(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 666 476**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.06.2012 E 12004347 (6)**

(97) Fecha y número de publicación de la concesión europea: **21.02.2018 EP 2536101**

(54) Título: **Método para establecer una conexión cifrada, unidad de distribución de red y sistema de telecomunicación**

(30) Prioridad:

14.06.2011 DE 102011106484

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.05.2018

(73) Titular/es:

T-MOBILE AUSTRIA GMBH (100.0%)
Rennweg 97-99
1030 Wien, AT

(72) Inventor/es:

GAILBERGER, VANJA y
SEDLACEC, MICHAEL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para establecer una conexión cifrada, unidad de distribución de red y sistema de telecomunicación

Técnica anterior

La invención se refiere a un método para establecer una conexión cifrada entre un abonado de red y una estación base de una red de radio móvil, estando dicha estación base acoplada a una unidad de distribución de red. La invención se refiere además a una unidad de distribución de red correspondiente y a una red de telecomunicaciones correspondiente.

Es conocido de manera general, por ejemplo, a partir de la publicación de patente europea EP 2 293 515 A1 o a partir de la publicación de patente americana US 2008/0 233 887 A1, cifrar conexiones de radio móvil para aumentar la seguridad por medio de algoritmos de cifrado. Se usan diferentes algoritmos de cifrado para esto: el algoritmo A5/1 es un algoritmo criptográfico para proteger la comunicación de voz a través de GSM (Sistema Global para Comunicaciones Móviles) que se usa principalmente en Europa Occidental y América del Norte. No obstante, este algoritmo de cifrado fue craqueado en 2003 y, por lo tanto, este método ya no proporciona más suficiente seguridad. El algoritmo A5/2 es un algoritmo de cifrado más débil que se usa predominantemente en Asia y Europa del Este.

También hay algoritmos A5/3 (también conocidos como cifrado KASUMI) que se usan para cifrar comunicaciones en GSM y ofrecen mayor seguridad que los cifrados A5/1 y A5/2. El algoritmo A5/3 se describe con más detalle para GSM, por ejemplo, en las especificaciones “TS 55.216 (V6.2.0) del 3GPP”, “TS 55.217 (V6.1.0) del 3GPP” y “TS 55.218 (V6.1.0) del 3GPP”.

Una desventaja cuando se usa el algoritmo A5/3 es que en algunos terminales implicados en una red de radio móvil, el flujo de mensajes con la red de radio móvil ya se interrumpe simplemente por la oferta del lado de red del algoritmo A5/3. En particular, los terminales que no soportan el algoritmo A5/3 no envían, durante la actualización de la ubicación en la red de radio móvil (conocida como “Procedimiento de Actualización de Ubicación”), cuándo han recibido un mensaje de señalización (“Comando de Modo de Cifrado”) desde la red de radio móvil, en qué mensaje se ofrecen, además del algoritmo de cifrado A5/1 convencional, también el algoritmo de cifrado A5/3 más nuevo, una respuesta de señalización (“Modo de Cifrado Completo”) a la red de radio móvil para seleccionar uno de los algoritmos de cifrado ofrecidos, incluso aunque podrían seleccionar el algoritmo A5/1 soportado por los mismos.

El resultado es que la “Actualización de Ubicación” y todos los demás eventos de señalización conocidos, tales como “Encendido, TMSI desconocida”, “Encendido, TMSI conocida”, “Actualización de Ubicación Periódica”, “Establecimiento de llamada”, “SMS MO/MT”, en los que normalmente se usa el cifrado, ya no se pueden realizar más para estos terminales. Los fallos suponen que no es posible la activación del algoritmo A5/3 comparativamente seguro por el operador de red. Tal fallo se describe aún más con la ayuda de la figura 3.

Descripción de la Invención

El objeto de la invención es de esta manera proporcionar un método para establecer una conexión de telecomunicaciones cifrada en la que, a pesar de la activación de un cifrado que da como resultado una interrupción de la comunicación entre el abonado de red y una unidad de distribución de red, se establece siempre una comunicación cifrada basada en otro cifrado.

Este objeto se logra según la invención mediante un método para establecer una conexión cifrada entre un abonado de red y una estación base de una red de radio móvil, estando dicha estación base acoplada a una unidad de distribución de red, comprendiendo dicho método los siguiente pasos: enviar un primer mensaje de señalización para ofrecer un mecanismo de cifrado desde la unidad de distribución de red al abonado de red en un primer paso del método, en donde al menos un primer algoritmo de cifrado y un segundo algoritmo de cifrado se ofrecen por medio del primer mensaje de señalización; esperar una respuesta de señalización enviada por el abonado de red a la unidad de distribución de red para seleccionar, en un segundo paso del método, uno de los mecanismos de cifrado ofrecidos por medio del primer mensaje de señalización; enviar un segundo mensaje de señalización para ofrecer un mecanismo de cifrado desde la unidad de distribución de red al abonado de red en un tercer paso del método cuando, en el segundo paso del método, una respuesta de señalización enviada por el abonado de red a la unidad de distribución de red no se detecta dentro de un periodo de tiempo predeterminado, en donde solamente el al menos un primer algoritmo de cifrado se ofrece por medio del segundo mensaje de señalización.

