(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 307 878**

(51) Int. Cl.:
H04Q 7/38 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03257057 .4**
(96) Fecha de presentación : **07.11.2003**
(97) Número de publicación de la solicitud: **1530393**
(97) Fecha de publicación de la solicitud: **11.05.2005**

(54) Título: **Procesamiento de mensajes de configuración y de gestión de movilidad con información ausente del tiempo de activación de cifrado para DPCH (canal físico dedicado) en un sistema universal de telecomunicaciones móviles (UMTS).**

(73) Titular/es: **Research in Motion Limited**
295 Phillip Street
Waterloo, Ontario N2L 3W8, CA

(45) Fecha de publicación de la mención BOPI:
01.12.2008

(72) Inventor/es: **Norton, Mark Dennis y**
Farnsworth, Andrew John

(45) Fecha de la publicación del folleto de la patente:
01.12.2008

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procesamiento de mensajes de configuración y de gestión de movilidad con información ausente del tiempo de activación de cifrado para DPCH (canal físico dedicado) en un sistema universal de telecomunicaciones móviles (UMTS).

Referencia cruzada a solicitud relacionada

No aplicable.

Antecedentes

Campo técnico

Esta solicitud se refiere al UMTS (Universal Mobile Telecommunications System) en general y a un método y aparato para procesar mensajes en un sistema universal de telecomunicaciones móviles en particular.

Descripción de la técnica relacionada

UMTS es un sistema de telecomunicación móvil terrestre público de tercera generación. Son conocidos diversos organismos de normalización que publican y establecen normas para UMTS, cada uno en sus áreas respectivas de competencia. Por ejemplo, se ha conocido que el 3GPP (Third Generation Partnership Project) publica y establece normas para el UMTS basado en GSM (Global System for Mobile Communications) y se ha conocido que el 3GPP2 (Third Generation Partnership Project 2) publica y establece normas para UMTS basado en CDMA (Code División Multiple Access = acceso múltiple por división de código). Dentro del alcance de un organismo particular de normalización, socios específicos publican y establecen normas en sus áreas respectivas.

Considérese un dispositivo móvil inalámbrico, denominado generalmente como equipo de usuario (UE: user equipment), que satisface las especificaciones 3GPP para el protocolo UMTS. La especificación 3GPP 25.331, v. 3.15.0, designada en esto la especificación 25.331, estudia el tema de las exigencias de protocolo de RRC (Radio Resource Control = control de recursos de radio) de UMTS entre la UTRAN (UMTS Terrestrial Radio Access Network = red terrrestre de acceso por radio de UMTS) y el equipo de usuario (UE).

La especificación 25.331 describe el procesamiento genérico de elementos de información (IEs: information elements) que están incluidos en mensajes de protocolo. La sección 8.6.3.4 describe el procesamiento del elemento de información (IE) de "información de modo de cifrado" e incluye cláusulas que describen el elemento de información de información de "tiempo de activación de cifrado para canal físico dedicado (DPCH)" que es un elemento opcional con el elemento de "información de modo de cifrado". Esta sección de la especificación está reducido para asegurar que el elemento de información de "tiempo de activación de cifrado para canal físico dedicado (DPCH)" está presente cuando el mensaje que es procesado es un mensaje de orden de modo de seguridad y hay portadores de radio en modo transparente en existencia. Además, la sección 8.1.12.2 de la especificación 25.331 impone el comportamiento en la UTRAN para expresar que debe incluir este elemento de información en el mensaje de orden de modo de seguridad cuando existen portadores de radio en modo transparente. Existen otros mensajes que pueden incluir el elemento de información de "información de modo de cifrado", además del mensaje de orden de modo de seguridad. Los inventores han comprendido que pueden existir condiciones en relación con estos mensajes donde el elemento de información de "tiempo de activación de modo de cifrado para canal físico dedicado" sería necesario para que el equipo de usuario (UE) exhiba comportamiento lógico, pero ningún mecanismo es especificado para asegurar que está disponible. Estos mensajes incluyen los cinco mensajes de reconfiguración especificados en la sección 8.2.2, los mensajes de confirmar actualización de célula y confirmar actualización de URA descritos en la sección 8.3.1 y el mensaje de información de movilidad de UTRAN especificado en la sección 8.3.3 de la especificación 25.331. El documento US6125123 concierne a un procedimiento de procesamiento de mensajes en un sistema de conmutación de ATM-LAN (Asynchonous Transfer Mode-Local Area Network = Modo de Transferencia Asíncrona - Red de Área Local).

Sumario

Un objeto de la presente invención es que un aparato y método según la invención puedan permitir que el equipo de usuario (UE) exhiba comportamiento lógico en respuesta a la presencia o ausencia del elemento de información de "tiempo de activación de cifrado para canal físico dedicado" en mensajes recibidos por el equipo de usuario (UE).

Según un aspecto de la presente invención, se proporciona un método para procesar un mensaje recibido en un equipo de usuario en un sistema de comunicaciones UMTS, en el que el mensaje incluye un elemento de información de información de modo de cifrado y es uno de una pluralidad de tipos de mensajes que comprenden un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar actualización de célula, un mensaje de confirma actualización de URA y un mensaje de información de movilidad de UTRAN, comprendiendo el método determinar si un elemento de información de tiempo de activación de cifrado para canal físico dedicado está presente en el mensaje cuando existen portadores de

radio que usan modo transparente de control de radioenlace y en el caso de que el elemento de información no esté presente, devolver un mensaje que indique la ausencia del elemento de información.

La ausencia del elemento de información de tiempo de activación de cifrado para canal físico dedicado puede ser indicada transmitiendo un mensaje de respuesta a la UTRAN con un valor de retorno de error de INVALID_CONFIGURATION (CONFIGURACIÓN INVÁLIDA) o UNSUPPORTED_CONFIGURATION (CON- FIGURACIÓN NO SOPORTADA).

Según un segundo aspecto de la invención, se proporciona un método para preparar un mensaje para transmisión a un equipo de usuario en un sistema de comunicaciones UMTS, incluyendo el mensaje un elemento de información de información de modo de cifrado, comprendiendo el método determinar si existen portadores de radio que usan modo transparente de control de radioenlace y si existen, determinar si el mensaje es uno de una pluralidad de tipos de mensajes para los que ha de ser incluido un elemento de información de tiempo de activación de cifrado para canal físico dedicado, comprendiendo la pluralidad de tipos de mensajes un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar autorización de célula, un mensaje de confirmar actualización de URA (UTRAN Registration Area = área de registro de UTRAN) y un mensaje de información de movilidad de UTRAN y en el caso de que el mensaje sea uno de dicha pluralidad de tipos de mensajes, incluir el elemento de información de tiempo de activación de cifrado para canal físico dedicado en el mensaje.

