(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 283 028**

(51) Int. Cl.:
H04Q 7/20 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **97946773 .5**
(86) Fecha de presentación : **02.12.1997**
(87) Número de publicación de la solicitud: **0890272**
(87) Fecha de publicación de la solicitud: **13.01.1999**

(54) Título: **Utilización de una estación móvil como teléfono inalámbrico.**

(30) Prioridad: **05.12.1996 FI 964876**

(45) Fecha de publicación de la mención BOPI:
16.10.2007

(45) Fecha de la publicación del folleto de la patente:
16.10.2007

(73) Titular/es: **Nokia Corporation**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Hokkanen, Petri**

(74) Agente: **Arpe Fernández, Manuel**

DESCRIPCIÓN

Utilización de una estación móvil como teléfono inalámbrico.

Campo de la invención

Esta invención se refiere a un sistema celular que comprende estaciones base y estaciones móviles con un interfaz entre ellas que es un interfaz radioeléctrico.

Antecedentes de la invención

En una red alámbrica fija el abonado que llama conoce las bases para el cargo de la llamada incluso al marcar el número del abonado B, ya que dicho cargo dependerá de sí la llamada es una llamada local, una llamada de larga distancia, una llamada a un móvil o una llamada a un país extranjero. El equipo terminal utilizado por el abonado A también afecta al cargo, ya que las llamadas originadas en móviles son más caras que las llamadas originadas en una red fija, independientemente del equipo terminal objetivo. Esto puede ser visto como el precio que el abonado tiene que pagar por su gran libertad de movimientos.

Al usuario normal doméstico se le han ofrecido teléfonos inalámbricos que proporcionan una movilidad limitada. La instalación comprende una estación base en el final de la línea de abonado que convierte la señal de audio procedente de la red fija en una señal radioeléctrica y la transmite además al teléfono inalámbrico. Hasta ahora, la modulación más usual utilizada es la modulación FM. La mayor desventaja de este tipo de modulación es que el tráfico en el trayecto radioeléctrico es escuchado ilegalmente por cualquier receptor de FM sintonizado a una frecuencia adecuada. Una mejora esencial de ello es utilizar modulación digital y transferencia de voz cifrada a través del trayecto radioeléctrico. Un sistema digital adecuado y ya estandarizado es el sistema DECT (Telecomunicaciones Digitales Inalámbricas Europeas), y son un hecho ya disponible los teléfonos inalámbricos que cumplen con la especificación de este sistema y destinados a usuarios domésticos - ver también WO-A-9524106.

Una gran desventaja del teléfono inalámbrico es la limitación de la movilidad permitida a un radio de 50 a 100 m de la estación base, pero siendo ventajoso los precios menores de la red fija comparados, por ejemplo, con la red móvil. Otra gran desventaja es la baja seguridad especialmente cuando se usa el sistema analógico tradicional.

Las bases para el cargo de la llamada, utilizadas en una red fija pueden no ser utilizados como tales en las redes móviles permitiendo una gran movilidad debido a la estructura de la red y a la manera de operar. En lo que sigue, se explicará la estructura y el funcionamiento de la red móvil utilizando como ejemplo la conocida red móvil GSM mostrada en la figura 1. La comunicación entre la MS (Estación Móvil) en una célula y la red tiene lugar por medios radioeléctricos a través de la estación base BTS (Estación Base Transmisora/Receptora). Las estaciones base BTS están conectadas al BSC (Controlador de Estación Base), por ejemplo, con funciones de intercambio de canal y de gestión del canal radioeléctrico como tareas. Varios controladores de estaciones base se encuentran conectados a un MSC (Centro Móvil de Conmutación) que realiza las principales funciones de conmutación de la red móvil y que conecta la red móvil con otros centros móviles de conmutación y con redes externas.

La red móvil también comprende varias bases de datos, tales como un HLR (Registro de Posiciones Base), en el que se almacena permanentemente la información de abonado. El número MSISDN del abonado, la IMSI (Identidad del Abonado Móvil Internacional) utilizados en la red y la información de servicio de abonado se almacenan en el registro de posiciones base así como la información de direccionamiento al VLR (Registro de Posiciones de Visitantes). El AuC (Centro de Autentificación) también se localiza en relación con el registro de posiciones base. La información de abonado recibida del HLR se almacena en el VLR durante el tiempo que le lleva al visitante permanecer en el área VLR.

Cuando se lleva a cabo la actualización de posiciones por primera vez, la red verificará sí el usuario tiene derecho a acceder a dicha red. El propósito de las funciones de seguridad del sistema GSM es prevenir el acceso no autorizado a la red, previniendo de ese modo que cualquiera utilice la red con la cuenta de alguien más y proteger la privacidad del usuario. El acceso no autorizado se previene mediante la autentificación, siendo identificado el usuario para estar seguro de que el abonado tiene derecho a utilizar la red. De hecho, el MS está formado de dos partes: el ME (Equipo Móvil) y la tarjeta SIM (Módulo de Identificación de Abonado), de modo que una estación móvil operativa MS se constituye sólo cuando la tarjeta SIM se introduce en el equipo móvil ME. Esta identificación con introducción por el usuario de su tarjeta SIM en su estación móvil MS, está destinada a prevenir la utilización no autorizada, por ejemplo, de equipo robado y asegurarse de que sólo utilizan la red aquellos abonados que pagan sus facturas. Desde el punto de vista del operador, la identificación es especialmente importante, en particular, en relación con la itinerancia internacional, ya que la red no conoce la información de abonado del visitante y es, de ese modo, desconocedor de cualquier insolvencia.

En primer lugar, durante la identificación se utiliza el identificador de usuario o código PIN (Número Personal de Identificación) dado por el propio usuario y almacenado en la tarjeta SIM. En el primer estadio, cuando se conecta la energía eléctrica del teléfono, el teléfono pedirá al usuario que introduzca un código de 4 a 8 dígitos y comparará el código introducido con un código almacenado en la memoria. Si el código es incorrecto después de tres intentos, la tarjeta se bloqueará y no podrá desbloquearse sin medidas especiales. Esta identificación se hace completamente de

forma local mediante la tarjeta SIM, de modo que el código PIN no se transmite por medios radioeléctricos y, de ese modo, el código no puede ser capturado.

En segundo lugar, después de haber introducido el código PIN correcto, la estación móvil transmitirá su número IMSI a la red o, si es posible, un TMSI (Identidad del Abonado Móvil Temporal), con el cual tendrá lugar la autentificación entre la red y la tarjeta, la cual se explicará mediante referencia a las figuras 1 y 2.

El principio es tal que la red hará una pregunta a la estación móvil de la que sólo la tarjeta SIM correcta conocerá la respuesta. En la parte fija de la red, la identificación se realiza mediante el AuC (Centro de Autentificación) localizado en conexión con el registro de posiciones base HLR mientras la tarjeta SIM realiza la identificación en el equipo terminal. La identificación se basa en el algoritmo de identificación A3 y en la clave de identificación basada en el abonado K_i. La IMSI (Identidad del Abonado Móvil Internacional), la clave de abonado específica K_i y el algoritmo de identificación A3 mencionados anteriormente se almacenan tanto en la red como en la tarjeta SIM.

