(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 738 886**

(51) Int. CI.:

H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.01.2014 PCT/EP2014/051108**

(87) Fecha y número de publicación internacional: **18.09.2014 WO14139709**

(96) Fecha de presentación y número de la solicitud europea: **21.01.2014 E 14705051 (2)**

(97) Fecha y número de publicación de la concesión europea: **05.06.2019 EP 2974421**

(54) Título: **Dispositivos de comunicación y estación base de radio celular de área extensa**

(30) Prioridad:

14.03.2013 US 201313803241

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.01.2020

(73) Titular/es:

INTEL DEUTSCHLAND GMBH (100.0%)
Am Campeon 10-12
85579 Neubiberg, DE

(72) Inventor/es:

SCHMIDT, ANDREAS;
BIENAS, MAIK;
LUFT, ACHIM y
HANS, MARTIN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Dispositivos de comunicación y estación base de radio celular de área extensa

Campo técnico

Diversos aspectos de esta divulgación se relacionan, en general, con los dispositivos de comunicación y la estación base de radio celular de área extensa.

Antecedentes

Diversas computadoras portátiles tienen una funcionalidad especial antirrobo. Dichos dispositivos se conectan periódicamente o esporádicamente a un servidor de seguridad donde el dispositivo y el propietario están registrados. Una vez que el dispositivo se ha perdido o ha sido robado, el propietario puede cambiar el estado del dispositivo a "perdido/robado" en un servidor de seguridad proporcionado. La próxima vez que se encienda el dispositivo, se conectará al servidor de seguridad, leerá el nuevo estado y el dispositivo se desactivará, de modo que nadie más pueda utilizarlo. El dispositivo podría volver a ser utilizable, si el propietario cambia el estado de nuevo a "normal" en el servidor de seguridad.

Además de la desactivación "basada en el estado del servidor", también se implementa una desactivación basada en temporizador. Esto es para el caso de que el dispositivo robado o perdido no se haya conectado a Internet después de que se haya perdido o haya sido robado. En este caso, se desactivará automáticamente si el temporizador se inicia después de que expire la última conexión exitosa al servidor de seguridad. Este temporizador se mantiene en el dispositivo.

En este sistema, la persona que lo encuentra puede utilizar el dispositivo hasta la expiración del temporizador si logra evitar que el dispositivo se conecte a Internet. El propietario (a quien también se hará referencia como "usuario autorizado") puede permitir que el dispositivo utilice su suscripción móvil en el dispositivo para conectarse a Internet para tales casos, p. ej., deshabilitando permanentemente la solicitud del PIN (Número de Identificación Personal) en caso de que el módem celular está activado, pero luego la persona que lo encontró puede hacer fácilmente mala utilización de la suscripción y potencialmente generar altas tarifas de conexión para el propietario del dispositivo.

El propietario podría configurar el valor del temporizador muy pequeño para limitar el período de utilización engañosa, pero esto puede hacer que la utilización sea muy incómoda para el usuario, p. ej., en caso de que se olvide de conectarse a Internet dentro de este pequeño período de tiempo, el dispositivo se bloqueará incluso para el propietario autorizado. Por lo tanto, es muy probable que la mayoría de los usuarios establezcan el temporizador en el valor máximo.

Otra característica convencional que también se conoce como "llamada de emergencia", permite que un dispositivo móvil realice una llamada de voz a un centro de llamadas de emergencia predefinido sin necesidad de una (U)SIM. Para la identificación se utiliza la Identidad Internacional de Equipo de Móvil (IMEI) del identificador (ID) del dispositivo del módem celular. En este caso, no se pudo establecer una conexión de datos, un proveedor de servicios de seguridad no puede ofrecer dicho servicio de seguridad mientras se le cobra la conexión de datos y las instrucciones del propietario del dispositivo no se podrían enviar al dispositivo.

Otra característica convencional que también se conoce como "Ecall" permite a un módem celular especial en un automóvil transmitir a un centro de emergencia predefinido datos de emergencia en caso de un accidente. Este servicio requiere una (U)SIM y no podría utilizarse para bloquear el automóvil en caso de pérdida o robo.

El documento US 2012/172039 A1 enseña un sistema y un método para asegurar un terminal perdido utilizando una red inalámbrica. El sistema incluye un servidor de registro de terminales perdidos para almacenar información de terminal única de un terminal perdido y un terminal que incluye un módulo inalámbrico de Red de Área Local (LAN) para conectarse al servidor de registro de terminales perdidos para determinar si el terminal está registrado como un terminal perdido en el servidor de registro de terminales perdidos. Si se determina que el terminal es un terminal perdido, entonces el terminal perdido se puede rastrear y/o bloquear para asegurar el terminal.

El documento US 2010/151884 A1 enseña un método para monitorizar un teléfono inteligente que incluye activar una función de conexión de red, conectarse a un dispositivo servidor a través de la función de conexión de red para recibir una señal de indicación que indica un estado perdido del teléfono inteligente y devolver información del teléfono inteligente al dispositivo servidor a través de la función de conexión de red cuando la señal de indicación indica que el teléfono inteligente se ha perdido.

Resumen

Se da a conocer una estación base de radio celular de área extensa, de acuerdo con la reivindicación 1, y un método para operar una estación base de radio celular de área extensa, de acuerdo con la reivindicación 2.

Breve descripción de los dibujos

En los dibujos, los caracteres de referencia similares, generalmente, se refieren a las mismas partes en las diferentes vistas. Los dibujos no están necesariamente a escala, sino que el énfasis generalmente se pone en ilustrar los principios de la invención. En la siguiente descripción, se describen diversas realizaciones de la invención con referencia a los siguientes dibujos, en los que:

la FIG. 1 muestra una arquitectura de sistema de comunicación;

la FIG. 2 muestra un diagrama de flujo de mensajes que ilustra un método de acuerdo con diversos aspectos de esta divulgación;

la FIG. 3 muestra una estación base;

la FIG. 4 muestra un servidor de seguridad;

la FIG. 5 muestra un diagrama de flujo que ilustra un método para operar un dispositivo de comunicación;

la FIG. 6 muestra un diagrama de flujo que ilustra un método para operar un dispositivo de comunicación; y

la FIG. 7 muestra un diagrama de flujo que ilustra un método para operar una estación base de radio celular de área extensa.

Descripción

La siguiente descripción detallada se refiere a los dibujos adjuntos que muestran, a modo de ilustración, detalles específicos y realizaciones en las que se puede poner en práctica la invención.

La palabra “ejemplar” se utiliza en el presente documento para indicar “que sirve como un ejemplo, instancia o ilustración”. Cualquier realización o diseño descrito en el presente documento como “ejemplar” no debe interpretarse necesariamente como preferido o ventajoso sobre otras realizaciones o diseños.

En lo que sigue, un “circuito” puede entenderse como cualquier tipo de entidad que implementa lógica, que puede ser hardware, software, firmware o cualquier combinación de los mismos. Por lo tanto, un “circuito” puede ser un circuito lógico cableado o un circuito lógico programable, tal como un procesador programable, p. ej., un microprocesador (p. ej., un procesador de Computador con Conjunto de Instrucciones Complejas (CISC) o un procesador de Computador con Conjunto de Instrucciones Reducidas (RISC)). Como se describirá con más detalle a continuación, un “circuito” también puede ser software que se implementa o ejecuta por un procesador, p. ej., cualquier tipo de programa informático, p. ej., un programa informático que utiliza un código de máquina virtual, tal como, p. ej., Java. Cualquier otro tipo de implementación de las respectivas funciones que se describirá con más detalle a continuación, también puede entenderse como un “circuito”.

Los términos “acoplamiento” o “conexión” pretenden incluir un “acoplamiento” directo o una “conexión” directa, así como un “acoplamiento” indirecto o una “conexión” indirecta, respectivamente.

El término “protocolo” pretende incluir cualquier pieza de software, que se proporciona para implementar parte de cualquier capa de la definición de comunicación. “Protocolo” puede incluir la funcionalidad de una o más de las siguientes capas: capa física (capa 1), capa de enlace de datos (capa 2), capa de red (capa 3) o cualquier otra subcapa de las capas mencionadas o cualquiera capa superior.

Diversos aspectos de esta divulgación proporcionan una conexión de datos sin SIM con cobro de terceros.

Diversos aspectos de esta divulgación proporcionan mecanismos para

- cómo hacer que un dispositivo robado o perdido (en general, un dispositivo que ha salido de manera no deseada fuera del control del usuario autorizado) que incluye un módem celular, sea menos atractivo (inutilizable) para la persona que lo encontró no autorizada;

- cómo ayudar al propietario de un dispositivo robado o perdido (en general, un dispositivo que ha salido de manera no deseada fuera de control del usuario autorizado) que incluye un módem celular a encontrar su dispositivo; y

- cómo proteger los datos sensibles del propietario en caso de que se pierda o sea robado (en general, que ha salido de manera no deseada fuera del control del usuario autorizado).

Las tres características anteriores pueden habilitarse sin la necesidad de una SIM (Módulo de Identificación del Abonado) o USIM (Módulo de Identificación del Abonado del UMTS (Sistema Universal de Telecomunicaciones Móviles)), de modo que funcione incluso en caso de que el ladrón retire la SIM o la USIM.

Se puede proporcionar un sistema que permita detectar que un dispositivo ha salido de manera no deseada fuera del control del usuario autorizado, p. ej., que un dispositivo se ha perdido o ha sido robado, y para establecer una conexión de comunicación desde el dispositivo, p. ej., perdido o robado, a un servidor predefinido utilizando un módem celular sin la necesidad de utilizar la suscripción móvil de un propietario, es decir, sin requerir la SIM o la USIM del usuario (o de cualquier otra persona).

Como se describirá con más detalle a continuación, diversos aspectos de esta divulgación ofrecen diversas funcionalidades nuevas, tales como:

- El dispositivo de comunicación detecta automáticamente que está potencialmente fuera del control del usuario autorizado, p. ej., perdido o robado.