De una manera ventajosa, en el método según la invención, el segundo mensaje de señalización se envía al abonado de red cuando se reconoce que el abonado de red no está respondiendo al primer mensaje de señalización. En el segundo mensaje de señalización, entonces todavía se ofrece al abonado de red pertinente solamente el primer algoritmo o algoritmos de cifrado mientras que el segundo algoritmo de cifrado no se ofrece de nuevo. Por lo tanto, de una manera ventajosa, se evita la interrupción del flujo de mensajes entre el abonado de red y la unidad de distribución de red en base a la oferta del segundo algoritmo de cifrado. Un algoritmo de cifrado A5/3 (también conocido como cifrado de bloques KASUMI) se ofrece preferiblemente como segundo algoritmo de cifrado, mientras que un algoritmo de cifrado A5/1 se ofrece como primer algoritmo de cifrado. De esta manera, el cifrado A5/3 comparativamente seguro se puede activar en el sistema de telecomunicaciones y en particular en toda la red

de radio móvil, en donde se asegura que además en aquellos abonados de red en los que la activación del cifrado A5/3 da como resultado interrupciones, los mensajes se transmiten de una manera ininterrumpida a través del cifrado A5/1 convencional. Alternativamente, también es factible, por supuesto, que para los primeros algoritmos de cifrado se ofrezca un algoritmo A5/0 (sin cifrado) y/o un algoritmo A5/2 en lugar del algoritmo A5/1 o además del algoritmo A5/1. El período de tiempo se define preferiblemente de manera fija y/o se puede ajustar arbitrariamente. También es factible que el período de tiempo se adapte o se optimice dinámicamente. El abonado de red 3 incluye en particular un terminal de abonado (también conocido como UE o Equipo de Usuario), tal como, por ejemplo, un teléfono móvil, un PDA (Asistente Personal Digital), un ordenador portátil equipado con un módulo GSM, o similar, que está conectado a la estación base a través de la interfaz aérea cifrada. El cifrado se controla a través de la unidad de distribución de red. La unidad de distribución de red incluye preferiblemente un punto de distribución de radio móvil (también conocido como MSC o Centro de Conmutación de Servicios Móviles) o un nodo de red o punto de señalización en la red de radio móvil (también conocido como SSP o Punto de Señalización de Servicio en una red SS7).

La realización ventajosa y los desarrollos de la invención se describen en las reivindicaciones dependientes y la descripción con referencia a los dibujos.

Según una realización preferida de la presente invención, se hace una previsión de que en un cuarto paso del método, una respuesta de señalización se envíe por el abonado de red a la unidad de distribución de red, por medio de la cual se seleccionan un primer algoritmo de cifrado o uno de los primeros algoritmos de cifrado, y en donde en un quinto paso del método se establece una conexión de telecomunicaciones, cifrada por medio del primer algoritmo de cifrado seleccionado, entre el abonado de red y la estación base acoplada a la unidad de distribución de red. De esta manera, se asegura que de una manera convencional se establezca una conexión de telecomunicaciones basada en el primer algoritmo de cifrado incluso si la oferta del segundo algoritmo de cifrado diese como resultado la interrupción de la transmisión de mensajes entre el abonado de red y la unidad de distribución de red.

Según una realización preferida de la presente invención, se hace una previsión de que en un sexto paso del método una identificación de abonado (IMSI) del abonado de red y una información de cifrado asociada con la identificación de abonado se almacenen en un registro de visitantes de la unidad de distribución de red. De una manera ventajosa, se señala de esta manera en el registro de visitantes cuándo un mensaje de señalización podría no ser detectado dentro del período de tiempo desde un abonado de red particular (o una IMSI particular) en respuesta al primer mensaje de señalización o la oferta del segundo algoritmo de cifrado, de modo que no se reenvía preferiblemente un primer mensaje de señalización, o no se vuelve a ofrecer el segundo algoritmo de cifrado, a este abonado de red. Preferiblemente, tras un restablecimiento de una conexión de telecomunicaciones cifrada entre el abonado de red y la estación base, la identificación de abonado del abonado de red se consulta en el registro de visitantes y un segundo mensaje de señalización se envía directamente por la unidad de distribución de red al abonado de red en función de la información de cifrado almacenada en el registro de visitantes. De esta manera, se asegura que todavía se ofrezcan solamente los primeros algoritmos de cifrado al abonado de red.

Según una realización preferida de la presente invención, se hace una previsión de que después de que haya expirado un período de tiempo de actualización predeterminado, la información de cifrado asociada con una identificación de abonado se borre del registro de visitantes y/o se envíe un primer mensaje de señalización por la unidad de distribución de red al abonado de red tras un restablecimiento de una conexión de telecomunicaciones cifrada entre el abonado de red y la estación base acoplada a la unidad de distribución de red. Preferiblemente, se asegura de esta manera que el segundo algoritmo de cifrado se ofrece al abonado de red de vez en cuando incluso si en el pasado nunca fue capaz de ser recibida entonces una respuesta de señalización, de modo que si este abonado de red ha cambiado su dispositivo, se puede hacer, sin embargo, una conmutación en algún punto de tiempo al segundo algoritmo de cifrado seguro. El período de tiempo de actualización se establece preferiblemente de manera fija o se puede establecer libremente. También es factible que el período de tiempo de actualización se adapte u optimice dinámicamente.

Según una realización preferida de la presente invención, se hace una previsión de que al menos los pasos del método primero, segundo y/o tercero se realicen durante un procedimiento para actualizar la ubicación del abonado de red en una red de radio móvil (también conocido como Procedimiento de Actualización de Ubicación), durante un procedimiento para asociar un módulo de identificación de abonado intercambiable (TMSI) con el abonado de red, por ejemplo, cuando se enciende un dispositivo de abonado de red (Encendido, TMSI desconocida o Apagado, TMSI conocida) y/o durante un procedimiento para realizar un servicio de comunicaciones, por ejemplo, establecer una llamada o enviar un SMS (Establecimiento de llamada, SMS MO/MT). De una manera ventajosa, en todos los procedimientos de señalización que se pueden realizar usando algoritmos de cifrado, se asegura que los mensajes se transmiten entre el abonado de red y la unidad de distribución de red de una manera libre de interrupciones.