A continuación nos referiremos a las figuras 1 y 2. En la parte inicial de la identificación, el centro de autentificación AuC enviará una pregunta a la estación móvil que es un número aleatorio RAND que tiene una longitud de 128 bits. De ese modo, su valor se encuentra en un rango de 2^{128}-1, por lo que existe una pequeñísima posibilidad de que el mismo número aleatorio pueda utilizarse dos veces. Este estadio se representa en la figura 1 mediante un uno rodeado por un círculo y en la figura 2 mediante una flecha que pasa a través del interfaz radioeléctrico. La estación móvil recibe el RAND, lo transfiere a la tarjeta SIM, que ejecuta el algoritmo A3 con su ayuda y con la ayuda de la clave de abonado específica K_i localizada en la tarjeta. La respuesta resultante es una SRES (Respuesta Firmada) de 32 bits que la estación móvil envía a la red. El centro de autentificación AuC la recibe, el dos rodeado por un círculo en la figura 1, y compara el valor de SRES con el valor que el mismo ha calculado utilizando el mismo algoritmo A3 al igual que el RAND y la clave K_i. Si las SRES son las mismas, la identificación se acepta, de otro modo, no se permitirá al abonado el acceso a la red (el estadio si/no de la figura 2).

La figura 3 ilustra cómo la estación móvil también utiliza los valores de K_i y RAND recibidos para el algoritmo A8, el cual produce una clave de cifrado de conexión específica Kc, que además se utiliza como clave para un tercer algoritmo A5, que se utiliza para cifrar voz y datos en los canales de tráfico radioeléctrico. En la red, el AuC realiza el mismo algoritmo con los mismos valores y, de ese modo, obtiene como resultado la misma clave de cifrado. Ambos almacenan la clave en la memoria.

Puesto que la información de identificación se calcula siempre en la red base, los operadores pueden utilizar diferentes algoritmos A3 y A8, no conociendo que algoritmos utilizan los otros. Por otro lado, el algoritmo de cifrado vocal A5 debe ser el mismo en todas las redes.

De ese modo, de toda la información contenida en la tarjeta SIM, la IMSI, la K_i y los algoritmos A3 y A8 son importantes para la identificación. Los algoritmos A3 y A8 se ejecutan en la tarjeta SIM de modo que la clave K_i nunca tiene que ser transmitida entre la tarjeta y el propio equipo móvil ME.

Como se mencionó anteriormente, el cálculo de los datos de identificación siempre tiene lugar en el AuC de la red base del abonado. Siendo este el caso, cuando el abonado está en otra identificación de red cargaría de forma nada moderada la red de señal entre el VLR y el AuC. Para evitar esto, el AuC envía, generalmente, tripletas preparadas al registro de posiciones de visitantes VLR mientras el visitante se registra en este. La tripleta contiene el RAND, SRES Y Kc. De este modo, el registro de posiciones de visitantes verificará si la estación móvil ha calculado los valores correctos, de modo que la señalización al AuC pueda reducirse.

Debe indicarse de la presentación anterior que en términos de seguridad el sistema digital celular es muy avanzado en lo relativo al uso no autorizado y al cifrado vocal. Puesto que todas las células son del mismo valor para la red móvil, no pueden ofrecerse otras bases para el cálculo del precio de las llamadas que, por ejemplo, una flexibilidad basada en las horas del día y de la noche y más barato de lo normal los precios entre la estación móvil y el teléfono doméstico. No pueden ofrecerse motivos de cargo especiales para una llamada con origen o finalización en una determinada célula. Estos factores reducen el uso del teléfono móvil como teléfono doméstico.

En el ámbito de la disposición doméstica o en cualquier otro lugar deseado por el abonado, se ha sugerido una HBS especial (Estación Base Doméstica) que puede conectarse a una conexión de teléfono normal y que sea un dispositivo tan simple como sea posible que sirve sólo a uno a unos pocos usuarios registrados en la estación base, los cuales utilizan un teléfono normal en una red celular. Con relación a sus funciones la estación base doméstica, de ese modo, correspondería a las estaciones base actuales para teléfonos inalámbricos, esto es, realiza una conversión entre la red alámbrica y el interfaz radioeléctrico. Incluso si la estación base fuera de la naturaleza de una estación base “desnuda” en una red celular, sería necesario autentificar, de una forma u otra, un teléfono de red celular que desea acceso a la red a través de la estación base. El teléfono no siempre funciona de la misma manera en la autentificación y espera a recibir una solicitud de RAND desde la red. Se han propuesto, al menos, dos formas.

En primer lugar, podría disponerse una conexión de módem desde la estación base doméstica al centro de autentificación AuC de la red celular, por el cual los parámetros a intercambiar en la autentificación se transfieren a través de esta conexión y la propia autentificación tendría lugar de una forma normal como se muestra en la figura 2. Puesto que

la señalización pasaría a través de otra red diferente a la red del operador de red celular, debe llegarse a un acuerdo en el tema con el operador en cuestión.

En segundo lugar, podría situarse un lector de tarjetas en la estación base doméstica y podría utilizarse una tarjeta especial conteniendo los datos relativos a esta estación base y al usuario. De este modo, la autentificación se realizaría entre la tarjeta y la estación base, de modo que el usuario activaría la estación base con su tarjeta.

Las desventajas de estos procedimientos propuestos son la difícil señalización de módem a través de una red fija (por ejemplo, PSTN) y la adquisición de tarjetas extra y lectores así como la realización del software relacionado.

De ese modo, la presente invención persigue ofrecer un sistema de teléfono inalámbrico que está basado en una red celular y que no tiene las desventajas expuestas y en el que el equipo terminal estándar de la red celular puede utilizarse en casa como teléfono inalámbrico sin requerir etapas especiales al usuario, lo que permite, de ese modo, llamadas más baratas.

Los objetivos se consiguen con las características distintivas presentadas en las reivindicaciones independientes.

Breve resumen de la invención

La estación base doméstica propuesta, que está conectada a una conexión de teléfono común, contiene como una estación base para teléfonos inalámbricos conocidos, un dispositivo de carga en el que el teléfono puede cargarse. Además de las clavijas que suministran la corriente de carga, tiene clavijas de comunicación especiales a través de las cuales el teléfono y la estación base pueden intercambiar información de autentificación mientras el teléfono se encuentra en el cargador. El cambio de teléfono de red celular a teléfono inalámbrico comienza, de ese modo, situando el teléfono en el cargador.

Durante la autentificación toda la transferencia de información tiene lugar sólo entre la estación base y el teléfono mientras el centro de autentificación AuC de la red celular queda completamente al margen. De este modo, puesto que entre la estación base doméstica y el teléfono existe una conexión alámbrica, no importa que medios de autentificación de parte generarán la autentificación y los datos de cifrado en tanto éstos sean acordados por adelantado. Incluso los algoritmos no necesitan ser los que se usan en el sistema celular. Es suficiente acordar por adelantado que cuando una parte envía una determinada solicitud, la otra parte responderá con una determinada respuesta, con lo cual ambos utilizarán una clave de cifrado acordada en el tráfico radioeléctrico. La autentificación es invisible para el usuario.