Otros escenarios en los que el dispositivo de comunicación está fuera del control del usuario autorizado se pueden ver en un extravío o reemplazo del dispositivo de comunicación, una destrucción (no deseada) del dispositivo de comunicación, una activación no autorizada del dispositivo de comunicación y similares. En otras palabras, el dispositivo de comunicación puede considerarse como operado o controlado sin el consentimiento o permiso del usuario autorizado.

- Después de la detección: el dispositivo de comunicación (p. ej., automáticamente) establece una “conexión de datos sin SIM” a un dispositivo servidor predefinido (p. ej., una computadora servidor) utilizando un módem celular del dispositivo de comunicación sin requerir una (U)SIM (es decir, p. ej., el dispositivo perdido o robado (o el dispositivo de comunicación que está generalmente fuera del control del usuario autorizado) puede habilitarse para iniciar de forma autónoma un tipo especial de establecimiento de conexión de comunicación) para:

-- obtener instrucciones de seguridad del propietario (es decir, del propietario del dispositivo de comunicación) (p. ej., “Bloquear mi dispositivo de comunicación. Se ha perdido o ha sido robado”); y/o

-- enviar la ubicación actual del dispositivo de comunicación para rastrear el dispositivo de comunicación.

- El dispositivo de comunicación puede tomar la o las acciones apropiadas después de obtener las instrucciones de seguridad del propietario del dispositivo de comunicación, p. ej., está bloqueado y/o hacerlo inutilizable y/o la información sensible puede encriptarse.

- Una vez que el dispositivo de comunicación ha establecido la conexión de comunicación de datos sin SIM, el propietario del dispositivo de comunicación puede forzarlo para permanecer en modo inactivo (p. ej., en modo inactivo de RRC (Control de Recursos de Radio)) en la red de comunicación por radio móvil celular (es decir, puede contactarse por la red de comunicación por radio móvil celular y puede realizar procedimientos en modo inactivo (p. ej., RRC) como “rastrear actualizaciones del área”) para:

-- obtener instrucciones de seguridad del propietario (es decir, del propietario del dispositivo de comunicación); y/o

-- enviar la ubicación actual del dispositivo de comunicación para rastrear el dispositivo de comunicación.

- Para la autorización, se genera un ID (identificador) único mediante un circuito criptográfico (que puede incluir o implementarse por medio de un Módulo de Plataforma de Confianza (TPM) a partir de un identificador único de un circuito del dispositivo de comunicación (p. ej., un CPU-ID (en lugar de utilizar credenciales de la (U)SIM o un ID de circuito de memoria (p. ej., una memoria de unidad de estado sólido) o un circuito de comunicación (p. ej., una Dirección de MAC (Control de Acceso al Medio)) o un identificador único del propio TPM, o cualquier otro ID único de un circuito del dispositivo de comunicación o una combinación de dos o más ID relacionados con hardware o software. El TPM (en general, el circuito criptográfico) puede almacenar claves criptográficas y puede configurarse para calcular una Identidad de CPU temporal, por ejemplo.

Un ID único puede entenderse como un identificador que es único en la arquitectura de comunicación involucrada, de modo que el respectivo circuito al que se asigna el ID único puede identificarse de manera inequívoca (p. ej., por un servidor de seguridad, como se describirá con más detalle a continuación). A modo de ejemplo, el ID único puede ser un valor hexadecimal que consta de 16 dígitos, p. ej., “BFEBFBFF00012345”, asignado al respectivo circuito (p. ej., ya por el fabricante del circuito), que no puede (o difícilmente) alterarse por el propietario del dispositivo de comunicación.

Como también se describirá con más detalle a continuación, se puede utilizar un nuevo tipo de conexión de comunicación que se indica mediante el dispositivo de comunicación en el establecimiento de conexión de comunicación (p. ej., radio móvil). La conexión de comunicación puede tener las siguientes propiedades:

- No se necesita SIM o USIM.

- La conexión de comunicación (p. ej., radio móvil) solo se establece si ciertas condiciones previas son válidas, p. ej., se detecta la pérdida del dispositivo de comunicación (como se describirá más adelante en esta memoria descriptiva).

- La conexión de comunicación no se inicia por humanos, sino que se inicia por un dispositivo de comunicación.

- La conexión de comunicación se establece solo para un determinado destino predefinido, p. ej., un servidor predefinido o una dirección predefinida.

- La conexión de comunicación se puede cobrar a un tercero que ofrece dichos servicios antirrobo, p. ej., la parte que proporciona el servidor de seguridad.

- La conexión de comunicación podría establecerse solo en caso de que se cumplan algunas o todas las siguientes condiciones. Esto puede evitar la utilización no permitida del servicio:

-- el circuito solicitante (p. ej., la CPU (unidad central de procesamiento) solicitante) puede registrarse en el transmisor (p. ej., un módem celular) del dispositivo de comunicación. Por lo tanto, el servidor de seguridad dio a conocer al transmisor (p. ej., el módem celular), p. ej., cuando se configuró el servicio de seguridad, es decir, antes de la primera utilización de la “conexión de datos sin SIM”;

-- el proveedor de servicios indicado por el dispositivo de comunicación en el establecimiento de conexión de comunicación está registrado en la red celular (p. ej., radio móvil) para aceptar las tarifas de llamadas para las conexiones relacionadas. El registro puede hacerse antes de que se establezca la conexión de comunicación; y/o

-- el circuito solicitante (p. ej., la CPU solicitante) se registra en el servidor de seguridad.

- Un valor que se calcula a partir del ID único del circuito (p. ej., la CPU) se utiliza para identificar el dispositivo de comunicación en el establecimiento de conexión de comunicación.

La red de comunicación celular (p. ej., la radio móvil de área extensa) puede manejar solicitudes de conexión de comunicación que utilizan este nuevo tipo de conexión de comunicación de manera diferente en comparación con otras solicitudes de conexión de comunicación, es decir, la autenticación se basa ilustrativamente en un ID único de circuito, p. ej., el CPU-ID, la tarifa de conexión de comunicación se puede cobrar a un tercero indicado, p. ej., en la solicitud y la selección de los parámetros relacionados con la Calidad de Servicio (QoS) se puede realizar en base a este tipo de conexión de comunicación.

Como se describió anteriormente y también se describirá con más detalle a continuación, diversos aspectos de esta divulgación pueden proporcionar algunos o todos de los siguientes efectos:

- El dispositivo de comunicación puede detectar automáticamente que está potencialmente fuera del control del usuario autorizado, p. ej., perdido o robado.

- El dispositivo de comunicación podría hacerse inutilizable inmediatamente después de la detección de perdido/robado.

- El dispositivo de comunicación puede encontrarse fácilmente mediante la función de rastreo.

- El mecanismo no puede evitarse por el usuario no autorizado.

- Los datos sensibles almacenados en el dispositivo de comunicación no son utilizables por el usuario no autorizado.

- El dispositivo de comunicación no puede utilizarse por un usuario no autorizado.

- Robar un dispositivo de comunicación de este tipo puede ser menos atractivo y, por lo tanto, puede que se roben menos dispositivos de comunicación con este tipo de mecanismo.

Algunos o todos los efectos pueden ser válidos incluso en el caso de que una persona no autorizada que encuentra, p. ej., un dispositivo de comunicación perdido o robado intente evitar una conexión de comunicación a Internet

apagando, p. ej., la Red de Área Local Inalámbrica (WLAN), desenchufando la Red de Área Local (LAN) y retirando la tarjeta SIM del propietario.

Diversos aspectos de esta divulgación pueden habilitar una conexión de comunicación iniciada por el dispositivo de comunicación (es decir, no iniciada por el usuario) a un servidor predefinido a través de la red celular sin requerir una SIM o USIM. La conexión de comunicación puede ser:

- cobrar a un tercero (proveedor de servicios) que también controla la conexión de comunicación;

- se utiliza para verificar el estado del dispositivo de comunicación en el servidor de seguridad;

- se utiliza para entregar una instrucción mediante el servidor al dispositivo de comunicación, p. ej., una instrucción de “bloquear dispositivo” o una instrucción de “cifrar datos sensibles” si el estado indica que el dispositivo de comunicación se ha perdido o ha sido robado;

- se utiliza para enviar la ubicación actual del dispositivo de comunicación al servidor de seguridad para encontrar fácilmente el dispositivo de comunicación.

Se pueden proporcionar diversos mecanismos para evitar la utilización no autorizada del dispositivo de comunicación utilizando los diversos procesos descritos en el presente documento:

1. El circuito (p. ej., la CPU) del dispositivo de comunicación “posee” un ID único (“ID de circuito”, p. ej., el “CPU-ID”) que se puede utilizar para autenticar el dispositivo de comunicación en diferentes entidades:

a) El ID de circuito, p. ej., el CPU-ID, puede registrarse en el proveedor de servicios. Un valor derivado de este ID de circuito, p. ej., el CPU-ID, se utiliza durante el procedimiento de establecimiento de conexión de comunicación para hacer cumplir la política de acceso y puede permitir que el proveedor de servicios rechace las solicitudes de conexión de comunicación de los dispositivos de comunicación no registrados.

b) La red de comunicación celular puede conocer los ID de circuito permitidos, p. ej., el CPU-ID, y, por lo tanto, está habilitada para rechazar los intentos de configuración de conexión de comunicación de los CPU-ID desconocidos. La red de comunicación celular puede obtener los ID de circuito, p. ej., los CPU-ID, del proveedor de servicios antes de que se establezca una conexión de comunicación relacionada. Como alternativa, la red de comunicación celular puede preguntar al proveedor de servicios si el ID indicado (ID de circuito, p. ej., el CPU-ID) está autorizado para el servicio durante el procedimiento de establecimiento de conexión de comunicación. En cualquier caso, si el proveedor de servicios lo desconoce o lo prohíbe, se rechaza el establecimiento de conexión de comunicación.

c) El proveedor de servicios puede informar al módem celular de los ID de circuito permitidos, p. ej., los CPU-ID, y, por lo tanto, está habilitado para rechazar los intentos de configuración de conexión de comunicación de los ID de circuitos desconocidos, p. ej., los CPU-ID. El transmisor del dispositivo de comunicación (p. ej., un módem celular) configura el servicio solo en caso de que un circuito autenticado, p. ej., la CPU, active la solicitud. Esto puede evitar la utilización no autorizada del transmisor, p. ej., el módem celular, para la conexión de datos sin SIM si el transmisor, p. ej., el módem celular, se utiliza en otro dispositivo de comunicación o con otro circuito, p. ej., otra CPU.

