(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 611 163**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.10.2008 PCT/FI2008/050608**

(87) Fecha y número de publicación internacional: **07.05.2009 WO09056679**

(96) Fecha de presentación y número de la solicitud europea: **29.10.2008 E 08844959 (0)**

(97) Fecha y número de publicación de la concesión europea: **07.12.2016 EP 2215795**

(54) Título: **Comunicación encriptada entre extremos**

(30) Prioridad:

31.10.2007 FI 20075776

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.05.2017

(73) Titular/es:

AIRBUS DEFENCE AND SPACE OY (100.0%)
Hiomotie 32
00380 Helsinki, FI

(72) Inventor/es:

KAUHANEN, LARI-MIKKO y
TAMMIO, MATTI

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Comunicación encriptada entre extremos

Sector de la invención

La presente invención se refiere a las comunicaciones y, en particular, a la comunicación encriptada entre extremos.

Antecedentes

En las redes avanzadas que ofrecen las características de comunicación necesarias para los exigentes usuarios modernos, los costes de inversión y mantenimiento fácilmente llegan a ser muy elevados. Esto se soluciona utilizando los recursos compartidos. En las redes públicas, los usuarios suscritos a ello comparten inherentemente los recursos disponibles de la red. Un operador establece una red y los abonados retornan la inversión y compensan los costes de mantenimiento abonando sus facturas mensuales.

En los sistemas profesionales, las redes han sido tradicionalmente privadas, pero una tendencia sensata en los últimos años ha sido hacia las redes compartidas. Existen ya algunas tecnologías en las que un operador puede establecer la red y la ejecuta, y se proporcionan organizaciones de usuarios con un recurso de comunicación contratado que pueden utilizar sin, no obstante, poner en peligro la privacidad de las comunicaciones entre los miembros de sus organizaciones. Las organizaciones pagan su recurso de comunicación adquirido de acuerdo con un contrato con el operador. Un ejemplo de dichos sistemas es TETRA (Radio truncada terrestre – TErrestrial Trunked RAdio, en inglés), especificado por el Instituto de Estándares de Telecomunicaciones Europeo (ETSI – European Telecommunications Standards Institute, en inglés).

Además de las medidas protectoras ofrecidas por la tecnología de red aplicada, algunos usuarios privados o profesionales están interesados en añadir un nivel más de seguridad a sus comunicaciones. La encriptación entre extremos es un mecanismo que proporciona protección continua de la confidencialidad e integridad de la información transmitida, mediante su encriptación en el origen y su desencriptación en su destino. En cualquiera de las etapas intermedias, la información está disponible solo en forma encriptada y, por lo tanto, es posible que un extremo de la comunicación envíe información a otro extremo de la comunicación sin que ningún elemento intermedio en el flujo del mensaje esté accesible.

El principio básico en la comunicación entre extremos es que entre los extremos exista un secreto compartido con cuya utilización la información se puede proteger en el extremo de transmisión y revocar la protección en el extremo de recepción. Típicamente, esto se implementa mediante la utilización de un algoritmo de encriptación en el extremo de transmisión y un algoritmo de desencriptación correspondiente en el extremo de recepción, y mediante el conocimiento compartido de una clave secreta de cifrado. El requisito esencial, sin embargo, es entonces que los dos extremos apliquen el mismo secreto, por ejemplo, la misma clave o par de claves que están en uso en ambos extremos. Típicamente, las claves de encriptación entre extremos se cambian, con el fin de evitar la posibilidad de que un tercero pueda determinar el código interceptando los mensajes transmitidos.

La gestión de las claves se refiere a las operaciones para la generación, el almacenamiento, la distribución, el borrado, el archivado y la aplicación de las claves de acuerdo con una política de seguridad. Cuando las claves de encriptación entre extremos se cambian dinámicamente, la gestión de las claves se convierte en un problema. Típicamente, el conocimiento del estado actual y de los ajustes de los parámetros que controlan las operaciones se mantiene en la red, es decir, está bajo el control del operador de la red. Por otro lado, la gestión de las claves de encriptación entre extremos está bajo el control de las partes en comunicación, o de la organización a la que pertenece. Cuando estas dos partes no tienen acceso directo a los procedimientos del otro, es posible que el conocimiento del cambio en las claves de encriptación entre extremos no esté disponible simultáneamente para todas las partes en comunicación. Por otro lado, un cambio no se puede llevar a efecto antes de que las partes sean conscientes de que se debe hacer un cambio. Por ejemplo, un usuario puede haber desconectado su terminal, o puede haber conectado su terminal pero no está lo suficientemente cerca o puede operar de otro modo el terminal para confirmar el cambio, o el usuario se puede encontrar en un área que está fuera de cobertura. En cualquiera de estos casos las operaciones relativas al cambio resultan complicadas, impredecibles en el tiempo o pueden implicar la realización de un número considerablemente mayor de comunicaciones. En el peor caso, se pueden perder vidas debido a que el personal de rescate que ha asumido una operación conjunta no se puede comunicar entre sí.

El documento EP1826984 da a conocer un método para la comunicación encriptada dentro de un grupo de dispositivos de comunicación. El método incluye una etapa de distribuir información de claves, que tienen un tiempo de validez limitado, a los dispositivos de comunicación del grupo

Compendio de la invención

Un objetivo de la presente invención es, así, proporcionar un método y aparato para implementar el método para solucionar al menos algunos de los problemas anteriores. Los objetivos de la invención se alcanzan mediante un método y una disposición, que están caracterizados por lo que se presenta en las reivindicaciones independientes. Las realizaciones preferidas de la invención se describen en las reivindicaciones dependientes.

La invención se basa en la idea de asociar claves de encriptación entre extremos con una indicación de validez que indica un grupo criptográfico en el que la clave se va a aplicar, y un periodo durante el cual la clave es aplicable en ese grupo criptográfico concreto. El grupo criptográfico puede corresponder a un grupo de dos terminales de usuario para una llamada individual, o a uno o más grupos de conversación que aplican la misma clave de encriptación entre extremos.

Debido a esto, la gestión de las claves de encriptación entre extremos resulta más fácil y predecible, y la seguridad de las operaciones basada en la comunicación mejora.

