(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 360 943**

(51) Int. Cl.:
H04L 9/32 (2006.01)
H04W 12/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06020441 .9**
(96) Fecha de presentación : **18.01.2002**
(97) Número de publicación de la solicitud: **1742411**
(97) Fecha de publicación de la solicitud: **10.01.2007**

(54) Título: **Método y aparato para proporcionar autenticación en un sistema de comunicaciones móviles.**

(30) Prioridad: **16.02.2001 US 785722**

(45) Fecha de publicación de la mención BOPI:
10.06.2011

(45) Fecha de la publicación del folleto de la patente:
10.06.2011

(73) Titular/es: **MOTOROLA SOLUTIONS, Inc.**
1303 East Algonquin Road
Schaumburg, Illinois 60196, US

(72) Inventor/es: **Sowa, Hans Christopher;**
McDonald, Daniel J.;
Chater-Lea, David J.;
Kremske, Randy;
Pappas, Scotta J.;
Johur, Jason;
Newkirk, Dennis y
Anderson, Walter F.

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Método y aparato para proporcionar autenticación en un sistema de comunicaciones móviles

Campo de la invención

Esta invención se refiere a comunicaciones cifradas, incluyendo pero sin limitarse a comunicaciones sobre la interfaz aire dentro de los sistemas de comunicaciones seguras.

Antecedentes de la Invención

Los sistemas de voz y datos cifrados son bien conocidos. Muchos de estos sistemas proporcionan comunicaciones seguras entre dos o más usuarios compartiendo un elemento de información entre los usuarios, que permite que sólo los usuarios que lo conocen descifren adecuadamente el mensaje. Este elemento de información se conoce como clave de cifrado variable, o clave para corto. Cargar esta clave dentro del dispositivo de cifrado real en la unidad del medio de comunicaciones seguras es un requisito básico que permite que se produzcan las comunicaciones seguras. Para mantener la seguridad sobre un largo periodo de tiempo, las claves se cambian periódicamente, típicamente semanalmente o mensualmente.

El cifrado es conocido por su realización sobre una base de extremo a extremo dentro de un sistema de comunicaciones, por ejemplo, el cifrado de un mensaje en la unidad de comunicaciones de origen (también conocida como una estación móvil), pasándola de forma transparente (es decir, sin descifrarla) a través de cualquier número de canales y/o elementos de infraestructura a la unidad de comunicaciones del usuario final, que descifra el mensaje.

La normativa de comunicaciones de la Radio Terrestre Troncal (TETRA) se utiliza actualmente en Europa (en adelante en este documento Normativa TETRA), con un potencial de expansión a otros lugares. Las llamadas en la Normativa TETRA para la interfaz aire, también se conocen como cifrado del tráfico aire o sobre el aire. El cifrado de la interfaz aire protege la información sobre la interfaz aire entre la infraestructura y el abonado móvil. Las llamadas de la Normativa TETRA a un centro de autenticación, también conocido como un servicio de gestión de claves o centro de gestión de claves, son para generar, distribuir, y autenticar claves de cifrado y usuarios. Sin embargo la normativa TETRA no especifica cómo implementar un centro de autenticación, ni cómo generar, distribuir y autenticar el material de claves para los dispositivos del sistema o estaciones móviles para la información que pasa a través de la infraestructura o la SwMI (Infraestructura de Conmutación y Gestión), como se denomina en la Normativa TETRA.

La normativa TETRA falla al proporcionar la definición para minimizar la carga para el procesamiento de llamadas y el ancho de banda, al proporcionar el cifrado y la autenticación de un modo tolerante a fallos de los equipos, soportar comunicaciones de área ancha, y para almacenar las claves para todas las unidades de comunicaciones sin la carga de almacenamiento indebida en los sitios locales.

El documento GB2332 594 describe un método de procesamiento de una petición de servicio en un sistema de comunicaciones en el que al menos parte de la petición del servicio está cifrada. El método incluye las etapas de recibir una petición de servicio desde una unidad de comunicaciones, intentando autenticar la petición de servicio, determinando, en respuesta a un fallo en la autenticación de la petición de servicio, el número de fallos que han ocurrido anteriormente para la unidad de comunicaciones, y proporcionar, en respuesta al número, el servicio de duración limitada para la unidad de comunicaciones.

Por consiguiente, hay una necesidad de un método y un aparato para proporcionar una infraestructura segura para un sistema de comunicaciones que utiliza el cifrado en la interfaz aire y genera, distribuye y autentica las claves de cifrado y usuarios sin causar una carga indebida en el procesamiento de la llamada, el ancho de banda, la seguridad y el almacenamiento.

Sumario de la Invención

De acuerdo con un aspecto de la invención se proporciona un método que comprende las etapas de, recibir, desde una estación móvil, una petición de comunicación en un sistema de comunicaciones; determinando si la petición está cifrada; cuando la petición no está cifrada, enviando una petición para autenticar la estación móvil con un dispositivo de la infraestructura del sistema en el sistema de comunicaciones; cuando la petición está cifrada, determinar si la estación móvil se está encendiendo; cuando la estación móvil se está encendiendo y la petición está cifrada, enviando una petición para autenticar la estación móvil con el dispositivo de la infraestructura del sistema en el sistema de comunicaciones; cuando la estación móvil no se está encendiendo y la petición está cifrada, determinando si la petición está cifrada usando una clave válida; cuando la estación móvil no se está encendiendo y la petición está cifrada usando una clave válida, permitiendo que la estación móvil acceda al sistema sin petición de autenticación.

Preferiblemente, el método comprende además las etapas de: almacenamiento de las peticiones de autenticación durante un periodo de tiempo cuando el dispositivo de la infraestructura del sistema no está disponible; cuando el dispositivo de la infraestructura del sistema se vuelve disponible, redirigiendo las peticiones de autenticación almacenadas al dispositivo de la infraestructura del sistema.

Preferiblemente enviando la petición de autenticación de la estación móvil a un dispositivo de la infraestructura del sistema que comprende enviar la petición de autenticación de la estación móvil a un controlador de zona en la zona en la que está localizada la estación móvil.

Comprendiendo el método además preferiblemente recibir una confirmación de que ha pasado la autenticación para la estación móvil.

Preferiblemente la autenticación se realiza por un primer dispositivo de la infraestructura del sistema usando una información de autenticación de sesión que se recibió desde un segundo dispositivo de la infraestructura del sistema.

Preferiblemente al menos un segmento de la información de autenticación de la sesión recibida está cifrado.

Preferiblemente el, al menos un segmento de la información de autenticación de sesión recibida está cifrado usando una intra-clave que se usa sólo por los dispositivos de la infraestructura del sistema distintos de la estación móvil dentro de una zona para cifrar al menos la información de autenticación de sesión que se distribuye dentro de la zona.

Preferiblemente, el primer dispositivo de la infraestructura del sistema es un registro de localización de visitantes localizado en una zona, y el segundo dispositivo de la infraestructura del sistema es un registro de localización local localizado en la misma zona.

Preferiblemente, el, al menos un segmento de la información de autenticación de sesión recibida está cifrado usando una inter-clave que se comparte por una pluralidad de zonas y que se usa por un dispositivo de la infraestructura del sistema distinto de la estación móvil en una zona en la pluralidad de zonas para cifrar al menos la información de autenticación de sesión para transportar a otro dispositivo de la infraestructura del sistema distinto que la estación móvil en otra zona en una pluralidad de zonas.

Preferiblemente, el primer dispositivo de la infraestructura del sistema es un registro de de localización de visitantes localizado en una zona, y el segundo dispositivo de la infraestructura del sistema es un registro de localización local localizado en una zona diferente.

Preferiblemente el método se realiza en una cualquiera de las estaciones base y sitio base

Breve Descripción de los Dibujos

La FIG. 1 es un diagrama de bloques de un sistema de comunicaciones seguro de acuerdo con la invención.
La FIG. 2 es un diagrama de bloques que muestra pilas de distribución de claves de acuerdo con la invención.
La FIG. 3 y la FIG. 4 son diagramas de bloques que muestran el almacenamiento de claves dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG. 5 es un diagrama que muestra el almacenamiento de claves y la distribución de la información de autenticación dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG. 6 es un diagrama que muestra el almacenamiento de información de autenticación y la decisión de autenticación que se realiza dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG. 7 es un diagrama que muestra la autenticación de una estación móvil por un centro de autenticación de acuerdo con la Normativa TETRA.
La FIG. 8 es un diagrama que muestra la autenticación de un centro de autenticación por una estación móvil de acuerdo con la Normativa TETRA.
La FIG. 9 es un diagrama que muestra el almacenamiento de claves y la distribución de la información de autenticación entre un sistema de comunicaciones y una estación móvil de acuerdo con la invención.
La FIG. 10 es un diagrama que muestra una extracción de claves dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG. 11 es un diagrama que muestra una introducción de claves dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG 12 es un diagrama que muestra la distribución de una clave de cifrado estática a una estación base dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG. 13 es un diagrama que muestra la distribución de una clave de cifrado estática a una estación móvil dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG. 14 es un diagrama que muestra la distribución de una clave de cifrado común para una estación móvil y una estación base dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG. 15 es un diagrama que muestra la distribución de una clave de cifrado de grupo a una estación base

dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG. 16 es un diagrama que muestra la distribución de una clave de cifrado de grupo a una estación móvil dentro de un sistema de comunicaciones de acuerdo con la invención.
La FIG. 17 es un diagrama de flujo que muestra un método de persistencia de claves en un sitio en un sistema de comunicaciones de acuerdo con la invención.

Descripción de una Realización Preferida

Lo siguiente describe un aparato y un método para proporcionar una infraestructura segura para un sistema de comunicaciones que utiliza el cifrado de la interfaz aire y genera, distribuye y autentica las claves de cifrado y los usuarios sin causar una carga indebida para el procesamiento de la llamada, el ancho de banda, la seguridad y el almacenamiento. Los dispositivos del sistema se dividen en grupos o pilas, y las claves de cifrado se definen para proporcionar una transferencia segura del material de claves entre los dispositivos del sistema.

En la FIG. 1 se muestra un diagrama de bloques de un sistema de comunicaciones seguras que está comprendido por una pluralidad de zonas. El sistema de comunicaciones seguras está comprendido de una pluralidad de dispositivos de sistema que comprenden la infraestructura del sistema. El Servicio de Gestión de Claves (KMF) 101 transfiere datos de seguridad, tales como la información de autenticación de sesión y las claves de cifrado, a un Servidor de Configuración de Usuario (UCS) 103, que redirige la información y los datos a la zona apropiada en base a los datos de configuración dentro del UCS 103. Las comunicaciones para una primera zona se proporcionan por una pluralidad de dispositivos del sistema incluyendo un Gestor de Zona (ZM) 105, un Controlador de Zona (ZC) 107 que incluye el Registro de Localización Local (HLR) 109 y un Registro de Localización de Visitados (también conocidos como del Visitante o de Visitantes) (VLR) 111, un dispositivo de encaminamiento del tráfico de aire (ATR) 113, y una pluralidad de estaciones base (BS) 115 y 117 localizadas en una pluralidad de sitios de comunicaciones dentro de la primera zona. Las comunicaciones para la segunda zona se proporcionan por una pluralidad de dispositivos del sistema incluyendo un ZM 119, un ZC 121 que incluye un HLR 123 y un VLR 125, un ATR 127, y una pluralidad de BS 129 y 131 localizadas en una pluralidad de sitios de comunicaciones dentro de la segunda zona. Las BS 115, 117, 129, y 131 comunican con una pluralidad de estaciona móviles (véase la FIG. 4). Los ZC 107 y 121 comunican a través de una red 133, tal como una red de área local o una red de área amplia tal como una red IP (Protocolo de Internet). Sólo se muestran dos zonas y sus dispositivos del sistema asociados en beneficio de la simplicidad, aunque puede incorporarse satisfactoriamente cualquier número de zonas en el sistema de comunicaciones seguras.