2. El proveedor de servicios puede estar registrado en la red celular (radio móvil de área extensa) para ofrecer dicho “servicio de datos sin SIM” y para aceptar las tarifas de llamadas para las conexiones de comunicación relacionadas. Por lo tanto, se puede establecer una entrada relacionada en un Registro de Ubicación Local (HLR). Esto puede impedir que el usuario no autorizado establezca una conexión de comunicación gratuita con cualquier dirección que el usuario seleccione.

3. En lugar de transmitir el CPU-ID en texto plano en el establecimiento de conexión de comunicación, se puede crear un ID único mediante el circuito criptográfico, p. ej., el TPM, p. ej., por transformación de claves del ID de circuito, p. ej., el CPU-ID, en un primer proceso. El resultado de este procedimiento de transformación de claves puede firmarse digitalmente en un segundo proceso y asignarse al circuito, p. ej., la CPU, en un tercer proceso. Este ID se puede utilizar durante el establecimiento de conexión de comunicación, como se describe en el elemento 1 anterior. La utilización de tal ID puede proporcionarse ya que evita que el ID de circuito real, p. ej., el CPU-ID, pueda derivarse y utilizarse por usuarios no autorizados.

Los procesos bajo los elementos 1 a 3 podrían utilizarse simultáneamente o individualmente. La protección contra la utilización engañosa es máxima, si se aplican todos los procesos.

La FIG. 1 muestra un sistema 100 de comunicación. El sistema 100 de comunicación puede incluir uno o más (en general, un número arbitrario de decenas, cientos, miles o incluso más) de dispositivos 102 terminales de

comunicación por radio móvil, que también se denominarán dispositivos 102 terminales de comunicación en lo siguiente.

Un dispositivo 102 terminal de comunicación puede ser cualquier tipo de dispositivo electrónico que tenga la capacidad de proporcionar la funcionalidad de comunicación, tal como se describió anteriormente y se describirá con más detalle a continuación. Solo por mencionar algunos ejemplos, un dispositivo 102 terminal de comunicación puede ser un teléfono móvil, un teléfono inteligente, una tableta, un ultraportátil, una ordenador portátil, una computadora portátil, una computadora (p. ej., personal), cualquier tipo de dispositivo multimedia, p. ej., incluyendo un televisor, o incluso un reloj que incluya un circuito adecuado, respectivamente, y similares.

Como se muestra en la FIG. 1, el dispositivo 102 terminal de comunicación puede incluir un circuito 116 que está identificado por un identificador único. El circuito 116 puede incluir o implementarse por una unidad 116 central de procesamiento (CPU). Debe mencionarse que el circuito puede ser cualquier tipo de hardware (p. ej., cualquier tipo de lógica de hardware, tal como p. ej., una lógica cableada (p. ej., una o más Matrices Lógicas Programables (PLA) y/o una o más Matrices de Compuertas programables en Campo (FPGA)) o lógica programable (p. ej., uno o más procesadores programables, p. ej., uno o más microprocesadores o nanoprocesadores programables), software (cualquier tipo de software de sistema operativo o componentes del software del sistema operativo o software de aplicación o componentes del software de aplicación), firmware, o cualquier combinación de los mismos, que tenga asignado un ID único, como se describió anteriormente.

El dispositivo 102 terminal de comunicación puede incluir además una o más antenas 106, un transceptor 108 acoplado a la una o más antenas 106, en donde el transceptor 108 puede incluir uno o más transmisores y/o uno o más receptores. El transceptor 108 (p. ej., uno o más de los transmisores) puede implementarse por medio de un módem 110 celular, que puede incluir una o más memorias, p. ej., una primera memoria 112 que almacena la Identidad Internacional de Equipo de Móvil (IMEI) del módem 110 celular y/o una segunda memoria 114 que almacena uno o más ID únicos asignados a los respectivos circuitos del dispositivo 102 terminal de comunicación, como se describió anteriormente y como se describirá con más detalle a continuación. A modo de ejemplo, el módem 110 celular puede configurarse de acuerdo con GSM (Sistema Global para Comunicaciones Móviles), UMTS (Sistema Universal de Telecomunicaciones Móviles), LTE (Evolución a Largo Plazo) u otras tecnologías de acceso por radio celular de área extensa.

Además, el dispositivo 102 terminal de comunicación puede incluir un circuito de tecnología de comunicación por radio celular de área extensa (que también puede implementarse, al menos parcialmente, por el transceptor 108) configurado para proporcionar una comunicación de acuerdo con una tecnología de comunicación por radio celular de área extensa. La tecnología de comunicación por radio celular de área extensa puede incluir una tecnología de comunicación del Proyecto de Asociación de Tercera Generación (3GPP), tal como, p. ej., UMTS (Sistema Universal de Telecomunicaciones Móviles), LTE (Evolución a Largo Plazo), LTE-Advanced y similares. Se debe tener en cuenta que se puede proporcionar cualquier otra tecnología de comunicación por radio celular de área extensa, tal como p. ej., una tecnología de comunicación por radio del Sistema Global para Comunicaciones Móviles (GSM), una tecnología de comunicación por radio del Servicio General de Paquete vía Radio (GPRS), una tecnología de comunicación por radio de Tasas de Datos Mejoradas para Evolución de GSM (EDGE), FOMA (Libertad de Acceso Multimedia), CDMA2000 (Acceso Múltiple por División de Código 2000), CDPD (Datos de Paquetes Digitales Celulares), Mobitex, HSCSD (Datos Conmutados por Circuito de Alta Velocidad), W-CDMA (UMTS) (Acceso Múltiple por División de Código de Banda Ancha (Sistema Universal de Telecomunicaciones Móviles)), HSPA (Acceso a Paquetes de Alta Velocidad), HSDPA (Acceso a Paquetes de Enlace Descendente de Alta Velocidad), HSUPA (Acceso a Paquetes de Enlace Ascendente de Alta Velocidad), HSPA + (Acceso a Paquetes de Alta Velocidad Plus), TD-CDMA (Acceso Múltiple por División de Código por División de Tiempo), TD-CDMA (Acceso Múltiple por División de Código Sincrónico por División de Tiempo), cdmaOne (2G), CDMA2000 (3G) (Acceso Múltiple por División de Código 2000 (Tercera generación)).

El dispositivo 102 terminal de comunicación puede incluir además un circuito 116, en donde el circuito 116 tiene un ID 118 único (en lo siguiente, el CPU-ID 118 (CPU-ID#1 en la FIG. 1) se utilizará por razones de simplicidad como un ejemplo para el ID 118 único) asignado al mismo y almacenado en una memoria 120 del circuito 116. A modo de ejemplo, el circuito 116 puede ser un procesador, p. ej., una unidad 116 central de procesamiento (CPU) del dispositivo 102 terminal de comunicación.

Además, el dispositivo 102 terminal de comunicación puede incluir, opcionalmente, un circuito 122 criptográfico, configurado para proporcionar una o más funciones criptográficas, tales como, p. ej., al menos una función criptográfica seleccionada de un grupo de funciones criptográficas que consiste en:

- una función de transformación de claves;

- cifrado y/o descifrado (en otras palabras, proporcionar cifrado y/o descifrado); y

- firma digital (en otras palabras, proporcionar una firma digital).

El circuito 122 criptográfico puede implementarse en la forma de un Módulo 122 de Plataforma de Confianza (TPM), en donde el CPU-ID 118 se puede almacenar en una memoria 124 del TPM 122. El circuito 122 criptográfico (p. ej., el TPM) puede configurarse para aplicar la función criptográfica respectivamente deseada al identificador único (p. ej., el CPU-ID 118) para proporcionar información que indique el identificador único. Alternativamente, la información que indica el identificador único puede proporcionarse en texto plano. Como una alternativa adicional, se puede proporcionar el propio identificador único (p. ej., en texto plano).

Además, el dispositivo 102 terminal de comunicación puede incluir, opcionalmente, un determinador 126 de ubicación (p. ej., un circuito de determinación de ubicación) configurado para determinar la ubicación del dispositivo 102 terminal de comunicación. El determinador de ubicación puede incluir o estar hecho de un circuito de posicionamiento basado en satélite, tal como p. ej., un circuito del Sistema de Posicionamiento Global (GPS), un circuito de Galileo y similares. A modo de ejemplo, se puede proporcionar cualquier otro tipo de circuito del Sistema Global de Navegación por Satélite (GNSS) como el determinador de ubicación.

El dispositivo 102 terminal de comunicación puede incluir un determinador (que puede implementarse por la CPU 116 o cualquier otro circuito separado no mostrado en la FIG. 1) configurado para determinar si el dispositivo 102 terminal de comunicación, p. ej., se ha perdido o ha sido robado. De manera ilustrativa, la CPU 116 puede habilitarse (p. ej., utilizando (p. ej. solicitando o requiriendo) un PIN (Número de Identificación Personal) de un usuario del dispositivo 102 terminal de comunicación, al determinar una ubicación inusual (geográfica) del dispositivo 102 terminal de comunicación (p. ej., utilizando el determinador 126 de ubicación), determinando una operación inusual (p. ej., determinando la utilización operacional inusual del dispositivo 102 terminal de comunicación), determinando hardware y/o software (componentes) reemplazado o adicional (sospechoso)) para detectar que el dispositivo 102 terminal de comunicación, p. ej., se ha perdido o ha sido robado, y para iniciar el establecimiento de una conexión de datos sin SIM (como alternativa, en lugar del CPU-ID 118, puede utilizarse un ID único de cualquier otro hardware y/o software (componente) en el dispositivo 102 terminal de comunicación).

En otras palabras, el determinador puede configurarse para determinar si el dispositivo de comunicación está fuera del control del propietario de manera no deseada utilizando al menos uno de los siguientes:

- información de identificación que identifica al usuario autorizado del dispositivo de comunicación;

- información sobre la ubicación del dispositivo de comunicación;

- información sobre el funcionamiento del dispositivo de comunicación; e

- información sobre al menos uno de hardware y de software del dispositivo de comunicación.