Breve descripción de los dibujos

A continuación, la invención se describirá con mayor detalle por medio de las realizaciones preferidas con referencia a los dibujos adjuntos, en los cuales

la figura 1 ilustra los principales elementos de un sistema de radio TETRA realizado;

la figura 2 muestra una configuración del hardware de referencia de un elemento KMC;

la figura 3 muestra una configuración del hardware de referencia de una estación de telefonía móvil;

la figura 4 ilustra una realización de un proceso de encriptación entre extremos aplicable en el sistema TETRA realizado;

la figura 5A ilustra una pluralidad de grupos de conversación TG1 a TG8;

la figura 5B muestra la división de los grupos de conversación en grupos de usuarios y grupos criptográficos;

la figura 6 ilustra un registro almacenado en el módulo de seguridad de la estación de telefonía móvil realizada en la figura 3;

la figura 7 ilustra un procedimiento de ejemplo para implementar la encriptación entre extremos en el contexto de la estación de telefonía móvil realizada de la figura 3; y

la figura 8 ilustra una procedimiento de ejemplo para implementar una encriptación entre extremos en el contexto del elemento KMC de la figura 2 realizado.

Descripción detallada de la invención

Las realizaciones siguientes son implementaciones de ejemplo de la presente invención. Aunque la especificación se puede referir a “una”, “alguna” o “algunas” realización o realizaciones, no es necesario hacer referencia a la misma realización o las mismas realizaciones, y/o una característica no aplica solo a una única realización. Las características únicas de diferentes realizaciones de esta memoria se pueden combinar para proporcionar otras realizaciones.

A continuación, la invención se describe utilizando los términos y elementos del sistema TETRA tal como se especifica en los Estándares de Telecomunicación Europeos ETSI EN 300 392-2; Estándar Europeo (Serie de Telecomunicaciones); Radio Truncada Terrestre (TETRA); Datos más Voz (V + D); Parte 2: Interfaz Aérea (AI – Air Interface, en inglés), y ETSI EN 300 392-7; Estándar Europeo (Serie de Telecomunicaciones); Radio Truncada Terrestre (TETRA); Datos más Voz (V + D); Parte 7: Seguridad, y Radio Truncada Terrestre (TETRA); Seguridad; mecanismo de sincronización para encriptación entre extremos, no obstante sin limitar la invención a esta una tecnología del sistema de radio. La presente invención se puede aplicar a cualquier sistema de comunicación, en el que se proporciona encriptación entre extremos entre dos o más partes en comunicación.

La figura 1 muestra una ilustración simplificada de los principales elementos de un sistema de radio TETRA realizado. TETRA en un sistema de radio para móviles que comprende al menos una infraestructura de conmutación y gestión (SwMI – SWitching and Management Infrastructure, en inglés) 1 y una estación de telefonía móvil (MS – Mobile Station, en inglés) 2. SwMI es equipo para una red de voz más datos (V + D), que permite a terminales de abonado comunicarse entre sí. En la figura 1, SwMI comprende una central digital (DXT) 3 y una estación de base (TBS) 4, pero naturalmente el tipo y número de elementos y sus interconexiones pueden variar de acuerdo con el sistema e implementación específicos. De este modo, el tipo y número de unidades que constituyen SwMI no son esenciales para la citada invención.

Un bloque de interfaz 5 denota las diferentes interfaces de la central digital. Estas facilitan conexiones entre las estaciones de telefonía móvil y, por ejemplo, las redes de datos interna y externa, otros sistemas de telefonía móvil analógicos o digitales, la red de telefonía conmutada pública, y otros.

De los terminales de abonado, la estación de telefonía móvil (MS) 2 está dispuesta para acceder a la SwMI a través de una interfaz aérea 6. Además, en los sistemas TETRA, se puede proporcionar asimismo un sistema de emisión para facilitar la comunicación de emisión. El sistema de emisión es típicamente una combinación de controladores

de estación emisora 7 y una o más estaciones de trabajo 8 de emisión o un sistema de servidores y estaciones de trabajo conectados con ellas. El sistema de emisión se comunica con la SwMI utilizando un protocolo de red adecuado, por ejemplo E1, ISDN-BA o IP. La estación de trabajo de emisión 8 se puede comunicar con los otros abonados de la red y/o gestionar el sistema, abonado, grupo y/o parámetros específicos de la organización del sistema de radio. En algunos sistemas, toda o parte de esta funcionalidad de gestión del abonado se pueden encontrar en el sistema de gestión de la red.

El sistema puede comprender asimismo un centro de gestión de claves (KMC – Key Management Centre, en inglés) 9 que gestiona las claves criptográficas de al menos algunos de los abonados del sistema. El KMC puede ser un solo elemento de la red o una combinación de elementos. En la figura 1, el KMC se muestra directamente conectado a la DXT, pero se puede aplicar cualquier otro protocolo aplicable, incluido E1, ISDN-BA o IP, para la conexión. Asimismo, resulta claro, no obstante, que para una mera provisión de claves de encriptación entre extremos, el KMC no necesita estar conectado de manera continua a la SwMI, en absoluto.

El diagrama de bloques de la figura 2 muestra una configuración del hardware de referencia de un elemento del KMC 9 de acuerdo con la presente realización de la invención. El elemento comprende una unidad de procesamiento 21, un elemento que comprende una función lógica aritmética; un número de registradores y de circuitos de control especiales. Conectada a la unidad de procesamiento está una unidad de memoria 22, un medio de datos en el que se pueden almacenar datos o programas legibles por ordenador o datos del usuario. La unidad de memoria 22 típicamente comprende componentes que permiten tanto lectura como escritura (RAM – Random Access Memory, en inglés) y memoria cuyo contenido solo se puede leer (ROM – Read Only Memory, en inglés). El elemento comprende además un bloque de interfaz 23 con una unidad de entrada 24 para introducir datos para procesamiento interno en el elemento, y una unidad de salida 25 para producir datos procedentes de procesos internos del elemento. Ejemplos de la citada unidad de entrada comprenden una unidad de enchufar que actúa como puerta de enlace para la información suministrada a sus puntos de conexión externa. Ejemplos de la citada unidad de salida incluyen una unidad de enchufar que proporciona información a las líneas conectadas a sus puntos de conexión externa.

La unidad de procesamiento 21, la unidad de unidad de memoria 22 y el bloque de interfaz 23 están interconectados eléctricamente para la ejecución sistemática de operaciones sobre los datos recibidos y/o almacenados de acuerdo con los procesos predefinidos, programados esencialmente, de un elemento del KMC. Estas operaciones se describen con más detalle con la figura 8.