Según un tercer aspecto de la invención, se proporciona un método para procesar un mensaje recibido en un equipo de usuario en un sistema de comunicaciones UMTS, en el que el mensaje incluye un elemento de información de información de modo de cifrado y es uno de una pluralidad de tipos de mensajes que comprende un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar actualización de célula, un mensaje de confirmar actualización de URA y un mensaje de información de movilidad de UTRAN, comprendiendo el método determinar si un elemento de información de tiempo de activación de cifrado para canal físico dedicado está presente en el mensaje cuando existen portadores de radio que usan modo transparente de control de radioenlace y en el caso de que el elemento de información no esté presente, seleccionar un tiempo de activación para aplicar cambios de cifrado para los portadores de radio en modo transparente.

El paso de seleccionar el tiempo de activación puede comprender usar un tiempo de activación de mensaje recibido desde la UTRAN.

El método puede comprender además devolver un mensaje de respuesta a la UTRAN que incluye un tiempo de activación seleccionado en el equipo de usuario, usando por ejemplo el elemento de información de tiempo de activación de CUENTA-C.

El método también puede comprender usar un tiempo de activación de “AHORA” para aplicar inmediatamente cambios de cifrado en el equipo de usuario.

Según un aspecto adicional de la invención, se proporciona equipo de usuario para recibir un mensaje en un sistema de comunicaciones UMTS, en el que el mensaje incluye un elemento de información de información de modo de cifrado y es uno de una pluralidad de tipos de mensajes que comprenden un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar actualización de célula, un mensaje de confirmar actualización de URA y un mensaje de información de movilidad de UTRAN, comprendiendo el equipo de usuario un módulo de control configurado para determinar si un elemento de información de tiempo de activación de cifrado para canal físico dedicado está presente en el mensaje cuando existen portadores de radio que usan modo transparente de control de radioenlace y un transmisor para devolver un mensaje que indica la ausencia del elemento de información en el caso de que el elemento de información de tiempo de activación de cifrado para canal físico dedicado no está presente.

Según otro aspecto más de la invención, se proporciona una UTRAN para transmitir un mensaje a un equipo de usuario en un sistema de comunicaciones UMTS, incluyendo el mensaje un elemento de información de información de modo de cifrado, comprendiendo la UTRAN un módulo de control configurado para determinar si existen portadores de radio que usan modo transparente de control de radioenlace y para determinar, en el caso de que existan dichos portadores de radio, si el mensaje es uno de una pluralidad de tipos de mensajes para los que ha de incluirse un elemento de información de tiempo de activación de cifrado para canal físico dedicado, comprendiendo la pluralidad de tipos de mensajes un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar actualización de célula, un mensaje de confirmar actualización de URA y un mensaje de información de movilidad de UTRAN, estando además el módulo de control configurado para incluir el elemento de información de tiempo de activación de cifrado para canal físico dedicado en el mensaje en el caso de que el mensaje sea uno de dicha pluralidad de tipos de mensajes.

La invención proporciona además equipo de usuario (UE) para recibir un mensaje desde una UTRAN en un sistema de comunicaciones UMTS, en que el mensaje incluye un elemento de información de información de modo de cifrado y es uno de una pluralidad de tipos de mensajes que comprenden un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar actualización de célula, un mensaje de confirmar actualización de URA y un mensaje de información de movilidad de UTRAN, comprendiendo el equipo de usuario un módulo de control configurado para determinar si un elemento de información de tiempo de activación de cifrado para canal físico dedicado está presente en el mensaje cuando existen portadores de radio que usan modo transparente de control de radioenlace, estando configurado además el módulo de control para seleccionar un tiempo de activación para aplicar cambios de cifrado para los portadores de radio en modo transparente, en el caso de que el elemento de información no esté presente.

Descripción breve de los dibujos

Realizaciones de la presente invención serán descritas ahora, a modo de ejemplo solamente, con referencia a los dibujos adjuntos, en los que:

la Figura 1 es un esquema de bloques que ilustra una realización de un aparato de pila de protocolo provisto de un módulo de control de recursos de radio de manejo de tiempo de activación de cifrado de canal físico dedicado (DCATH RRC: DPCH ciphering activation time handling Radio Resource Control), de acuerdo con la presente invención;

la Figura 2 es un esquema de bloques que ilustra el módulo 200 de DCATH RRC de la Figura 1 en el contexto de un equipo de usuario (UE) y una UTRAN;

la Figura 3 es un organigrama que ilustra el procesamiento realizado por un módulo de DCATH RRC de UE al recibir en el equipo de usuario (UE) un mensaje desde la UTRAN que puede incluir el elemento de información de información de modo de cifrado;

la Figura 4 muestra los pasos realizados por un módulo de DCATH RRC de UTRAN para asegurar que el elemento de información de "tiempo de activación de cifrado para canal físico dedicado (BPCH)" está incluido en mensajes donde esto es necesario; y

la Figura 5 es un esquema de bloques que ilustra un dispositivo móvil que puede actuar como un equipo de usuario (UE) y cooperar con el aparato y los métodos de las Figuras 1 a 4.

Los mismos números de referencia son usados en figuras diferentes para designar elementos similares.

Descripción detallada de los dibujos

Refiriéndose a los dibujos, la Figura 1 es un esquema de bloques que ilustra una realización de un aparato de pila de protocolo provisto de un módulo de control de recursos de radio de manejo de tiempo de activación de cifrado de canal físico dedicado (DCATH RRC), de acuerdo con la presente invención.

El módulo 200 de DCATH RRC es una subbcapa de la Capa 3 130 de una pila 100 de protocolo UMTS. El módulo 200 de DCATH RRC existe en el plano de control solamente y proporciona un servicio de transferencia de información al estrado sin acceso NAS 134. El módulo 200 de DCATH RRC es responsable de controlar la configuración de la capa 1 110 y la Capa 2 120 de interfaz de radio. La UTRAN emite uno de una pluralidad de mensajes posibles al equipo de usuario (UE) que pueden incluir el elemento de información de "información de modo de cifrado" descrito en la Sección 8.6.3.4 de la especificación 25.331. Los mensajes son un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar actualización de célula, un mensaje de confirmar actualización de URA y un mensaje de información de movilidad de UTRAN.

La capa de módulo 200 de DCATH RRC del equipo de usuario (UE) descodifica este mensaje y comprueba si el elemento de información de tiempo de activación de cifrado para canal físico dedicado (DPCH: dedicated physical channel) está presente si es necesario. Si lo está, inicia el procedimiento apropiado de control de recursos de radio (RRC), cuyo procedimiento puede requerir que el módulo 200 de DCATH RRC envía un mensaje de respuesta a la UTRAN (por vía de las capas inferiores) que informa a la UTRAN del resultado del procedimiento. Si el elemento de información de tiempo de activación de cifrado para el canal físico dedicado (DPCH) está ausente pero es necesario para el procedimiento, el bloque 200 de DCATH RRC emprende la acción apropiada, como se describe con detalle a continuación.