Además, el dispositivo 102 terminal de comunicación puede incluir un establecedor de conexión de comunicación (que también puede implementarse por la CPU 116 o cualquier otro circuito separado no mostrado en la FIG. 1) configurado para establecer una conexión de comunicación sin Módulo de Identificación de Abonado (SIM).

Además, el transmisor puede configurarse para transmitir un mensaje de solicitud de estado de verificación que incluye información que indica el identificador único a otro dispositivo de comunicación (p. ej., un servidor, p. ej., un servidor de seguridad), como se describirá con más detalle a continuación con referencia a la FIG. 2).

Como también se describirá con más detalle a continuación, un receptor del transceptor 108 puede configurarse para recibir una instrucción para entrar en un estado de dispositivo de comunicación predefinido. El dispositivo 102 terminal de comunicación puede configurarse para entrar en el estado de dispositivo de comunicaciones predefinido, p. ej., un estado de seguridad predefinido o un estado de bloqueo del dispositivo 102 terminal de comunicación. En otras palabras, se puede proporcionar un circuito en el dispositivo 102 terminal de comunicación (p. ej., también implementado por la CPU 116), configurado para hacer que el dispositivo 102 terminal de comunicación entre en el estado de dispositivo de comunicación predefinido de acuerdo con la instrucción recibida.

Como se muestra en la FIG. 1, el transceptor 108 puede acoplarse a la CPU 116 a través de una primera interfaz (p. ej., una interfaz IF_C). Además, el transceptor 108 puede acoplarse al circuito 122 criptográfico a través de una segunda interfaz (p. ej., una interfaz IF_B). Además, la CPU 116 también puede acoplarse al circuito 122 criptográfico, p. ej., a través de una tercera interfaz (p. ej., un interfaz IF_A). El determinador 126 de ubicación puede acoplarse al transceptor 108, a la CPU 116, así como al circuito 122 criptográfico.

El sistema 100 de comunicación puede incluir, además, una o más estaciones 128 base (p. ej., uno o más NodoB, p. ej., uno o más eNodosB) y una red 130 central (p. ej., una Red Móvil Terrestre Pública (PLMN)), que puede incluir, p. ej., un Registro 132 de Ubicación Local (HLR). En general, se puede proporcionar cualquier número de estaciones

128 base, p. ej., decenas, cientos, miles o incluso más estaciones 128 base en el sistema 100 de comunicación. El HLR 132 tiene almacenados proveedores 134 de servicios registrados (de seguridad), como se describirá con más detalle a continuación. El dispositivo 102 terminal de comunicación puede acoplarse a la estación 128 base a través de una interfaz de aire, p. ej., a través de una red de acceso de radio (RAN), p. ej., una UTRAN (UMTS RAN) o cualquier otra RAN, dependiendo de la tecnología o las tecnologías de comunicación por radio de área extensa proporcionadas respectivamente.

Además, el sistema 100 de comunicación puede incluir un proveedor 136 de servicios, que puede proporcionar uno o más servidores 138 de seguridad, en donde el uno o más servidores 138 de seguridad pueden tener almacenados loa ID 118 permitidos (p. ej., el CPU-ID) en una respectiva memoria 140. El uno o más servidores 138 de seguridad pueden estar acoplados a la red 130 central a través de una conexión 142.

La FIG. 2 muestra un diagrama de flujo de mensajes que ilustra un método 200 de acuerdo con diversos aspectos de esta divulgación.

Debe observarse que el sistema operativo del dispositivo 102 terminal de comunicación puede o no arrancarse cuando se lleva a cabo el método 200.

En otras palabras, la FIG. 2 muestra el flujo de mensajes para el establecimiento de una conexión de datos sin SIM.

Un primer proceso 202 se lleva a cabo dentro del dispositivo 102 terminal de comunicación, p. ej., por la CPU 116. La necesidad de establecer una conexión de datos sin SIM puede detectarse por la CPU 116, p. ej., de la manera descrita anteriormente. Por lo tanto, la CPU 116 puede transmitir un mensaje 204 de solicitud de conexión de datos sin SIM al módem 110 celular (p. ej., a través de la interfaz IF_C). El mensaje 204 de solicitud de conexión de datos sin SIM puede incluir el CPU-ID 118, opcionalmente, la dirección del servidor 138 de seguridad, opcionalmente, el nombre de la parte a ser cobrada por la conexión de datos sin SIM solicitada y la PLMN 130 a ser utilizada para esta conexión de datos sin SIM.

Un segundo proceso 206 subsiguiente también puede llevarse a cabo dentro del dispositivo 102 terminal de comunicación, p. ej., por el módem 110 celular. El segundo proceso 206 puede incluir un proceso de verificación de autorización. En el proceso 206 de verificación de autorización, el módem 110 celular puede verificar que el CPU-ID 118 recibido está permitido para utilizar la conexión de datos sin SIM. Esto se puede hacer involucrando al TPM 122 (p. ej., a través de la interfaz IF_B) y leyendo información relacionada desde la memoria interna (p. ej., la segunda memoria 114) del módem 110 celular (simbolizado en la FIG. 2 por medio de una flecha 208 doble). Esta autorización puede evitar la utilización engañosa del módem 110 celular si se utiliza en otro dispositivo de comunicación.

Un tercer proceso 210 subsiguiente también puede llevarse a cabo dentro del dispositivo 102 terminal de comunicación, p. ej., por el módem 110 celular. En este tercer proceso 210, si el CPU-ID 118 está permitida para utilizar la conexión de datos sin SIM, el módem 110 celular puede solicitar, opcionalmente, al TPM 122 que genere un ID único a partir de (en otras palabras, en base a) el CPU-ID 118 a ser utilizado para la autorización del dispositivo 102 terminal de comunicación en la red 130 celular y en el proveedor 136 de servicios. Esto se puede hacer, p. ej., por transformación de claves del CPU-ID 118 con un mecanismo predefinido. Además, el resultado puede estar firmado digitalmente por el TPM 122. El resultado puede transmitirse nuevamente al módem 110 celular. Este ID único derivado del CPU-ID 118 puede transmitirse por el aire en lugar de transmitir el CPU-ID 118 en texto plano. Esto puede evitar la utilización engañosa del CPU-ID 118 por otro dispositivo de comunicación.

En un cuarto proceso subsiguiente, el módem 110 celular puede iniciar el procedimiento de establecimiento de conexión de comunicación a la red 130 celular indicada mediante la transmisión de un preámbulo 212 de acceso aleatorio a través de la interfaz 136 de aire celular.

A continuación, en un quinto proceso subsiguiente, la red 130 celular puede responder a la recepción del preámbulo 212 de acceso aleatorio con un mensaje 214 de respuesta de acceso aleatorio.

A continuación, en un sexto proceso, el módem 110 celular puede generar y transmitir un mensaje 216 de RRCConnectionRequest a la red 130 celular. Se solicita un nuevo tipo de servicio por el dispositivo 102 terminal de comunicación, que se indica a la red 130 celular durante el establecimiento de conexión. Se puede agregar una nueva “Causa de establecimiento” al “mensaje 216 de solicitud de conexión de RRC” (p. ej., en un campo de mensaje específico agregado), que puede denominarse, p. ej., “3pc mo-data” (datos de origen móvil cobrados a terceros) en una implementación del mensaje 216 de solicitud de conexión de RRC en ASN.1, como se describirá con más detalle a continuación. El nuevo tipo de servicio puede incluir información sobre la parte a ser cobrada y una dirección del servidor de seguridad. Esta información puede incluirse en el mensaje 216 de solicitud de conexión de RRC o en un mensaje similar (incluso en un mensaje separado que puede proporcionarse únicamente para este propósito). La utilización de este tipo de servicio puede permitir que la red 130 celular utilice un comportamiento

diferente en el manejo del establecimiento de conexión de comunicación, es decir, la autenticación para dicho tipo de servicio puede ser en base a un ID derivado a partir del CPU-ID 118 (único), la tarifa de conexión se puede cobrar a un tercero como se indica en el mensaje 216 de solicitud después de que se verifique la validez y se pueda realizar la selección de los parámetros relacionados con la Calidad de Servicio (QoS) en base a este tipo de conexión de comunicación. Las credenciales de la tarjeta SIM o USIM no se requieren en este caso. Por lo tanto, no es posible el cifrado de la conexión en base a credenciales de la SIM o USIM. Pero se pueden utilizar circuitos alternativos para el cifrado, p. ej., IPSec. En este caso, las credenciales pueden negociarse entre el proveedor 136 de servicios y la CPU 116. Como alternativa, el CPU-ID 118 o un ID único asociado calculado sobre el CPU-ID 118, pueden servir como un parámetro de entrada para establecer el contexto de seguridad.

A continuación, en un séptimo proceso 218, que puede llevarse a cabo en la red 130 celular, se puede llevar a cabo una comprobación de validez. La red 130 celular puede verificar la validez del servicio solicitado, p. ej., preguntando al HLR 132 si el proveedor 136 de servicios indicado está registrado para ofrecer dicho servicio. Por lo tanto, el HLR 132 puede provisionarse con este tipo de información antes de esta solicitud. Este proceso 218 puede evitar la utilización no permitida en una etapa temprana del procedimiento de establecimiento de conexión de comunicación.

Entonces, en un octavo proceso, que puede llevarse a cabo en la red 130 celular y/o la estación 128 base, si el proveedor 136 de servicios indicado está registrado para ofrecer el servicio solicitado, la red 130 celular establece la conexión de RRC p. ej., generando y transmitiendo un mensaje 220 de “establecimiento de conexión de RRC” al módem 110 celular. Además, esta verificación exitosa del registro puede desencadenar el cobro del servicio por parte del proveedor 136 de servicios indicado, si se desea, como una opción.