En beneficio de la simplicidad, no se mostrarán todos los dispositivos del sistema en cada una de las Figuras, sino más bien se proporcionará un conjunto representativo de dispositivos del sistema que ilustra un concepto particular. De forma similar, no todo el material de claves se muestra almacenado en cada uno de los dispositivos del sistema en beneficio del espacio. Cada uno de los mensajes que contiene una clave, material de clave, configuración, u otra información se transfiere con una identidad relacionada (ID) tal como la ITSI o la GTSI, aunque la ID generalmente no se muestra en los dibujos por consideraciones de espacio.

El KMF 101 es una entidad segura que almacena la clave de autenticación (K) para cada una de las estaciones móviles (MS) o unidad de comunicaciones, tal como una radio portátil o móvil de dos direcciones, la puerta de acceso de la Operación del Modo Directo (DMO), el receptor, el escáner, o el transmisor (por ejemplo, véanse los dispositivos 401, 403, y 405 en la FIG. 4). El KMF 101 proporciona una semilla aleatoria (RS) y claves de autenticación de sesión asociadas (KS y KS') para cada una de las estaciones móviles asociadas con el sistema de comunicaciones seguro. El KMF 101 también importa/genera diversas claves de la interfaz aire, tales como la Clave de Cifrado Estático (SCK), la Clave de Cifrado de Grupo (GCK), y la Clave de Cifrado Común (CCK), para su distribución en el sistema. El KMF 101 funciona como el centro de Autenticación (AuC), como se denomina en la normativa de comunicaciones TETRA, en el sistema. Típicamente, hay un servidor KMF por sistema, aunque puede haber uno o más KMF clientes por sistema.

El UCS 103 es un punto único de entrada para los datos de configuración en el sistema. En la realización preferida, el UCS 103 almacena y distribuye la información de autenticación de sesión, tal como las RS, KS, y KS', a la zona local apropiada en el sistema. El UCS 103 funciona como un punto de distribución no en tiempo real para la información de autenticación de sesión en el sistema.

El ZM 105 ó 119 es una base de datos de gestión para una zona. En la realización preferida, el ZM 105 ó 119 almacena la información de autenticación de sesión, tal como las RS, KS, y KS', para la zona gestionada por el ZM particular 105 ó 119. El ZM funciona como un servicio de almacenamiento no en tiempo real para la información de autenticación en la zona.

El ZC 107 ó 121 realizan la autenticación en tiempo real para las estaciones móviles en su zona. El ZC usa la información de autenticación de sesión, tal como las RS, KS, y KS', para realizar la autenticación en tiempo real. El HLR 109 ó 123 almacenan la información de autenticación de sesión para cada una de las MS que tiene el HLR 109 ó 123 como su HLR local. El VLR 111 ó 125 almacena la información de autenticación de sesión para cada una de las MS visitante de la zona del VLR 111 ó 125. El ZC 107 ó 121 realizan la distribución en tiempo real de su

información de autenticación de sesión de las estaciones móviles locales cuando la MS está en itinerancia fuera de su zona local. En la realización preferida, un HLR 109 ó 123 y un VLR 111 ó 125 son parte de cada uno de los controladores de zona y funcionan en nombre de la misma zona a la cual está asociado el controlador de zona. El HLR 109 ó 123 y el VLR 111 ó 125 pueden ser parte de otros dispositivos del sistema o pueden ser dispositivos independientes. La clave de cifrado derivada (DCK) se genera durante la autenticación. El ZC 107 ó 121 generan y distribuyen la DCK para las MS a las BS 115, 117, 129, y 131 que requieren la DCK para comunicaciones seguras.

El ATR 113 ó 127 es el conducto utilizado por el KMF 101 para enviar los mensajes de reaprovisionamiento de claves o actualizaciones de claves para una MS tal como la SCK y la GCK. El KMF 101 envía actualizaciones de claves para las estaciones móviles al ATR de la zona local 113 ó 127 para su diseminación. Todas las confirmaciones (ACK) de reaprovisionamiento de claves, tanto si están originadas en la infraestructura como en la MS, pasan a través del ATR 113 ó 127 al KMF 101.

Cada una de las BS 115, 117, 129 y 131 reciben y transmiten mensajes de autenticación sobre la interfaz aire. Cada una de las BS 115, 117, 129 y 131 actúa como un transmisor para su ZC asociado 107 ó 121 y como un receptor para la MS en el sistema. Las BS 115, 117, 129 y 131 usan la DCK para el cifrado de la interfaz aire con la MS. Las BS 115, 117, 129 y 131 son responsables de enviar material de claves a las MS 401, 403, 405, y 407. El resultado de algunas de estas operaciones (SCK, GCK) se envía de vuelta al KMF 101. Debido a que cada uno de los sitios base está comprendido sustancialmente de una o más estaciones base, los términos de sitio base (o sitio) y estación base se usan de forma intercambiable en este documento, compartiendo ambos el acrónimo BS. En la realización preferida, el controlador del sitio TETRA (TSC) conecta todas las estaciones base en un sitio, almacena el material de claves, y distribuye el material de claves a las estaciones base según se necesite, haciendo las claves disponibles, por lo tanto, a todas las estaciones base en un sitio. De este modo, cuando se dice que una clave está almacenada en una estación base o un sitio base, en la realización preferida, el TSC realmente proporciona almacenamiento para la estación base para el material de claves. Debido a que el almacenamiento y distribución de claves y otras funciones relacionadas con las claves pueden realizarse por un sitio base, estación base o TSC, estos términos se consideran intercambiables para los propósitos de este documento.

La Estación Móvil (MS) autentica el sistema y/o se autentica por el sistema usando un protocolo de reto-respuesta. Cada una de las MS tiene su propia clave, K, para su uso durante la autenticación. Cada una de las MS está asignada a un HLR, que típicamente permanece igual. Cada una de las MS está también asociada con sólo un VLR en la zona en la cual la MS está localizada actualmente. Una MS no está registrada sobre un sistema hasta que la MS está activa y ha pasado la autenticación.

La FIG. 2 es un diagrama de bloques que muestra pilas de distribución de claves. Usando una única clave de cifrado de claves (KEK) para cifrar las claves para su distribución a lo largo del sistema es una elección conveniente, aunque una única KEK daría como resultado una seguridad degradada debido a la probabilidad más elevada de que pueda comprometerse la KEK y el compromiso resultante afectaría a todo el sistema. Usar una KEK diferente para cada uno de los dispositivos del sistema sería más seguro, pero cargaría el almacenamiento dentro de los dispositivos del sistema y añadiría retardos innecesarios en el procesamiento de llamadas. La FIG. 2 muestra un sistema para usar las KEK que es más seguro que una única clave de ancho-sistema, aunque sin carga alguna, respecto a una KEK diferente para cada uno de los dispositivos del sistema. Se asignan dos tipos de KEK para distribuir confidencialmente el material de claves (tal como las claves de la interfaz aire, la información de autenticación de sesión, los datos utilizados para generar claves de cifrado, y otro material relacionado con las calves) para los dispositivos del sistema de la infraestructura de un sistema: las intra-claves y las inter-claves. Las KEK son de 80 bits en la realización preferida.

El primer tipo de KEK es una intra-clave, también denominado como una clave intra-pila o una clave intra-zona, KEK_Z. Los dispositivos del sistema están divididos en pilas o grupos 201, 203, 205, y 207. Cada una de las pilas tiene asignada su propia intra-clave única, KEK_Z. En la realización preferida, cada una de las pilas de dispositivos corresponde a una zona en el sistema de comunicaciones, y cada una de las pilas tiene una colección mutuamente excluyente de dispositivos de sistema, es decir, cada uno de los dispositivos de sistema sólo pertenece a una pila. La primera pila 201 utiliza una KEK_{Z1} para cifrar material de claves, tal como las claves de cifrado y/o la información de autenticación de sesión, para transferir dentro de la primera pila (o zona en la realización preferida) y comprende el primer controlador de zona ZC1 107 y sus BS asociadas 115, 117 y 211. La segunda pila 203 utiliza KEK_{Z2} para cifrar el material de claves para transferencias dentro de la segunda pila (o zona en la realización preferida) y comprende el segundo controlador de zona ZC2 121 y sus BS asociadas 129, 131 y 213. La tercera pila 205 utiliza KEK_{Z3} para cifrar el material de claves para transferencias dentro de la tercera pila (o zona en la realización preferida) y comprende el tercer controlador de zona ZC3 223 y sus BS asociadas 225, 227, y 229. La cuarta pila 207 utiliza KEK_{Z4} para cifrar el material de claves para transferencias dentro de la cuarta pila (o zona en la realización preferida) y comprende el cuarto controlador de zona ZC4 215 y sus BS asociadas 217, 219, y 221. En la realización preferida, la intra-clave se usa por un controlador de zona para distribuir el material de claves a los sitios base/estaciones base dentro de su zona. KEK_Z también se usa por el KMF 101 para distribuir la SCK.

El segundo tipo de KEK es una inter-clave, KEK_M, también denominada como una clave inter-pila o clave inter-zona. La inter-clave se usa para cifrar material de claves enviado entre pilas o zonas en la realización preferida, o dentro

de un cierto grupo 209 de dispositivos del sistema, particularmente desde el KMF 101. En la realización preferida, la inter-clave se usa por el KMF 101 para distribuir la GCK y la información de autenticación individual para la infraestructura. En la realización preferida la inter-clave está almacenada en un dispositivo de sistema en cada una de las zonas, en cada uno de los controladores de zona 107 y 121, y también está almacenada en el KMF101. Las conexiones mostradas entre el KMF 101 y los controladores de zona 107, 121, 215, y 223 son conexiones virtuales en la realización preferida, en que otros dispositivos, tales como el UCS 103 y los ZM 105 y 119 están físicamente localizados entre el KMF 101 y los controladores de zona 107, 121, 215, y 223. El UCS y los ZM 105 y 119 pasan la información de claves cifrada de modo transparente entre el KMF 101 y los controladores de zona 107, 121, 215, y 223, es decir, el UCS 103 y los ZM 105 y 119 no descifran ni cifran la información, de este modo no se requiere ningún almacenamiento de KEK en los UCS 103 y los ZM 105 y 119, aunque el material de claves puede almacenarse en forma cifrada en los UCS 103 y los ZM 105 y 119.

Preferiblemente, un mensaje se cifra por una de las intra-claves y una inter-clave, típicamente usando TA31 (descifrada usando TA32), en base a un dispositivo del sistema al cual se redirige el mensaje. Por ejemplo, cuando el mensaje se pretende para un dispositivo de sistema en una zona distinta de la zona que contiene el dispositivo transmisor, se usa la inter-clave. Cuando el mensaje se pretende para un dispositivo de sistema en la misma zona que la zona que contiene el dispositivo transmisor, se usa la intra-clave. En la realización preferida, cuando el KMF 101 cifra el material de claves, tales como la SCK, CCK, SAI, y GCK, con cualquiera de la inter-clave o la intra-clave, el KMF 101 usa TA31.

Por ejemplo, de vez en cuando, el material de claves se distribuye desde el HLR a un VLR y a continuación a los sitios base dentro de la zona del VLR. En este caso, el material de claves se cifra por KEK_M y pasa de forma transparente desde el HLR al VLR. El VLR objetivo descifra el material de claves usando su KEK_M y lo re-cifra con la KEK_Z de la zona para su distribución a los sitios dentro de la zona.

Cada uno de los dispositivos de sistema que contiene una KEK de infraestructura tiene su propia clave de infraestructura única o de protección, KI, en la realización preferida. La clave de protección sólo se utiliza para descifrar/cifrar las KEK enviadas por el KMF 101 a los dispositivos de la infraestructura del sistema. Preferiblemente, la KI, sólo puede cargarse por un cargador de claves variables y no puede actualizase con una operación OTAR (reaprovisionamiento de claves sobre el aire). Además para la distribución por el KMF 101, las KEK pueden proporcionarse también manualmente con un Cargador de Claves Variables. KI es de 128 bits de longitud en la realización preferida.

Como se muestra en la parte inferior de la Tabla 1, KEK_M sólo se almacena por los controladores de zona 107 y 121 y el KMF 101. La intra-clave KEK_Z se mantiene sólo por el KMF 101, los sitios/estaciones base, y los controladores de zona 107 y 121 dentro de cada una de las zonas. Cada una de las zonas tiene una única KEK_Z. Cada uno de los dispositivos de sistema tiene su propia KI.