Convenientemente, el módulo 200 de DCATH RRC permite que la pila 100 de protocolo se comporte de modo inequívoco en el caso de que uno de los mensajes recibidos anteriormente sea recibido desde la UTRAN.

La Figura 2 es un esquema de bloques que ilustra el módulo 200 de DCATH RRC de la Figura 1 en el contexto de un equipo de usuario (UE) y una UTRAN, mientras que la Figura 3 es un organigrama que ilustra el procesamiento

realizado por un módulo de DCATH RRC de equipo de usuario (UE) al recibir en el equipo de usuario un mensaje desde la UTRAN que puede incluir el elemento de información de información de modo de cifrado.

Una UTRAN 210 envía un mensaje 215 que es recibido por un receptor 212 en el equipo de usuario (UE) 220 (paso s1). El mensaje es uno de los ocho mensajes posibles expuestos anteriormente, que son un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar actualización de célula, un mensaje de confirmar actualización de URA y un mensaje de información de movilidad de UTRAN. El mensaje es pasado al bloque 230 de DCATH RRC de UE para procesamiento (paso s2). El módulo 230 de DCATH RRC de UE determina primero si el mensaje incluye el elemento de información de "información de modo de cifrado" (paso s3). Si es así, determina si existen portadores de radio que usan el modo transparente de control de radioenlace (paso s4). Si es así, el módulo 230 de DCATH RRC de UE comprueba la presencia del elemento de información de "tiempo de activación de cifrado para canal físico dedicado" (paso s5). Si este está presente, el procedimiento continúa y la nueva configuración de cifrado puede ser aplicada como se expone en la especificación 25.331 (paso s6). Si las respuestas a las pruebas planteadas en los pasos s3 y s4 son negativas, otro procesamiento apropiado del mensaje continuará de acuerdo con los procedimientos expuestos en la especificación 25.331 (paso s12).

Si la prueba en el paso s5 indica que el elemento de información de "tiempo de activación de cifrado para canal físico dedicado" está ausente, el módulo 230 de DCATH RRC de UE puede implementar uno de un número de procedimientos posibles.

En una primera realización, el módulo 230 de DCATH RRC de UE rechaza el mensaje y envía una respuesta a la UTRAN por vía de un transmisor 214 con un valor de retorno de error de CONFIGURACIÓN INVÁLIDA (INVALID_CONFIGURATION (paso S7).

En una segunda realización, el módulo 230 de DCATH RRC de UE rechaza el mensaje y envía una respuesta a la UTRAN con un valor de retorno de error de CONFIGURACIÓN NO SOPORTADA (UNSUPPORTED_ CONFIGURATION) (paso s8).

En una tercera realización, el módulo 230 de DCATH RC de UE selecciona un tiempo de activación adecuado para implementación de la configuración de cifrado (paso s9). El tiempo de activación puede ser el valor especial "Ahora" (paso s9A) de modo que el equipo de usuario (UE) aplica los cambios de cifrado inmediatamente (paso s10) y el procedimiento de cifrado continúa (paso s6). En este caso, es necesario que la UTRAN decida sobre un tiempo adecuado para comenzar el cifrado. El tiempo de activación seleccionado puede ser alternativamente el tiempo de activación de mensaje suministrado por la UTRAN en el elemento de información de "tiempo de activación" (paso s9B). Como antes, después de esta selección, el procedimiento de cifrado puede continuar (paso s6). En este caso se supone que la UTRAN implementa el mismo comportamiento.

En una realización adicional, el módulo 230 de DCATH RRC de UE selecciona el tiempo de activación independientemente de la UTRAN (paso s9C), por ejemplo, usando un método similar que el especificado en la sección 8.2.2.3 de la especificación 25.331, es decir que incluye el elemento de información de "tiempo de activación de CUENTA-C" y especificando un valor de número de cuadros de conexión (CFN: connection frame number) para este elemento de información que es un múltiplo de 8 cuadros (CFN módulo 8=0) y está situado al menos 200 cuadros delante del número de cuadros de conexión (CFN) en el que el mensaje de respuesta es transmitido primero. En contraste con las realizaciones descritas anteriormente con referencia a los pasos 9A y 9B, el tiempo de activación seleccionado es transmitido a la UTRAN con el mensaje de respuesta que usa el elemento de información de "tiempo de activación de CUENTA-C" (paso s11). Después de la transmisión, el procedimiento de cifrado puede continuar en el equipo de usuario (paso 6) mientras que la UTRAN usa el tiempo de activación transmitido para implementar el cambio de cifrado (paso S12a).

Aunque ejemplos del proceso de implementar la invención en el equipo de usuario (UE) han sido descritos anteriormente, es alternativamente posible implementar la invención en la UTRAN. Este ejemplo de la invención es ilustrado con referencia a las Figuras 2 y 4. La Figura 4 muestra los pasos realizados por un módulo de DCATH RRC de UTRAN para asegurar que el elemento de información de "tiempo de activación de cifrado para canal físico dedicado" es incluido en mensajes donde este es necesario.

La UTRAN 210 incluye un módulo 240 de DCATH RRC de UTRAN. Cuando un mensaje está siendo preparado para ser enviado al equipo de usuario (paso s20), que es uno de los ocho mensajes especificados anteriormente, es decir un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar actualización de célula, un mensaje de confirmar actualización de URA y un mensaje de información de movilidad de UTRAN, el mensaje es pasado al módulo 240 de DCATH RRC de UTRAN (paso s21). Esto determina si existe el elemento de información de "información de modo de cifrado" (paso s22). Si existe, el módulo 240 de DCATH RRC de UTRAN comprueba la existencia de portadores de radio en modo transparente (paso s23). Si estos existen, el módulo 240 de DCATH RRC de UTRAN inserta un elemento de información de "tiempo de activación de cifrado para canal físico dedicado" dentro del elemento de información

de “información de modo de cifrado” (paso s24) y transmite el mensaje al equipo de usuario (paso s25) por vía del transmisor 250 de UTRAN.

En el caso de que las respuestas a las pruebas en los pasos s22 y s23 sean negativas, cualquier otro procesamiento necesario es realizado entonces para el mensaje (paso s26) y el mensaje es transmitido (paso s25).

Volviendo ahora a la Figura 5, la Figura 5 es un esquema de bloques que ilustra un dispositivo móvil que puede actuar como un equipo de usuario (UE) y cooperar con el aparato y los métodos de las Figuras 1 a 4, y que es un dispositivo de comunicación inalámbrica ejemplar. La estación móvil 300 es preferiblemente un dispositivo de comunicación inalámbrica bidireccional que tiene al menos capacidades de comunicación de voz y datos. La estación móvil 300 tiene preferiblemente la capacidad de comunicar con otros sistemas de ordenador en Internet. Dependiendo de la funcionalidad exacta proporcionada, el dispositivo inalámbrico puede ser denominado como un dispositivo de mensajería de datos, un buscapersonas bidireccional, un dispositivo de correo electrónico inalámbrico, un teléfono celular con capacidades de mensajería de datos, un aparato de Internet inalámbrico o un dispositivo de comunicación de datos, como ejemplos.