A continuación, en un noveno proceso, que puede realizarse en el módem 110 celular, el dispositivo 102 terminal de comunicación puede generar y transmitir un mensaje 222 de “establecimiento de conexión de RRC completado” de vuelta a la red 130 celular y puede solicitar establecer una conexión de Red Pública de Datos (PDN) generando y transmitiendo un mensaje 224 de “solicitud de conectividad de PDN”.

Además, en un décimo proceso, que puede llevarse a cabo por la red 130 celular, se puede proporcionar para reestablecer la conexión de RRC, p. ej., en caso de que el establecimiento inicial no coincida con la necesidad actual de esta solicitud. En este caso, un mensaje 226 de “reestablecimiento de conexión de RRC” puede generarse y transmitirse al módem 110 celular.

En un decimoprimer proceso 228, que puede llevarse a cabo por la red 130 celular, la red 130 celular puede establecer un portador para la conexión de PDN en base a la petición recibida. Una vez que se establece el portador en la red 130 celular, puede generarse un mensaje 230 “Solicitud de activación de contexto de portador de EPS por defecto” y transmitirse al módem 110 celular para configurar el portador de EPS por defecto. (Este mensaje y los siguientes están destinados al denominado “Estrato de No Acceso” (NAS), mientras que los mensajes de los procesos cuatro a diez están destinados al “Estrato de Acceso” (AS)).

En una decimosegundo proceso, el módem 110 celular puede aplicar las configuraciones indicadas y puede indicar la disposición del portador a la red 130 celular, p. ej., generando y transmitiendo un mensaje 232 de “Activar aceptación de contexto de EPS por defecto” (que está destinado a NAS) y un mensaje de “Reestablecimiento de conexión de RRC completado” (destinado a AS), si aplica.

A continuación, en un decimotercer proceso, el módem 110 celular puede indicar el establecimiento exitoso de la conexión de datos sin SIM a la CPU (p. ej., a través de la Interfaz IF_C), p. ej., generando y enviando una notificación 234 de conexión de datos sin SIM lista a la CPU 116.

Además, en un decimocuarto proceso, se pueden establecer una conexión 236 de comunicación segura entre el servidor 136 de seguridad y la CPU 116, p. ej., utilizando IPSec. El TPM 122 en el dispositivo 102 terminal de comunicación puede estar implicado para establecer el contexto de seguridad (p. ej., a través de la Interfaz IF_A). Cabe señalar que este proceso es opcional.

En un decimoquinto proceso, el módem 110 celular puede generar y transmitir un mensaje 238 de “obtener estado de seguridad del dispositivo” (destinado a NAS) al servidor 136 de seguridad con el fin de obtener el estado del dispositivo terminal de comunicación definido por el usuario. Se puede incluir el ID único (que puede ser un “CPU-ID” 118 o el ID único generado en el tercer proceso). El ID único se puede transmitir desde el dispositivo 102 terminal de comunicación a la red 130 celular como parte del mensaje 238 de NAS de “Obtener Estado de Seguridad del Dispositivo”, mientras que, como alternativa, también puede incluirse en otros mensajes de enlace ascendente de la FIG. 2, tal como el mensaje 216 de “Solicitud de Conexión de RRC” del sexto proceso (es decir, un mensaje destinado al AS) o un mensaje 232 de “Activar aceptación de contexto del portador EPS por defecto” 232 (destinado a NAS).

En un decimosexto proceso 240, el servidor 138 de seguridad puede verificar que la CPU 116 está registrada para el servicio, si esto no se ha realizado ya en el decimocuarto proceso. Si la verificación es verdadera, el estado de seguridad del dispositivo puede leerse de un almacenamiento interno (p. ej., la memoria 140) del servidor 138 de seguridad y puede transmitirse a la CPU 116. El mensaje 242 generado y transmitido respectivamente (p. ej., denominado mensaje de estado de seguridad del dispositivo) puede firmarse digitalmente por el servidor 138 de seguridad.

En un decimoséptimo proceso 244, la CPU 116 puede leer el estado de seguridad del mensaje 242 recibido. En este ejemplo, se supone que el estado de seguridad se estableció en, p. ej., “perdido/robado” (véase la definición a continuación). Esto puede activar la CPU 116 para que bloquee el dispositivo 102 terminal de comunicación. El TPM 122 puede estar involucrado (p. ej., a través de la interfaz IF_A) para verificar la firma digital de este comando para prevenir el fraude. Es inusable por cualquier usuario hasta que el propietario cambie el estado de seguridad a “normal”.

En un decimoctavo proceso 246, se supone que el propietario del dispositivo 102 terminal de comunicación desea conocer la ubicación del dispositivo 102 terminal de comunicación. Por lo tanto, se supone que el propietario ha establecido la opción para la derivación de ubicación a “una vez” en el servidor 138 de seguridad (véase la definición de estado de seguridad a continuación). La CPU 116 puede solicitar al determinador 126 de ubicación (p. ej., el módulo de GNSS) que derive la ubicación actual. Esta ubicación puede transmitirse al servidor 138 de seguridad y almacenarse en el dominio del propietario. El propietario puede leer la ubicación si ha iniciado sesión en el servidor 138 de seguridad, o el servidor 138 de seguridad puede transmitir la ubicación a la dirección de correo electrónico del propietario.

En un decimonoveno proceso 248, la CPU 116 puede activar el módem 110 celular para terminar la conexión 246 de comunicación, debido a que se toman todas las acciones del estado 138 de seguridad. Esto es cierto en caso de que la opción de derivación de ubicación se haya establecido en “ninguna” o “una vez” y la opción de conectividad se haya establecido en “ninguna”. Como alternativa, en caso de que la opción de “derivación de ubicación” se establezca en “periódicamente”, la CPU 116 puede instruir al módem 110 celular que se apague hasta que expire el período para la próxima actualización de ubicación. Luego puede volver a iniciar el establecimiento de conexión de datos sin SIM con el primer proceso. En una alternativa más, en caso de que la opción de “conectividad” esté establecida en “inactivo”, la CPU 116 puede indicar al módem 110 celular que entre en el “modo inactivo” (RRC), es decir, está preparado para ser localizado por la red 130 celular y, por lo tanto, también está preparado para un nuevo establecimiento de conexión de comunicación si se activa por el servidor 138 de seguridad o por el propietario.

En un vigésimo proceso 250, el módem 110 celular puede terminar la conexión de comunicación y puede apagar, es decir, ya no está activado en cualquier interfaz hacia la red 130 celular, este proceso puede incluir además generar (por el módem 110 celular) y transmitir una notificación 252 de conexión terminada a la CPU 116.

Un estado de seguridad puede entenderse como una parte de la información almacenada en un dispositivo legible por computadora (p. ej., el servidor). Puede pertenecer a un determinado dispositivo de comunicación que posee una CPU (p. ej., la CPU 116). Esta CPU (p. ej., la CPU 116) está identificada de manera única por un CPU-ID. El estado lo establece el propietario del dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación). El estado habitual se establece en “normal”, p. ej., mientras el propietario utiliza su dispositivo de comunicación. Este estado permite la utilización normal del dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación). Una vez que el dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación) se ha perdido o ha sido robado, el usuario puede conectarse al servidor (p. ej., el servidor 138 de seguridad) que tiene almacenado el estado de seguridad y cambiar el estado a, p. ej., “perdido/robado”. Esto se puede hacer a través de cualquier tipo de dispositivo de comunicación que ofrezca acceso a Internet. El estado de seguridad puede obtenerse por la CPU (p. ej., la CPU 116) del dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación) y puede activar ciertas acciones por parte de la CPU (p. ej., la CPU 116), p. ej., bloquear el dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación) si el estado de seguridad se establece en, p. ej., “perdido/robado”. Además del estado de seguridad, el usuario puede configurar otras opciones para el estado de seguridad, p. ej., “perdido/robado” con respecto a la derivación de la ubicación del dispositivo de comunicación. Esta opción se puede establecer en “ninguno”, “una vez” o “periódicamente”. Además, el usuario puede configurar una opción con respecto a la conectividad en, p. ej., estado perdido/robado. Esto se puede establecer en “ninguno” y en “inactivo”. “Inactivo” significa que el transceptor, p. ej., el módem celular (p. ej., el módem 110 celular) permanecerá en modo inactivo en la red celular (p. ej., la red 130 celular) después de que se reciba el estado de seguridad, p. ej., “perdido/robado”. Esto puede permitir al usuario establecer una conexión de comunicación con el dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación) en cualquier momento para realizar una acción adicional en el dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación), p. ej., tomar fotos del ladrón, obtener documentos o datos personales importantes del dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación), permitir una conexión de voz con el dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación) y así sucesivamente. “Ninguno” significa que el

transceptor, p. ej., el módem celular (p. ej., el módem 110 celular) terminará la conexión de comunicación después de que se tomen las instrucciones de seguridad del propietario.

En lo siguiente, se describe una posible implementación ASN.1 (notación de sintaxis abstracta 1) del mensaje 216 de RRCConnectionRequest. Los nuevos valores comparados con un mensaje de RRCConnectionRequest convencional están subrayados. La nueva causa de establecimiento “3pc-MO-data” puede reemplazar el valor no utilizado “spare2”.

```
-- ASN1START
RRCConnectionRequest ::=                SEQUENCE {
criticalExtensions                          CHOICE {
    rrcConnectionRequest-r8                 RRCConnectionRequest-r8-IEs,
    criticalExtensionsFuture            SEQUENCE {}
}
}
RRCConnectionRequest-r8-IEs ::=         SEQUENCE {
ue-Identity                             InitialUE-Identity,
establishmentCause                      EstablishmentCause,
spare                                   BIT STRING (SIZE (1))
}

InitialUE-Identity ::=                  CHOICE {
s-TMSI                                  S-TMSI,
randomValue                             BIT STRING (SIZE (40))
CPU-derived-ID                          CPU-derived ID
}

EstablishmentCause ::=                  ENUMERATED {
                                        3pc mo-data, emergency, highPriorityAccess,
                                        mt-Access, mo-Signalling, mo-Data,
                                        delayTolerantAccess-v1020, spare2, spare1}
-- ASN1STOP
```

Con respecto a la detección de la necesidad de un establecimiento de conexión de datos sin SIM, cabe señalar lo siguiente:

Una conexión de datos sin SIM puede establecerse solamente, si no es posible otra manera de conectarse a Internet y se cumplen una o más de las siguientes condiciones:

- Después de un cierto número de fallos de inicio de sesión (contraseña incorrecta).