Tabla 1

Distribución de Tipos de Claves de Cifrado de Claves		
Elemento de Infraestructura	**Zona 1**	**Zona 2**
Controlador de Zona (HLR, VLR)	KI_1, KEK_M, KEK_{Z1}	KI_2, KEK_M, KEK_{Z2}
Sitios Base	KI_3, KEK_{Z1}	KI_4, KEK_{Z2}

El uso de intra-claves e inter-claves socaba el compromiso único entre la seguridad y la complejidad de gestión de claves así como la velocidad del procesamiento de llamadas. El KMF 101 sólo necesita mantener una inter-clave más una intra-clave para cada una de las pilas o zonas en el sistema. Si una KEZ_Z se ve comprometida, la afección y la respuesta están localizadas a esa zona, en lugar de a todo el sistema, y KI permanece intacta para redistribuir una nueva KEK_Z a esa zona. La KEK_M se almacena sólo en el KMF 101 y el HLR 109 y 123 y el VLR 111 y 125 en cada una de las zonas, dispositivos estos que están típicamente más protegidos físicamente de un ataque. Si KEK_M se ve comprometida, el KMF 101 cambia KEK_M en los ZC 107 y 121, dejando los sitios sin afectar.

Se usan cinco tipos básicos de claves de la interfaz aire para cifrar el tráfico de la interfaz aire en el sistema de comunicaciones seguras: una Clave de Cifrado Estático (SCK) una Clave de Cifrado Común (CCK), una Clave de Cifrado de Grupo (GCK), una Clave de Cifrado Derivada (DCK), y una Clave de Cifrado de Grupo Modificada (MGCK). Se usan tres tipos básicos de claves entre los dispositivos del sistema: una clave de infraestructura (KI) también conocida como clave de protección, una clave de cifrado de claves de inter-zona o inter-pila (KEK_M) también conocida como una inter-clave y una clave de cifrado de claves de intra-zona o intra-pila también conocida como intra-clave (KEK_Z).

La Clave de Cifrado Estático (SCK) es la más básica de las claves de la interfaz aire y se usa para cifrar la información entrante (de la MS a la infraestructura) y saliente (de la infraestructura a la MS) cuando la autenticación y/o el cifrado dinámico de la interfaz aire no están disponibles. De este modo, la generación y la distribución de esta clave no tienen ninguna relación con la autenticación.

La Clave de Cifrado Derivada (DCK) es una clave de sesión derivada dentro del procedimiento de autenticación. La

DCK cambia cada vez que se realiza una autenticación con la MS y la infraestructura, también llamada SwMI en la Normativa TETRA. La DCK se usa también para el cifrado del tráfico entrante. La DCK se usa también para el tráfico saliente dirigido de forma individual a la MS. La DCK se usa cuando se utiliza un cifrado dinámico de la interfaz aire que opera en la clase 3 de seguridad de la Normativa TETRA. Esta Clave de Cifrado Común (CCK) es una clave de grupo en el sentido de que múltiples MS tienen la misma CCK. A diferencia de la GCK, sin embargo, la CGK no tiene ninguna relación con un grupo de conversación particular (TG). La CCK es geográficamente específica, es decir la CCK sirva a todas las unidades dentro de un área de localización determinado. El área de localización como se define en la normativa TETRA puede ser tan pequeña como un sitio o tan grande como todo un sistema. Cada una de las unidades dentro de un área de localización usan la misma CCK. Las comunicaciones de grupo en la dirección saliente usan la CCK cuando no hay ninguna GCK/MGCK disponible para esa llamada de grupo. La CCK se usa para el cifrado del tráfico de grupo saliente y sólo identidades. Las identidades entrantes se cifran con CCK cuando DCK está en uso.

Indirectamente, la Clave de Cifrado de Grupo (CCK) se usa para cifrar llamadas de grupos de conversación salientes. En la realización preferida, se define una GCK para cada uno de los grupos de conversación en el sistema. Realmente, la GCK sólo se usa indirectamente para el cifrado de la información de tráfico; la clave de cifrado de grupo modificada (MGCK), que es una derivada de la GCK, se usa directamente para el cifrado del tráfico. La GCK nunca se usa para el cifrado real del tráfico ya que se considera una clave de largo plazo.

La Clave de Cifrado de Grupo Modificada (MGCK) se usa para cifrar el tráfico saliente de llamadas de grupos de conversación. La MGCK se forma por la combinación de GCK y CCK. Cada una de las GCK tiene una MGCK correspondiente definida dentro de un área de localización.

Cada uno de los elementos de infraestructura tiene una clave de infraestructura o protección, KI, que se usa como la clave de cifrado para cualesquiera actualizaciones de claves de cifrado de las claves de infraestructura. KI es similar en funcionamiento a la clave de autenticación, K, en una estación móvil. En la realización preferida, KI se actualiza sólo por un dispositivo de aprovisionamiento tal como un cargador de claves variables. En la realización preferida, las actualizaciones de la clave de cifrado de claves de infraestructura (KEK) no pueden realizarse sin esta clave.

Cada uno de los controladores de zona tiene una inter-clave KEK_M, también denominada como clave de inter-zona o inter-pila, que se usa para cifrar todo el tráfico de claves que pasa entre el KMF y cada una de las zonas. La KEK_M también se usa por el controlador de zona para pasar GCK, CCK, y DCK, así como la información de autenticación de sesión, entre zonas. En la realización preferida, está presente una KEK_M en el KMF y cada uno de los controladores de zona en cada uno de los sistemas.

Cada una de las zonas tiene su propia intra-clave, KEK_Z, también denominada como clave de intra-zona o de intra-pila. La intra-clave se usa para cifrar todo el tráfico de claves dentro de la zona, entre el controlador de zona y cada uno de lo sitios dentro de las zonas. Cada uno de los sitios base y el controlador de zona tienen la misma KEK_Z en una zona. El KMF almacena la KEK_Z para cada una de las zonas en el sistema.

Un método de la presente invención establece un periodo de vida esperado, o un intervalo de reaprovisionamiento de claves para una clave de cifrado. La tabla 2 de más adelante muestra un ejemplo de intervalos de actualización de claves para cada una de las claves almacenadas en el sistema de comunicaciones seguras. Cuando el tiempo de vida esperado para una clave de cifrado expira, es decir, cuando se produce el intervalo de actualización de clave, la clave de cifrado se reemplaza.

Se determinan el número de localizaciones de almacenamiento para cada uno de los tipos de dispositivos de sistema dentro de un sistema de comunicaciones. Por ejemplo, un KMF 101, un UCS 103, un ZM 105 ó 109 por zona, un controlador de zona por zona 107 ó 121, un HLR 109 ó 123 por zona, un VLR 111 ó 125 por zona, y el número de sitios y las correspondientes estaciones base por sitio que dependen de los requisitos de cobertura para cada una de las zonas. En base al tiempo de vida esperado para cada una de las claves de cifrado y el número de localizaciones de almacenamiento para cada uno de los dispositivos del sistema, se asigna un tipo de dispositivo de sistema para almacenar cada una de las claves de cifrado, y las claves de cifrado se almacenan en el dispositivo del sistema del tipo asignado. Por ejemplo, las claves de cifrado derivadas se almacenan en las estaciones base y en el HLR/VLR, las claves de cifrado común se almacenan en las estaciones base, las claves de cifrado de grupo modificadas se almacenan en las estaciones base, y las claves de cifrado de grupo se almacenan en los HLR y los VLR.

La Tabla 2 muestra el objetivo (usuario) de cada una de las claves y el intervalo de actualización de claves, es decir el tiempo entre cambios o actualizaciones de la clave específica en una realización preferida. Por ejemplo, la MGCK, que es una combinación de la CCK y la GCK se actualiza cada vez que se cambia la CCK y cada vez que se cambia la GCK. La Tabla 2 puede cambiarse por el operador del KMF.

Tabla 2

	OBJETIVO DE LA CLAVE	INTERVALO DE ACTUALIZACIÓN DE CLAVE
SCK	Todas las MS y BS	1 año / o si se ve comprometida
DCK	MS, BS, HLR, VLR	< 24 horas, cada vez que la unidad autentica
CCK	Grupo (TG HLR), todas las MS, todas las BS	24 horas
GCK	Grupo (TG HLR)	6 meses
MGCK	Grupo (BS, MS)	24 horas - Mínimo del intervalo de CCK, GCK
KI	Todos los dispositivos que usan KEK_Z o KEK_M (BS, ZC)	Nunca cambia
KEK_Z	Zona	6 meses /o si se ve comprometida
KEK_M	Sistema	6 meses /o si se ve comprometida

Existen programas software basados en PC (ordenador personal) que aprovisionan tanto las estaciones móviles como a los dispositivos de la infraestructura del sistema con las claves. Un método más seguro utiliza las capacidades del Cargador de Claves Variables (KVL), o el cargador de claves para acortar, para cargar las claves en los dispositivos de infraestructura así como en las MS. El cargador de claves tiene un dispositivo de cifrado basado en hardware para la seguridad de las claves almacenadas dentro del dispositivo. El KVL puede obtener claves directamente desde el KMF actuando como un agente de almacenamiento y redirección para diseminar las claves de cifrado de claves para los diversos dispositivos.

Aunque un KVL es un modo muy seguro de proporcionar claves, es un proceso que emplea mucho tiempo para usar uno o más KVL para proporcionar claves en cada uno de los dispositivos del sistema y estaciones móviles. Se necesita un método de gestión de claves para almacenar y distribuir las KEK y otro material de claves a los dispositivos del sistema tales como los controladores de zona y los sitios base.

El KMF 101 es responsable de la generación, distribución de claves, y seguimiento de la mayor parte de las claves de la interfaz aire (no DCK ni MGCK) en el sistema. Los sitios base 115 y 117 y cada uno de los controladores de zona 107 sirven como un Proxy para el KMF 101 para la distribución de claves. El KMF 101 distribuye el material de claves a las zonas a través del UCS 103, los ZM 105 y 119, y/o los ATR 113 y 127 dependiendo de la clave a distribuir. El KMF 101 procesa la información de confirmación desde el ATR 113 y 127 para mantener la actualización de los dispositivos del sistema y las MS 401, 403, 405, y 407. La FIG. 3 y la FIG. 4 muestran el almacenamiento del material de claves dentro del sistema de comunicaciones.

Como se muestra en la FIG. 3, el KMF 101 almacena una clave de protección y las KEK asociadas para cada uno de los dispositivos del sistema. El KMF 101 almacena una clave de protección (infraestructura), una inter-clave, y una intra-clave para cada uno de los controladores de zona. Por ejemplo, el primer controlador de zona 107 está asociado con las claves KI_{ZC1}, KEK_M, y KEK_{Z1}. El KMF 101 almacena estas claves cifradas por una clave hardware y el primer controlador de zona 107 almacena KI_{ZC1} y las KEK_M y KEK_{Z1} cifradas. El KMF101 almacena una clave de protección y una intra-clave, ambas protegidas por una clave hardware, para cada una de las BS. Por ejemplo, el KMF 101 y la primera BS 115 almacenan ambos la clave de protección KI_{BS1} y la intra-clave KEK_{Z1}. En la realización preferida, el KMF 101 almacena claves cifradas/protegidas por una clave hardware.

Antes de la distribución de una KEK en una realización predeterminada, el KMF 101 cifra las KEK con la clave de protección KI, y el uso de los algoritmos de cifrado TA41 y TA51, de forma similar a lo que se muestra en la FIG. 10 titulada "Distribución de SCK para un individuo por un centro de autenticación" y su texto asociado en la Radio Troncal Terrestre (TETRA); Voz más Datos (V+D), Parte 7: Seguridad, EN 300 392.7 v2.1.1, 2000-12 (denominada en este documento como "Normativa TETRA"), que se incorpora en su totalidad en este documento por referencia. El KMF 101 almacena un proceso de cifrado 301 que combina RSO y la clave apropiada KEK, KEKN, y KEK-VN utilizando los algoritmos de cifrado TA41 303 y TA51 obteniendo SKEK, que es una versión sellada de la KEK. RSO, SKEK, KEKN y KEK-VN se redirigen al dispositivo del sistema objetivo. Las llaves {} seguidas por un nombre de clave indican que el material dentro de las llaves se creó usando TA41 y T151 y el nombre de la clave después de los paréntesis.