El diagrama de bloques de la figura 3 muestra una configuración de hardware de referencia de la estación de telefonía móvil (MS) 2 de acuerdo con la presente realización de la invención. La estación de telefonía móvil 2 comprende una unidad de interfaz de usuario 31 con al menos una unidad de entrada para la introducción de datos por parte del usuario de la estación de telefonía móvil y al menos una unidad de salida para la emisión de datos. Ejemplos de las citadas unidades de entrada comprenden un teclado numérico, una pantalla táctil, un micrófono u otros. Ejemplos de las citadas unidades de salida comprenden una pantalla, una pantalla táctil, un altavoz u otros. La interfaz de usuario está conectada eléctricamente a una unidad de procesamiento 32 para la ejecución sistemática de operaciones sobre los datos. La unidad de procesamiento 32 es un elemento central que comprende esencialmente una unidad de lógica aritmética, y un número de registradores y circuitos de control especiales. Por ejemplo, las funciones implementadas por la unidad de procesamiento 32 en la transmisión comprenden típicamente: codificación, reordenación, intercalado, aleatorización, multiplexación de canales y construcción de ráfaga. Las funciones de la unidad de procesamiento se controlan, al menos parcialmente, mediante un código de programa, de tal manera que la estación de telefonía móvil implementa los procedimientos que se describen a continuación en la descripción.

Una unidad de memoria 33 de la estación de telefonía móvil es un medio de datos en el que se pueden almacenar datos o programas legibles por ordenador, o datos del usuario, y está conectada a la unidad de procesamiento 32. En una estación de telefonía móvil la unidad de memoria 33 comprende típicamente componentes que permiten tanto la lectura como la escritura (RAM) y la memoria cuyo contenido solo se puede leer (ROM).

Una unidad de transmisión recepción 34 que comprende un transmisor 35 y un receptor 36 está conectada eléctricamente a la unidad de procesamiento 32. El transmisor 35 recibe una secuencia de datos desde la unidad de procesamiento 32, y la convierte en una señal de radio para su transmisión por parte de una antena 37. De manera correspondiente, las señales de radio recibidas por la antena 37 con conducidas al receptor 36, que convierte las señales de radio en una secuencia de bits que es enviada para su posterior procesamiento a la unidad de procesamiento 32.

La estación de telefonía móvil realizada comprende asimismo un módulo de seguridad 38. El módulo de seguridad 38 es un medio seguro para almacenar y transportar información. En esta realización, se aplica un modelo de seguridad separable que puede ser insertado de manera extraíble en la estación de telefonía móvil para la identificación del usuario e información relacionada con la seguridad. El módulo de seguridad 38 separable es accesible para la unidad de procesamiento 32 a través de una interfaz definida entre la estación de telefonía móvil y el módulo de abonado extraíble. Un ejemplo del módulo de abonado extraíble es una tarjeta inteligente utilizada como módulo de identidad del abonado de la estación de telefonía móvil. El Memorándum del Grupo de Seguridad y

de Protección contra el Fraude de TETRA de la Asociación de Comprensión ha especificado una interfaz entre una tarjeta inteligente y terminales TETRA para los propósitos de la encriptación entre extremos.

Un módulo separable resulta ventajoso por que permite la adaptación de la estación de telefonía móvil al usuario de tal manera que el resto del equipo de la estación de telefonía móvil puede ser implementado sin información relativa a la identificación del usuario y a la seguridad. Esto significa que el resto de la configuración de la estación de telefonía móvil se adapta fácilmente al uso personal de diferentes abonados. Sin embargo, la capacidad de separación no es esencial para la invención. El módulo se puede implementar de otras maneras que se desvían del alcance de protección. Por ejemplo, el módulo de seguridad puede corresponder a una unidad lógica que comprende las funciones para las operaciones del módulo de seguridad descritas en esta memoria, y se implementa como una parte integrada del hardware y el software de la estación de telefonía móvil.

La unidad de procesamiento 32, la unidad de memoria 33, la unidad de interfaz de usuario 32, la unidad de transmisión recepción 34 y el módulo de seguridad 38 están interconectados eléctricamente para proporcionar medios para ejecutar sistemáticamente operaciones sobre los datos recibidos y/o almacenados de acuerdo con los procesos predefinidos programados esencialmente de la estación de telefonía móvil. En las soluciones realizadas de acuerdo con la invención, las operaciones comprenden funciones para la comunicación encriptada entre extremos con otros terminales accesibles a través del sistema TETRA. Estas operaciones se describen con más detalle en las figuras 4 a 7.

Se debe observar que solo se ilustran en las figuras 2 y 3 los elementos necesarios para dar a conocer la presente realización. Para una persona experta en la materia, resulta claro que una estación de telefonía móvil y los elementos de conmutación y de infraestructura de gestión comprenden una pluralidad de otros elementos y funcionalidades no ilustrados explícitamente en esta memoria. Además, los bloques ilustran unidades lógicas o funcionales que pueden ser implementadas en o con una o más unidades físicas, sin perjuicio de si se ilustran como uno o más bloques en las figuras 2 y 3. Además, la estación de telefonía móvil representa una amplia variedad de terminales de usuario diferentes que pueden ser fijos, portátiles o móviles.

La seguridad es un factor crítico en muchas implementaciones de TETRA, y por lo tanto la comunicación en un sistema TETRA necesita estar protegida de muchas maneras. Una de las maneras para asegurar la confidencialidad y la integridad de las comunicaciones es la encriptación. La encriptación se refiere a un mecanismo de seguridad de la información que realiza una transformación de la información de acuerdo con un sistema criptográfico. Un sistema criptográfico típicamente comprende un algoritmo y claves criptográficas correspondientes.

La encriptación de la interfaz aérea se refiere a un mecanismo en el que los mensajes de datos, la señalización y la conversación codificada enviados en la trayectoria de radio están cifrados con una clave de encriptación y un algoritmo. La encriptación de la interfaz aérea protege la confidencialidad de la comunicación en el enlace de radio de manera efectiva. La encriptación entre extremos se refiere a una encriptación dentro o en el sistema de extremo de la fuente de tal manera que la correspondiente desencriptación se produce solo dentro de o en el sistema del extremo de destino. Se debe observar que la encriptación de la interfaz aérea está típicamente separada del servicio de encriptación entre extremos, y típicamente es re-encriptada con la función de encriptación de la interfaz aérea. En la encriptación entre extremos el tráfico de usuario puede, por consiguiente, ser transmitido desde el terminal de usuario de transmisión a través de una red en forma encriptada hasta que llega al terminal de usuario en el que es desencriptada.