Donde la estación móvil 300 está capacitada para comunicación bidireccional, incluirá un subsistema 311 de comunicación que incluye tanto un receptor 312 como un transmisor 314 así como componentes asociados tales como uno o más elementos 316 y 318 de antenas, preferiblemente incrustados o internos, osciladores locales (OLs) 313 y un módulo de procesamiento tal como un procesador de señales digitales (PSD) 320. Como será evidente para los expertos en el campo de las comunicaciones, el diseño particular del subsistema 311 de comunicación dependerá de la red de comunicación en la que el dispositivo está destinado a funcionar. Por ejemplo, la estación móvil 300 puede incluir un subsistema 311 de comunicación diseñado para funcionar dentro del sistema de comunicación móvil Mobitex™, el sistema de comunicación móvil Data TAC™, una red GPRS (General Packet Radio Service), una red UMTS (Universal Mobile Telecommunications System) o una red EDGE (Enhanced Data rates for GSM Evolution).

Las exigencias de acceso a red también variarán dependiendo del tipo de red 319. Por ejemplo, en las redes Mobitex y Data TAC, la estación móvil 300 es registrada en la red usando un número único de identificación asociado con cada estación móvil. Sin embargo, en las redes UMTS y GPRS, el acceso a red está asociado con un abonado o usuario de estación móvil 300. Por tanto, una estación móvil GPRS necesita una tarjeta de módulo de identidad de abonado (SIM: subcriber identity module) para funcionar en una red GPRS. Sin una tarjeta válida de módulo de identidad de abonado (SIM), una estación móvil GPRS no será completamente funcional. Las funciones de comunicación locales o no de red, así como las funciones requeridas legalmente (si las hay) tal como la llamada de emergencia “911”, pueden estar disponibles pero la estación móvil 300 será incapaz de realizar cualesquiera otras funciones que impliquen comunicaciones por la red 319. La interfaz 344 de SIM es normalmente similar a una ranura de tarjeta dentro de la que una tarjeta SIM puede ser insertada y expulsada como un disquete o tarjeta PCMCIA (Personal Computer Memory Card International Association). La tarjeta SIM puede tener 64 K de memoria aproximadamente y contener muchas configuraciones 351 de claves y otra información 353 tal como identificación e información relacionada con el abonado.

Cuando los procedimientos necesarios de registro o activación de red han sido completados, la estación móvil 300 puede enviar y recibir señales de comunicación por la red 319. Las señales recibidas por la antena 316 a través de la red 319 de comunicación son introducidas en el receptor 312 que puede realizar tales funciones corrientes de receptor como amplificación de señales, reducción de frecuencia, filtración, selección de canales, etc. y, en el sistema ejemplar mostrado en la Figura 5, la conversión analógica a digital (A/D). La conversión A/D de una señal recibida permite que funciones de comunicación más complejas, tales como desmodulación y descodificación, sean realizadas en el procesador 320 de señales digitales (PSD). De una manera similar, las señales a ser transmitidas son procesadas, incluyendo modulación y codificación por ejemplo, por el procesador 320 de señales digitales (PSD) e introducidas en el transmisor 314 para conversión digital a analógica, aumento de frecuencia, filtración, amplificación y transmisión por la red 319 de comunicación por vía de la antena 318. El procesador 320 de señales digitales no solo procesa señales de comunicación sino que también se encarga del control del receptor y del transmisor. Por ejemplo, las ganancias aplicadas a las señales de comunicación en el receptor 312 y el transmisor 314 pueden ser controladas adaptablemente mediante algoritmos de control automático de ganancia implementados en el procesador 320 de señales digitales.

La estación móvil 300 incluye preferiblemente un microprocesador 338 que controla el funcionamiento global del dispositivo. Las funciones de comunicación, que incluyen al menos comunicaciones de datos y de voz, son realizadas mediante el subsistema 311 de comunicación. El microprocesador 338 también interacciona con subsistemas adicionales de dispositivo tales como la pantalla 322, la memoria flash 324, la memoria 326 de acceso aleatorio (RAM), los subsistemas auxiliares (328) de entrada/salida (E/S), el puerto 330 en serie, el teclado 332, el altavoz 334, el micrófono 336, un subsistema 340 de comunicaciones de corto alcance y cualesquier otros subsistemas de dispositivo designados generalmente como 342.

Algunos de los subsistemas mostrados en la Figura 5 realizan funciones relacionadas con la comunicación mientras que otros sistemas pueden proporcionar funciones “residentes” o en el dispositivo. Notablemente, algunos subsistemas, tales como el teclado 332 y la pantalla 322 por ejemplo, pueden ser usados tanto para funciones relacionada con la comunicación, tal como introducir un mensaje de texto para transmisión por una red de comunicación, como para funciones residentes en el dispositivo tales como una calculadora o lista de tareas.

El software de sistema operativo usado por el microprocesador 338 es almacenado preferiblemente en un almacenamiento persistente tal como la memoria flash 324, que puede ser en cambio una memoria de solo lectura (ROM) o elementos de almacenamiento similar (no mostrado). Los expertos en la técnica apreciarán que el sistema operativo, aplicaciones específicas de dispositivo, o partes de ellas, pueden ser cargadas temporalmente en una memoria volátil tal como la RAM 326. Las señales de comunicación recibidas también pueden ser almacenadas en la memoria RAM 326.

Como se muestra, la memoria flash 324 puede ser separada en áreas diferentes tanto para programas 358 de ordenador como para almacenamiento 350, 352, 354 y 356 de datos de programas. Estos tipos de almacenamiento diferentes indican que cada programa puede asignar una porción de memoria flash 324 para sus propias exigencias de almacenamiento de datos. El microprocesador 338, además de sus funciones de sistema operativo, permite preferiblemente la ejecución de aplicaciones de software en la estación móvil. Un conjunto predeterminado de aplicaciones que controlan operaciones básicas, incluyendo al menos aplicaciones de comunicación de datos y de voz por ejemplo, serán instaladas normalmente en la estación móvil 300 durante la fabricación. Una aplicación preferida de software (PIM: personal information manager = gestor de información personal) que tiene la capacidad de organizar y gestionar elementos de datos relativos al usuario de la estación móvil tales como, pero no limitados a, correo electrónico (e-mail), acontecimientos de calendario, correos de voz, compromisos y elementos de tareas. Naturalmente, uno o más almacenamientos de memoria estarían disponibles en la estación móvil para facilitar el almacenamiento de elementos de datos de gestor de información personal (PIM). Tal aplicación de gestor de información personal (PIM) tendría preferiblemente la capacidad de enviar y recibir elementos de datos por vía de la red inalámbrica 319. En una realización preferida, los elementos de datos de PIM son integrados sin uniones, sincronizados y actualizados, por vía de una red inalámbrica 319, con los elementos de datos correspondientes de usuario de estación móvil almacenados o asociados con un sistema de ordenador principal. Aplicaciones adicionales también pueden ser cargadas en la estación móvil 300 a través de la red 319, un subsistema 328 de entrada/salida (E/S) auxiliar, el puerto 330 en serie, el subsistema 340 de comunicaciones de corto alcance o cualquier otro subsistema 342 adecuado, e instaladas por un usuario en la memoria RAM 326 o preferiblemente un almacenamiento no volátil (no mostrado) para ejecución por el microprocesador 338. Tal flexibilidad en la instalación de aplicaciones aumenta la funcionalidad del dispositivo y puede proporcionar funciones mejoradas en el dispositivo, funciones relacionadas con la comunicación o ambas. Por ejemplo, aplicaciones de comunicación protegida pueden permitir que funciones de comercio electrónico y otras transacciones financieras tales sean realizadas usando la estación móvil 300.