De acuerdo con una realización ventajosa, los parámetros utilizados en la autentificación se generan mediante primeros medios situados en la estación móvil, transfiriéndose los parámetros a través de una conexión fija a segundos medios, que se sitúan en la estación base doméstica y la cual los almacenará. Esto hace más sencilla la estación base. Además, resulta ventajoso utilizar las mismas peticiones, respuestas, algoritmos y claves de cifrado que en el sistema celular con el cual cumple el teléfono en cuestión. De este modo, cualquier cambio a realizar en el software del teléfono será un cambio menor.

De acuerdo con otra realización, los parámetros utilizados para la autentificación se generan mediante segundos medios de la estación base y los parámetros se transfieren a través de una conexión fija a los primeros medios de la estación móvil, la cual los almacenará.

Resulta ventajoso que en el mismo instante de situar el teléfono en el cargador comience el desregistro del teléfono de la red celular. De este modo, cualquier transferencia de una llamada a un teléfono base funcionará normalmente, si la estación móvil no responde. Puede quedar en la memoria del teléfono información del tiempo de la red celular, por lo que podría ponerse en uso cuando el teléfono se mueve en la red celular. Tal puesta en uso podría tener lugar automáticamente, cuando el teléfono se mueve fuera del rango de la estación base doméstica.

Cuando la estación móvil se ha transformado en teléfono inalámbrico, la autentificación se realiza al comienzo de la formación de la llamada, utilizando parámetros que se han calculado por adelantado y almacenado en la memoria.

Relación de figuras

La invención se explicará en mayor detalle haciendo referencia a las figuras esquemáticas adjuntas, en las que:

Figura 1 muestra el principio de un sistema celular;

Figura 2 muestra la autentificación en un sistema celular conocido;

Figura 3 muestra la formación de una clave de cifrado en un sistema celular conocido;

Figura 4 muestra el principio de un sistema de acuerdo con la invención;

Figura 5 ilustra el registro en un sistema de acuerdo con la invención;

Figura 6 ilustra la autentificación en un sistema de acuerdo con la invención;

Figura 7 representa otra realización; y

Figura 8 muestra la autentificación en otra realización.

Descripción detallada de la invención

La figura 4 muestra elementos básicos del sistema. Una línea de abonado 1 llega a la casa del abonado, a la oficina o a cualquier otro lugar desde la centralita telefónica local de una red fija PSTN o ISDN 3. La línea de abonado 1 está conectada a una HBS (Estación Base Doméstica), la cual convertirá los datos y voz que llegan de la línea de abonado al formato del interfaz aéreo del sistema celular y lo enviará además a la comunicación radioeléctrica y, de forma correspondiente, convertirá los datos y voz que llegan en la forma del sistema celular desde la comunicación radioeléctrica en la forma utilizada en la red fija, en el caso de una red PSTN en una señal de audio y en el caso de una red ISDN en una señal PCM. La energía de transmisión es baja para minimizar la interferencia causada por las frecuencias utilizadas en la estación base doméstica, de modo que el radio de la célula es de la misma magnitud que con los teléfonos inalámbricos, unos pocos cientos de metros en espacio libre.

Por otro lado, los elementos básicos comprenden una estación móvil MS, que es un dispositivo de acuerdo con algún sistema digital celular. Se utiliza como ejemplo el conocido sistema GSM.

Al moverse dentro del área del sistema celular, la estación móvil está en conexión con la estación base que proporciona la mejor conexión en cada momento y realizará el tráfico en la red celular de forma normal. Cuando el usuario se mueve en la red celular desde el lugar A hacia su base en el lugar B, movimiento que se muestra mediante una flecha, la estación móvil MS permanece aún registrada con la red celular. Sólo cuando el usuario conecta su teléfono a una conexión alámbrica directamente a la estación base doméstica, flecha de A a C, tendrá lugar el desregistro del teléfono de la red celular. La estación de carga de batería del teléfono de la estación base doméstica, representada por un hueco en la estación base doméstica HBS, puede contener, además de las clavijas de corriente de carga, una o más clavijas de contacto, con las que cuando el teléfono se sitúa en la estación de carga dicha clavija de contacto se pondrá en contacto con una correspondiente clavija del teléfono, lo que iniciará el desregistro del teléfono de la red celular y el registro en la estación base doméstica.

De acuerdo con una primera realización, todo el cálculo relacionado con la autentificación se realiza en la estación móvil MS. Esta realización se explicará con referencia a la figura 5.

El registro en la estación base doméstica tiene lugar de modo que el equipo del abonado ME genera un número aleatorio RAND, el cual alimenta a la tarjeta SIM. La tarjeta SIM calcula un algoritmo X utilizando el número aleatorio y la clave K_i, obteniendo como resultado SRES. Utilizando los mismos valores pero con el algoritmo Y la tarjeta SIM realiza el algoritmo Y obteniendo como resultado una calve de cifrado de conexión específica Kc. Estos algoritmos pueden ser los mismos que los utilizados en el sistema celular, esto es, en el caso del sistema GSM los algoritmos A3 y A8, pero igualmente podría ser cualquier otro algoritmo. La tarjeta SIM también dará la IMSI (Identidad Internacional de Abonado Móvil) o la TMSI (Identidad Temporal de Abonado Móvil), que puede ser cualquier valor aceptado. En su características principales la función corresponde al lado izquierdo de las figuras 2 y 3, excepto que el ME, en lugar del centro de autentificación AuC, generará el número aleatorio RAND.

La tarjeta SIM enviará la respuesta SRES que ha generado, la clave Kc y el valor IMSI/TMSI al equipo del abonado ME, el cual los transmitirá a través de la conexión fija mediante las clavijas de contacto 51, las cuales conectan la estación móvil y la estación base doméstica HBS, a la estación base doméstica HBS, que almacenará los datos recibidos. Ahora tiene lugar el registro y la estación base doméstica conoce los parámetros de autentificación y de cifrado que se utilizan. La estación móvil MS se transforma en un teléfono inalámbrico, puede ser retirado de la estación base doméstica HBS y puede iniciar o recibir una llamada de la red fija. Su número de teléfono es el número dado por el operador de la red fija a esta conexión de abonado.

Cuando se inicia o recibe una llamada, la primera etapa a realizar es la autentificación, la cual se explica con referencia a la figura 6. Primero, la estación móvil MS envía a la estación base doméstica HBS por radio su identificador TMSI, que la estación base doméstica utiliza para buscar en su memoria tales valores recibidos con anterioridad desde la estación móvil que se relaciona con el identificador. Posteriormente la estación base doméstica autentificará a la estación móvil enviándola el número RAND que ha recuperado de la memoria. Con la recepción del RAND, la tarjeta SIM realizará el algoritmo X, obteniendo como resultado el valor SRES, el cual enviará la estación móvil MS a la estación base doméstica. El valor debe ser el mismo que se generó anteriormente en relación con el registro, de modo que la estación base doméstica realizará la validación comparando los valores recibidos SRES con el que tiene en su memoria. Si son idénticos, la llamada puede comenzar. Para cifrar la información que ha enviado a la estación móvil, la estación base utiliza la clave de cifrado Kc que tiene almacenada, y la estación móvil utiliza la misma clave, que también ha almacenado anteriormente, o puede recalcular la clave luego utilizando el algoritmo Y, como se muestra en la figura.