La figura 4 ilustra una realización de un proceso entre extremos aplicable en el sistema TETRA realizado. El proceso implica un extremo de transmisión 402 y un extremo de recepción 404 y un elemento de sistema 400 que suministra la secuencia de información desde el extremo de transmisión 402 al extremo de recepción 404. Desde el punto de vista del proceso de encriptación entre extremos, el elemento de sistema 400 representa una mera conducción a través de la cual la información es suministrada de manera transparente en una forma substancialmente no modificada entre los extremos. En el extremo de transmisión, un códec 406 representa funciones que introducen en el proceso una secuencia de datos que corresponde a datos de entrada por parte del usuario o una aplicación del terminal. Por ejemplo, en el caso de la entrada de voz, la entrada de voz analógica a través de la interfaz de usuario se convierte en una señal digital que se proporciona desde el códec al proceso. La secuencia de datos se denomina secuencia de datos de texto plano para denotar que los contenidos semánticos de la secuencia de datos son inteligibles sin utilizar algoritmos de desencriptación entre extremos.

La función de un generador de secuencia de clave (KSG – Key Stream Generator, en inglés) 408 es proporcionar un segmento de la secuencia de clave que se utiliza en el proceso para encriptar y desencriptar esa secuencia de datos de texto plano. Con el fin de conseguir esto, KSG comprende un algoritmo E1 que requiere dos entradas, una clave de cifrado CK (Cypher Key, en inglés) y un valor de inicialización IV (Initialization Value, en inglés). El valor de inicialización IV se refiere a un parámetro variable en el tiempo (por ejemplo, un número de secuencia o una marca de tiempo) que se utiliza para inicializar la sincronización de las unidades de encriptación, y proporciona con ello protección frente a una nueva reproducción. La clave de cifrado CK se refiere a un secreto compartido por los extremos de transmisión y recepción, y se implementa típicamente como una secuencia de símbolos que controla la operación de cifrado y descifrado. Un acuerdo mutuo sobre una clave de cifrado CK común a utilizar en un proceso de cifrado / descifrado subsiguiente garantiza que la comunicación sigue siendo segura en su ruta a través del

elemento del sistema 400. La función de encriptación primera 410combina la secuencia de datos de texto plano de la etapa 406 con el segmento de la secuencia de clave de la etapa 408, lo que resulta en una secuencia de datos de texto cifrada encriptada.

Permitir la encriptación, KSG debe estar sincronizado en el extremo de transmisión. Para ello, se utiliza un vector de sincronización SV (Synchronization Vector, en inglés). La transferencia de los datos de sincronización se consigue robando tramas de conversación (semi-intervalos) del tráfico de U-plano. Un constructor de tramas SF 412 crea tramas de sincronización y las proporciona a la segunda función de encriptación SC 416. En los tiempos controlados por el gestor de la sincronización 414, la segunda función de encriptación 416 reemplaza la mitad de un intervalo de la secuencia de datos de texto cifrado encriptada con la trama de sincronización. La secuencia de datos codificados entre extremos (E2EE) se proporciona a través del elemento del sistema 400 al extremo de recepción 404.

En el extremo de recepción 404, una primera función de desencriptación 420 comprueba si existe una trama de sincronización en la secuencia de datos E2EE recibida. Si la respuesta es sí, la primera función de desencriptación 420 proporciona la trama de sincronización detectada a un detector de sincronización SD (Synchronization Detector, en inglés) 422. El vector de sincronización SV recibido en la trama de sincronización se carga en el KSG 426 y se utiliza con la clave de cifrado CK para proporcionar un segmento de la secuencia de claves que se introduce en la segunda función de desencriptación 424. Asimismo, la secuencia encriptada de datos de texto cifrados se proporciona a la segunda función de desencriptación 424, en la que el segmento de la secuencia de clave de la etapa 420 y la secuencia encriptada de datos de texto cifrados se combina resultando en una secuencia de bits desencriptados. Esta secuencia de bits es introducida en un códec 428. En el extremo de recepción, el códec 428 representa funciones que introducen desde el proceso una secuencia de datos que corresponde a una señal digital para ser proporcionada al usuario o a una aplicación del terminal. Por ejemplo, en el caso de una entrada de voz, la secuencia de datos desencriptada constituye una señal digital que es proporcionada al códec para ser convertida en una salida de voz analógica a través de la interfaz de usuario.

Para una persona experta en la materia resulta claro que en un extremo de la comunicación, por ejemplo, en un terminal de usuario o de aplicación, un códec típicamente comprende funciones de los codecs 406, 428 o ambos de los extremos de finalización. Además, un extremo de la comunicación típicamente comprende funciones del extremo tanto de transmisión 402 como de recepción 404.

Tal como resulta evidente a partir de la figura 4, el uso de un algoritmo de encriptación entre extremos requiere el conocimiento de un secreto compartido, la clave de cifrado CK. Además de esto, la implementación de la encriptación entre extremos típicamente requiere algunas otras claves, por ejemplo para soportar procedimientos seguros de gestión de claves. En la realización de la figura 3, estas claves se almacenarán en una tarjeta inteligente utilizada como módulo de seguridad de la estación de telefonía móvil.

En TETRA, existen al menos dos maneras utilizadas habitualmente para cargar las claves en una base de datos segura del módulo de seguridad. En una operación fuera de banda, el módulo de seguridad está conectado eléctricamente a un ordenador, por ejemplo un ordenador personal, un software de aplicación que se ejecuta en el módulo de seguridad, y el ordenador carga las claves en el módulo de seguridad. La seguridad de la disposición es confirmada por el usuario de usuarios que realizan el procedimiento de carga. Para una mejora adicional de la seguridad de la disposición, las secuencias de datos entre la aplicación del ordenador y la aplicación del terminal se pueden encriptar.

En codificación en el aire (OTAK – Over The Air Keying, en inglés) las claves se cargan en el módulo de seguridad procedentes de un centro de gestión de claves situado en la red. La información del centro de gestión de claves se proporciona a la estación de telefonía móvil utilizando mensajes cortos definidos basados en mensajes de OTAK. Estos mensajes están habitualmente encriptados.