- Después de la retirada de la tarjeta SIM.

- Después de cambiar hardware (HDD (unidad de disco duro),...).

- Después de arrancar desde otro dispositivo (DVD, USB,...).

- Después de encenderse en una ubicación extraña.

Hay que señalar que la conexión de datos sin SIM con el servidor de seguridad puede no bloquear el dispositivo terminal de comunicación de inmediato en cualquier caso, p. ej., si el propietario ingresa accidentalmente una contraseña incorrecta. Solo en caso de que el propietario haya establecido el estado de seguridad en el servidor antirrobo en, p. ej., “perdido/robado”, el dispositivo terminal de comunicación se bloquea.

En cualquier caso, se puede establecer una conexión ordinaria a Internet (p. ej., utilizando WLAN, LAN, Bluetooth, red de telefonía móvil,...), se recomienda utilizar esto para la señalización antirrobo en lugar de la conexión de datos sin SIM.

Las enseñanzas de diversos aspectos de la presente divulgación también se pueden utilizar para escenarios diferentes a los descritos anteriormente. Si las definiciones de estado de seguridad se mejoran en consecuencia, el método también se puede utilizar para apagar dispositivos de forma remota si el usuario de un dispositivo de comunicación no ha pagado la tarifa por su utilización (p. ej., en caso de ventas a plazos y similares).

Además las enseñanzas de los diversos aspectos de esta divulgación también se pueden utilizar para diferentes tipos de dispositivos de comunicación aparte de una computadora portátil, p. ej., para coches, barcos, aviones u otros vehículos, para teléfonos móviles o cualquier otro dispositivo que utilice, p. ej., una CPU y que merezca la pena proteger contra la utilización engañosa.

La FIG. 3 muestra una estación 128 base, p. ej., una estación 128 base de radio celular de área extensa.

Con el fin de implementar las funciones y procesos descritos anteriormente en la estación 128 base, la estación 128 base puede tener una estructura de una estación 128 base de radio celular de área extensa como se muestra en la FIG. 3. Como se muestra en la FIG. 3, la estación 128 base de radio celular de área extensa puede incluir una o más antenas 302 y un transceptor 304, en donde el transceptor puede incluir un transmisor y un receptor configurados para recibir desde un dispositivo de comunicación una solicitud para establecer una conexión de comunicación sin Módulo de Identificación de Abonado, y un identificador que identifica de forma única un circuito (p. ej., la CPU 116) del dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación). Además, la estación 128 base puede incluir un determinador (p. ej., un circuito 306 de determinación) configurado para determinar si debe proporcionarse conexión de comunicación sin Módulo de Identificación de Abonado al dispositivo de comunicación en base al identificador. Además, la estación 128 base puede incluir un circuito 308 configurado para proporcionar la conexión de comunicación sin Módulo de Identificación de Abonado al dispositivo de comunicación.

El receptor puede estar además configurado para recibir, además, una dirección de un servidor que proporciona un servicio de seguridad al dispositivo de comunicación. El circuito 306 de determinación también puede configurarse para determinar si la conexión de comunicación sin Módulo de Identificación de Abonado solicitada debe proporcionarse al dispositivo de comunicación en base a la dirección del servidor.

La estación base de radio celular de área extensa puede configurarse de acuerdo con una tecnología de comunicación por radio del Proyecto de Asociación de Tercera Generación, tal como se describió anteriormente.

Además, puede incluir un circuito de la tecnología de comunicación por radio celular de área extensa (no mostrado en la FIG. 3), configurado para proporcionar una comunicación de acuerdo con una tecnología de comunicación por radio celular de área extensa. Además, se puede proporcionar un controlador configurado para establecer una conexión de comunicación por radio celular de área extensa con el dispositivo 102 terminal de comunicación.

El transceptor 304, el circuito 306 de determinación, el circuito 308 y, en su caso, el circuito de tecnología de comunicación por radio celular de área extensa pueden estar acoplados entre sí, p. ej., a través de una o más líneas 310, p. ej., una o más líneas 310 de bus. Además, se puede proporcionar un controlador que puede implementar algunas o todas las funciones proporcionadas en el contexto de los procesos, como se ha descrito anteriormente. Además, uno o más de los siguientes circuitos también pueden implementarse por el controlador: el transceptor 304, el determinador 306, el circuito 308 y, si aplica, el circuito de tecnología de comunicación por radio celular de área extensa.

La FIG. 4 muestra un servidor 138 de seguridad. El servidor 138 de seguridad puede incluir un transceptor 402, en donde el transceptor 402 puede incluir un transmisor y un receptor configurados para recibir un mensaje de solicitud de estado de verificación (p. ej., el mensaje 238 de “obtener estado de seguridad del dispositivo”) de otro dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación), p. ej., a través de la estación 128 base. El

mensaje de solicitud de estado de verificación puede incluir la información que indica un identificador único de un circuito del otro dispositivo de comunicación. El servidor 138 de seguridad puede incluir además una memoria 404 que almacena una pluralidad de identificadores únicos, respectivamente, identificando cada uno de los identificadores de manera única un circuito, en donde se puede asignar un estado de seguridad a cada uno de los identificadores únicos almacenados. Además, se puede proporcionar un determinador (p. ej., un circuito 406 de determinación) que puede configurarse para determinar el estado de seguridad almacenado asignado al identificador único indicado por la información incluida en el mensaje de solicitud de estado de verificación recibido (p. ej., el mensaje 238 de “obtener estado de seguridad del dispositivo”). El transceptor 402 puede incluir el transmisor configurado para transmitir el estado de seguridad determinado al otro dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación), p. ej., a través de la estación 128 base. Como se describió anteriormente, el estado de seguridad puede ser configurable por un usuario (en otras palabras, configurable por usuario). Además, el servidor 138 de seguridad puede incluir un circuito criptográfico configurado para proporcionar una función criptográfica; en donde el circuito criptográfico está configurado para aplicar la función criptográfica al estado de seguridad determinado. El circuito criptográfico puede configurarse para proporcionar al menos una función criptográfica seleccionada de un grupo de funciones criptográficas que consiste en: función de transformación de claves; cifrado; y firma digital. El circuito criptográfico puede configurarse además para proporcionar una firma digital al estado de seguridad determinado.

Al menos uno del receptor y del transmisor se puede configurar de acuerdo con una tecnología de comunicación por radio celular de área extensa. Al menos uno del receptor y del transmisor se puede configurar de acuerdo con una tecnología de comunicación por radio del Proyecto de Asociación de Tercera Generación.

Además, el servidor 138 de seguridad puede incluir un solicitante de ubicación configurado para solicitar la ubicación del otro dispositivo de comunicación (p. ej., el dispositivo 102 terminal de comunicación).

La FIG. 5 muestra un diagrama de flujo que ilustra un método 500 para operar un dispositivo de comunicación. El método (que puede llevarse a cabo por el dispositivo 102 de comunicación, por ejemplo), puede incluir, en 502, determinar si el dispositivo de comunicación (p. ej., el dispositivo 102 de comunicación) está fuera del control del usuario autorizado de manera no deseada. El método puede incluir además, en 504, establecer una conexión de comunicación sin Módulo de Identificación de Abonado y, en 506, transmitir a otro dispositivo de comunicación un mensaje de solicitud de estado de verificación que incluye información que indica un identificador único que identifica un circuito del dispositivo de comunicación.

La FIG. 6 muestra un diagrama de flujo que ilustra un método 600 para operar un dispositivo de comunicación. El método (que puede llevarse a cabo por el servidor 138 de seguridad, en donde el servidor 138 de seguridad puede incluir una memoria que almacena una pluralidad de identificadores respectivamente únicos, cada uno de los identificadores identifica un circuito de manera única, en donde a cada uno de los identificadores únicos almacenados se asigna un estado de seguridad), puede incluir, en 602, recibir un mensaje de solicitud de estado de verificación de otro dispositivo de comunicación, el mensaje de solicitud de estado de verificación que incluye información que indica un identificador único de un circuito del otro dispositivo de comunicación. El método puede incluir además, en 604, determinar el estado de seguridad almacenado asignado al identificador único indicado por la información incluida en el mensaje de solicitud de estado de verificación recibido y, en 606, transmitir el estado de seguridad determinado al otro dispositivo de comunicación.

La FIG. 7 muestra un diagrama de flujo que ilustra un método 700 para operar una estación base de radio celular de área extensa. El método (que puede realizarse por la estación 128 base, por ejemplo), puede incluir, en 702, recibir desde un dispositivo de comunicación una solicitud para establecer una conexión de comunicación sin Módulo de Identificación de Abonado y un identificador que identifique de manera única un circuito del dispositivo de comunicación. El método puede incluir además, en 704, determinar si la conexión de comunicación sin Módulo de Identificación de Abonado solicitada debe proporcionarse al dispositivo de comunicación en base al identificador y, en 706, proporcionar la conexión de comunicación sin Módulo de Identificación de Abonado al dispositivo de comunicación.

Otra aplicación de los aspectos anteriormente descritos se puede ver en un dispositivo de comunicación de apoyo específico de IT (información y telecomunicación).

Además, en la estación base de radio celular de área extensa, el receptor puede estar además configurado para recibir, además, un nombre de un proveedor de servicios que proporciona un servicio de seguridad al dispositivo de comunicación; en donde el determinador puede configurarse además para determinar si la conexión de comunicación sin Módulo de Identificación de Abonado solicitada debe proporcionarse al dispositivo de comunicación en base al nombre del proveedor de servicios.