En un modo de comunicación de datos, una señal recibida tal como un mensaje de texto o descarga de página Web será procesada por el subsistema 311 de comunicación e introducida en el microprocesador 338 que preferiblemente procesa además la señal recibida para salida a la pantalla 322 o, alternativamente, a un dispositivo 328 de entrada/salida (E/S) auxiliar. Un usuario de estación móvil 300 también puede componer elementos de datos, tales como mensajes de correo electrónico (e-mail) por ejemplo, usando el teclado 332, que es preferiblemente un teclado alfanumérico completo o teclado auxiliar de tipo teléfono, en conjunción con la pantalla 322 y posiblemente un dispositivo 328 de entrada/salida (E/S) auxiliar. Después, tales elementos compuestos pueden ser transmitidos por una red de comunicación a través del subsistema 311 de comunicación.

Para comunicaciones de voz, el funcionamiento global de la estación móvil 300 es similar excepto en que las señales recibidas serían extraídas preferiblemente a un altavoz 334 y las señales para transmisión serían generadas por un micrófono 336. Subsistemas alternativos de entrada/salida de voz o audio, tal como un subsistema de grabación de mensajes de voz, también pueden ser implementados en la estación móvil 300. Aunque la salida de señales de voz o audio es efectuada preferiblemente de modo principal a través del altavoz 334, la pantalla 322 también puede ser usada para proporcionar una indicación de la identidad de un corresponsal que llama, la duración de una llamada de voz u otra información relacionada con llamada de voz por ejemplo.

En la Figura 5, el puerto 330 en serie sería implementado normalmente en una estación móvil de tipo asistente digital personal para la que la sincronización con un ordenador de sobremesa de usuario (no mostrado) puede ser deseable, pero es un componente opcional de dispositivo. Tal puerto 330 permitiría que un usuario establezca preferencias mediante un dispositivo externo o aplicación de software y ampliaría las capacidades de la estación móvil 300 proveyendo descargas de software o información a la estación móvil 300 distintas que a través de una red de comunicación inalámbrica. El trayecto alternativo de descarga puede ser usado por ejemplo para cargar una clave criptográfica en el dispositivo a través de una conexión directa, y por tanto fiable y de confianza, para permitir de tal modo la comunicación protegida del dispositivo.

Otros subsistemas 340 de comunicaciones, tal como un subsistema de comunicaciones de corto alcance, son componentes opcionales adicionales que pueden proveer comunicación entre la estación móvil 300 y sistemas o dispositivos diferentes que no necesitan ser necesariamente dispositivos similares. Por ejemplo, el subsistema 340 puede incluir un dispositivo de infrarrojos y circuitos y componentes asociados o un módulo de comunicación Bluetooth™ para proveer comunicación con sistemas y dispositivos capacitados de modo similar.

Cuando el dispositivo móvil 300 es usado como un equipo de usuario, las pilas 346 de protocolo incluyen un método y un aparato para procesar mensajes en un sistema universal de telecomunicaciones móviles.

Las realizaciones antes descritas de la presente solicitud pretenden ser ejemplos solamente. Los expertos en la técnica pueden efectuar alteraciones, modificaciones y variaciones en las realizaciones particulares sin apartarse del alcance de la solicitud como es definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para procesar un mensaje (215) recibido en un equipo (220) de usuario en un sistema (100) de comunicaciones UMTS, en el que el mensaje incluye un elemento de información de información de modo de cifrado y es uno de una pluralidad de tipos de mensajes que comprenden un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar actualización de célula, un mensaje de confirmar autorización de URA y un mensaje de información de movilidad de UTRAN, comprendiendo el método:

determinar si un elemento de información de tiempo de activación de cifrado para canal físico dedicado está presente en el mensaje (s3) cuando existen portadores de radio que usan modo transparente de control de radioenlace: y

en el caso de que el elemento de información de tiempo de activación de cifrado para canal físico dedicado no esté presente, devolver un mensaje que indica la ausencia de dicho elemento de información de tiempo de activación de cifrado para canal físico dedicado.

2. Un método según la reivindicación 1, en el que el paso de devolver un mensaje que indica la ausencia del elemento de información de tiempo de activación de cifrado para canal físico dedicado comprende devolver un mensaje que incluye el valor CONFIGURACIÓN INVÁLIDA (INVALID_CONFIGURATION) (s7).

3. Un método según la reivindicación 1, en el que el paso de devolver un mensaje que indica la ausencia del elemento de información de tiempo de activación de cifrado para canal físico dedicado comprende devolver un mensaje que incluye el valor CONFIGURACIÓN NO SOPORTADA (UNSUPPORTED_CONFIGURATION) (s8).

4. Un método según la reivindicación 1, que comprende el paso adicional, en el caso de que el elemento de información de tiempo de activación de cifrado para canal físico dedicado no esté presente, de seleccionar un tiempo de activación para aplicar cambios de cifrado para los portadores de radio (s9).

5. Un método según la reivindicación 4, en el que el paso de seleccionar el tiempo de activación para aplicar cambios de cifrado comprende usar un tiempo de activación de mensaje recibido desde la UTRAN (s9B).

6. Un método según la reivindicación 5, en el que el tiempo de activación de mensaje está incluido en el elemento de información de tiempo de activación.

7. Un método según la reivindicación 4, que comprende, en ausencia de un elemento de información de tiempo de activación, usar un tiempo de activación de AHORA (S9a).

8. Un método según la reivindicación 4, en el que el paso de seleccionar un tiempo de activación comprende seleccionar un tiempo de activación en el equipo de usuario (UE) independientemente de la UTRAN y enviar un mensaje de respuesta que incluye el tiempo de activación seleccionado a la UTRAN (s9C).

9. Un método según la reivindicación 8, que comprende devolver el tiempo de activación seleccionado usando un elemento de información de tiempo de activación de CUENTA-C (s11).