La presente invención también se refiere a una unidad de distribución de red para un sistema de telecomunicaciones, en particular para una red de radio móvil, en donde la unidad de distribución de red está configurada para enviar un primer mensaje de señalización para ofrecer al menos un primer algoritmo de cifrado y un segundo algoritmo de cifrado al abonado de red, y en donde la unidad de distribución de red está configurada para enviar un segundo mensaje de señalización al abonado de red para ofrecer solamente el al menos un primer

algoritmo de cifrado cuando una respuesta de señalización enviada por el abonado de red no se detecta dentro de un periodo de tiempo predeterminado. De una manera ventajosa, el método según la invención se implementa de esta manera en el sistema de telecomunicaciones por medio de la unidad de distribución de red configurada en consecuencia.

La presente invención se refiere además a un sistema de telecomunicaciones, en particular una red de radio móvil, que comprende al menos una unidad de distribución de red según la invención y al menos un abonado de red. Preferiblemente, el algoritmo de cifrado A5/3 se activa en el sistema de telecomunicaciones, en donde de una manera ventajosa no hay ninguna razón para ser cauteloso de ningún fallo de abonados de red particulares debido al método descrito anteriormente.

La presente invención se refiere además a un programa de ordenador que comprende medios de código de programa, con la ayuda de los cuales se pueden realizar todos los pasos del método según la invención cuando el programa de ordenador se ejecuta en una unidad de distribución de red según la invención, un ordenador o una unidad de cálculo correspondiente, en particular en un sistema de telecomunicaciones según la invención.

La presente invención se refiere además a un producto de programa de ordenador que tiene un medio legible por ordenador y un programa de ordenador almacenado en el medio legible por ordenador, comprendiendo dicho programa de ordenador medios de código de programa que son adecuados de manera que todos los pasos de un método según la invención se pueden realizar cuando el programa de ordenador se ejecuta en una unidad de distribución de red según la invención, un ordenador o una unidad de cálculo correspondiente, en particular en un sistema de telecomunicaciones según la invención.

Detalles, características y ventajas adicionales de la invención son evidentes a partir de los dibujos y a partir de la siguiente descripción de las realizaciones preferidas con la ayuda de los dibujos. Los dibujos ilustran meramente realizaciones ejemplificadas de la invención que no limitan el concepto inventivo esencial.

Breve descripción de los dibujos

La figura 1 muestra una vista esquemática de una unidad de distribución de red y un sistema de telecomunicaciones según una realización ejemplificada de la presente invención.

Las figuras 2a, 2b y 2c muestran vistas esquemáticas de un método para establecer una conexión de telecomunicaciones cifrada según las realizaciones ejemplificadas de la presente invención.

La figura 3 muestra una vista esquemática de un método para establecer una conexión de telecomunicaciones cifrada según la técnica anterior.

Realizaciones de la Invención

A lo largo de las diversas figuras, partes similares se dotan siempre con signos de referencia similares y, de esta manera, se nombra o se menciona de manera general cada una solamente una vez.

La figura 1 ilustra una vista esquemática de una unidad de distribución de red 2 y un sistema de telecomunicaciones 1 según una realización ejemplificada de la presente invención. El sistema de telecomunicaciones 1 incluye preferiblemente una red de radio móvil GSM (Sistema Global para Comunicaciones Móviles) 4. El sistema de telecomunicaciones 1 comprende además al menos un abonado de red 3 que está acoplado a una estación base 3' (también conocida como BTS o Estación Base Transceptora en redes GSM) y una unidad de control de estación base 3'' (también conocida como BSC o Controlador de Estación Base en redes GSM). Se establece una conexión cifrada 6 (también conocida como interfaz aérea) entre el abonado de red 3 y la estación base 3', estando el cifrado controlado por la unidad de distribución de red 2. El abonado de red 3 incluye en particular un terminal de abonado (también conocido como UE o Equipo de Usuario). El terminal de abonado incluye, por ejemplo, un teléfono móvil, un PDA (Asistente Digital Personal), un ordenador portátil equipado con un módulo GSM, o similar. La unidad de distribución de red 2, por una parte, se proporciona para acoplarse al abonado de red 3 a través de la estación base 3' y, por otra parte, está conectada al resto de la red de radio móvil 4 a través de una conexión 6' adicional con el fin de producir una conexión entre el abonado de red 3 y el resto de la red de radio móvil 4. Además, la unidad de distribución de red 2 comprende un registro de visitantes 5 que se usa para almacenar la identificación de abonado IMSI (Identidad de Abonado Móvil Internacional) del abonado de red 3 y la información de cifrado asociada con el abonado de red 3. La unidad de distribución de red 2 incluye preferiblemente un punto de distribución de radio móvil (también conocido como MSC o Centro de Conmutación de Servicios Móviles) o un nodo de red o punto de señalización (también conocido como SSP o Punto de Señalización de Servicio en una red SS7).

La unidad de distribución de red 2 está configurada además de manera que la unidad de distribución de red 2 envía, cuando se realiza un servicio de señalización, para establecer la conexión de telecomunicaciones cifrada 6 de la interfaz aérea entre el abonado de red 3 y la estación base 3', un primer mensaje de señalización al abonado de red 3 en el que se ofrece el uso tanto de un primer algoritmo de cifrado, en particular un algoritmo A5/1, como también un segundo algoritmo de cifrado, en particular un algoritmo A5/3 (también conocido como cifrado de bloques KASUMI). La unidad de distribución de red 2 está configurada además de manera que cuando el abonado de red 3 no envía una respuesta de señalización correspondiente durante un período de tiempo predeterminado, se envía un

segundo mensaje de señalización al abonado de red 3 en el que todavía se ofrece solamente el uso del primer algoritmo de cifrado, en particular el algoritmo A5/1.

El método según la invención para establecer la conexión de telecomunicaciones cifrada 6 se describe en detalle en lo sucesivo con la ayuda de las figuras 2a, 2b y 2c, en donde el método según la invención se explica en la presente memoria en cada caso usando tres configuraciones diferentes.