Por ejemplo se pretende transferir KEK_{Z1} al primer controlador de zona 107 y a la BS1 115. RSO, KEK_{Z1}, KEK_{Z1}-VN, y KEK_{Z1}-N y KI_{ZC1} se combinan utilizando los algoritmos de cifrado TA41 y TA51, obteniendo $SKEK_{Z1}$, El material de claves RSO, $SKEK_{Z1}$, KEK_{Z1}-VN y KEK_{Z1}N se redirigen de forma transparente a través del ZM1 105 al primer controlador de zona 107, que combina este material de claves con KI_{ZC1} usando TA41 y TA52 (como se describe en la Normativa TETRA), obteniendo KEK_{Z1}, que se almacena en ZC1 107. RSO, KEK_{Z1}, KEK_{Z1}-VN, y KEK_{Z1}N y KI_{BS1} se combinan utilizando los algoritmos de cifrado TA41 y TA51, obteniendo $SKEK_{Z1}$. El material de claves RSO, $SKEK_{Z1}$, KEK_{Z1}-VN y KEK_{Z1}N se redirigen de forma transparente a través de ZM1 105 a la BS1 115, que combina este material de claves con KI_{BS1} utilizando TA41 y TA52, obteniendo KEK_{Z1}, que se almacena en la BS1 115. En la realización referida, se devuelve al KMF 101 una confirmación no cifrada de un recibo satisfactorio de cada una de las claves a través del ATR 113.

En la FIG 4 se muestra un diagrama de bloques que muestra el almacenamiento de claves dentro de un sistema de comunicaciones. En particular, se muestra el almacenamiento de la información de autenticación de sesión a través del sistema de comunicaciones. En la realización preferida, la información de autenticación de sesión incluye una semilla aleatoria, RS, y dos claves de sesión, KS, para la autenticación de una MS y KS' para la autenticación de la infraestructura, para cada una de las estaciones móviles 401, 403, y 405 (sólo se muestran tres debido a restricciones de espacio, aunque numerosas MS forman parte del sistema). La información de autenticación de sesión (SAI) se usa para generar una clave de cifrado derivada (DCK) para cada una de las MS 401.

Para cada una de las MS 401, 403, y 405, el KMF 101 almacena una Identidad de Abonado TETRA individual (ITSI), la Identidad de Equipo TETRA (TEI), y una clave de autenticación de MS ("clave de MS") que es única para cada una de las MS 401, 403, y 405 y se almacena dentro de cada una. En la realización preferida, las claves de la interfaz aire y las claves de la MS se almacenan de forma cifrada por hardware usando una clave hardware K_H dentro del KMF 101. El algoritmo DVI-XL, disponible en Motorota, Inc., se usa para cifrar las claves para su almacenamiento en el KMF 101 en la realización preferida. Los paréntesis rectos [] seguidos de un nombre de clave indican que el material dentro de los paréntesis rectos está cifrada por esa clave.

El KMF 101 genera información de autenticación de sesión para cada una de las MS 401, 403, y 405, cuya SAI está cifrada al menos parcialmente y se redirige no en tiempo real al UCS 103 para su almacenamiento. Para cada una de las MS 401, 403, y 405, el UCS 103 almacena las ITSI, TEI e ID del HLR asociado con cada una de las MS, así como la SAI. En la realización preferida, KS y KS' se almacenan cifradas por la inter-clave (como se reciben desde el KMF 101) en el UCS 103 para un transporte rápido y sencillo, y la RS se almacena sin cifrar El UCS 103 es un dispositivo transparente en la realización preferida, de modo que no realiza ninguna función de cifrado o descifrado. Para eliminar la potencial doble entrada de información, el KMF 101 recibe información de configuración desde el UCS 103. Ejemplos de información de configuración son: la Identidad de Abonado TETRA Individual (ITSI), la Identidad de Grupo de Abonados TETRA (GTSI), zona local, y gestores de zona. El KMF usa una tabla de búsqueda, tal como una tabla de búsqueda de DNS (Servidor de Nombres de Dominio), para obtener las direcciones de ATR 113 y 127. La distribución de cada uno de los diferentes tipos de claves tiene requisitos de configuración diferentes, como se describe en este documento.

El UCS 103 redirige la SAI apropiada a cada uno de los ZM 105 no en tiempo real, en base a la ID del HLR asociado con cada una de las MS 401. El ZM 105, como el UCS 103, es un dispositivo transparente y no realiza ninguna función de cifrado ni descifrado. El ZM 105 almacena, para cada una de las MS que tienen el HLR 109 como su localización local, una ITSI, TEI y SAI. En la realización preferida, KS y KS' se almacenan cifradas por la inter-clave (como se reciben desde el UCS 103) en el ZM 105 ó 119 para un transporte rápido y sencillo, y RS se almacena sin cifrar.

El ZM 1.05 redirige la SAI al HLR 109 no en tiempo real. El HLR 109 almacena una ITSI y la SAI para cada una de las MS 401, 403, y 405. En la realización preferida, KS y KS' se almacenan cifradas por la inter-clave (según se recibe desde el ZM 103) en el HLR 109, y RS se almacena sin cifrar. En la realización referida, RS, KS y KS' se almacenan sin cifrar en el VLR 111 para una autenticación más rápida. En una realización alternativa, KS y KS' pueden almacenarse sin cifrar en el HLR 109 para una autenticación más rápida.

Cuando se autentica una MS 401 en la zona, se genera una nueva DCK para la MS 401 por el VLR 111 en el controlador de zona 107 a partir de la SAI en tiempo real, después de que se descifra cualquier SAI cifrada debido a la transferencia de la SAI desde el HLR 109. (La ITSI, SAI, y la DCK anterior asociadas con esa MS 401 se redirigen al VLR 111 en tiempo real antes de que se cree la nueva DCK). La ITSI, SAI y la nueva DCK se redirigen al HLR 109 en tiempo real para su almacenamiento. En la realización preferida la ITSI, SAI y DCK vienen desde el HLR para la MS 401, de este modo esta información puede venir de una zona diferente si la MS 401 no usa el HLR 109 para su zona local. Cuando la SAI/DCK viene de una zona diferente, esa zona cifra/descifra la información si es necesario, con la inter-clave para su transporte a la zona apropiada, lo cual también proporciona el cifrado/descifrado apropiado dentro de la zona. La DCK se almacena cifrada por la intra-clave KEK_Z para la zona en la cual se almacena, para un transporte fácil y rápido a la BS local 115 ó 117. En el ejemplo mostrado en la FIG. 4, cada una de las DCK se almacena cifrada por la KEK_{Z1}. En la realización preferida, KS y KS' están siempre cifradas con la inter-clave KEK_M, para un transporte fácil y rápido durante el proceso de autenticación, incluso cuando la transferencia es dentro de la misma zona.

Durante el proceso de autenticación, la BS 115 que comunica con la MS 401 recibe, desde el ZC1 107 en tiempo real, la DCK de la MS 401, cifrada por la intra-clave KEK_{Z1}. La BS 115 almacena la ITSI y la DCK descifradas para su uso inmediato mientras que la MS 401 está en el área de cobertura de la BS 115. Véase la FIG. 17 y su texto asociado para la información respecto a la persistencia de claves en cada uno de los sitios.

Cada una de las MS 401, 403, y 405 almacenan sus propias ITSI, TEI y DCK de forma descifrada, y K se almacena de forma aleatorizada o cifrada. Cada una de las MS 401, 403, y 405 también almacena en forma descifrada las CCK, GCK, MGCK y SCK relevantes según se reciben. Estas claves pueden almacenarse cifradas en la infraestructura en una realización alternativa.

El controlador de zona 107 es responsable de la distribución de claves en tiempo real y de la gestión de movilidad de las mismas. Mantiene las claves que pueden necesitarse para su distribución en modo de tiempo real necesarias cuando está en itinerancia, por ejemplo. La clave de cifrado de grupo es un elemento en cada uno de los registros del grupo de conversación y se mantiene en el HLR del grupo de conversación. La clave de cifrado común es una clave específica de una zona o de un sitio y se mantiene también en el controlador de zona. El ZC es responsable de la creación de MGCK (en base a la GCK y la CCK) y su distribución a los sitios.

Como las claves residen en el grupo de conversación y el HLR individual 109, el controlador de zona 107 no es transparente con respecto al cifrado del material de claves. El ZC 107 mantiene una clave de protección KI, y dos claves de cifrado de las claves de infraestructura, la inter-clave KEK_M y la intra-clave KEK_Z, para la distribución del material de claves. KI se usa para sellar (cifrar) KEK_M y KEK_Z cuando se envían al KMF 101. La mayor parte de la información de claves se cifra por el KMF 101 con la inter-clave, KEK_M. El controlador de zona 107 descifra el material de claves usando KEK_M y cifra de nuevo la misma información usando KEK_Z cuando se envía la información a un sitio dentro de la zona. De este modo, el controlador de zona, 107 tiene los algoritmos TETRA utilizados para el cifrado/descifrado de las claves de infraestructura (tales como TA41 y TA52 y TA31 y TA32), como se describe en este documento.

El controlador de zona envía confirmaciones ACK de las operaciones de reaprovisionamiento de claves de la infraestructura para el KMF 101 a través del ATR 113. Cuando un ZC 107 ó HLR 109 recibe una actualización de claves, el dispositivo en primer lugar descifra la actualización de claves y comprueba la inexistencia de corrupción verificando la integridad de los datos y envía el resultado de esta operación al KMF 101 a través del ATR 113 en la forma de una confirmación ACK.

El sitio es un punto final para el cifrado de la interfaz aire. El audio sobre la interfaz aire entre la BS 115 y la MS 401 está cifrado. El audio dentro de la infraestructura no está cifrado. El tráfico saliente se cifra con algoritmos que usan MGCK, CCK, y SCK, o DCK para las llamadas individuales. Todo el tráfico entrante se cifra con algoritmos que usan DCK o SCK. Los sitios mantienen los algoritmos de tráfico y el almacenamiento de claves para SCK, CCK, y MGCK, así como DCK. Como el sitio base tiene un almacenamiento de claves de tráfico, el sitio base no es transparente con respecto al cifrado del material de claves. Todo el material de claves distribuido a los sitios base está cifrado por la intra-clave, KEK_Z. De este modo, el sitio base mantiene una clave de protección, KI, y una inter-clave KEK_Z. De este modo, los sitios base tienen los algoritmos TETRA utilizados para el cifrado/descifrado de claves de infraestructura (tales como TA41 y TA52 y TA31 y TA32), como se describe en este documento.

La MS es otro punto final para el cifrado de la interfaz aire. El tráfico saliente se cifra con algoritmos que usan MGCK, CCK, y SCK, o la DCK si se dirigen individualmente. Todo el tráfico entrante está cifrado con algoritmos que usan DCK o SCK, y las identidades pueden cifrarse con SCK o CCK. La MS mantiene los algoritmos de tráfico y el almacenamiento de claves para SCK, CCK, GCK, y MGCK así como DCK.

Las siguientes figuras proporcionan ejemplos del papel del controlador de zona 107 ó 121 en alguna de sus funciones de generación de claves, de distribución de claves y de autenticación, así como las operaciones de la estación base/sitio base y las MS en los procesos de generación de claves, de distribución de claves y de autenticación.

Un diagrama que muestra un ejemplo de almacenamiento de claves y distribución de la información de autenticación dentro de un sistema de comunicaciones se muestra en la FIG. 5. La información de autenticación de sesión (RS, KS y KS') es necesaria para facilitar la autenticación en tiempo real de la MS 401 por el ZC 107 y la autenticación en tiempo real del sistema por la MS, así como la autenticación mutua. Las activaciones para la transferencia de SAI pueden ser una iniciación manual por el operador de KMF, un disparador automático de fraude desde el sistema, o un cambio periódico de la SAI por el KMF 101.