10. Un método según la reivindicación 8, que comprende además recibir el tiempo de activación seleccionado en la UTRAN y usar el tiempo de activación recibido como el tiempo de aplicar cambios de cifrado para portadores de radio en modo transparente (s12).

11. Un método según la reivindicación 4, que comprende seleccionar un tiempo de activación de AHORA para aplicar inmediatamente cambios de cifrado para portadores de radio en modo transparente (s10).

12. Equipo (220) de usuario para recibir un mensaje (215) en un sistema (100) de comunicaciones UMTS, en el que el mensaje incluye un elemento de información de información de modo de cifrado y es uno de una pluralidad de tipos de mensajes que comprenden un mensaje de establecimiento de portador de radio, un mensaje de reconfiguración de portador de radio, un mensaje de desconexión de portador de radio, un mensaje de reconfiguración de canal de transporte, un mensaje de reconfiguración de canal físico, un mensaje de confirmar autorización de célula, un mensaje de confirmar actualización de URA y un mensaje de información de movilidad de UTRAN, comprendiendo el equipo de usuario:

un módulo (230) de control configurado para determinar si un elemento de información de tiempo de activación de cifrado para canal físico dedicado está presente en el mensaje cuando existen portadores de radio que usan modo transparente (TM) de control de radioenlace (RLC); y

un transmisor (214) para devolver un mensaje que indica la ausencia del elemento de información en el caso de que el elemento de información de tiempo de activación de cifrado para canal físico dedicado no esté presente.

13. Equipo de usuario (UE) según la reivindicación 12, que comprende además que el módulo (230) de control está configurado para seleccionar un tiempo de activación para aplicar cambios de cifrado para los portadores de radio en el caso de que el elemento de información de tiempo de activación de cifrado para canal físico dedicado no esté presente.

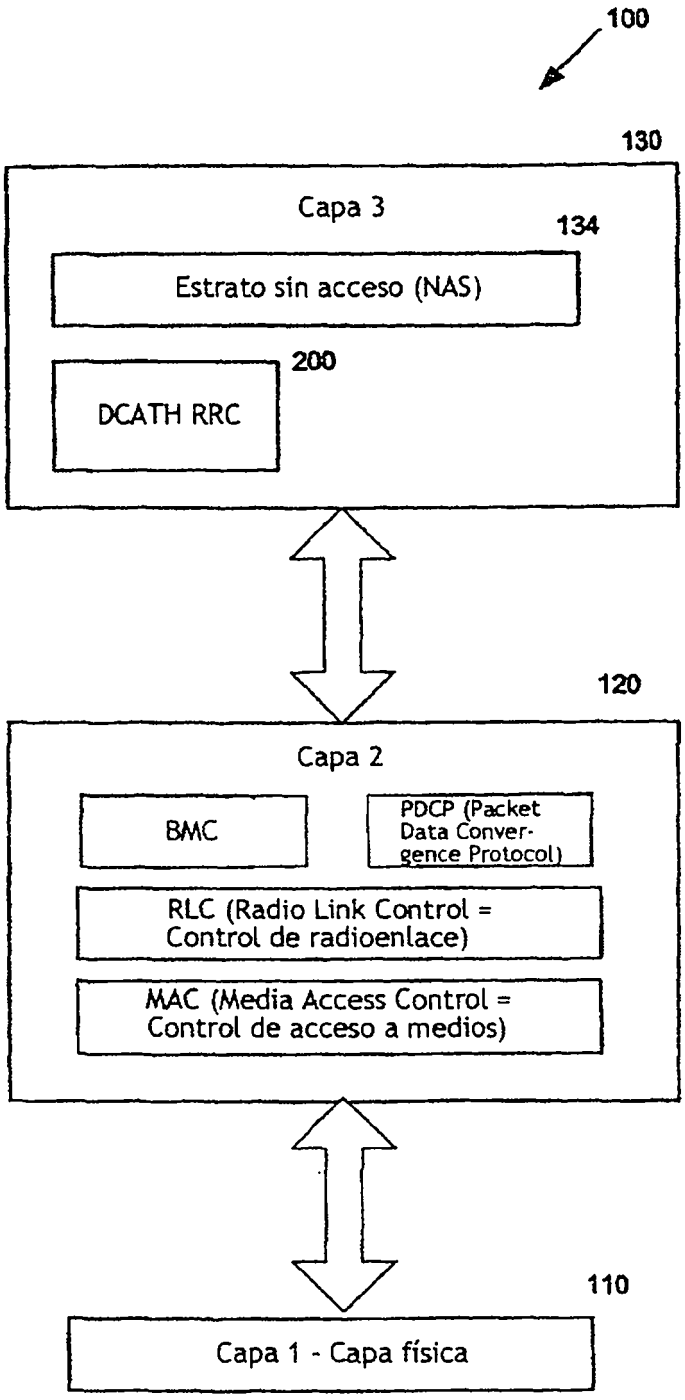
100
130
Capa 3
134
Estrato sin acceso (NAS)
200
DCATH RRC
120
Capa 2
BMC
PDCP (Packet Data Conver-gence Protocol)
RLC (Radio Link Control = Control de radioenlace)
MAC (Media Access Control = Control de acceso a medios)
110
Capa 1 - Capa física