Debe indicarse que ambos, los valores RAND y SRES pueden ser enviados incluso varias veces por el interfaz radioeléctrico, por lo que una tercera parte puede capturarlos. Esto también es posible en el caso del sistema GSM. Sin

embargo, esto no es un problema, ya que la clave de cifrado no se transmite en ningún momento por radio, sino sólo a través de la conexión fija cuando la estación móvil se encuentra fijada en la estación base doméstica.

La figura 7 muestra otra realización, en la que la estación base doméstica es parte activa en la autentificación.

El registro en la estación base doméstica tiene lugar de modo que la estación móvil MS transmite su IMSI (Identidad del Abonado Móvil Internacional) o su TMSI (Identidad del Abonado Móvil Temporal) a la estación base doméstica HBS. En respuesta a esto, la estación base doméstica generará un número aleatorio RAND y calculará el algoritmo X utilizando el número aleatorio y la clave K_i, obteniendo como resultado la respuesta SRES. Utilizando los mismos valores iniciales pero con el algoritmo Y, también realiza el algoritmo Y obteniendo como resultado una clave de cifrado de conexión específica Kc. Estos algoritmos pueden ser los mismos que los utilizados en el sistema celular. Todos los valores se almacenan en la memoria.

De aquí en adelante, la estación base doméstica envía su petición RAND generada, su respuesta calculada SRES y la clave Kc al equipo del abonado ME a través de las clavijas de contacto 51, el cual almacenará la información que recibe. Ahora tiene lugar el registro y ahora la estación móvil conoce los parámetros de autentificación y cifrado a utilizar. La estación móvil se ha transformado en un teléfono inalámbrico, pudiendo ser retirado de la estación base doméstica HBS y puede originar o recibir una llamada de la red fija.

Cuando se inicia o recibe una llamada, lo primero que se realiza es la autentificación y esto se explica con relación a la figura 8. Primero, la estación móvil MS envía a la estación base doméstica HBS por radio su identificador TMSI, que la estación base doméstica utiliza para buscar en su memoria cualquiera de los valores que se refieran al identificador y que han sido recibidos con anterioridad desde la estación móvil. Posteriormente la estación base doméstica autentifica a la estación móvil enviándola el número RAND que ha buscado en la memoria. Habiendo recibido el RAND, la tarjeta SIM ejecutará el algoritmo X, obteniendo como resultado el valor SRES, el cual enviará la estación móvil MS a la estación base doméstica. El valor debe ser el mismo que se generó anteriormente en relación con el registro, de modo que la estación base doméstica realiza la validación comparando el valor SRES que ha recibido con el que tiene en su memoria. Si estos son iguales, la llamada puede comenzar. Para cifrar la información que ha enviado a la estación móvil, la estación base utiliza la clave de cifrado Kc que ha almacenado, y la estación móvil utiliza la misma clave, que también ha almacenado anteriormente, o puede recalcular la clave luego utilizando el algoritmo Y.

También es posible actuar de modo que la estación móvil autentifique a la estación base. De este modo, envía a la estación base amos IMSI y RAND, en respuesta a lo cual la estación base devuelve el número SRES. La estación móvil verifica para estar segura de que el número se corresponde con el valor SRES recalculado o ya almacenado.

Disponer las funciones de acuerdo con la invención en los teléfonos actuales de red celular requerirá adiciones de software menores y nuevos algoritmos, si se requieren, además de los existentes, tales como los algoritmos A3 y A8. Cualquier adición a realizar en la estación base doméstica será menor, si se ejecuta la primera realización. La gran ventaja es que cualquier teléfono de red celular registrado con la estación base doméstica funcionará como teléfono inalámbrico. En la práctica, el teléfono es un teléfono bi-modo, por lo que el mismo teléfono funcionará en la base como teléfono inalámbrico con tarifas de llamada más baratas y fuera de la base como teléfono de red celular normal. Si el registro con la estación base tiene lugar automáticamente, como se proponía anteriormente, y cuando el registro en la red celular tiene lugar automáticamente, utilizando parámetros almacenados anteriormente en la memoria del teléfono, el usuario cambia al modo necesario conectando sólo por un momento el teléfono a la estación base doméstica cuando vuelve a casa, a la oficina o a cualquier otro lugar semejante.

Cuando el teléfono se registra en la estación base doméstica, por supuesto, uno debe asegurarse de que su energía de transmisión caerá considerablemente por debajo de la energía de transmisión mínima determinada para la estación móvil en el sistema de red celular de modo que el alcance se reducirá a unos pocos cientos de metros en espacio abierto. Esto debe hacerse para que cuando opere como teléfono inalámbrico, la estación móvil no provoque interferencia en tales conexiones del sistema celular que utilizan la misma frecuencia.

Incluso podría ser posible programar el teléfono de modo que fuera capaz cuando se registra en la estación base doméstica de recibir llamadas de ambos, del lado de la red fija y desde el lado de la red celular, pero las llamadas salientes serían dirigidas a la red fija.

La disposición propuesta puede ejecutarse en la práctica en muchas formas diferentes manteniéndose dentro del propósito de las reivindicaciones. Los programas y algoritmos pueden elegirse libremente así como la parte que generará la información de cifrado y la autentificación. Preferentemente, el registro puede iniciarse introduciendo el teléfono en la estación de carga, pero, alternativamente, la estación base podría tener algún otro lugar en el que situar el teléfono mientras tiene lugar el registro. Podrían registrarse varios teléfonos con la estación base doméstica. Las llamadas dentro de la casa entre estos teléfonos podrían ejecutarse mediante el software adecuado de la estación base.

REIVINDICACIONES

1. Sistema telefónico comprendiendo equipo terminal y una estación base doméstica conectada con una línea de abonado a una centralita telefónica, con lo cual una parte de la conexión de abonado está constituida por un enlace radioeléctrico entre el equipo terminal y la estación base,

caracterizado porque

el equipo terminal es una estación móvil de un sistema telefónico celular móvil que también contiene primeros medios para ejecutar un procedimiento de autentificación entre el mismo y la estación base doméstica (HBS),

la estación base contiene segundos medios para ejecutar un procedimiento de autentificación entre ella misma y la estación móvil, adaptados para

generar e intercambiar parámetros de autentificación entre la estación móvil y la estación base doméstica para comenzar en el instante en que la estación móvil se coloca en la estación base doméstica, de modo que entre ambas se establece una conexión alámbrica, con lo cual después de la transmisión de los parámetros de autentificación, la estación móvil se convierte en un teléfono inalámbrico registrado en la estación base doméstica.

2. Sistema como el definido en la reivindicación 1,

caracterizado porque

los primeros medios comprenden un primer algoritmo (algoritmo X), una clave de identificación (K_i) y un generador de números aleatorios (RAND),

los segundos medios comprenden una memoria, adaptada para que

después de colocar la estación móvil en la estación base doméstica, dichos primeros medios generen un número aleatorio (RAND), en respuesta al cual el primer algoritmo (algoritmo X) produce una respuesta (SRES) utilizando la clave de identificación (K_i) y transmitiendo la estación móvil el número aleatorio (RAND), la respuesta (SRES) y su identificador (IMSI/TMSI) a la estación base doméstica (HBS) para ser almacenados en la memoria.