De acuerdo con ello, las claves aplicadas en la presente realización comprenden claves de encriptación de claves, claves de encriptación del tráfico y claves de encriptación de la señalización. Un terminal de usuario puede tener una clave de encriptación de claves (KEK – Key Encryption Key, en inglés) para proteger otras claves de encriptación durante su suministro y/o almacenamiento. Para un terminal de usuario existe típicamente una sola KEK que se carga en el módulo de seguridad utilizando el método de fuera de banda. Otra clave aplicable para proteger otras claves es la clave de encriptación de grupo (GEK – Group Encryption Key, en inglés). Se puede cargar en el módulo de seguridad utilizando OTAK protegida con la KEK del módulo de seguridad. GEK se utiliza a menudo con preferencia sobre la KEK en la protección de la clave de cifrado real, la clave de de encriptación del tráfico (TEK – Traffic Encryption Key, en inglés). El módulo de seguridad puede comprender una o más TEK que se pueden cargar en el módulo de seguridad utilizando el método de fuera de banda u OTAK. Las claves de encriptación de la sincronización (SEK – Signalling Encryption keys, en inglés) son claves opcionales que se pueden utilizar para proteger los mensajes de OTAK. El módulo de seguridad típicamente contiene solo una SEK por sistema criptográfico. En ocasiones se utiliza TEK en la SEK para proteger los datos tanto de sincronización como de usuario.

Debido a la idea básica del secreto compartido, resulta claro que ambos extremos deben utilizar entre ellos la misma TEK en la comunicación encriptada entre extremos. El uso de claves estáticas no es suficientemente seguro;

necesitan ser cargadas dinámicamente de tal manera que la integridad de la comunicación se pueda mantener. El cambio de claves se ha efectuado convencionalmente de tal manera que un grupo de TEK han sido almacenadas en el módulo de seguridad. En OTAK, un mensaje que comprende una orden para cambiar a otra clave ha sido proporcionado con una secuencia de mensaje de OTAK definida. En el método de fuera de banda los usuarios han sido contactados y se les solicita que activen nuevas claves.

Cuando se trata solo con comunicación de uno a uno, ninguno de estos esquemas es un problema, porque dos terminales de usuario son gestionados fácilmente. No obstante, si la comunicación de grupo protegido entre extremos debe estar soportada, existen problemas evidentes en la implementación del cambio de claves. Si se utiliza OTAK, cada miembro del grupo debe ser contactado antes de que se pueda realizar el cambio. Especialmente con los terminales de usuario móviles, todos los usuarios de un grupo pueden no estar accesibles necesariamente al mismo tiempo. Por ejemplo, un usuario puede estar en otro turno y haber desconectado su estación de telefonía móvil para poder dormir. La estación de telefonía móvil puede estar también fuera de cobertura u operar por alguna otra razón en modo directo. Gestionar estas clases de retardos puede resultar muy complicado, e implicar una cantidad considerable de mensajes de OTAK. Tales complicaciones pueden perturbar fácilmente la comunicación o la seguridad de todo el grupo.

De manera similar, la codificación fuera de banda requiere operaciones simultáneas de todos los usuarios. Por las mismas razones anteriores, situaciones en las que todos los usuarios del grupo se alcanzan y son libres de operar en sus terminales son muy extrañas. Esto complica la decisión en el tiempo en que se efectúa el cambio de una clave a otra. Tales dificultades poseen un considerable riesgo de utilizar la encriptación entre extremos en las comunicaciones de grupo.

La situación se ilustra con más detalle en las figuras 5A y 5B. La figura 5A muestra varios grupos de conversación TG1 a TG8 (Talk Group, en inglés). Un grupo de conversación representa un grupo de uno o más usuarios de terminales que pueden estar implicados en la comunicación utilizando una dirección común, una dirección de grupo. Cada uno de los grupos de conversación TG1 a TG8 está asociado con uno de los grupos criptográficos CG1 a CG5. Un grupo criptográfico se refiere a un conjunto de material clave que se utiliza para la comunicación en un grupo de conversación. En la figura 5A, los grupos de conversación se muestran además divididos en tres grupos de usuario UG1, UG2, UG3 (User Group, en inglés). Un grupo de usuarios se refiere a un conjunto de usuarios cuyas suscripciones y claves de encriptación están gestionadas por una entidad de gestión.

La figura 5B muestra una tabla que ilustra la división de la gestión de los grupos de usuarios (columnas) y los grupos criptográficos (filas). Resulta claro que todos los miembros en un grupo de conversación necesitan aplicar el mismo grupo criptográfico durante una llamada de grupo encriptada entre extremos. Un grupo criptográfico puede ser utilizado por más de un grupo de conversación y grupo de usuarios.

En TETRA tal dirección de grupo es GTSI (identidad de abonado de TETRA de grupo, en inglés), y se puede realizar una llamada de grupo seleccionando la GTSI y pulsando la tecla PTT del terminal de usuario. La figura 6 ilustra un registro 60 almacenado en el módulo de seguridad de la estación de telefonía móvil realizado en la figura 3. El registro 60 proporciona un conjunto de claves de encriptación entre extremos 61 aplicables en un grupo de conversación G1 particular. Con el fin de asegurar que todos los miembros del grupo G1 son capaces de aplicar simultáneamente la misma clave E2EE, las claves E2EE están asociadas con una marca de tiempo 62. La marca de tiempo 62 actúa como indicación en un periodo durante el cual la clave de encriptación entre extremos es aplicable en G1. En el ejemplo de la figura 6, la marca de tiempo denota específicamente la hora de expiración de la clave E2EE asociada. Otros métodos de denotar los periodos de tiempo y tipos de indicación se pueden aplicar sin desviarse del alcance de la protección. De manera similar, se pueden almacenar registros en la estación de telefonía móvil para otros grupos de conversación G2, G3, etc.

Se debe asimismo observar que incluso si las ventajas de la disposición inventada son más evidentes con la comunicación de grupo, la solución no está limitada a la comunicación de grupo, sino que es también aplicable directamente a la comunicación individual. En el caso de la presente realización, uno o más conjuntos de claves E2EE almacenados pueden ser aplicables a llamadas individuales entre el terminal de usuario de almacenamiento y otro terminal de usuario. Estos se consideran que forman un grupo de comunicación de dos terminales de usuario.