Figura 1

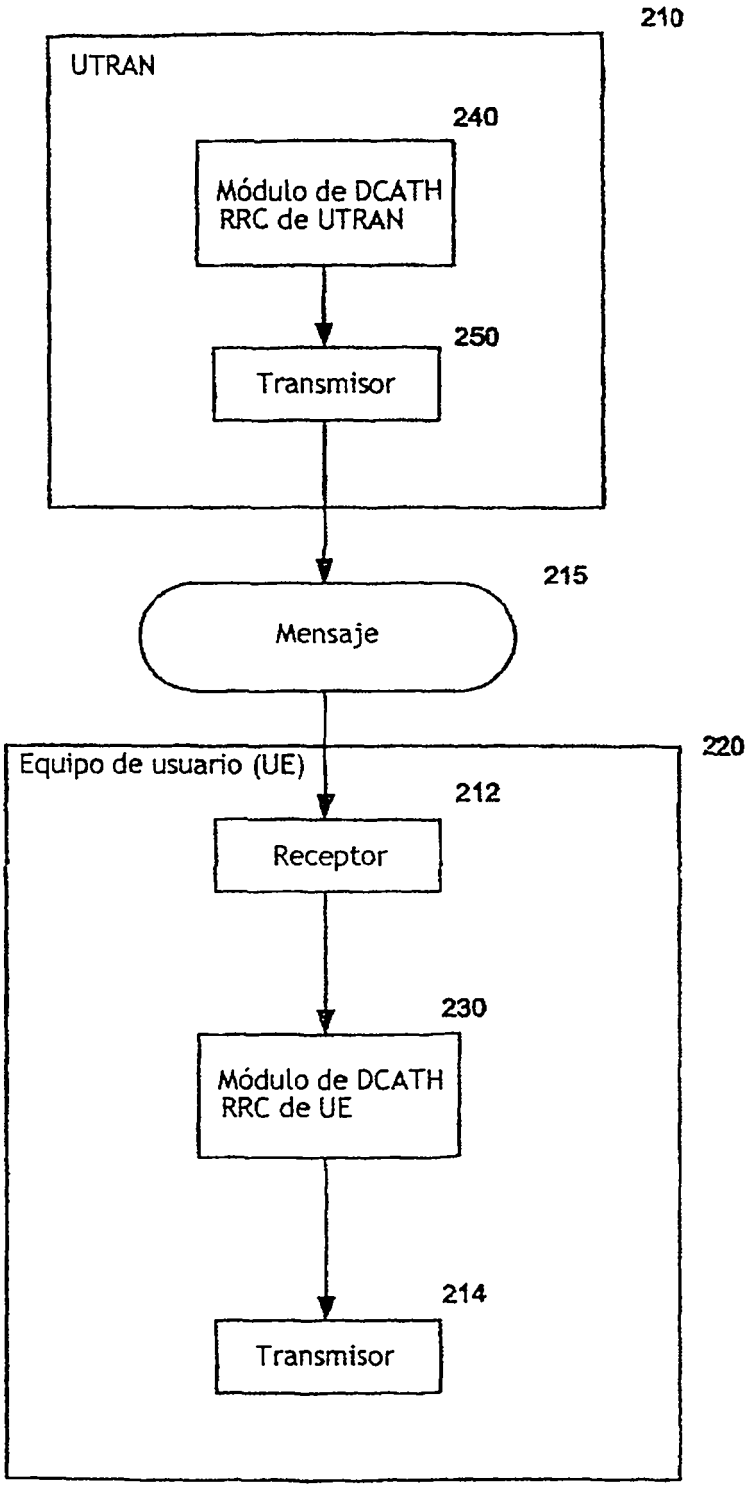
210
UTRAN
240
Módulo de DCATH RRC de UTRAN
250
Transmisor
215
Mensaje
220
Equipo de usuario (UE)
212
Receptor
230
Módulo de DCATH RRC de UE
214
Transmisor

Figura 2

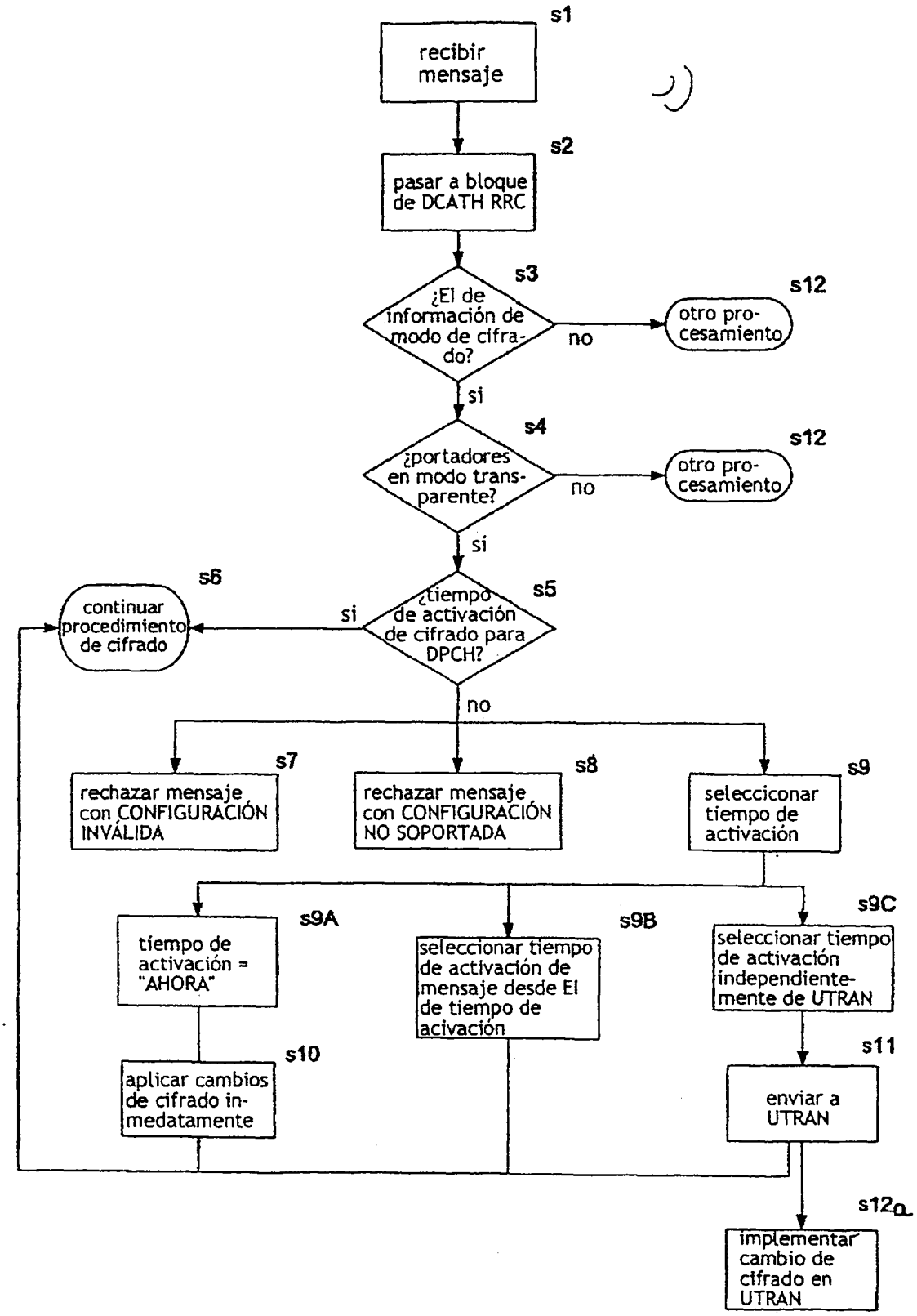
s1
recibir mensaje
s2
pasar a bloque de DCATH RRC
s3
¿El de información de modo de cifrado?
no
s12
otro procesamiento
si
s4
¿portadores en modo transparente?
no
s12
otro procesamiento
si
s5
¿tiempo de activación de cifrado para DPCH?
si
s6
continuar procedimiento de cifrado
no
s7
rechazar mensaje con CONFIGURACIÓN INVÁLIDA
s8
rechazar mensaje con CONFIGURACIÓN NO SOPORTADA
s9
selecciconar tiempo de activación
s9A
tiempo de activación = "AHORA"
s10
aplicar cambios de cifrado inmedatamente
s9B
seleccionar tiempo de activación de mensaje desde El de tiempo de acivación
s9C
seleccionar tiempo de activación independientemente de UTRAN
s11
enviar a UTRAN
s12a
implementar cambio de cifrado en UTRAN