La FIG. 5 muestra la transferencia de SAI para dos estaciones móviles, ITSI1 401 e ITSI2 403 (no mostradas ninguna). El KMF 101 cifra al menos parte de la SAI (por ejemplo, KS y KS') con la inter-clave KEK_M para el sistema, y redirige ITSI1, ITSI2, RS, y KS y KS' cifradas por la KEK_M al UCS 103. El UCS 103 almacena una copia y la redirige a su ZM local 105 ó 119 para cada una de las ITSI. Las líneas discontinuas dentro de un dispositivo de sistema indican el paso transparente de la información a través del dispositivo del sistema. El ZM 105 ó 109 también almacenan una copia y la dirige a su ZC 107 ó 121, en particular, el HLR 107 ó 123. El ZC 107 ó 121 almacena KS y KS' cifradas junto con RS en el HLR 107 ó 123. Una vez que el HLR 109 ó 123 recibe la SAI, se envía una confirmación si cifrar (ACK), cuando falla el descifrado usando KEK_M, de vuelta al KMF 101 a través del ATR 113 ó 127 desde la zona en la cual reside el HLR 109 ó 123. Si existe un VLR 111 para la MS 403, tal como la ITSI2, el ZC 121 envía KS y KS' cifradas con la inter-clave KEK_M al VLR 111. La coordinación entre una información de sesión de autenticación anterior y la información de una nueva de sesión de autenticación no es necesaria. El HLR 109 ó 123 sólo necesitan una copia de la SAI por ITSI registrada. El UCS 103 y el ZM 105 ó 119 almacenan copias de la información de sesión de autenticación para proporcionar la recuperación desde los fallos o mantenimiento del sistema.

Proporcionando almacenamiento y redirigiendo la información de autenticación de sesión y las claves no en tiempo

real (es decir, si restricción de tiempo) entre los dispositivos del sistema de primer nivel y en tiempo real (es decir, a petición) entre los dispositivos del sistema de segundo nivel como se ha descrito anteriormente, el sistema de autenticación proporciona un sistema tolerante a fallos que permite también la rápida recuperación de fallos. Si el KMF 101, el UCS 103, y/o los ZM 105 y 119 fallan o están separados del resto del sistema, aún puede realizarse la autenticación plena sin interrupción en base a tiempo real con la información de autenticación de sesión, por ejemplo para la MS2 403, almacenadas en el HLR 123 y el VLR 111. Un fallo en cualquiera de estos dispositivos 101, 103, 105 y 119 no es catastrófico, ya que los datos almacenados pueden descargarse desde cualquiera de los otros dispositivos que almacenan la información. Si un controlador de zona 107, el HLR 109, y/o el VLR 119 experimentan una falta o fallo, la SAI puede descargarse inmediatamente desde el ZM 105 en la zona. Eliminando la necesidad de que el KMF 101 participe en tiempo real en el proceso de autenticación, hay menos carga sobre el KMF 101 y menos tráfico en general sobre los enlaces de comunicaciones entre los dispositivos de la infraestructura del sistema.

En la FIG. 6 se muestra un diagrama que muestra el almacenamiento de la información de autenticación y que realiza la decisión de autenticación dentro de un sistema de comunicaciones. Se muestran cuatro estaciones móviles dentro de un sistema donde tres estaciones móviles 401, 403, y 405 usan el HLR1 109 del primer controlador de zona 107, una estación móvil 407 usa el HLR2 123 del segundo controlador de zona 121, las dos estaciones móviles 401 y 403 usan el VLR1 111, y las dos estaciones móviles 405 y 407 usan el VLR2 125. Se muestra el almacenamiento de SAI a través de los dispositivos de sistema. También se muestran las decisiones de la estación base de si autentica o no a un móvil en un activador particular. Por ejemplo, los mensajes de encendido, tanto cifrados como no cifrados, requieren autenticación. Cualquier mensaje enviado en claro (es decir, sin cifrar) requiere autenticación. Los mensajes de itinerancia cifrados pueden autenticarse implícitamente, es decir, el mecanismo de reto y respuesta puede evitarse si el mensaje de itinerancia cifrado se descifra satisfactoriamente por la BS 131. Los mensajes de encendido, los mensajes de itinerancia, las actualizaciones de localización y otros tipos de mensajes se consideran peticiones para comunicar dentro del sistema de comunicaciones. Cuando se requiere autenticación la BS 115, 117, 129, ó 131 envía una petición de autenticación de la MS con la infraestructura (con un controlador de zona en la realización preferida). En el caso de que el dispositivo de infraestructura al cual se envían las peticiones de autenticación pase a no disponible, por ejemplo cuando el dispositivo falla, está fuera de servicio para mantenimiento, o el enlace de comunicaciones con el dispositivo no esté operativo, la BS almacena las peticiones de autenticación durante el periodo de tiempo en el que el dispositivo de infraestructura no está disponible. Cuando el dispositivo de infraestructura pasa a estar disponible, por ejemplo, si el dispositivo vuelve al servicio después de un fallo o mantenimiento o cuando el enlace de comunicaciones se repone, la BS redirige las peticiones de autenticación almacenadas al dispositivo de la infraestructura.

En una situación mostrada en la FIG. 6, una primera MS 401 envía un mensaje de encendido en claro (sin cifrar) a la primera BS 115. En la realización preferida, se requiere la autenticación de la MS 401 en esta situación. Como la MS 401 usa el HLR 109 en la zona en la que está localizada la BS 115, se redirige la información de autenticación de sesión SAI1 para la MS 401 desde el HLR 109 al VLR 111 en la zona de terminación del proceso de autenticación.

La segunda MS 403 está en itinerancia desde la BS1 115 a la BS2 117 y envía un mensaje de itinerancia en claro (sin cifrar) a la segunda BS 117. En la realización preferida, se requiere la autenticación de la MS 403 en esta situación. Como la MS 403 usa el HLR 109 en la zona donde está localizada la BS 115, y como la MS 403 transitó desde un sitio servido por el mismo VLR que el nuevo sitio, la información de autenticación de sesión SAI2 para la MS 403 está ya situada en el VLR 111 en la zona para la terminación del proceso de autenticación.

La tercera MS 405 envía un mensaje de encendido cifrado a la tercera BS 129. En la realización preferida, se requiere la autenticación de la MS 405 en esta situación. Como la MS 405 usa el HLR 123 en la zona donde está localizada la BS 129, la información de autenticación de sesión SAI3 para la MS 405 se redirige desde el HLR 123 al VLR 125 en la zona para la terminación del proceso de autenticación.

La cuarta MS 407 está en itinerancia desde la BS2 117 a la BS4 131 y envía un mensaje de itinerancia cifrado a la cuarta BS 131. En la realización preferida, en esta situación no se requiere la autenticación (plena) de la MS 403. En cambio, la MS está autenticada implícitamente, es decir, el mecanismo de reto y respuesta se evita si el mensaje de itinerancia cifrado se descifra satisfactoriamente por la BS 131, Como la MS 407 usa el HLR 109 en una zona distinta de la zona donde está localizada la BS 131, la clave de cifrado (y si es necesario, la información de autenticación de sesión SAI4) para la MS 407 debe redirigirse desde el HLR 109 al VLR 125 donde ha transitado la MS 407 para la terminación del proceso de autenticación, Típicamente, al menos una parte de la SAI se cifra por la inter-clave antes de transferirla a otra zona. Si falla la autenticación implícita, entonces se realiza la autenticación completa de la MS 407.

En la FIG. 7 se muestra un diagrama que muestra el proceso de reto y respuesta para autenticar una estación móvil por un centro de autenticación de acuerdo con la Normativa TETRA. Cuando se produce la autenticación de una MS 707, un centro de autenticación 701, tal como un KMF 101, combina la clave de autenticación móvil, K, con RS utilizando el algoritmo de cifrado TA11, como se define en la Normativa TETRA. La salida del proceso de TA11 703 es KS, la cual se introduce con RAND1 (un número aleatorio) al algoritmo de cifrado TA12, como se define en la

Normativa TETRA. El proceso de TA12 705 saca XRES1, una respuesta esperada, y DCK1, una clave de cifrado derivada para el móvil. RAND1 y RS se proporcionan a la MS 707. La MS 707 va a través de un proceso similar combinando su clave de autenticación móvil, K, con la RS recibida desde el AuC 701 utilizando el proceso TA11 703. El proceso TA11 703 saca KS, que se introduce con RAND1 al proceso de TA12 705. El proceso de TA12 705 en la MS 707, saca RES1, una respuesta al reto, y DCK1, la clave de cifrado derivada para el móvil. La MS 707, redirige RES1 al AuC 701. Si XRES1 y RES1 coinciden, el AuC 701 envía un mensaje de paso de autenticación a la MS 707, y la comunicación sobre la interfaz aire con la DCK1 nuevamente creada puede comenzar. Si XRES y RES no coinciden, el AuC 701 envía un mensaje de fallo de la autenticación, a la MS 707, y la comunicación sobre la interfaz aire con la DCK1 nuevamente creada está prohibida, aunque la vieja DCK1 puede usarse una vez que ha fallado la autenticación.

En la FIG. 8 se muestra un diagrama que muestra el proceso de reto y respuesta para autenticar un centro de autenticación por una estación móvil de acuerdo con la Normativa TETRA. Cuando se produce la autenticación de un AuC 701, tal como el KMF 101, una MS 707 combina la clave de autenticación móvil, K, con RS utilizando el algoritmo de cifrado TA21, como se define en la Normativa TETRA. El proceso TA21 801 del AuC 701 saca KS', que se introduce con RAND2 (un número aleatorio) al algoritmo de cifrado TA22, como se define en la normativa TETRA. El proceso TA22 803 saca XRES2, una respuesta esperada, y DCK2, una clave de cifrado derivada para el móvil 707. RAND2 se proporciona al AuC 701. El AuC 701 va a través de un proceso similar combinando la clave de autenticación móvil, K, para la MS 707 con RS utilizando el proceso TA21 801. El proceso TA21 801 del AuC 701 saca KS', que se introduce con RAND2 al proceso TA22 803. La salida del proceso TA22 803 en el AuC 701 es RES2, una respuesta al reto, y DCK1, la clave de cifrado derivada para el móvil. El AuC 701 redirige RES y RS a la MS 707. Si XRES y RES coinciden, la MS 707 envía un mensaje de paso de autenticación al AuC 701, y la comunicación sobre la interfaz aire con la DCK1 nuevamente creada puede comenzar. Si XRES y RES no coinciden, la MS 707 envía un mensaje de fallo de autenticación al AuC 701, y la comunicación sobre la interfaz aire con la DCK1 nuevamente creada no tiene lugar.

En la FIG. 9 se muestra un diagrama que muestra la distribución de SAI y el proceso de autenticación entre un sistema de comunicaciones y una estación móvil en tiempo real de acuerdo con la invención. La FIG. 9 muestra una implementación del proceso de autenticación de la Normativa TETRA incluyendo cómo los diversos dispositivos del sistema dentro de la infraestructura actúan dentro del proceso de autenticación. La FIG 9 muestra cómo el ZC 107, incluyendo el HLR 109 y el VLR 111, y la BS 115 actúan como Proxy, o agentes de autenticación, para el KMF 101 en el proceso de autenticación. En tiempo no real, KS y KS' cifradas por la inter-clave, y RS se pasan a través del KMF 101 al UCS 103, al primer ZM 105, y al HLR 109 del primer controlador de zona 107.

Después de que la BS 115 envía una petición de autenticación de la MS 401 al ZC 107, el VLR 111 genera PAND1 y usa KS y PAND1 con el proceso TA12 para generar XRES1 y DCK1, de acuerdo con la FIG. 7, en este documento, y redirige RAND1 y RS a la BS 115, la cual redirige RAND1 y RS sobre el aire a la MS 401. La MS 401 combina su propia K y RS con el proceso TA11 para generar KS, a continuación combina RAND1 y KS de acuerdo con la FIG. 7 en este documento, obteniendo RES1 y DCK1, y redirige RES1 a la BS 115, la cual redirige RES1 al VLR 111 en el ZC 107. El VLR 111 compara RES1 y XRES1, y el resultado es R1. Cuando RES1 y XRES1 coinciden, DCK1 y SAI para la MS 401 se almacenan en el VLR 111 y el HLR 109 y DCK1 (cifrada por la inter-clave). En la realización preferida, DCK1 está cifrada con la intra-clave para la primera zona antes de enviase a la BS 115. R1 se redirige a la BS 115 en reconocimiento de que pasó la autenticación, y la BS 115 almacena DCK1 y envía R1 a la MS 401 indicando que ha pasado la autenticación, Cuando RES1 y XRES1 no coinciden, el VLR 111 rechaza la DCK1 nuevamente creada sin almacenarla o redirigirla a la BS 115 y redirige R1, una confirmación negativa del proceso de autenticación, a la BS 115, y la BS 115 envía R1 a la MS 401 indicando que ha fallado la autenticación.