La figura 7 ilustra un procedimiento de ejemplo para implementar encriptación entre extremos en el contexto de la estación de telefonía móvil realizada de la figura 3. El procedimiento empieza con la estación de telefonía móvil recibiendo (70) un conjunto de claves aplicable a la comunicación encriptada entre extremos. La recepción puede tener lugar utilizando OTAK o una operación fuera de banda, tal como se ha explicado anteriormente. En OTAK, la estación de telefonía móvil transmite las claves recibidas en el mensaje de OTAK al módulo de seguridad a través de la interfaz definida. En las operaciones fuera de banda, el módulo de seguridad puede estar conectado directamente con el ordenador, o la conexión se puede establecer hasta la estación de telefonía móvil y las aplicaciones en el ordenador y el módulo de seguridad, y a continuación, comunicarse sobre una interfaz de programación de aplicación definida de la estación de telefonía móvil. Las claves están asociadas con una indicación que indica un grupo criptográfico en el que se debe aplicar la clave, y un periodo de tiempo durante el cual la clave es aplicable a ese grupo concreto. La estación de telefonía móvil realizada almacena (etapa 71) las claves recibidas en el módulo de seguridad y se queda en espera (etapa 72) para un nuevo inicio de comunicación. Cuando la

estación de telefonía móvil detecta (etapa 73) un inicio de comunicación, comprueba (etapa 74) si existe un nuevo registro válido para el grupo criptográfico de la comunicación. Un grupo criptográfico puede ser otro abonado para comunicación individual o un grupo de conversación para la comunicación en grupo. La validez del registro se comprueba sobre la base de las marcas de tiempo asociadas con las claves almacenadas. Si no existen registros válidos (etapa 75), el procedimiento vuelve a la etapa 72. Si se encuentra un registro válido (etapa 75), la estación de telefonía móvil selecciona (etapa 76) la clave E2EE almacenada en el registro en uso y vuelve a la etapa 72.

La figura 8 ilustra un procedimiento de ejemplo para implementar encriptación entre extremos en el contexto del elemento de KMC realizado de la figura 4. El procedimiento empieza con el KMC obteniendo (etapa 81) un conjunto de claves aplicables como claves E2EE en los grupos criptográficos definidos. Las claves se pueden generar en el KMC utilizando una aplicación apropiada de generación de números aleatorios, o descargarse de otra fuente de generación de claves, y asignarse a los grupos criptográficos definidos. De acuerdo con la invención, etas claves están asociadas con una marca de tiempo que indica el periodo de validez para la clave. Tras el primer tiempo, el proceso de obtención puede ser continuo, de tal manera que tiene lugar en segundo plano durante otros procedimientos de KMC de tal manera que siempre hay claves disponibles durante un periodo definido en el futuro. El KMC se queda en espera (etapa 82) de una solicitud de suministro de clave. Cuando se detecta la solicitud (etapa 83), el KMC determina (etapa 84) un conjunto de uno o más registros y los proporciona (etapa 85) a un terminal de usuario. La determinación es una función ajustable de acuerdo con la aplicación. Por ejemplo, en la operación fuera de banda, el KMC puede determinar los grupos criptográficos a los que el terminal de usuario está autorizado a acceder, o se le puede autorizar a acceder, y carga un conjunto de claves criptográficas aplicables en esos grupos criptográficos al terminal de usuario. En OTAK, son posibles grandes descargas similares, pero típicamente se prefieren solicitudes menores y más específicas que se refieren a uno o más grupos criptográficos. Tras esto, el KMC vuelve a la etapa 81.

Se debe observar que las realizaciones anteriores se describen utilizando una estación de telefonía móvil como ejemplo de terminales de usuario, pero la invención no está limitada solo a estaciones de telefonía móvil. Cualquier tipo de terminales capaces de absorber tráfico del plano U se pueden considerar como terminales de usuario, incluyendo estaciones de trabajo emisores y servidores de aplicación conectados al sistema de comunicación. Adicionalmente, las realizaciones anteriores aplican encriptación simétrica en la que las partes en comunicación utilizan el conocimiento de la información secreta que se comparte con las partes en comunicación pero que no está disponible o se puede inferir sin un esfuerzo significativo para cualquier otra parte. Se debe observar que también se puede aplicar autenticación asimétrica en la que se utilizan pares de claves privada – pública para encriptar y desencriptar datos, sin desviarse del alcance de la protección.

Resultará obvio para una persona experta en la materia, a medida que la tecnología avanza, que el concepto de la invención se puede implementar de varias maneras. La invención y sus realizaciones no están limitadas a los ejemplos descritos anteriormente, sino que pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método para la comunicación encriptada entre extremos, que comprende:

almacenar (71) en un terminal de usuario (2) un conjunto (60) de las claves (61) aplicables en la encriptación entre extremos de comunicaciones, estando una o más claves asociadas con una indicación de validez (62) que indica un grupo criptográfico (CG1… CG5) de dos o más terminales de usuario en los que la clave se va a aplicar, y un periodo durante el cual es aplicable la clave en ese grupo criptográfico particular;

en el terminal de usuario que conecta a una comunicación del grupo criptográfico, seleccionar la clave que se debe aplicar de entre el conjunto de claves almacenadas sobre la base del presente grupo criptográfico y el tiempo actual de acuerdo con las indicaciones de validez asociadas.

2. Un método de acuerdo con la reivindicación 1, caracterizado por cargar el conjunto de claves y las indicaciones de validez como conjunto de sucesivos registros asociados con un grupo criptográfico, comprendiendo un registro un campo para una clave de encriptación entre extremos y un campo para una marca de tiempo asociada.

3. Un método de acuerdo con la reivindicación 2, caracterizado por seleccionar la clave que se debe aplicar en el grupo criptográfico del registro de tal manera que la marca de tiempo del registro es anterior al tiempo actual, y la marca de tiempo del siguiente registro es posterior al tiempo actual.