3. Sistema como el definido en la reivindicación 2,

caracterizado porque

los primeros medios comprenden un segundo algoritmo (algoritmo Y) y en respuesta al número aleatorio los primeros medios están adaptados para realizar un segundo algoritmo (algoritmo Y) utilizando el número aleatorio y la clave de identificación (K_i) y como resultado de un segundo algoritmo transmitir una clave de cifrado de conexión específica (Kc) a la estación base para que la almacene en la memoria.

4. Sistema como el definido en la reivindicación 1,

caracterizado porque

los primeros medios comprenden una memoria,

los segundos medios comprenden un primer algoritmo (algoritmo X), una clave de identificación (K_i) y un generador de números aleatorios (RAND), adaptados para que después de situar la estación móvil en la estación base doméstica, la estación móvil transmita su identificador (IMSI/TMSI) a la estación base doméstica, en respuesta a la cual los segundos medios generarán un número aleatorio (RAND), en respuesta al cual el primer algoritmo (algoritmo X) producirá una respuesta (SRES), utilizando la clave de identificación (K_i) y transmitiendo la estación base doméstica el número aleatorio (RAND) y la respuesta (SRES) a la estación móvil para almacenarla en la memoria.

5. Sistema como el definido en la reivindicación 4,

caracterizado porque

los segundos medios también comprenden un segundo algoritmo (algoritmo Y) y en respuesta al número aleatorio (RAND) los primeros medios están adaptados para ejecutar un segundo algoritmo (algoritmo Y) utilizando el número aleatorio y la clave de identificación (K_i) y como resultado del segundo algoritmo transmitir una clave de cifrado de conexión específica (Kc) a la estación móvil para almacenarla en la memoria.

6. Sistema como el definido en la reivindicación 2,

caracterizado porque cuando la estación móvil funciona como teléfono inalámbrico independientemente de la estación base doméstica, dicho sistema se encuentra adaptado para realizar autentificación en la formación de la llamada de modo que

a) la estación móvil envía su identificador (IMSI/TMSI) a la estación base doméstica,

b) en respuesta al identificador, la estación base doméstica busca en la memoria el número aleatorio almacenado (RAND) y lo envía a la estación móvil,

c) en respuesta al número aleatorio almacenado (RAND) la estación móvil busca en la memoria la respuesta almacenada (SRES) y la envía a la estación base doméstica,

d) la estación base doméstica compara la respuesta que recibe con la respuesta que ha almacenado en la memoria y acepta la estación móvil si las respuestas son idénticas.

7. Sistema como el definido en la reivindicación 4,

caracterizado porque cuando la estación móvil funciona como teléfono inalámbrico independientemente de la estación base doméstica, dicho sistema se encuentra adaptado para realizar autentificación en la formación de la llamada de modo que

a) la estación móvil envía su identificador (IMSI/TMSI) a la estación base doméstica,

b) en respuesta al identificador, la estación base doméstica busca en la memoria el número aleatorio almacenado (RAND) y lo envía a la estación móvil,

c) en respuesta al número aleatorio almacenado (RAND) la estación móvil realiza un primer algoritmo (algoritmo X) utilizando el número aleatorio y la clave de identificación (K_i) y envía la respuesta resultante (SRES) a la estación base doméstica (HBS),

d) la estación base doméstica compara la respuesta que recibe con la respuesta que ha almacenado en la memoria y acepta la estación móvil si las respuestas son idénticas.

8. Sistema como el definido en la reivindicación 6 o 7, **caracterizado** porque la estación móvil está adaptada para cifrar la información que envía utilizando la clave de cifrado de conexión específica (Kc) que ha almacenado en la memoria, y la estación base doméstica está adaptada para cifrar la información que envía utilizando la clave de cifrado de conexión específica (Kc) que tiene almacenada en la memoria.

9. Sistema como el definido en la reivindicación 1, **caracterizado** porque cuando la estación móvil está situada en la estación base doméstica, está adaptada para desregistrarse automáticamente de la red celular.

10. Sistema como el definido en la reivindicación 1, **caracterizado** porque cuando la estación móvil está situada en la estación base doméstica, está adaptada para desregistrarse automáticamente de la red celular pero mantiene en la memoria los parámetros de autentificación utilizados en la red celular, por lo que cuando la estación móvil se mueve más allá del alcance de la estación base doméstica intentará acceder automáticamente a la red celular utilizando estos parámetros.

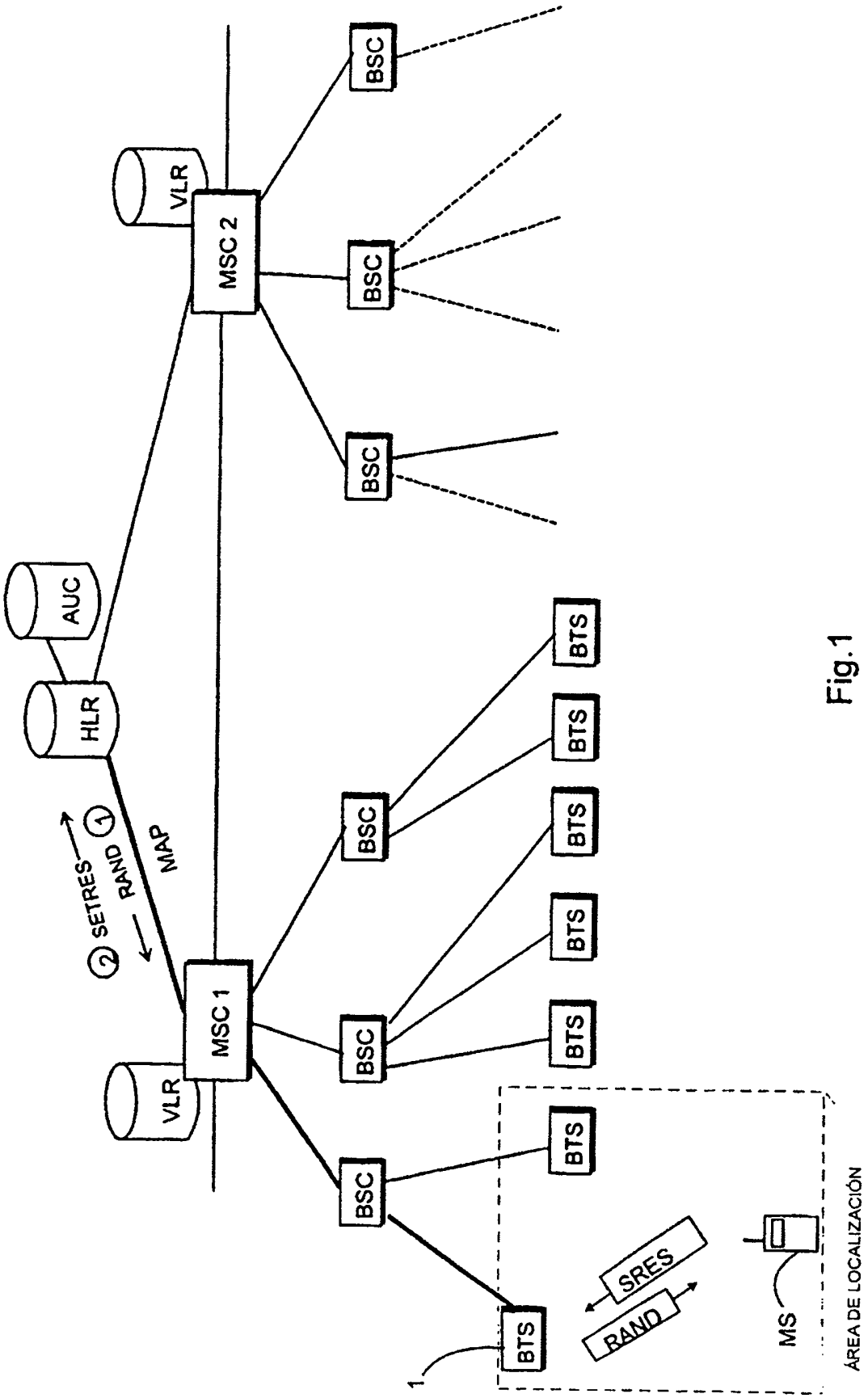
BSC
VLR
MSC 2
BSC
BSC
AUC
HLR
MAP
SETRES
RAND
BTS
BTS
BSC
BTS
BTS
MSC 1
BSC
BTS
VLR
BSC
BTS
BTS
SRES
RAND
MS
1
ÁREA DE LOCALIZACIÓN