La figura 2a ilustra el flujo de mensajes en un procedimiento para actualizar la ubicación del abonado de red 3 (un Procedimiento de Actualización de Ubicación) entre la unidad de distribución de red 2 y el abonado de red 3 en una configuración en la que la unidad de distribución de red 2 ofrece el uso del segundo algoritmo de cifrado - o el algoritmo A5/3 - y el abonado de red 3 es capaz de usar el segundo algoritmo de cifrado - el algoritmo A5/3. En un primer mensaje 10, el abonado de red 3 envía una “Solicitud de Actualización de Ubicación” a la unidad de distribución de red 2. La unidad de distribución de red 2 confirma en un segundo mensaje 11 la presencia de una conexión de datos entre la unidad de distribución de red 2 y la unidad de control de estación base 3 (“Confirmación de Conexión”). Entonces, la unidad de distribución de red 2 envía una “Solicitud de Identidad” al abonado de red 3 por medio de un tercer mensaje 12. El abonado de red 3 transmite una “Actualización de Marca de Clase” a la unidad de distribución de red 2 en un cuarto mensaje 13 y transmite sus datos de identidad (“Respuesta de Identidad”) en un quinto mensaje 14. Entonces, en un sexto mensaje 15, se envía una solicitud de autenticación al abonado de red 3, tras la recepción de la cual el abonado de red 3 transmite datos de autenticación en un séptimo mensaje 16.

La unidad de distribución de red 2 luego envía un primer mensaje de señalización 17 al abonado de red 3 en el que el uso de un primer algoritmo de cifrado basado en el algoritmo A5/1 y el uso de un segundo algoritmo de cifrado basado en el algoritmo A5/3 se ofrecen al abonado de red 3. El primer mensaje de señalización 17 se lee, por ejemplo, como sigue:

```
BSSAP
  00000000 BSSMAP = 0 (BSSMAP)
  00010010 Length Field = 18
BSSMAP
  Msg: CIPHER MODE COMMAND
    01010011 Tag = 83 (x53)
    IE: Layer 3 header information
      00000111 Tag = 7 (x07)
      00000010 Length Field = 2
      ---0000 Not used = 0
      0110-Protocol discriminator = 6 (Radio resources management messages)
      ----0000 Not used = 0
      ---0---- TI flag = 0 (The message is sent from the side that originates the TI)
  000----- TI value = 0
IE: Encryption information
  00001010 Tag = 10 (x0A)
  00001001 Length Field = 9
  -------1 No encryption = 1 (BSS may use the option)
  ------1-GSM A5/1 = 1 (BSS may use the option)
  -----0-- GSM A5/2 = 0 (BSS shall not use the option)
  ----1--- GSM A5/3 = 1 (BSS may use the option)
  ---0---- GSM A5/4 = 0 (BSS shall not use the option)
  --0----- GSM A5/5 = 0 (BSS shall not use the option)
  -0------ GSM A5/6 = 0 (BSS shall not use the option)
  0-GSM A5/7 = 0 (BSS shall not use the option)
  Key = eb b4 23 57 a3 27 2c 00
IE: Cipher response mode
  00100011 Tag = 35 (x23)
  -0000000 Spare = 0 (Spare field (7 bits))
  1------- Cipher response mode = 1 (IMEISV must be included by the Mobile Station)
```

Si el abonado de red 3 es capaz de procesar el algoritmo A5/3 - como es el caso en el presente ejemplo- envía, en una respuesta de señalización 18, a la unidad de distribución de red 2 el mensaje de que se debería usar el algoritmo A5/3.

La respuesta de señalización 18 entonces se lee, por ejemplo, como sigue:

```
BSSAP
  00000000 BSSMAP = 0 (BSSMAP)
  00010000 Length Field = 16
BSSMAP
  Msg: CIPHER MODE COMPLETE
    01010101 Tag = 85 (x55)
    IE: Layer 3 message contents
      00100000 Tag = 32 (x20)
      00001011 Length Field = 11
      Mobile identity
        00010111 Tag = 23 (x17)
        00001001 Length Field = 9
        -----011 Type of identity = 3 (IMEISV)
        ----0--- Odd/even indicator = 0 (Even number of identity digits and also when the TMSI is used)
        Address signals = 3532330165997424f
    IE: Chosen encryption algorithm
      00101100 Tag = 44 (x2C)
        00000100 Algorithm identifier = 4 (GSM A5/3)
```

El algoritmo A5/3 se estipula como el algoritmo de cifrado para cifrar la interfaz aérea (conexión 6) entre el abonado de red 3 y la unidad de distribución de red 2. La unidad de distribución de red 2 entonces envía una confirmación de la actualización de ubicación realizada (“Aceptar Actualización de Ubicación”) en un octavo mensaje 19 al abonado de red 3, en donde en este caso se usa el cifrado A5/3. Entonces, por medio de un noveno mensaje 20, se envía un “Comando Borrar” a la unidad de control de estación base 3’’, tras la recepción del cual la unidad de control responde en un décimo mensaje con una confirmación de “Borrar Completo”. Finalmente, la unidad de distribución de red 2 envía un comando “Liberado” por medio de un undécimo mensaje 22 a la unidad de control de estación base 3’’ y la unidad de control de estación base 3 responde con una respuesta de “Liberación Completada” en un duodécimo mensaje 23.