4. Un elemento de gestión de claves (9) que comprende:

una unidad de interfaz de comunicación (23) para intercambiar información con un terminal de usuario;

una unidad de control, siendo las funciones de la unidad de control al menos parcialmente controladas por un código de programa, configurando el citado código de programa el citado elemento de gestión para enviar a un terminal de usuario un conjunto de claves aplicables en la encriptación entre extremos de comunicaciones de un grupo criptográfico de al menos dos grupos de usuario, refiriéndose un grupo de usuarios a un conjunto de usuarios cuyas suscripciones y claves de encriptación están gestionadas por una entidad de gestión, estando una o más claves asociadas con una indicación de validez que indica el grupo criptográfico de dos o más grupos de usuario en el que se debe aplicar la clave, y un periodo durante el cual es aplicable la clave en ese grupo criptográfico concreto.,

5. Un terminal de usuario (2) para una red de comunicación, que comprende:

una unidad de interfaz de comunicación (34) para intercambiar información sobre la red de comunicación;

una unidad de memoria (33);

una unidad de control (32), estando las funciones de la unidad de control controladas, al menos parcialmente, por un código de programa, configurando el citado código de programa el citado terminal de usuario para

almacenar en la unidad de memoria un conjunto de claves aplicables en la encriptación de comunicaciones entre extremos, estando una o más claves asociadas con una indicación de validez que indica un grupo criptográfico de dos o más terminales de usuario en los que se debe aplicar la clave, y un periodo durante el cual la clave es aplicable en ese grupo criptográfico concreto;

seleccionar, durante la conexión a una comunicación del grupo criptográfico, la clave que se debe aplicar del conjunto de claves almacenado sobre la base del grupo criptográfico actual y el tiempo actual de acuerdo con las indicaciones de validez asociadas.

6. Un terminal de usuario de acuerdo con la reivindicación 5, caracterizado por un medio para recibir el conjunto de claves sobre la interfaz aérea.

7. Un terminal de usuario de acuerdo con la reivindicación 6, caracterizado por un medio para cargar el conjunto de claves en el terminal de usuario en un mensaje corto.

8. Un terminal de usuario de acuerdo con la reivindicación 7, caracterizado por un medio para cargar el conjunto de claves en el terminal de usuario desde un ordenador conectado localmente al terminal de usuario.

9. Un terminal de usuario de acuerdo con la reivindicación 8, caracterizado por un medio para cargar el conjunto de claves en el terminal de usuario utilizando procedimientos de una aplicación informática instalada en el terminal de usuario y el ordenador.

10. Un terminal de usuario de acuerdo con cualquiera de las reivindicaciones 5 a 9, caracterizado por un medio para cargar el conjunto de claves y las indicaciones de validez como un conjunto de registros sucesivos asociados con un grupo, comprendiendo un registro un campo para una clave de encriptación entre extremos y un campo para una marca de tiempo asociada.

11. Un terminal de usuario de acuerdo con la reivindicación 10, caracterizado por un medio para seleccionar la clave que se debe aplicar en un grupo criptográfico del registro, de tal manera que la marca de tiempo del registro es anterior al tiempo actual, y la marca de tiempo del registro subsiguiente es posterior al tiempo actual.

12. Un terminal de usuario de acuerdo con cualquiera de las reivindicaciones anteriores 5 a 11, caracterizado por que el actual grupo criptográfico corresponde a un grupo de dos terminales de usuario y la comunicación corresponde a la comunicación individual.

13. Un terminal de usuario de acuerdo con cualquiera de las reivindicaciones 5 a 12 anteriores, caracterizado por que comprende un módulo de seguridad, y un medio para almacenar el conjunto de claves en el módulo de seguridad.

14. Un sistema de comunicaciones que comprende un elemento de gestión de claves (9) de acuerdo con la reivindicación 4, y uno o más terminales de usuario (2) de acuerdo con la reivindicación 5.

15. Un programa informático que codifica un proceso informático de instrucciones para ejecutar un proceso informático para gestionar una solicitud en un recurso de comunicación para un terminal de usuario, comprendiendo el proceso:

almacenar en un terminal de usuario un conjunto de claves aplicables en la encriptación de las comunicaciones entre extremos, estando una o más claves asociadas con una indicación de validez que indica un grupo criptográfico de dos o más terminales de usuario en los que se debe aplicar la clave, y un periodo durante el cual es aplicable la clave en ese grupo particular;

en el terminal de usuario que se conecta a una comunicación del grupo criptográfico, seleccionando la clave que se va a aplicar del conjunto de claves almacenado sobre la base del presente grupo criptográfico y el tiempo actual de acuerdo con las indicaciones de validez asociadas.