Figura 3

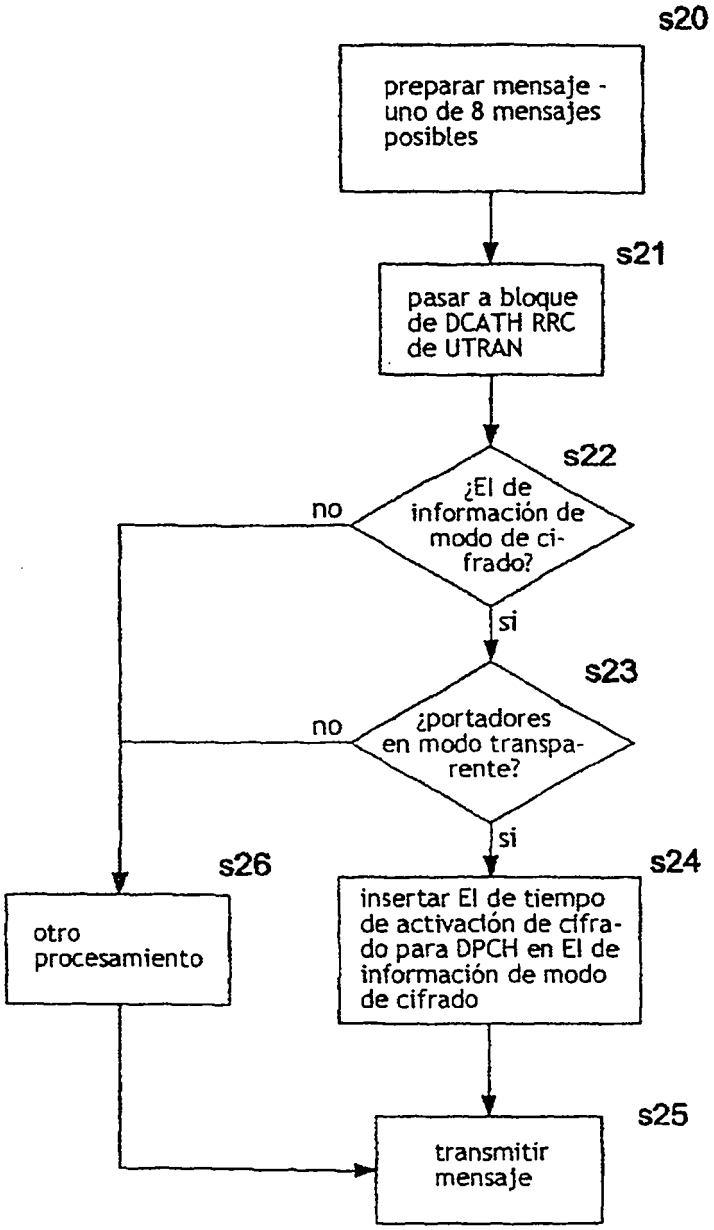
s20
preparar mensaje - uno de 8 mensajes posibles
s21
pasar a bloque de DCATH RRC de UTRAN
s22
¿El de información de modo de cifrado?
no
si
s23
¿portadores en modo transparente?
no
si
s24
insertar El de tiempo de activación de cifrado para DPCH en El de información de modo de cifrado
s25
transmitir mensaje
s26
otro procesamiento

Figura 4

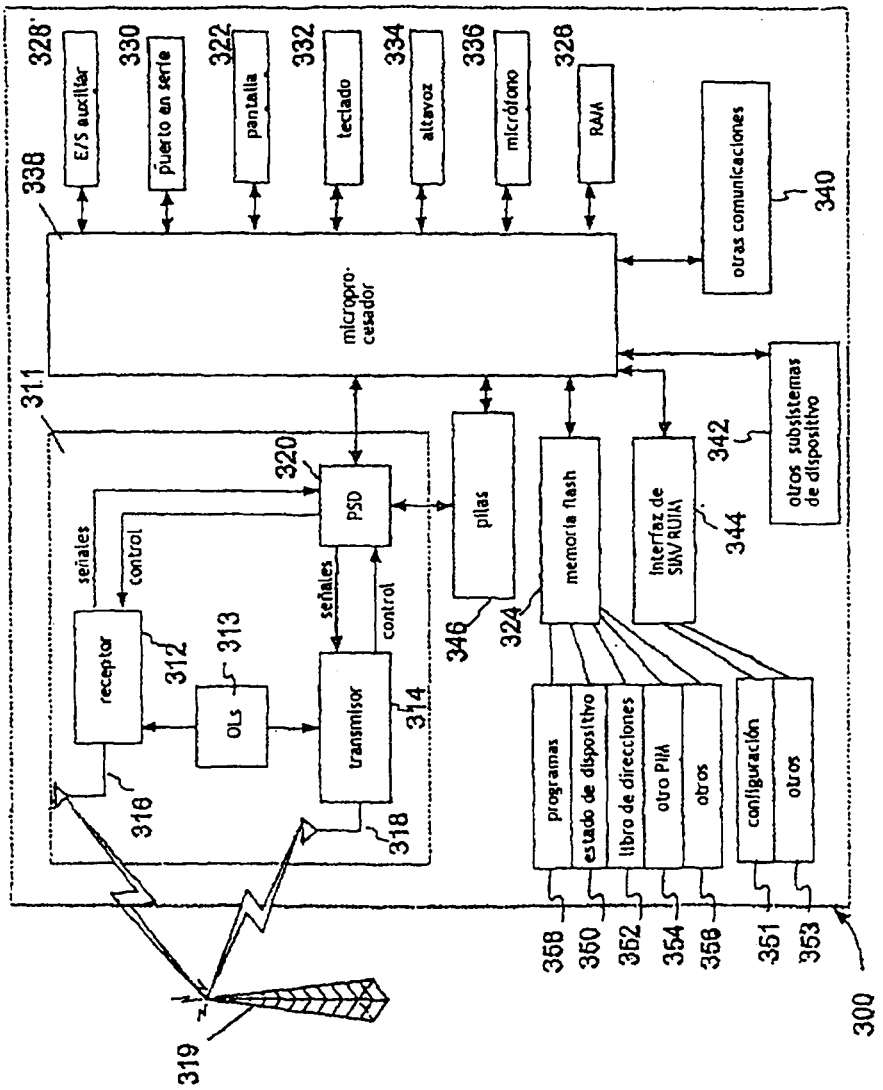
328
E/S auxiliar
330
puerto en serie
322
pantalla
332
teclado
334
altavoz
336
micrófono
328
RAM
338
otras comunicaciones
340
micropro-cesador
311
320
PSD
señales
control
receptor
312
313
OLS
transmisor
314
pilas
346
324
memoria flash
Interfaz de SIM/RUIM
342
344
otros subsistemas de dispositivo
316
318
319
programas
estado de dispositivo
libro de direcciones
otro PIM
otros
configuración
otros
348
350
352
354
356
351
353
300

Figura 5