La figura 2b ilustra de nuevo el flujo de mensajes en un procedimiento para actualizar la ubicación del abonado de red 3 (un Procedimiento de Actualización de Ubicación) entre la unidad de distribución de red 2 y el abonado de red 3, en donde ahora se muestra una configuración en la que la unidad de distribución de red 2 ofrece de nuevo el uso del segundo algoritmo de cifrado - el algoritmo A5/3 - y el abonado de red 3, a diferencia de la configuración ilustrada en la figura 2a, no es capaz de usar el segundo algoritmo de cifrado - el algoritmo A5/3. Los mensajes primero, segundo, tercero, cuarto, quinto, sexto y séptimo 10, 11, 12, 13, 14, 15, 16 son idénticos a la configuración ilustrada en la figura 2a. El primer mensaje de señalización 17’ en el que el uso de un primer algoritmo de cifrado basado en el algoritmo A5/1 y el uso de un segundo algoritmo de cifrado basado en el algoritmo A5/3 se ofrecen por la unidad de distribución de red 2 al abonado de red 3 también es idéntico El primer mensaje de señalización 17’ se lee, por ejemplo, como sigue:

```
BSSAP
  00000000 BSSMAP = 0 (BSSMAP)
  00010010 Length Field = 18
BSSMAP
  Msg: CIPHER MODE COMMAND
    01010011 Tag = 83 (x53)
    IE: Layer 3 header information
      00000111 Tag = 7 (x07)
      00000010 Length Field = 2
      ----0000 Not used = 0
      0110-Protocol discriminator = 6 (Radio resources management messages)
      ---0000 Not used = 0
      ---0---- TI flag = 0 (The message is sent from the side that originates the TI)
      000----- TI value = 0
```

```
    IE: Encryption information
      00001010 Tag = 10 (x0A)
      00001001 Length Field = 9
  -------1 No encryption = 1 (BSS may use the option)
  ------1- GSM A5/1 = 1 (BSS may use the option)
  -----0-- GSM A5/2 = 0 (BSS shall not use the option)
  ----1--- GSM A5/3 = 1 (BSS may use the option)
  ---0---- GSM A5/4 = 0 (BSS shall not use the option)
  --0----- GSM A5/5 = 0 (BSS shall not use the option)
  -0------ GSM A5/6 = 0 (BSS shall not use the option)
  0-GSM A5/7 = 0 (BSS shall not use the option)
  Key = eb b4 23 57 a3 27 2c 00
IE: Cipher response mode
  00100011 Tag = 35 (x23)
  -0000000 Spare = 0 (Spare field (7 bits))
  1------- Cipher response mode = 1 (IMEISV must be included by the Mobile Station)
```

A diferencia de la configuración mostrada en la figura 2a, el abonado de red 3 no es capaz de seleccionar el algoritmo A5/3. El abonado de red 3, de esta manera, envía una respuesta de señalización 18' a la unidad de distribución de red 2 en la que se selecciona el primer algoritmo de cifrado, es decir, el algoritmo A5/1.

La respuesta de señalización 18' entonces se lee, por ejemplo, como sigue:

```
BSSAP
  00000000 BSSMAP = 0 (BSSMAP)
  00010000 Length Field = 16
BSSMAP
  Msg: CIPHER MODE COMPLETE
    01010101 Tag = 85 (x55)
    IE: Layer 3 message contents
      00100000 Tag = 32 (x20)
      00001011 Length Field = 11
      Mobile identity
        00010111 Tag = 23 (x17)
        00001001 Length Field = 9
        -----011 Type of identity = 3 (IMEISV)
        ----0--- Odd/even indicator = 0 (Even number of identity digits and also when the
TMSI is used)
        Address signals = 3532330165997424f
IE: Chosen encryption algorithm
      00101100 Tag = 44 (x2C)
        00000010 Algorithm identifier = 2 (GSM A5/1)
```

Los mensajes posteriores octavo, noveno, décimo, undécimo y duodécimo 19, 20, 21, 22, 23 también son idénticos a la configuración mostrada en la figura 2a, en donde ahora se usa el cifrado A5/1 (al menos en el octavo paso).

La figura 2c ilustra de nuevo el flujo de mensajes en un procedimiento para actualizar la ubicación del abonado de red 3 (un Procedimiento de Actualización de Ubicación) entre la unidad de distribución de red 2 y el abonado de red 3, en el que la unidad de distribución de red 2 de nuevo ofrece el uso del segundo algoritmo de cifrado - el algoritmo A5/3. En la configuración mostrada en la figura 2c, el abonado de red 3, como en la figura 2b, no es capaz de nuevo de usar el segundo algoritmo de cifrado - el algoritmo A5/3 - en donde, a diferencia de la figura 2b, la oferta del algoritmo A5/3 da como resultado que el abonado de red 3 no envíe ninguna respuesta de señalización en absoluto a la unidad de distribución de red 2.

Los mensajes primero, segundo, tercero, cuarto, quinto, sexto y séptimo 10, 11, 12, 13, 14, 15, 16 son idénticos a la configuración ilustrada en la figura 2b. El primer mensaje de señalización 17'' en el que el uso de un primer algoritmo de cifrado basado en el algoritmo A5/1 y el uso de un segundo algoritmo de cifrado basado en el algoritmo A5/3 se ofrecen por la unidad de distribución de red 2 al abonado de red 3 también es idéntico. El primer mensaje de señalización 17'' se lee, por ejemplo, como sigue:

```
BSSAP
  00000000 BSSMAP = 0 (BSSMAP)
  00010010 Length Field = 18
BSSMAP
  Msg: CIPHER MODE COMMAND
    01010011 Tag = 83 (x53)
    IE: Layer 3 header information
      00000111 Tag = 7 (x07)
      00000010 Length Field = 2
      ---0000 Not used = 0
      0110-Protocol discriminator = 6 (Radio resources management messages)
      ----0000 Not used = 0
      ---0---- TI flag = 0 (The message is sent from the side that originates the TI)
000----- TI value = 0
    IE: Encryption information
      00001010 Tag = 10 (x0A)
      00001001 Length Field = 9
      -------1 No encryption = 1 (BSS may use the option)
      ------1- GSM A5/1 = 1 (BSS may use the option)
      -----0-- GSM A5/2 = 0 (BSS shall not use the option)
      ----1--- GSM A5/3 = 1 (BSS may use the option)
      ---0---- GSM A5/4 = 0 (BSS shall not use the option)
      --0----- GSM A5/5 = 0 (BSS shall not use the option)

      -0------ GSM A5/6 = 0 (BSS shall not use the option)
      0------- GSM A5/7 = 0 (BSS shall not use the option)
      Key = eb b4 23 57 a3 27 2c 00
IE: Cipher response mode
  00100011 Tag = 35 (x23)
  -0000000 Spare = 0 (Spare field (7 bits))
  1------- Cipher response mode = 1 (IMEISV must be included by the Mobile Station)
```