REIVINDICACIONES

1. Una estación (128) base de radio celular de área extensa, que comprende:

un receptor (304) configurado para recibir desde un dispositivo de comunicación una solicitud para establecer una conexión de datos sin Módulo de Identificación de Abonado, SIM, de acuerdo con una tecnología de comunicación por radio celular de área extensa para facilitar la comunicación de instrucciones de seguridad y mensajes de solicitud y de respuesta de estado de verificación, y un identificador que identifica de manera única una unidad central de procesamiento, CPU, del dispositivo de comunicación;

un determinador (306) configurado para determinar si la conexión de datos sin SIM solicitada debe proporcionarse al dispositivo de comunicación en base al identificador; y

un circuito (308) configurado para proporcionar la conexión de datos sin SIM al dispositivo de comunicación, en donde:

el receptor (304) está además configurado para recibir una dirección de un servidor que proporciona un servicio de seguridad al dispositivo de comunicación o un nombre de un proveedor de servicios que proporciona un servicio de seguridad al dispositivo de comunicación; y

el determinador (306) está además configurado para determinar si la conexión de datos sin SIM solicitada debe proporcionarse al dispositivo de comunicación en base a la dirección del servidor o al nombre del proveedor de servicios.

2. Un método para operar una estación (128) base de radio celular de área extensa, que comprende

recibir (702) desde un dispositivo de comunicación una solicitud para establecer una conexión de datos sin Módulo de Identificación de Abonado, SIM, de acuerdo con una tecnología de comunicación por radio celular de área extensa para facilitar la comunicación de las instrucciones de seguridad y mensajes de solicitud y de respuesta de estado de verificación, y un identificador que identifica de manera única una unidad central de procesamiento, CPU, del dispositivo de comunicación;

determinar (704) si la conexión de datos sin SIM solicitada debe proporcionarse al dispositivo de comunicación en base al identificador; y

proporcionar (706) la conexión de datos sin SIM al dispositivo de comunicación, que comprende además

recibir una dirección o un nombre de un servidor que proporciona un servicio de seguridad al dispositivo de comunicaciones: y

determinar si la conexión de datos sin SIM solicitada debe proporcionarse al dispositivo de comunicación en base a la dirección o al nombre del servidor.

FIG 1

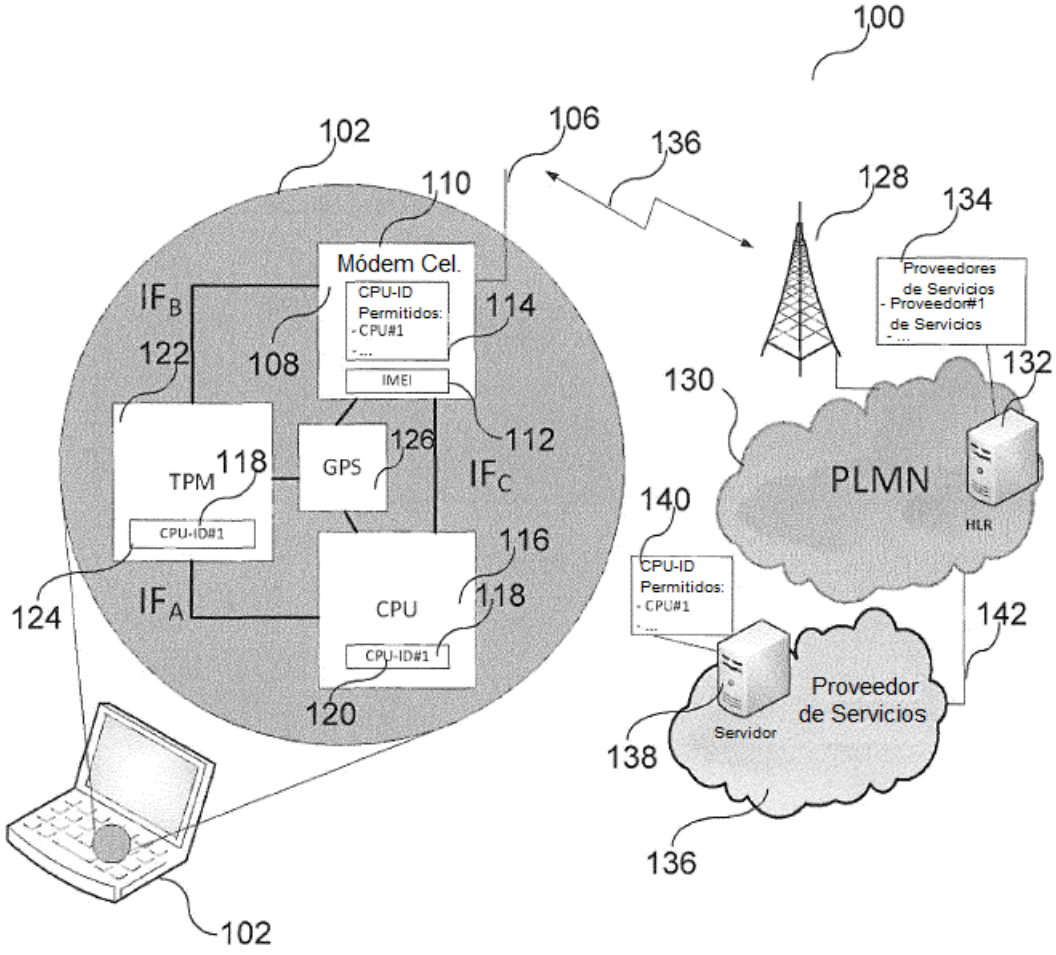

100
102
106
136
110
128
134
Módem Cel.
CPU-ID
Permitidos:
- CPU#1
- ...
IMEI
114
IF_B
122
108
112
TPM
118
GPS
126
IF_C
CPU-ID#1
116
124
IF_A
CPU
118
CPU-ID#1
120
Proveedores
de Servicios
- Proveedor#1
de Servicios
- ...
132
130
PLMN
HLR
140
CPU-ID
Permitidos:
- CPU#1
- ...
142
Proveedor
de Servicios
Servidor
138
136
102

FIG 2

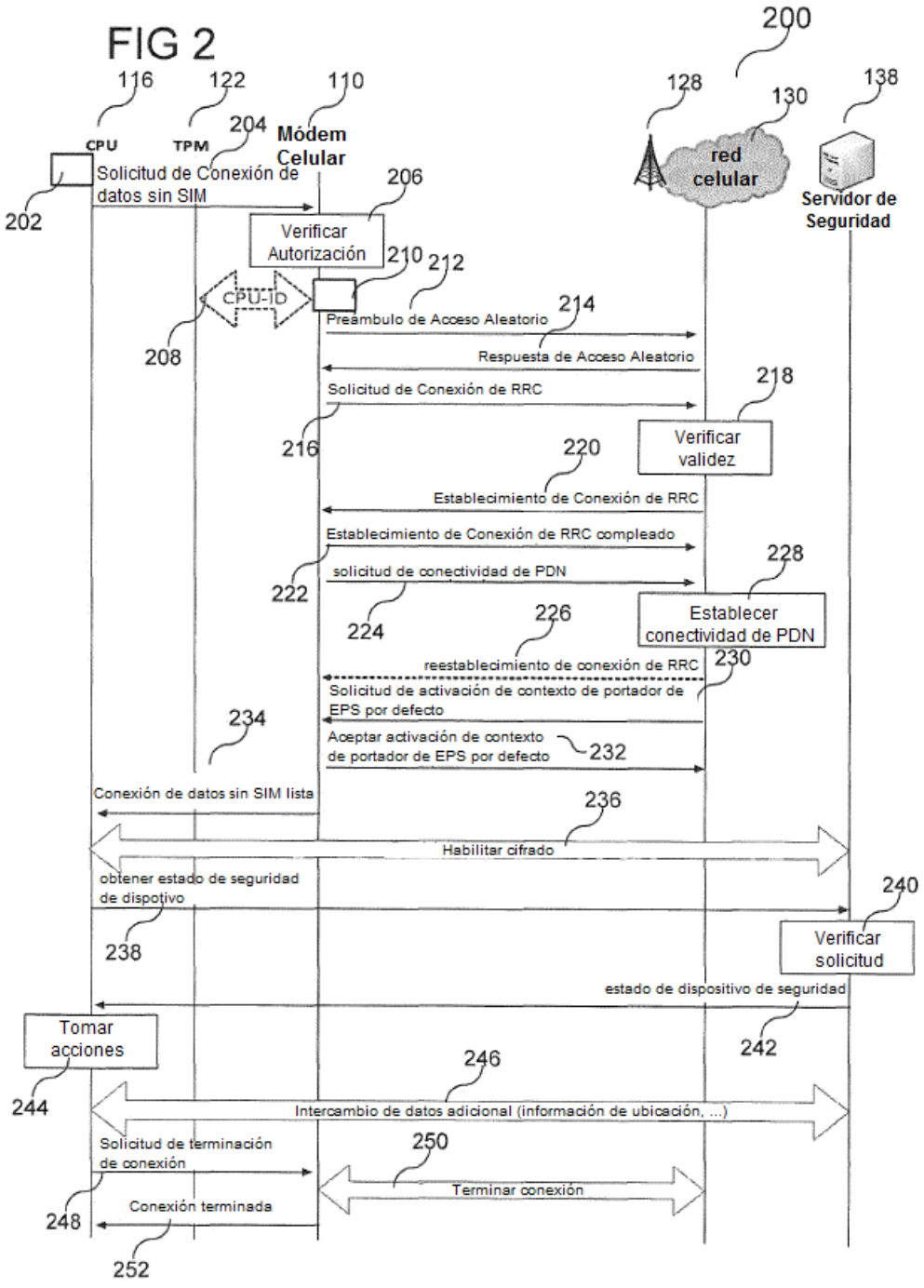

200
116
122
110
128
130
138
CPU
TPM
Módem Celular
red celular
Servidor de Seguridad
204
Solicitud de Conexión de datos sin SIM
202
206
Verificar Autorización
210
212
CPU-ID
208
Preambulo de Acceso Aleatorio
214
Respuesta de Acceso Aleatorio
Solicitud de Conexión de RRC
218
216
Verificar validez
220
Establecimiento de Conexión de RRC
Establecimiento de Conexión de RRC compleado
228
222
solicitud de conectividad de PDN
224
226
Establecer conectividad de PDN
reestablecimiento de conexión de RRC
230
Solicitud de activación de contexto de portador de EPS por defecto
234
Aceptar activación de contexto de portador de EPS por defecto
232
Conexión de datos sin SIM lista
236
Habilitar cifrado
obtener estado de seguridad de dispotivo
240
238
Verificar solicitud
estado de dispositivo de seguridad
Tomar acciones
242
246
244
Intercambio de datos adicional (información de ubicación, ...)
Solicitud de terminación de conexión
250
Terminar conexión
248
Conexión terminada
252