Para solicitar la autenticación de la infraestructura, la MS 403 envía RAND2 a la BS 129, la cual redirige RAND2 al VLR 125 en el ZC 121. El VLR 125 busca RS y KS' y genera RES2 y DCK2 usando el proceso TA22 de acuerdo con la FIG. 8 en este documento, y redirige RES2 y RS a la BS 129, la cual redirige RES2 y RS sobre el aire a la MS 403. La MS 403 combina RS y su propia K con el proceso TA21, obteniendo KS', la cual se combina a continuación con RAND2 en el proceso TA22 de acuerdo con la FIG. 8 en este documento, obteniendo XRES2 y DCK2. La MS 403 compara RES2 y XRES2. Cuando RES2 y XRES2 coinciden, la MS 403 envía el mensaje R2 a la BS 129 confirmando que pasó la autenticación, la BS 129 envía R2 al ZC 121, y el VLR 125 causa DCK2 y la SAI para el móvil 403 se almacenen en el VLR 125 y el HLR 123 para la MS 403 y redirige DCK2 a la BS 129, que almacena DCK2. En la realización preferida, DCK2 está cifrada con la intra-clave para la segunda zona antes de enviarse a la BS 129. Cuando RES2 y XRES1 no coinciden, la MS 403 envía el mensaje R2 a la BS 129 indicando que falló la autenticación, la BS 129 envía R2 al ZC 121, y el VLR 125 rechaza la DCK2 nuevamente creada sin enviarla a la BS 129.

En cualquier proceso de autenticación, si el VLR 111 en la zona donde MS 401 ó 403 está localizada en el presente no tiene la SAI almacenada para la MS 401 ó 403, el VLR 111 obtiene la SAI desde el HLR para la MS 401 ó 403. Cuando el HLR 109 para la MS 401 ó 403 está en la misma zona, la SAI simplemente se pasa dentro del ZC 107 al VLR 111. Cuando el HLR 109 para la MS 401 ó 403 está en una zona diferente, la zona para el HLR local se determina a partir de una tabla de mapeo de la zona local que realiza el mapeo de ITSI a su Zona Local, y la SAI se

redirige al ZC 107 para el VLR 111. En la realización preferida, cuando el material de claves se redirige desde el HLR para la MS 401 ó 403 al VLR 111, al menos parte de la SAI, en particular KS y KS', se cifran con la inter-clave. Cuando se transfiere la DCK dentro de una zona, la DCK está cifrada con KEK_Z. De forma similar, si la zona donde tiene lugar la autenticación no es la zona local para la MS 401 ó 403, la información actualizada de SAI y DCK se cifrará con la inter-clave, al menos en parte, y se redirigirá al VLR apropiado. Como las claves se pasan entre dispositivos que requieren una clave de cifrado diferente, un dispositivo recibe un mensaje, lo descifra con una clave y re-cifra el resultado con otra clave para el siguiente dispositivo.

La autenticación mutua, cuando la MS y la infraestructura se autentican mutuamente entre sí, se describe con respecto a la FIG. 3 titulada "Autenticación mutua iniciada por la SwMI" y la FIG. 4 titulada "Autenticación mutua iniciada por la MS" y sus textos asociados de la Normativa TETRA. Las DCK resultantes (DCK1 y DCK2) de cada uno de los procesos se combinan usando el algoritmo de cifrado TB4, y la DCK resultante se usa para la comunicación. La MS 403 ha enviado un mensaje cifrado, por ejemplo, un mensaje de actualización de localización cifrado por la DCK. El BS 115 puede redirigir opcionalmente una confirmación de la recepción del mensaje cifrado a la estación móvil MS 403. La identidad, ITSI2, de la MS 403 está cifrada con la CCK, de modo que la BS 115 es capaz de determinar qué MS ha enviado el mensaje, incluso aunque no tenga la DCK2 para la MS 403. La BS 115 solicita la DCK2 desde el ZC 107. El ZC 107 determina si necesita solicitar la DCK2 desde una zona diferente, lo cual se requiere en este caso, porque MS2 403 está en itinerancia desde una zona diferente, la zona 2, y el HLR 123 para la MS 403 está en la zona 2. El ZC 107 determina qué zona tiene el material de claves necesario y envía una petición a la zona objetivo del material de claves. En el ejemplo, DCK2 se encuentra en el HLR 123 para la zona 2, que es la zona objetivo, y DCK2 se envía al ZC 107 desde el HLR de esa zona 123 después de cifrarse con la inter-clave, KEK_M. El ZC 107 envía DCK2 a la BS 115 cifrada con la intra-clave KEK_{Z1}. La BS 115 usa DCK2 para descifrar el mensaje de actualización de localización para la MS 403; y cualquier mensaje posterior desde la MS 403, y redirige la actualización de localización al ZC 107. RS, KS, KS' se solicitan en un tiempo posterior desde el HLR 123 de modo que puede realizarse una autenticación completa si es necesario. En la realización preferida, el VLR 111 para la MS 403 no se actualiza con la localización de la MS hasta que la MS se autentica implícitamente o realiza una autenticación completa. El recibo del mensaje de actualización de localización descifrado adecuadamente se considera como una autenticación implícita, en cuyo momento el VLR 111 se actualizaría.

En la situación donde puede desearse introducir una GCK/MGCK, el proceso es el mismo que se ha descrito anteriormente con respecto a la DCK, excepto que el VLR 111 obtiene la GCK, la combina con la CCK, como se describe más adelante en la FIG. 15 y su texto asociado, y redirige la MGCK resultante, cifrada con la intra-clave KEK_{Z1}, a la BS 115 ó 117.

En la FIG. 11 se muestra un diagrama que ilustra una introducción de clave dentro de un sistema de comunicaciones. El procedimiento de introducción de clave se utiliza para redirigir una clave, tal como la DCK o la GCK/MGCK, a un sitio de redirección cuando una MS conmuta entre sitios desde su sitio actual al sitio de redirección. Este proceso proporciona de este modo un mecanismo para redirigir una clave a un sitio antes de la llegada de la MS 401 ó 403, de modo que puedan producirse las transferencias y la itinerancia cifradas sin interrupciones. La FIG. 11 muestra un ejemplo de transferencia de DCK2 entre zonas y una transferencia de DCK1 dentro de una zona. La MS inicia el procedimiento. Aunque las KS, KS', y DCK están almacenadas cifradas en el HLR, y la DCK está almacenada cifrada en el HLR y el VLR en la realización preferida, se muestran sin cifrar en la FIG. 11 en beneficio de la simplicidad.

La MS1 401 comienza el proceso de itinerancia desde la BS1 115, que tiene la Identificación del Área de Localización 1 (LAID1), en el sitio 1 a la BS2 117, que tiene la Identificación del Área de Localización 2 (LAID2) en el sitio 2 en la zona 1. El MS 401 envía a la BS1 115 un mensaje indicando que la MS1 transitará al sitio 2. En la realización preferida, este mensaje es un mensaje de Preparación OTAR. La BS 115 retransmite este mensaje al ZC 107. El ZC 107 determina si se necesita transferir la DCK a otra zona o no determinando si el sitio al cual está transitando la MS 401 está en su zona o no. En este ejemplo, el sitio 2 también está servido por el ZC 107, de modo que no hay ninguna necesidad de transferir la DCK a otra zona. Como la DCK se transfiere dentro de la zona, el ZC 107 responde a la BS 115 con el uso de un mensaje de retardo corto. En este caso, la BS 115 rechaza la conmutación de la MS 401 al sitio 2 por un retardo equivalente al retardo corto, que retarda aproximadamente el tiempo que tardará en redirigir la DCK al siguiente sitio desde el VLR 111 en la misma zona. En la realización preferida, el retardo corto es menor de 50 ms. La MS 401 espera un OK desde la BS 115 antes de operar en el nuevo sitio, por ejemplo, con itinerancia, conmutando sitios, o comunicando, y la BS 115 envía el OK después de que expira el periodo de retardo corto. Durante el periodo de retardo, el VLR 111 en el ZC1 107 cifra DCK1 con la intra-clave y la redirige a la BS2 117 en el sitio 2, donde la MS 401 y la BS2 117 podrán intercambiar mensajes cifrados usando la DCK1. En la realización preferida, el VLR 111 para la MS 401 no está actualizado con la localización de la MS hasta que la MS 401 se autentica implícitamente o realiza una autenticación completa.

La MS2 403 comienza el proceso de itinerancia desde la BS3 129, que tiene la Identificación del Área de Localización 3 (LAID3) en el sitio 3 en la zona 2 para la BS1 115, que tiene la Identificación del Área de Localización 1 (LAID1) en el sitio 1 en la zona 1. La MS 403 envía a la BS3 129 un mensaje indicando que la MS2 transitará al sitio 1. En la realización preferida, este mensaje es un mensaje de Preparar OTAR. La BS 129 retransmite este mensaje al ZC 121. El ZC 121 determina si se necesita transferir la DCK a otra zona o no determinando si el sitio al

cual está transitando la MS 401 está en su zona o no. En este ejemplo, el sitio 1 no está servido por el ZC 121, de este modo es necesario transferir la DCK a otra zona. Como la DCK se transfiere a otra zona, el ZC 121 responde a la BS 129 con el uso de un mensaje de retardo largo. En este caso el BS 129 rechaza la conmutación de la MS 403 al sitio 1 por un retardo equivalente al retardo largo, cuyo retardo se aproxima al tiempo que tardará redirigir DCK desde el VLR 111 al sitio en la siguiente zona. En la realización preferida, el retardo largo es mayor o igual de 50 ms. La MS 403 espera un OK desde la BS 129 antes de conmutar entre sitios, y la BS 129 envía el OK después de que expira el periodo del largo retardo. Durante el periodo de retardo, el VLR 125 en ZC1 121 cifra DCK2 con la inter-clave y la redirige al ZC1 107, que la descifra con la inter-clave, la cifra con la intra-clave KEK_{Z1}, y redirige el resultado a la BS1 115 en el sitio 1, donde la MS 403 y la BS2 115 podrán intercambiar mensajes cifrados usando DCK2. En la realización preferida, el VLR 111 para la MS 403 no está actualizado con la localización del MS hasta que la MS 403 se autentica implícitamente o realiza una autenticación completa, en cuyo instante el VLR 125 para la MS2 en ZC2 121 se elimina. RS, KS, KS' se solicitan un tiempo más tarde desde el HLR en ZC3 223 (el HLR de la zona local para la MS 403) de modo que puede realizarse una autenticación completa si es necesario.

La FIG. 12 es un diagrama que muestra la distribución de una clave de cifrado estático para una BS dentro de un sistema de comunicaciones. La SCK es una clave del tráfico de voz a nivel de sistema que se usa para cifrar la voz o los datos, la ESI (Identidad Corta Cifrada), y el tráfico de señalización cuando no está disponible la autenticación. Las SCK se identifican por SCKN y SCK-VN y se almacenan en el KMF 101 cifradas por una clave hardware y en los ZM 105 y 119 cifrada con TA31. En la realización preferida, puede haber hasta 32 SCK distintas en todo el sistema. Cada una de las BS almacena un SCK, identificada por un número de SCK (SCKN), cada uno de los cuales tiene un número de versión de SCK (SCK-VN), aunque la SCK puede tener múltiples versiones que se usan o se usaron en el sistema. Cada uno de los SCKN tiene un número de versión SCK-VN, y en la realización preferida, dos números de versión es decir, dos claves, se almacenan para cada uno de los SCKN. La MS debe poder almacenar 32 SCK para un SCK-VN, además de 32 SCK para otro SCK-VN. Las 31 SCK adicionales en la MS se definen para la operación directa entre estaciones móviles. Una nueva SCK reemplaza al SCK-VN más antiguo. La SCK puede proporcionarse a las BS y las estaciones móviles de varias formas, incluyendo a través de un Cargador de Claves Variables (KVK), a través de un software de ordenador tal como el Software RSS disponible en Motorota, Inc., y a través de la OTAR (Reaprovisionamiento de Claves Sobre el Aire) a través del ATR de la zona local de la MS. Aunque no mostrado en el dibujo por restricciones de espacio, SCKN y SCK-VN se envían junto con SCK para propósitos de identificación.