Fig.1

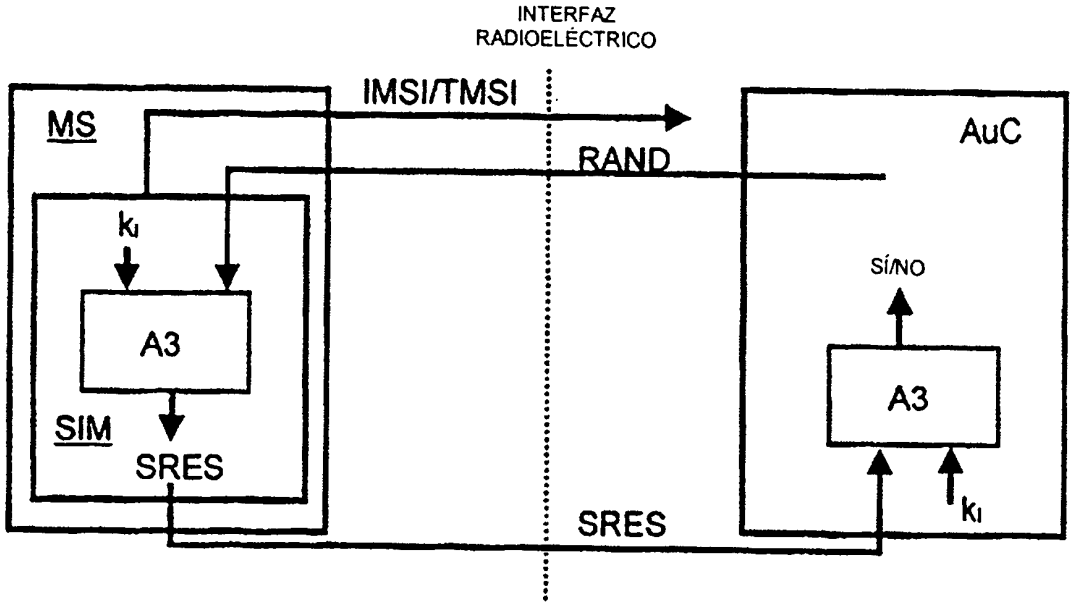
INTERFAZ
RADIOELÉCTRICO
IMSI/TMSI
MS
AuC
RAND
kI
SÍ/NO
A3
A3
SIM
SRES
kI
SRES

Fig. 2

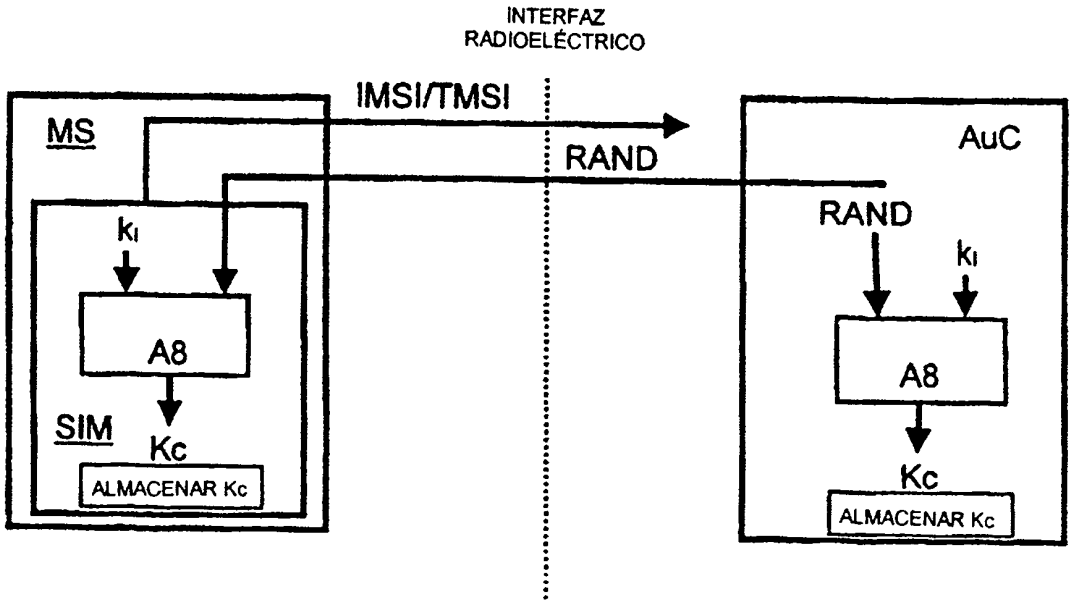
INTERFAZ
RADIOELÉCTRICO
IMSI/TMSI
MS
AuC
RAND
RAND
kI
kI
A8
A8
SIM
Kc
Kc
ALMACENAR Kc
ALMACENAR Kc