FIG 3

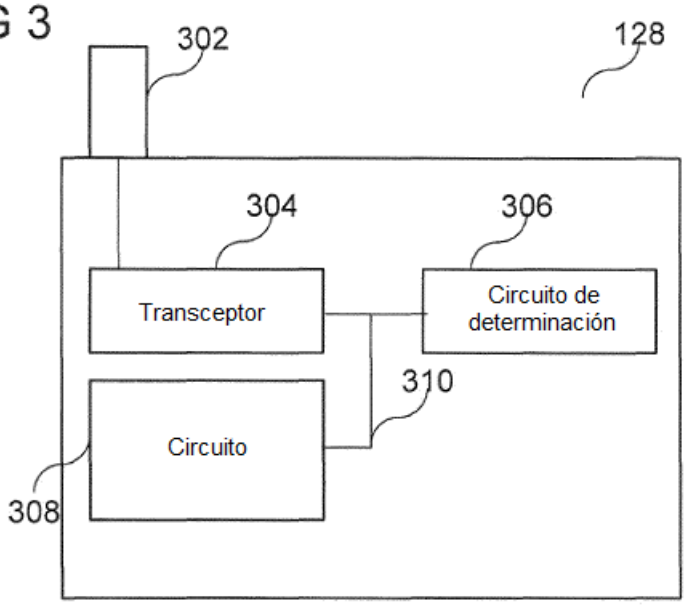

302
128
304
306
Transceptor
Circuito de determinación
310
Circuito
308

FIG 4

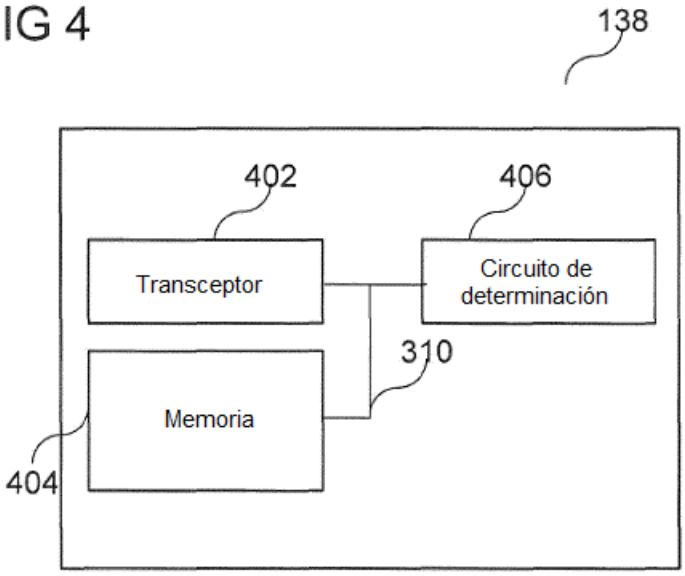

138
402
406
Transceptor
Circuito de determinación
310
Memoria
404

FIG 5

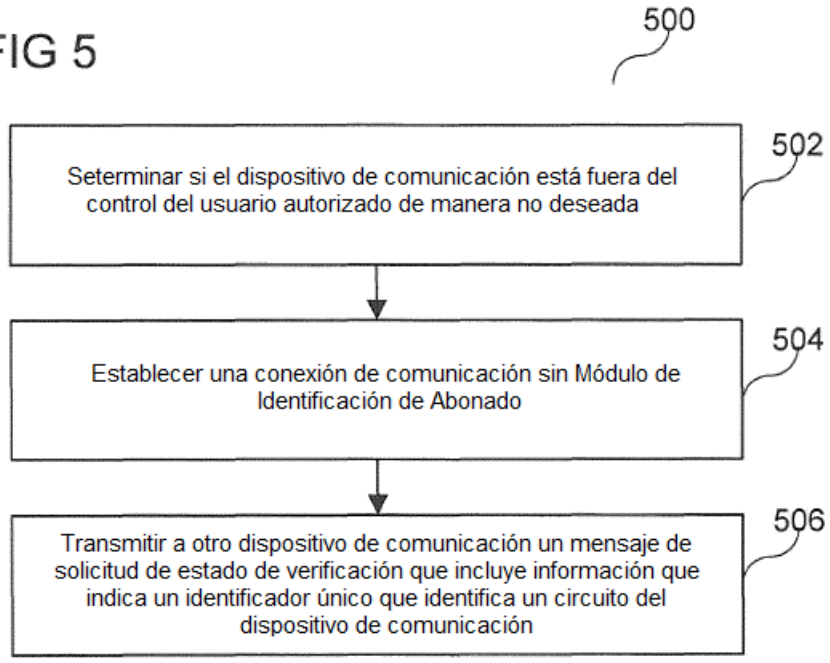

500
Seterminar si el dispositivo de comunicación está fuera del control del usuario autorizado de manera no deseada
502
Establecer una conexión de comunicación sin Módulo de Identificación de Abonado
504
Transmitir a otro dispositivo de comunicación un mensaje de solicitud de estado de verificación que incluye información que indica un identificador único que identifica un circuito del dispositivo de comunicación
506

FIG 6

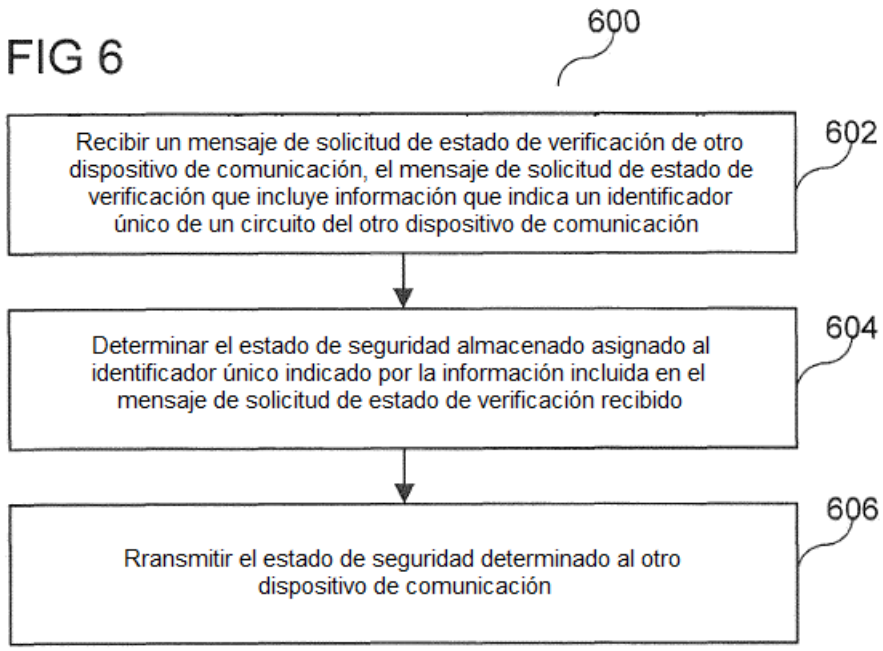
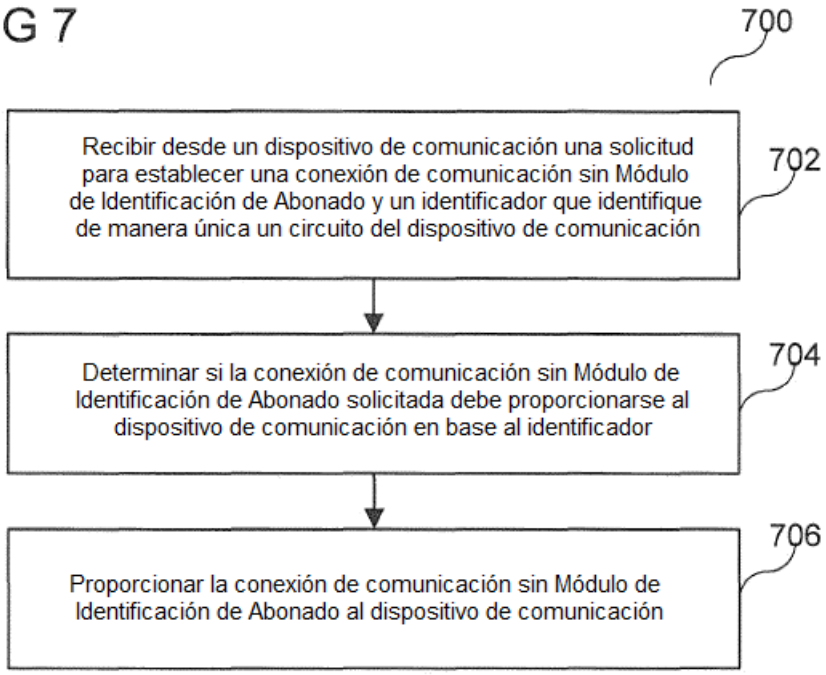

600
Recibir un mensaje de solicitud de estado de verificación de otro dispositivo de comunicación, el mensaje de solicitud de estado de verificación que incluye información que indica un identificador único de un circuito del otro dispositivo de comunicación
602
Determinar el estado de seguridad almacenado asignado al identificador único indicado por la información incluida en el mensaje de solicitud de estado de verificación recibido
604
Rransmitir el estado de seguridad determinado al otro dispositivo de comunicación
606

FIG 7


700
Recibir desde un dispositivo de comunicación una solicitud para establecer una conexión de comunicación sin Módulo de Identificación de Abonado y un identificador que identifique de manera única un circuito del dispositivo de comunicación
702
Determinar si la conexión de comunicación sin Módulo de Identificación de Abonado solicitada debe proporcionarse al dispositivo de comunicación en base al identificador
704
Proporcionar la conexión de comunicación sin Módulo de Identificación de Abonado al dispositivo de comunicación
706