La oferta del segundo algoritmo de cifrado da como resultado que el abonado de red 3 no responda al primer mensaje de señalización 17''. La unidad de distribución de red 2 espera un período de tiempo predeterminado el mensaje de señalización del abonado de red 3. Si no se recibe un mensaje de señalización dentro de este período de tiempo ("Tiempo de Espera de MSS" 24), la unidad de distribución de red 2 envía un segundo mensaje de señalización 25 al abonado de red 3 en el que todavía se ofrece solamente el primer algoritmo de cifrado, es decir, el algoritmo A5/1. El segundo algoritmo de cifrado, es decir, el algoritmo A5/3, ya no se ofrece más.

El segundo mensaje de señalización 25 se lee, por ejemplo, como sigue:

```
BSSAP
  00000000 BSSMAP = 0 (BSSMAP)
  00010010 Length Field = 18
BSSMAP
  Msg: CIPHER MODE COMMAND
    01010011 Tag = 83 (x53)
    IE: Layer 3 header information
      00000111 Tag = 7 (x07)
      00000010 Length Field = 2
      ---0000 Not used = 0
      0110-Protocol discriminator = 6 (Radio resources management messages)
      ----0000 Not used = 0
      ---0---- TI flag = 0 (The message is sent from the side that originates the TI)
      000----- TI value = 0
```

IE: Encryption information
00001010 Tag = 10 (x0A)
00001001 Length Field = 9
-------1 No encryption = 1 (BSS may use the option)
------1- GSM A5/1 = 1 (BSS may use the option)
-----0-- GSM A5/2 = 0 (BSS shall not use the option)
----0--- GSM A5/3 = 0 (BSS may not use the option)
---0---- GSM A5/4 = 0 (BSS shall not use the option)
--0----- GSM A5/5 = 0 (BSS shall not use the option)
-0------ GSM A5/6 = 0 (BSS shall not use the option)
0-GSM A5/7 = 0 (BSS shall not use the option)
Key = eb b4 23 57 a3 27 2c 00
IE: Cipher response mode
00100011 Tag = 35 (x23)
-0000000 Spare = 0 (Spare field (7 bits))
1------- Cipher response mode = 1 (IMEISV must be included by the Mobile Station)

El abonado de red 3 es capaz ahora de seleccionar el primer algoritmo de cifrado – el algoritmo A5/1 – y ya no se interrumpe más por la oferta del segundo algoritmo de cifrado. El abonado de red 3, de esta manera, envía una respuesta de señalización 18'' a la unidad de distribución de red 2 en la que se selecciona el primer algoritmo de cifrado - el algoritmo A5/1.

La respuesta de señalización 18'' entonces se lee, por ejemplo, como sigue:

BSSAP
00000000 BSSMAP = 0 (BSSMAP)
00010000 Length Field = 16
BSSMAP
Msg: CIPHER MODE COMPLETE
01010101 Tag = 85 (x55)
IE: Layer 3 message contents
00100000 Tag = 32 (x20)
00001011 Length Field = 11
Mobile identity
00010111 Tag = 23 (x17)
00001001 Length Field = 9
-----011 Type of identity = 3 (IMEISV)
----0--- Odd/even indicator = 0 (Even number of identity digits and also when the TMSI is used)
Address signals = 3532330165997424f
IE: Chosen encryption algorithm
00101100 Tag = 44 (x2C)
00000010 Algorithm identifier = 2 (GSM A5/1)

Los mensajes posteriores octavo, noveno, décimo, undécimo y duodécimo 19, 20, 21, 22, 23 también son idénticos a la configuración mostrada en la figura 2a, en donde ahora se usa el cifrado A5/1 (al menos en el octavo paso).

Se hace opcionalmente una previsión de que el punto de distribución de red 2 almacene la identificación de abonado (IMSI) del abonado de red 3 en el registro de visitantes 5 cuando se reconoce que este abonado de red 3 solamente responde al segundo mensaje de señalización 25. La información de cifrado correspondiente se almacena entonces en el registro de visitantes 5 indicando que en el futuro el segundo algoritmo de cifrado ya no se ofrece más a este abonado de red 3, sino que en su lugar se ofrece directamente todavía solamente el primer algoritmo de cifrado por medio del segundo mensaje de señalización 25. El registro de visitantes 5, de esta manera, comprende preferiblemente una lista de abonados 3 para los cuales no funciona el cifrado A5/3, de modo que el operador de la red puede determinar con qué frecuencia tiene lugar un retroceso a un cifrado alternativo.

Es factible que un período de tiempo de actualización sea fijado de manera que cuando haya expirado este período de tiempo de actualización, el segundo algoritmo de cifrado se ofrezca de nuevo al abonado de red por medio del primer mensaje de señalización 17, 17', 17'' de modo que, por ejemplo, cuando el abonado de red 3 cambia su

dispositivo o realiza una actualización de software (lo que significa que llegue a ser posible el procesamiento del segundo algoritmo de cifrado), se puede hacer una conmutación al algoritmo A5/3 mejorado.

Es factible además que el método para “Itinerancia Nacional”, “Compartición de Red” y para “Abonados Itinerantes” se use en el mismo registro de visitantes correspondiente a la función para abonados HPMLN (Red Móvil Terrestre Pública Doméstica).

El método según la invención se describe en las figuras 2a, 2b y 2c solamente a modo de ejemplo usando un Procedimiento de Actualización de Ubicación. Por supuesto, se puede usar igualmente en todas las demás funciones de señalización en las que se requiera cifrado.

