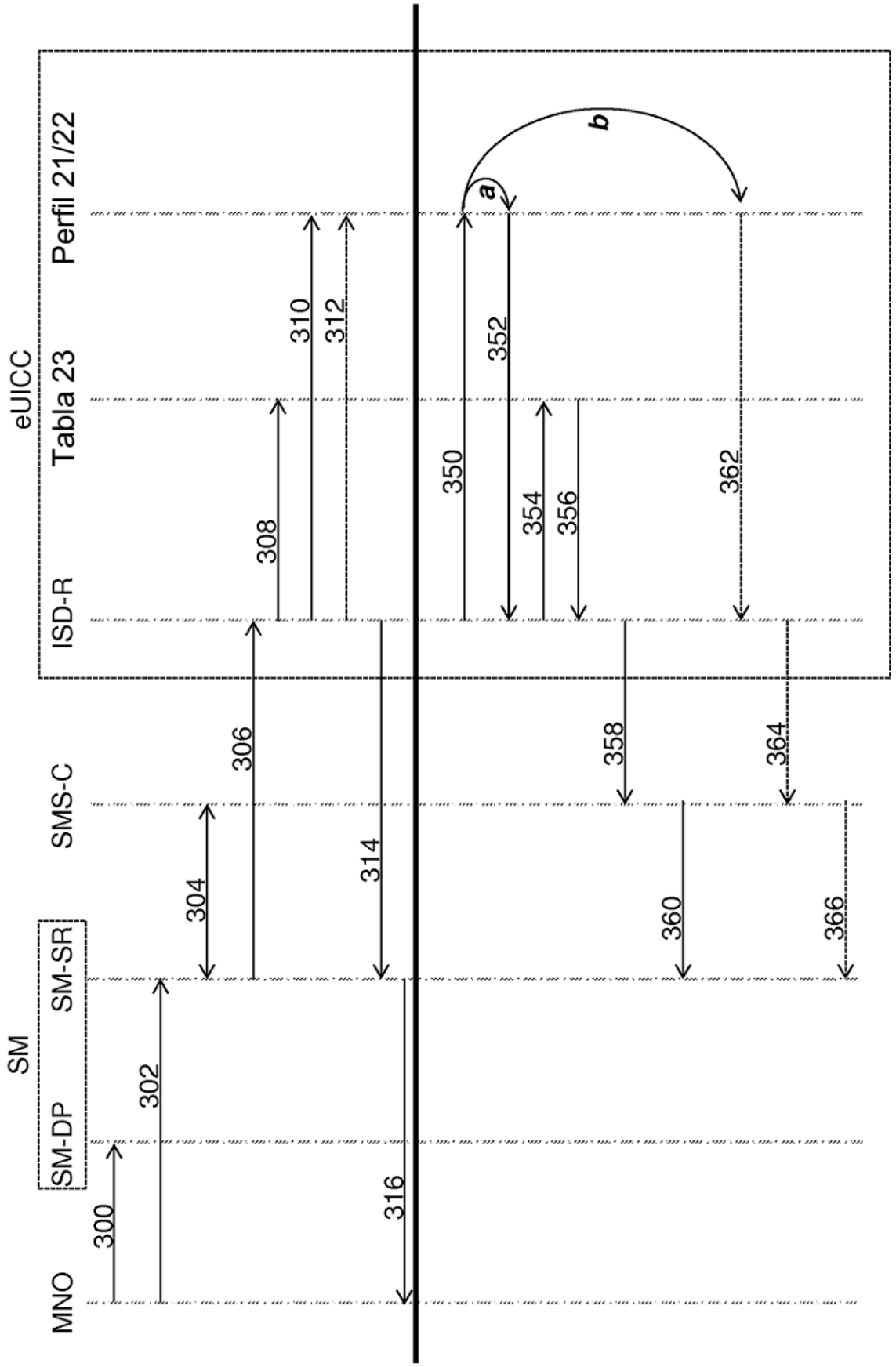
MNO
SM
SM-DP
SM-SR
SMS-C
eUICC
ISD-R
Tabla 23
Perfil 21/22
a
b
300
302
304
306
308
310
312
314
316
350
352
354
356
358
360
362
364
366

Fig. 3