Un proceso para transferir una SCK a cada una de las BS en el sistema se muestra en la FIG. 12. Cuando el KMF 101 determina que se debe actualizar la SCK, el KMF 101 genera una nueva SCK. Para determinar la zona local de una BS, en la realización preferida, el KMF 101 usa un mapa de BS para el ZC local desde el UCS 103 y la tabla de búsqueda basada en la zona para obtener la dirección para el ATR en la zona. El KMF 101 cifra la SCK con la intra-clave, KEK_Z, para la zona en la cual está localizada la BS, y envía la clave cifrada al ZM para esa BS. El ZM almacena una copia y la redirige a la BS pretendida. Una confirmación ACK no cifrada se envía desde la BS al ZC y al KMF 101 a través del ATR en la zona en la que reside la BS. La confirmación ACK representa que la SCK se recibió correctamente en la BS.

Un ejemplo específico de una transferencia de SCK a la BS1 115 incluye una transferencia de la información del sitio, incluyendo un mapa de BS para el controlador de zona local, desde el UCS 103 al KMF 101. El KMF 101 usa el mapa para determinar que la BS1 115 está localizada en la zona 1. El KMF 101 genera la SCK y la cifra con la intra-clave KEK_{Z1}, para la zona 1 donde está localizada la BS1. El KMF 101 redirige la SCK cifrada al ZM 105 para la zona 1. El ZM1 105 almacena una copia de la SCK cifrada y la redirige a la BS1 115 a través de un enlace cableado. La BS1 115 descifra la SCK cifrada usando KEK_{Z1} y almacena la SCK descifrada. Cuando se recibe la SCK correctamente por la BS1, la BS1 115 envía una confirmación ACK sin cifrar al KMF 101 a través de ZC1 107 y el ATR 13 en la zona 1. Las transferencias de SCK para BS3 y BS4 se realizan de forma similar.

En la FIG. 13 se muestra un diagrama que muestra la distribución de una clave de cifrado estático para una estación móvil dentro de un sistema de comunicaciones. Cuando el KMF 101 determina que se debe actualizar la SCK para una MS 401, el KMF 101 genera un nuevo material de la clave SCK para la MS 401 de acuerdo con la FIG 10 titulada "Distribución de SCK a un individuo por un centro de autenticación" y su texto asociado en la Normativa TETRA. El proceso de generación de SCK obtiene el material de la clave SSCK (una SCK sellada), SCKN (el número de SCK), SCK-VN (el número de versión de SCK), y RSO (la semilla aleatoria usada en el proceso). Para determinar el ATR para la zona local de la MS 401, en la realización preferida, el KMF 101 usa la ITSI para su mapa de ZC local desde el UCS 103 y la tabla de búsqueda basada en la zona para obtener la dirección del ATR para la zona local. En el ejemplo de la FIG. 13, la zona local para la MS1 401 es la zona 2. El KMF 101 redirige SSCK, SCKN, SCK-VN, y RSO al ATR 127 de la zona local (2) para la MS 401. Si la MS 401 no está sobre el sistema, el ATR 127 envía una confirmación negativa NACK de vuelta al KMF 101. Si la MS 401 está sobre el sistema, la SCK se suministra a la MS 401 a través de la zona en la cual se localiza actualmente la MS 401. En la realización preferida el material de claves de SCK (por ejemplo, SSCK, SCKN, SCK-VN, y RSO) no se cifran para la transferencia entre dispositivos del sistema. El material de la clave SCK puede opcionalmente cifrarse para la transferencia entre dispositivos del sistema.

Cuando la MS 401 no está localizada en su zona local, el controlador de la zona local 121 de la zona 2 determina en

qué zona está actualmente localizada la MS 401 (la zona 1 en la FIG. 12) buscándola en el HLR 123 de la zona 2. El ZC2 121 redirige SSCK, SCKN, SCK-VN y RSO al controlador de zona 107 de la zona donde la MS 401 está localizada actualmente. El ZC1 107 redirige SSCK, SCKN, SCK-VN, y RSO a la BS 115 donde está localizada la MS 401. La BS 115 descifra la SSCK, SCK-VN, y RSO con la intra-clave KEK_{Z1},y redirige el resultado a la MS 401. Se envía una confirmación ACK no cifrada desde la MS 401 a la BS 115 al ZC 107 y al KMF 101 a través del ATR 113 en la zona donde reside la BS 115. La confirmación ACK representa que la SCK se recibió y se deselló correctamente en la MS (el proceso de desellado se describe en la Normativa TETRA).

Cuando la MS 401 está localizada en su zona local (no mostrado, pero se asume que es la BS3 129 en beneficio de este ejemplo), el VLR del controlador de la zona local 121 redirige SSCK, SCKN, SCK-VN y RSO a la BS 129 donde está localizada la MS 401 (no mostrada pero asumida para este ejemplo). La BS 129 redirige SSCK, SCKN, SCK-VN y RSO a la MS 401. Se envía un ACK sin cifrar desde la MS 401 a la BS 129 al ZC 121 y al KMF 101 a través del ATR 127 en la zona donde reside la BS 115. La confirmación ACK representa que la SCK se recibió y se deselló correctamente en la MS (el proceso de desellado se describe en la Normativa TETRA).

La FIG. 14 es un diagrama que muestra la distribución de una clave de cifrado común para una estación móvil y una BS dentro de un sistema de comunicaciones. La CCK es una clave de tráfico basado en el área de localización que se usa para cifrar voz, datos y señalización dentro del área de localización (LA) y se usa sólo para comunicaciones salientes. La CCK se destina para el uso con el cifrado del tráfico de llamadas de grupo en la Normativa TETRA. La CCK también se usa para cifrar la identidad del abonado creando la identidad corta cifrada (ESI). El tráfico de la llamada de grupo dentro de LA usa la CCK cuando no hay ninguna GCK disponible o está inhibida. Hay una CCK por área de localización. Un área de localización puede ser tan pequeña como un sitio, de este modo podría haber tantas CCK como sitios en el sistema. Es posible para más de un área de localización tener la misma CCK. La CCK se identifica por la CCK-ID (por ejemplo, CCK1, CCK2, y así sucesivamente) y la LAID (identificación del área de localización). Dos copias de cada una de las CCK (las dos últimas CCK-ID) están en el ZC y la BS para posibilitar una actualización de claves gradual de las MS en el sistema. Mientras que una CCK está en uso, se distribuye la siguiente a la MS. En la realización preferida, cada uno de los sitios mantiene una CCK para cada sitio adyacente al sitio, para transferencias sin interrupciones entre sitios y para facilitar la gestión consistente de la movilidad. Cuando se da una CCK adyacente a una MS, las dos últimas CCK se transfieren a la MS. Una nueva CCK reemplaza a la última CCK-ID. El almacenamiento a largo plazo de las CCK se produce en los ZM 105 y 119. La Normativa TETRA soporta varios métodos para la provisión de CCK sobre el aire, y la misma metodología de petición/provisión utilizada para cada una de las claves de la interfaz aire, y también permite la petición de claves bajo registro y cambio de célula por la estación móvil.

El procedimiento de la CCK para la BS ilustrado en la FIG. 14 se usa para transferir una CCK desde el KMF 101 a la BS (sitio) 115. El KMF 101 determina que es el momento para actualizar la CCK de una BS 115 y genera la CCK apropiada. En la realización preferida, cada una de las BS es un Área de Localización (LA) y tiene su propia Identificación del Área de Localización (LAID). La FIG. 14 muestra la transferencia de CCK1 y CCK2 para la zona 1 y la transferencia de CCK3 para la zona 2. Las CCK se cifran con la intra-clave, KEK_Z, para la zona donde está localizada LA. El UCS 103 proporciona un mapa de sitio a zona y un mapa de ZM a zona para el KMF 101. El KMF 101 usa estos mapas para enviar las claves directamente al ZM apropiado 105 ó 119, el cual almacena la CCK y redirige la CCK al controlador de zona 107 ó 121. El UCS 103 obtiene los parámetros del sitio a partir de los ZM 105 y 119 para crear la lista de sitios adyacente que se envía al KMF 101 y se redirige a los ZM 105 y 119 para redirigirse a los controladores de zona 107 y 121 para su uso. Si un sitio adyacente está en una zona diferente, la clave se transfiere entre los ZC involucrados. El ZC cifra la CCK con la inter-clave, KEK_M, para la transferencia entre controladores de zona. Usando la lista de sitios adyacentes, los controladores de zona 107 y 121 envían las CCK de los sitios adyacentes a los sitios apropiados. De este modo, cada uno de los sitios sobre la lista de sitios adyacentes tendrá las CCK para los sitios adyacentes a ese sitio. Las CCK adyacentes se usan de modo que las MS pueden solicitar la CCK para el sitio adyacente antes de que la MS conmute entre sitios. La BS 115 puede también redirigir las CCK a las MS según se reciben las nuevas CCK en la BS 115. Las CCK se cifran con la DCK para la MS 401 particular antes de transmitir la CCK cifrada a la MS 401. Se envían confirmaciones ACK por la BS al ZC y se devuelven al KMF 101 a través del ATR (donde reside la BS). Como el KMF 101 carece de adyacencia, no necesita confirmaciones ACK de las distribuciones adyacentes de CCK. Como el KMF 101 sigue a qué BS se da una CCK, la BS sigue la circulación de las CCK, es decir, qué MS tienen una CCK para un Área de Localización predeterminado, y redirige las ACK una vez que la CCK es actual.

Como la MGCK es una combinación de la CCK y la GCK, el controlador de zona creará cuatro MGCK usando las dos últimas CCK-ID y los dos últimos GCK-VN y las distribuirá consecuentemente (véanse la FIG. 15 y la FIG. 16).

La CCK es un parámetro específico de la zona de modo que no tiene ninguna necesidad de ir a través de los UCS 103. De este modo, el KMF 101 envía la información de CCK directamente al gestor de zona apropiado 105 ó 119, que es diferente que la metodología de reaprovisionamiento de las otras claves de la interfaz aire. El UCS 103 obtiene la información del sitio a partir de los gestores de zona 105 ó 119 para crear la lista de sitios adyacentes. Colocando las CCK en sitios adyacente, el procesamiento de las CCK en tiempo real se reduce, es decir la BS no necesita solicitar al controlador de zona la CCK para una BS adyacente cuando una MS solicita una CCK para un sitio vecino, de este modo la MS no necesita procesar una CCK cuando la MS conmuta entre sitios.

La FIG. 15 es un diagrama que muestra la distribución de una clave de cifrado de grupo para una BS dentro de un sistema de comunicaciones. La GCK se identifica por GTSI (ID de Abonado de Grupo TETRA como se denomina en la normativa TETRA) y el GCK-VN. En la realización preferida, GCKN es lógicamente equivalente a la GTSI desde una perspectiva de la gestión de claves. El almacenamiento de largo plazo de GCK se produce en el UCS y el ZM. La MGCK, que es una combinación de la GCK y la CCK, se identifica por la GTSI (o el GCKN), la CCK-ID (con LAID), y el GCK-VN. Se identifican cuatro MGCK por grupo de conversación (GTSI) por las dos últimas CCK-ID y los dos últimos GCK-VN. Las MGCK no se almacenan en un ZC 107 ó 121, sino que se crean por un ZC 107 ó 121 y se envían a la BS 115 supuesto que una MS afiliada con esa GTSI está en el sitio de la BS 115, que no recibe la GCK porque es una clave de largo plazo. Aunque no mostrado en el dibujo por restricciones de espacio, GCK-VN se envía junto con la GCK y la MGCK para propósitos de identificación.