Con propósitos ilustrativos, la figura 3 ilustra una configuración similar a la figura 2c en la que no se usa el método según la invención.

Los mensajes primero, segundo, tercero, cuarto, quinto, sexto y séptimo 10, 11, 12, 13, 14, 15, 16 son idénticos a la configuración ilustrada en la figura 2c. El primer mensaje de señalización 17'' en el que el uso de un primer algoritmo de cifrado basado en el algoritmo A5/1 y el uso de un segundo algoritmo de cifrado basado en el algoritmo A5/3 se ofrecen por la unidad de distribución de red 2 al abonado de red 3 también es idéntico. En respuesta, el abonado de red 3 no envía una respuesta de señalización y, por lo tanto, ocurre un Tiempo de Espera de MSS 24. La unidad de distribución de red 2 envía entonces un decimotercer mensaje 26 en el que se indica el rechazo del cifrado (“Rechazar Modo de Cifrado”). El decimotercer mensaje entonces se lee, por ejemplo, como sigue:

BSSAP

00000000 BSSMAP = 0 (BSSMAP)
00000100 Length Field = 4

BSSMAP

Msg: CIPHER MODE REJECT
01011001 Tag = 89 (x59)
IE: Cause
00000100 Tag = 4 (x04)
00000001 Length Field = 1
-------0 Extension = 0 (Last octet)
0000000- Cause Value = 0 (Radio interface message failure)

El flujo de mensajes entre el abonado de red 3 y la unidad de distribución de red 2 se interrumpe de esta manera y no se puede realizar una Actualización de Ubicación (el octavo mensaje 19 “Aceptar Actualización de Ubicación” se omite de esta manera en la figura 3). Los mensajes posteriores noveno, décimo, undécimo y duodécimo 20, 21, 22, 23 son idénticos también a la configuración mostrada en la figura 2c.

REIVINDICACIONES

1. Un método para establecer, a través de GSM, una conexión cifrada (6) entre un abonado de red (3) y una estación base (3') de una red de radio móvil (4), estando dicha estación base acoplada a una unidad de distribución de red (2), comprendiendo dicho método los siguientes pasos:

- enviar un primer mensaje de señalización (17, 17', 17'') para ofrecer un mecanismo de cifrado desde la unidad de distribución de red (2) al abonado de red (3) en un primer paso del método, en donde al menos un primer algoritmo de cifrado y un segundo algoritmo de cifrado se ofrecen por medio del primer mensaje de señalización (17, 17', 17''), - esperar una respuesta de señalización (18, 18', 18'') enviada por el abonado de red (3) a la unidad de distribución de red (2) para seleccionar, en un segundo paso del método, uno de los mecanismos de cifrado ofrecidos por medio del primer mensaje de señalización, y
- enviar un segundo mensaje de señalización (25) para ofrecer un mecanismo de cifrado desde la unidad de distribución de red (2) al abonado de red (3) en un tercer paso del método cuando, en el segundo paso del método, una respuesta de señalización (18, 18', 18'') enviada por el abonado de red (3) a la unidad de distribución de red (2) no se detecta dentro de un período de tiempo predeterminado, en donde solamente se ofrece el primer algoritmo de cifrado por medio del segundo mensaje de señalización (25).

2. Un método según la reivindicación 1, en donde un algoritmo de cifrado A5/3 se ofrece como un segundo algoritmo de cifrado por medio de 13 5 10 15 20 25 30 35 40 45 50 55 del documento EP 2 536 101 B1 del primer mensaje de señalización (17, 17', 17'').

3. Un método según una cualquiera de las reivindicaciones precedentes, en donde al menos un algoritmo de cifrado A5/1 se ofrece como primer algoritmo de cifrado en cada caso por medio del primer (17, 17', 17'') y segundo (25) mensaje de señalización.

4. Un método según una cualquiera de las reivindicaciones precedentes, en donde en un cuarto paso del método, se envía una respuesta de señalización (18, 18', 18'') por el abonado de red (3) a la unidad de distribución de red (2), por medio de la cual se selecciona el primer algoritmo de cifrado, y en donde en un quinto paso del método se establece una conexión (6), cifrada por medio del primer algoritmo de cifrado seleccionado, entre el abonado de red (3) y la estación base (3').

5. Un método según una cualquiera de las reivindicaciones precedentes, en donde en un sexto paso del método, una identificación de abonado (IMSI) del abonado de red (3) y una información de cifrado asociada con la identificación de abonado se almacenan en un registro de visitantes (5) de la unidad de distribución de red (2).

6. Un método según la reivindicación 5, en donde tras un restablecimiento de una conexión cifrada (6) entre el abonado de red (3) y la estación base (3') la información de cifrado, asociada con la identificación de abonado, del abonado de red (3) se consulta en el registro de visitantes (5) y se envía directamente un segundo mensaje de señalización por la unidad de distribución de red (2) al abonado de red (3) en función de la información de cifrado almacenada en el registro de visitantes (5).

7. Un método según una cualquiera de las reivindicaciones 5 o 6, en donde después de que haya expirado un período de tiempo de actualización predeterminado, la información de cifrado asociada con una identificación de abonado se borra del registro de visitantes (5) y/o un primer mensaje de señalización (17, 17', 17'') se envía por la unidad de distribución de red (2) al abonado de red (3) tras un restablecimiento de una conexión cifrada (6) entre el abonado de red (3) y la estación base (3').

8. Un método según una cualquiera de las reivindicaciones precedentes, en donde al menos el primer, segundo y tercer pasos del método se realizan durante un procedimiento para actualizar la ubicación del abonado de red (3) en una red de radio móvil (4), durante un procedimiento para asociar un módulo de identificación de abonado intercambiable (TMSI) con el abonado de red (3) y/o durante un procedimiento para realizar un servicio de comunicaciones.