Fig. 3

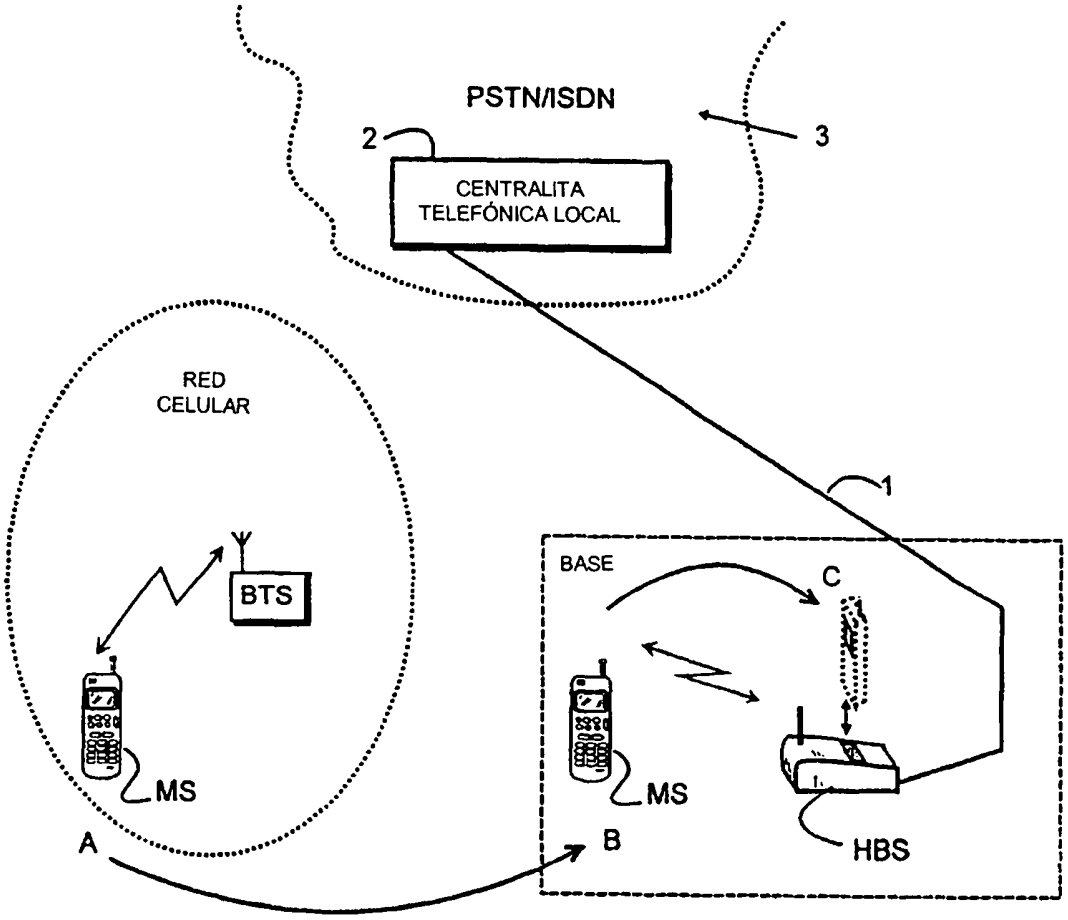
PSTN/ISDN
2
3
CENTRALITA
TELEFÓNICA LOCAL
RED
CELULAR
1
BTS
BASE
C
MS
MS
A
B
HBS

Fig. 4

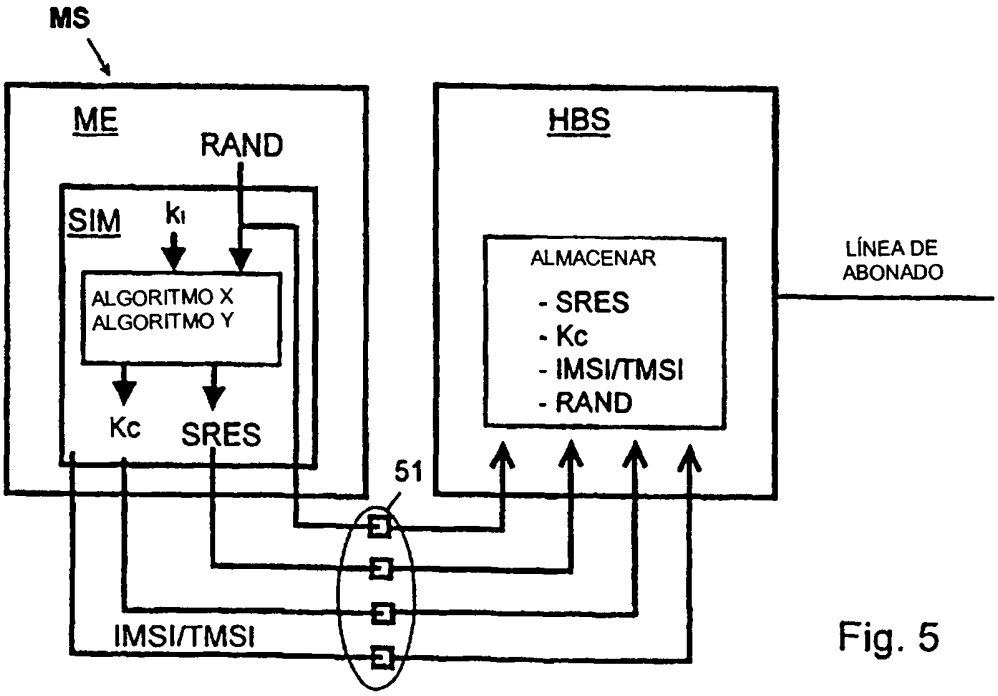
MS
ME
RAND
SIM
Ki
ALGORITMO X
ALGORITMO Y
Kc
SRES
HBS
ALMACENAR
- SRES
- Kc
- IMSI/TMSI
- RAND
LÍNEA DE
ABONADO
51
IMSI/TMSI

Fig. 5

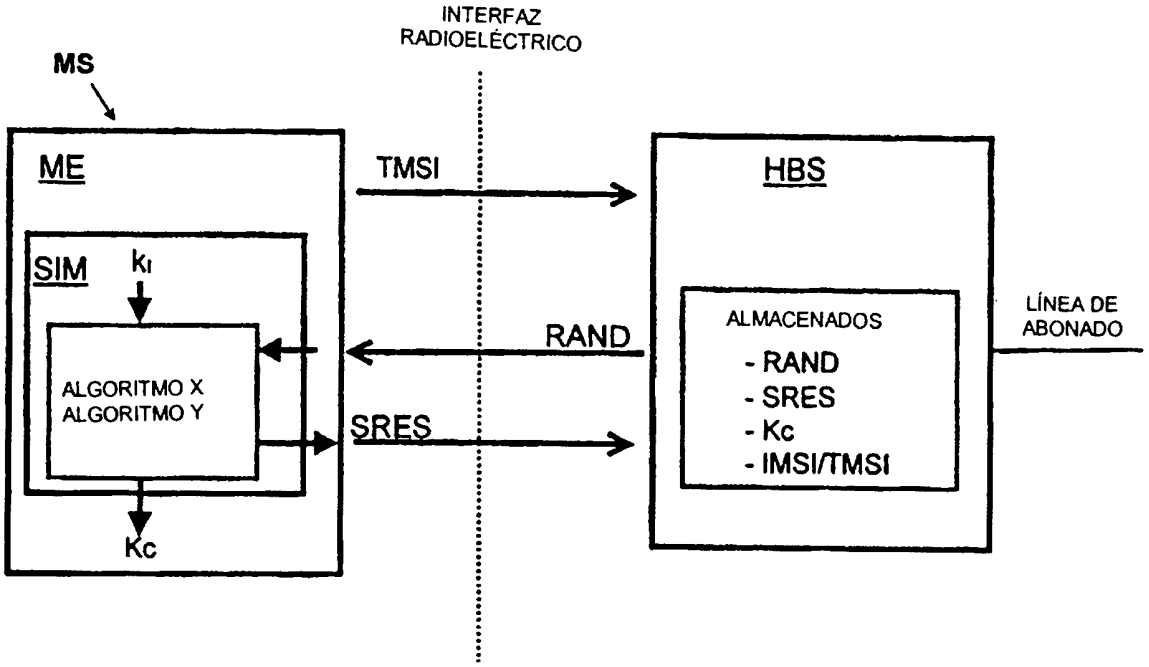
INTERFAZ
RADIOELÉCTRICO
MS
ME
SIM
ki
ALGORITMO X
ALGORITMO Y
Kc
TMSI
RAND
SRES
HBS
ALMACENADOS
- RAND
- SRES
- Kc
- IMSI/TMSI
LÍNEA DE
ABONADO