Fig. 1

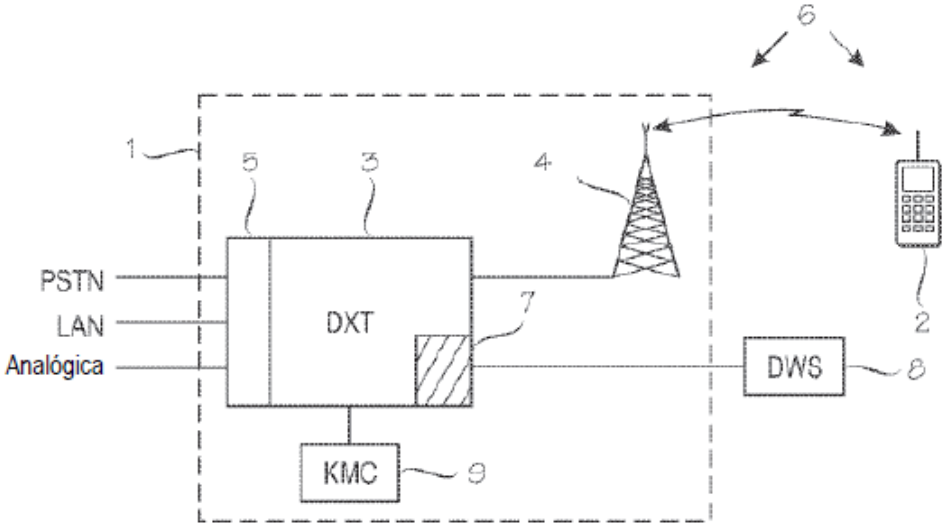

Fig. 2

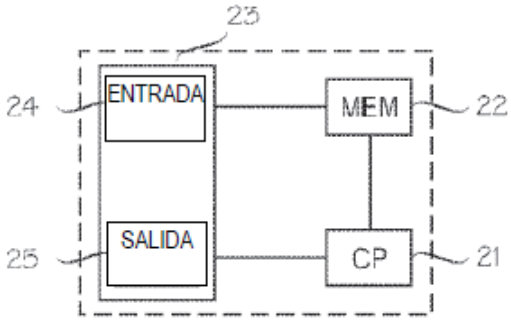

Fig. 3

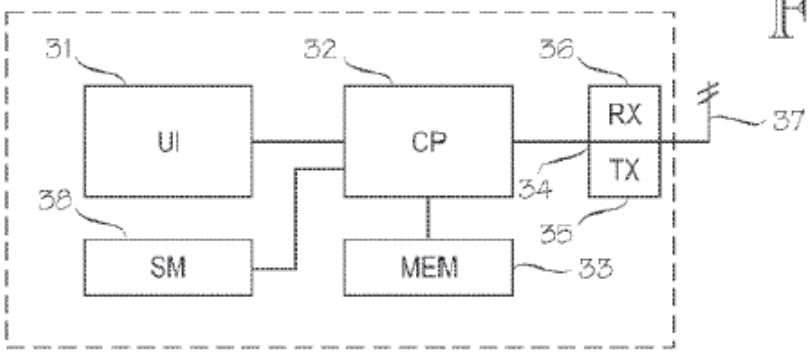

Fig. 4

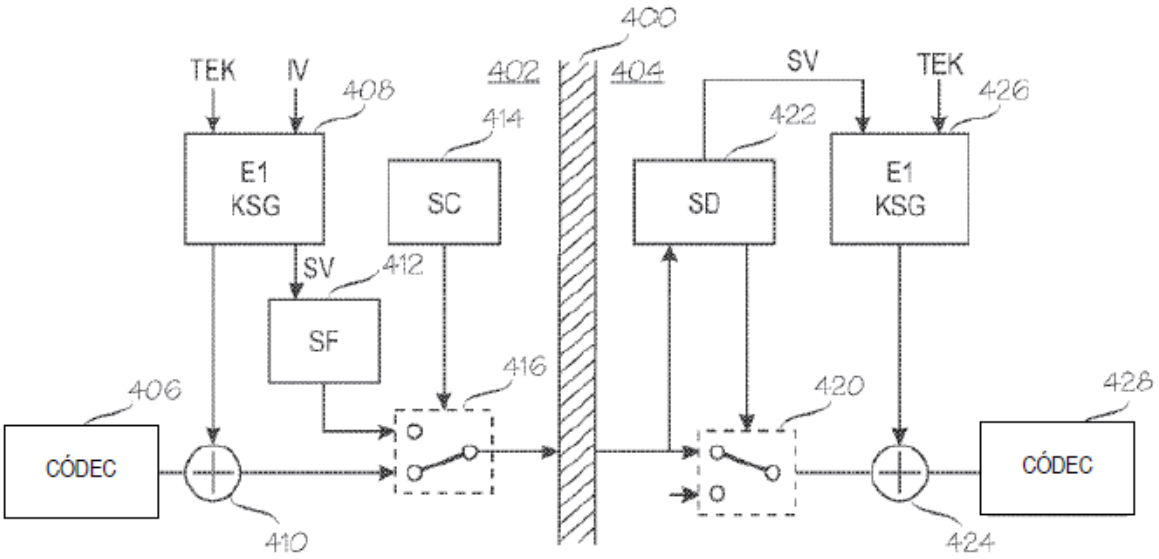

Fig. 5A

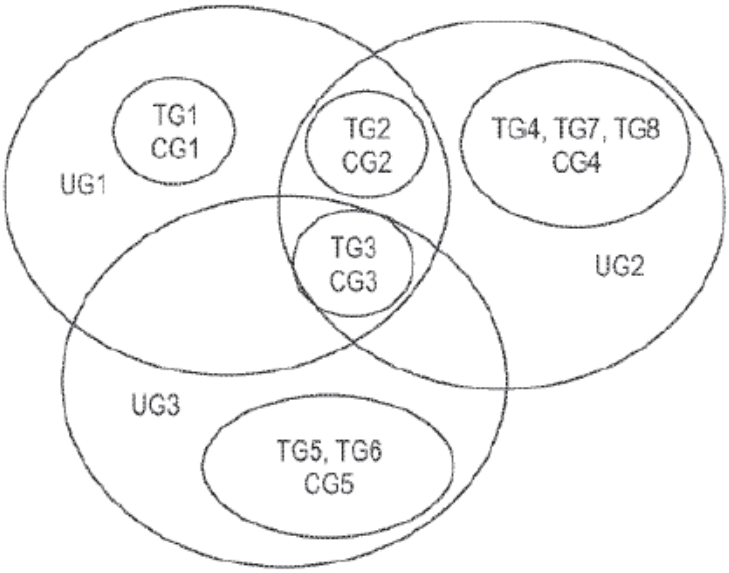

Fig. 5B

	UG1	UG2	UG3
CG1	X		
CG2	X		X
CG3	X	X	X
CG4			X
CG5		X	

Fig. 6

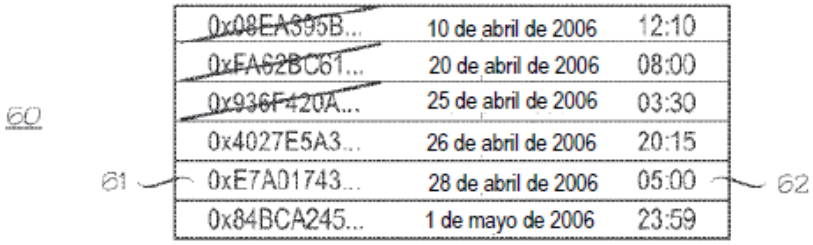

Fig. 7

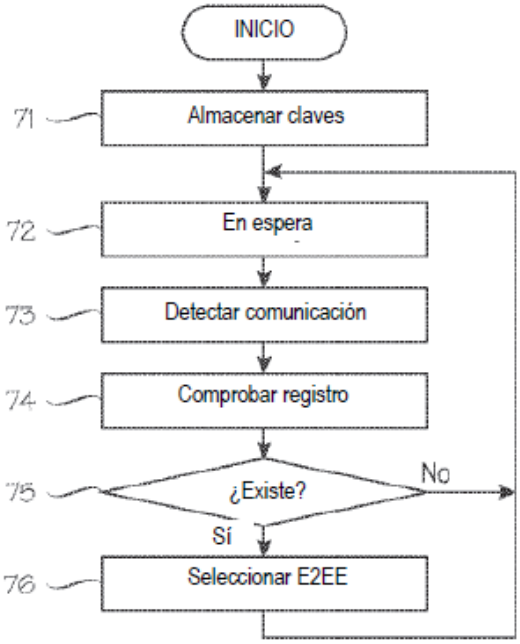

Fig. 8