9. Una unidad de distribución de red (2) para un sistema de telecomunicaciones (1), en donde la unidad de distribución de red (2) está configurada para enviar un primer mensaje de señalización (17, 17', 17'') para ofrecer al menos un primer algoritmo de cifrado y un segundo algoritmo de cifrado a un abonado de red (3) a través de GSM, y en donde la unidad de distribución de red (2) está configurada para enviar un segundo mensaje de señalización (25) al abonado de red (3) para ofrecer solamente el primer algoritmo de cifrado cuando una respuesta de señalización (18, 18', 18'') enviada por el abonado de red (3) no se detecta dentro de un período de tiempo predeterminado.

10. Un sistema de telecomunicaciones (1) para una red de radio móvil (4) que comprende al menos una unidad de distribución de red (2) según la reivindicación 9 y al menos un abonado de red (3).

11. Un programa de ordenador que comprende medios de código de programa, por medio de los cuales se pueden realizar todos los pasos de un método según una cualquiera de las reivindicaciones 1 a 8 cuando el programa de ordenador se ejecuta en una unidad de distribución de red (2) o en un ordenador.

12. Un producto de programa de ordenador que tiene un medio legible por ordenador y un programa de ordenador almacenado en el medio legible por ordenador, comprendiendo dicho programa de ordenador medios de código de programa que son adecuados de manera que todos los pasos de un método según una cualquiera de las reivindicaciones 1 a 8 se puedan realizar cuando el programa de ordenador se ejecuta en una unidad de distribución de red (2) o en un ordenador.

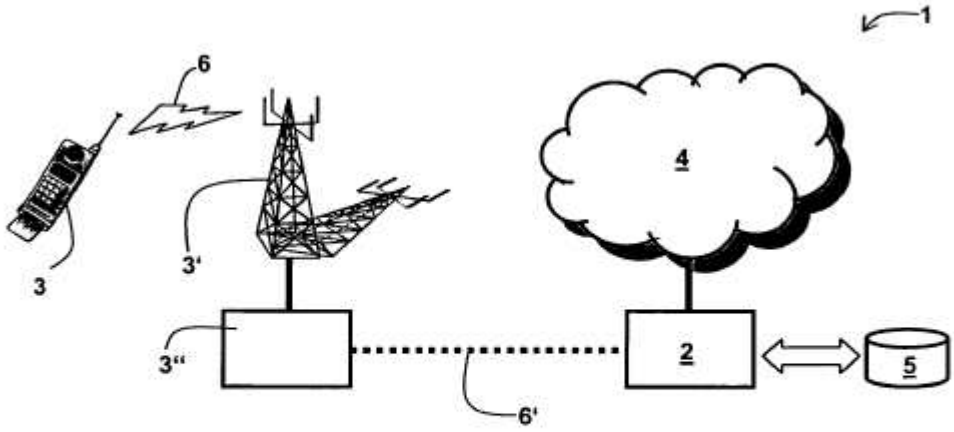

Fig. 1

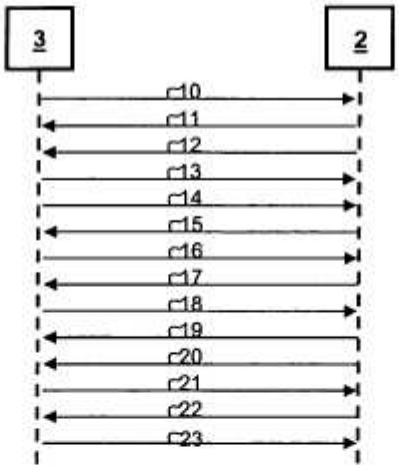

Fig. 2a

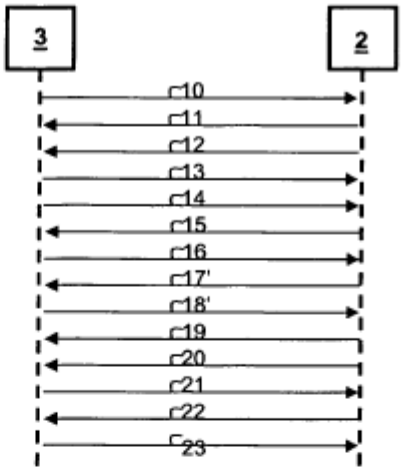
3
2
10
11
12
13
14
15
16
17'
18'
19
20
21
22
23

Fig. 2b

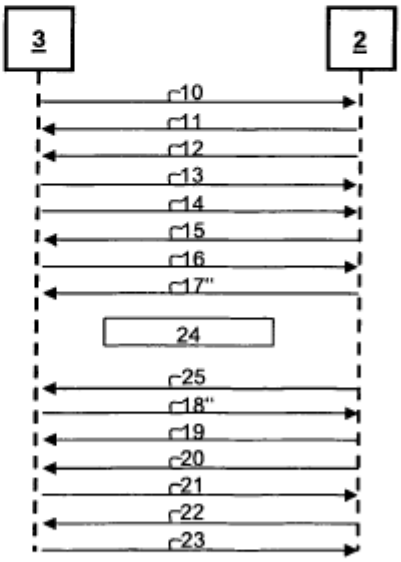
3
2
10
11
12
13
14
15
16
17''
24
25
18''
19
20
21
22
23

Fig. 2c

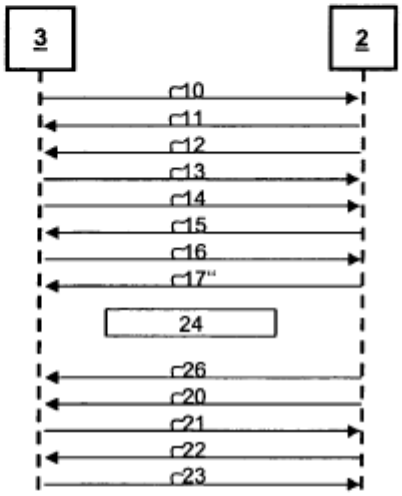

Fig. 3