Fig. 6

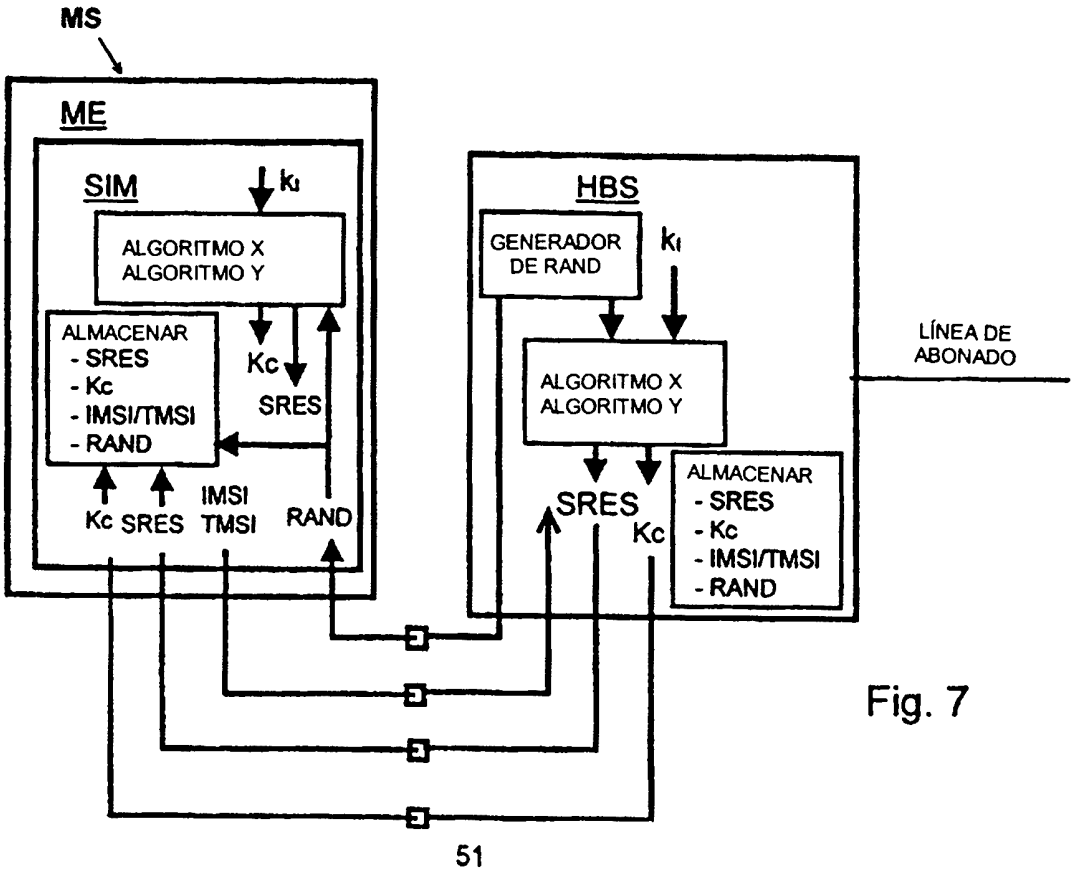
MS
ME
SIM
ki
ALGORITMO X
ALGORITMO Y
ALMACENAR
- SRES
- Kc
- IMSI/TMSI
- RAND
Kc
SRES
Kc SRES IMSI TMSI RAND
HBS
GENERADOR
DE RAND
ki
ALGORITMO X
ALGORITMO Y
SRES
Kc
ALMACENAR
- SRES
- Kc
- IMSI/TMSI
- RAND
LÍNEA DE
ABONADO
51

Fig. 7

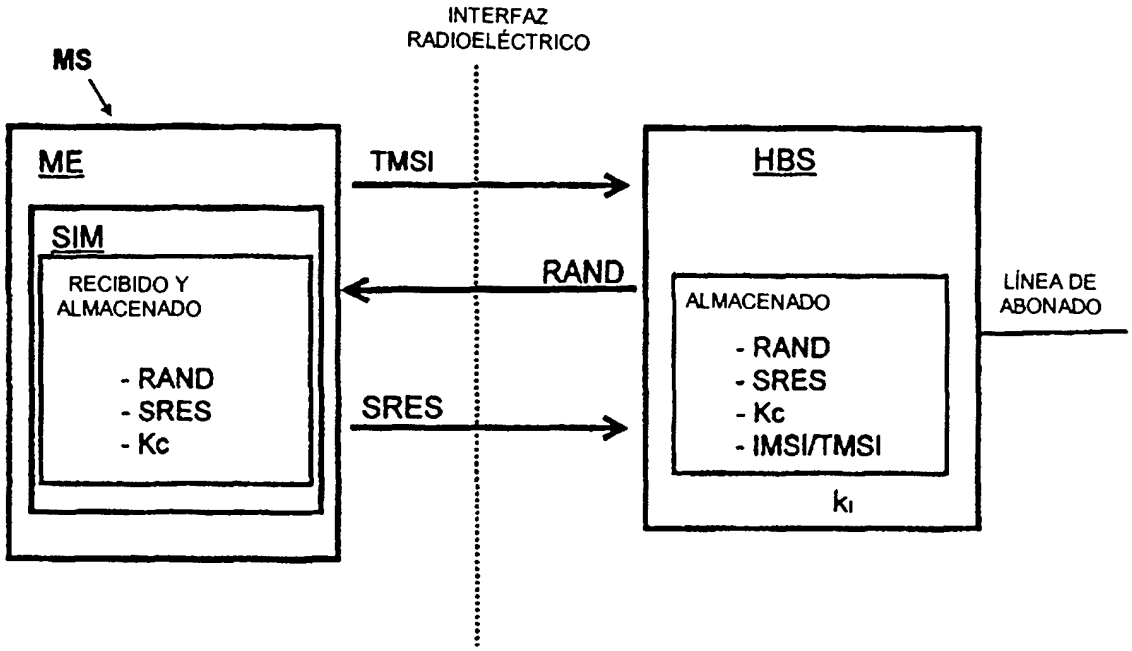
INTERFAZ
RADIOELÉCTRICO
MS
ME
SIM
RECIBIDO Y
ALMACENADO
- RAND
- SRES
- Kc
TMSI
RAND
SRES
HBS
ALMACENADO
- RAND
- SRES
- Kc
- IMSI/TMSI
Ki
LÍNEA DE
ABONADO

Fig. 8