El procedimiento para actualizar una GCK para un registro de un grupo de conversación tiene dos partes. La primera parte incluye actualizar la GCK real para el grupo de conversación, la segunda parte incluye generar la MGCK resultante como resultado de la actualización y la distribución de la MGCK a los sitios.

El procedimiento de la FIG. 15 transfiere una GCK desde el KMF 101 al HLR del grupo de conversación en el controlador de zona en la zona local para el grupo de conversación. Cuando el KMF 101 determina que es el momento para la actualización de la GCK, el KMF 101 genera una GCK para cada uno de los grupos de conversación y mantiene una tabla de GTSI-GCK. Las GCK se almacenan cifradas por hardware en el KMF 101. El KMF 101 no conoce qué ZC tiene el HLR para la GTSI, de modo que el KMF 101 envía la GCK cifrada con la inter-clave, KEK_M, al UCS 103. El UCS 103 almacena el material de claves y lo redirige a su ZM local 105 o 110 para el grupo de conversación (GTSI) asociado con la GCK. El ZM 105 ó 119 redirige el material de claves a su ZC 107 ó 121, que almacena el material de clave en el HLR de grupo para la GTSI cifrada por la KEK_M. El ZC 107 verifica que el material de clave puede descifrarse correctamente y envía una confirmación ACK de vuelta al KMF 101 a través del ATR 113, donde reside el HLR de grupo 109 para la GTSI. La confirmación ACK refleja que el HLR 109 contiene una copia cifrada correcta de la GCK. El ZC 107 descifra el material de clave con KEK_M y lo re-cifra con la intra-clave KEK_Z, para su almacenamiento en el VLR 111. Cualesquiera otros VLR, tal como el VLR2 125, fuera de la zona local asociada con la GTSI tendrá la GCK cifrada con KEK_M redirigida a los mismos. La FIG. 15 muestra ambos casos de la inter-zona y la intra-zona.

Como la MGCK es una combinación de la GCK y la CCK generadas por un ZC usando el algoritmo TA71 1501, 1503, ó 1505, cuando la GCK cambia o la CCK cambia, la MGCK también debe cambiar consecuentemente. Las cuatro MGCK se envían a todos los sitios que tiene afiliación de grupo de conversación que coincide con la GTSI para la GCK. Como las dos últimas CCK-ID y las dos últimas GCK-VN están almacenadas, se necesita enviar cuatro versiones de MGCK a la BS.

Como en otros casos, cuando se envía la MGCK a un sitio, necesita cifrarse usando la intra-clave KEK_Z. La GCK se obtiene a partir del registro del grupo de conversación del VLR y se descifra con la intra-clave KEK_Z, y se combina con CCK para crear la MGCK. La MGCK resultante se cifra usando la intra-clave KEK_Z, y se envía a los sitios apropiados.

La transferencia de una MGCK a una BS puede activarse por varios eventos. Ejemplos de activadores incluyen una estación móvil asociada con la GCK para la MGCK que reside en la BS cuando se genera bien la GCK o la CCK; una estación móvil llegando en la BS cuando no se ha producido ninguna afiliación anterior de un grupo de conversación en la BS; y una estación móvil que cambia la afiliación del grupo de conversación, mientras que reside en la BS, para un grupo de conversación no asociado anteriormente con la BS.

En la FIG. 16 se muestra un diagrama que muestra una distribución de una clave de cifrado de grupo para una estación móvil dentro de un sistema de comunicaciones. Cuando el KMF 101 determina que se debe actualizar la GCK para una MS 401, el KMF 101 genera un nuevo material de la clave GCK para la MS 401 de acuerdo con la FIG. 8 titulada "Distribución de una clave de cifrado de grupo a un individuo" y su texto asociado en la Normativa TETRA. El proceso de generación de GCK obtiene el material de la clave SGCK (una GCK sellada), el GCKN (el Número de la GCK), el GCK-VN (Número de Versión de la GCK), y RSO (la semilla aleatoria usada en el proceso). Para determinar el ATR para la zona local de la MS 401, en la realización preferida, el KMF 101 utiliza la ITSI para el mapa de ZC local desde el UCS 103 y una tabla de búsqueda basada en la zona para obtener la dirección del ATR para la zona local. En el ejemplo de la FIG. 16, la zona local para la MS1 401 es la zona 2. El KMF 101 redirige SGCK, GCKN, GCK-VN, y RSO al ATR 127 de la zona local (2) para la MS 401. Si la MS 401 no está en el sistema, el ATR 127 envía una confirmación negativa NACK de vuelta al KMF 101. Si la MS 401 está en el sistema, la GCK se suministra a la MS 401 a través de la zona en la cual está localizada actualmente la MS 401. En la realización preferida, el material de la clave GCK (por ejemplo, SGCK, GCKN, GCK-VN, y RSO) no están cifradas para la transferencia entre los dispositivos del sistema. El material de la clave GCK puede cifrarse opcionalmente para la transferencia entre los dispositivos del sistema.

Cuando la MS 401 no está localizada en su zona local, el controlador de zona local 121 de la zona 2 determina en qué zona está localizada actualmente la MS 401 (zona 1 en la FIG. 16) buscándola en el HLR 123 de la zona 2. El

ZC2 121 redirige SGCK, GCKN, GCK-VN, y RSO al controlador de zona 107 de la zona donde está actualmente localizada la MS 401. El ZC1 107 redirige SGCK, GCKN, GCK-VN, y RSO a la BS 115 donde está localizada la MS 401. La BS 115 redirige SGCK, GCKN, GCK-VN, y RSO a la MS 401. Se envía una confirmación ACK no cifrada desde la MS 401 a la BS 115, al ZC 107 y al KMF 101 a través del ATR 113 en la zona donde reside la BS 115. La confirmación ACK representa que la GCK se recibió y se deselló correctamente en la MS (el proceso de desellado se describe en la Normativa TETRA).

Cuando la MS 401 está localizada en su zona local (no mostrada, pero asumiendo que es la BS3 129 en beneficio de este ejemplo), el controlador de la zona local 121 redirige SGCK, GCKN, GCK-VN, y RSO a la BS 129 donde está localizada la MS 401 (no mostrada pero se asume para este ejemplo). La BS 129 redirige SGCK, GCKN, GCK-VN, y RSO a la MS 401. Se envía una confirmación ACK no cifrada desde la MS 401 a la BS 120, al ZC 121 y al KMF 101 a través de la ATR 127 en la zona donde reside la BS 115. La confirmación ACK representa que la GCK se recibió y se deselló correctamente en la MS (el proceso de desellado se describe en la Normativa TETRA).

La FIG. 17 es un diagrama de flujo que muestra un método de persistencia de claves en un sitio en un sistema de comunicaciones de acuerdo con la invención. La persistencia de claves se refiere al tiempo que una clave se mantiene almacenada una clave en cualquier dispositivo del sistema o una MS. Si se borra una clave de tráfico de la interfaz aire desde un sitio cuando la MS deja el sitio, y la clave se elimina demasiado rápidamente, la MS puede volver al sitio requiriendo de nuevo el establecimiento de la clave. Si la MS está viajando entre los límites de zonas o las fronteras de sitios durante un periodo de tiempo, el material de la clave para la MS puede necesitar establecerse constantemente si se borra el material de la clave de un sitio demasiado rápidamente después de que la MS deje el sitio. Si el material de clave se deja en un sitio durante demasiado tiempo, pueden establecerse claves duplicadas, creando ambigüedad y la probabilidad de fallos de autenticación, particularmente para la autenticación implícita. De ese modo, se necesita fijar adecuadamente la persistencia de la clave para cada una de las claves para impedir tales problemas. En la realización preferida, el tiempo de persistencia se basa en la tasa de autenticación promedio esperada en el sistema de comunicaciones y preferiblemente el tiempo de persistencia es menor que la tasa de autenticación promedio esperada en el sistema de comunicaciones. La tasa de autenticación promedio esperada se basa en el número promedio de veces que una estación móvil se autentica en un periodo de tiempo.

En la etapa 1701, cuando llega una MS a un sitio, se almacenan la clave y/o el material de clave asociado con la MS 401 en el sitio. Si en la etapa 1703 se determina que el móvil ha dejado el sitio, el temporizador de persistencia se fija en la etapa 1705, a menos que ya se haya fijado o inicializado, en cuyo caso el proceso simplemente continúa en la etapa 1709. Cuando el temporizador expira en la etapa 1707, el proceso continúa con la etapa 1709 donde la clave y/o el material de clave asociado con el móvil 401 se borran del sitio, y el proceso termina. Si el móvil 401 no ha dejado el sitio en la etapa 1703, y es el momento de reemplazar la clave del móvil o el material de claves en la etapa 1711, las claves o material de claves se reemplazan en la etapa 1713 y el proceso continúa con la etapa 1703. La etapa 1709 también puede alcanzarse si un dispositivo de sistema, tal como un controlador de zona, se dirige al sitio para borrar ciertas claves y/o material de claves por alguna razón. El controlador de zona típicamente determina cuándo el móvil deja un sitio en base a las actualizaciones de HLR y VLR.

La presente invención puede realizarse de otras formas específicas sin apartarse de sus características esenciales. Las realizaciones descritas deben considerarse en todos los aspectos como ilustrativas y no restrictivas. El alcance de la invención está indicado, por lo tanto, por las reivindicaciones adjuntas en lugar de por la descripción anterior. Todos los cambios que caen dentro del significado y rango de equivalencia de las reivindicaciones quedan abarcados dentro de su alcance.

REIVINDICACIONES

1. Un método que comprende las etapas de:

recibir desde una estación móvil (401, 403, 405), una petición para comunicar en un sistema de comunicaciones; determinando si la petición está cifrada;
cuando la petición no está cifrada, enviar una petición de autenticación a la estación móvil (401, 403, 405) con un dispositivo de la infraestructura del sistema (107, 121) en el sistema de comunicaciones;
cuando la petición está cifrada, determinar si la estación móvil (401, 403, 405) se está encendiendo;
cuando la estación móvil (401, 403, 405) se está encendiendo y la petición está cifrada, enviar una petición de autenticación de la estación móvil (401, 403, 405) al dispositivo de la infraestructura del sistema (107, 121) en el sistema de comunicaciones;
cuando la estación móvil no se está encendiendo y la petición está cifrada, determinar si la petición está cifrada usando una clave válida;
cuando la estación móvil (401, 403, 405) no se está encendiendo y la petición está cifrada usando una clave válida, permitir que la estación móvil (401, 403, 405) acceda al sistema sin petición de autenticación.

2. El método de la Reivindicación 1, que comprende además las etapas de:

almacenar las peticiones de autenticación durante un periodo de tiempo cuando el dispositivo de la infraestructura del sistema (107, 121) no está disponible.
cuando el dispositivo de la infraestructura del sistema (107, 121) se vuelve disponible, redirigir las peticiones de autenticación almacenadas al dispositivo de la infraestructura del sistema (107, 121).

3. El método de la Reivindicación 1, en el que, el envío de la petición de autenticación de la estación móvil (401, 403, 405) con un dispositivo de la infraestructura del sistema (107, 121) comprende enviar la petición de autenticación de la estación móvil con un controlador de zona, en la zona en la que está localizada la estación móvil.

4. El método de la Reivindicación 1, que comprende además recibir una confirmación de que la estación móvil (401, 403, 405) ha pasado la autenticación.

5. El método de la Reivindicación 4, en el que la autenticación se realizó por un primer dispositivo de la infraestructura del sistema (407, 121) usando la información de autenticación de sesión que se recibió desde un segundo dispositivo de la infraestructura del sistema (107, 121),

6. El método de la Reivindicación 5, en el que al menos un segmento de la información de autenticación de sesión recibida está cifrado.

7. El método de la Reivindicación 6, en el que el, al menos un segmento de la información de autenticación de sesión recibida está cifrado usando una intra-clave que se usa sólo por los dispositivos de la infraestructura del sistema distintos que una estación móvil dentro de una zona para cifrar al menos la información de autenticación de sesión que está distribuida dentro de la zona.

8. El método de la Reivindicación 7, en el que el primer dispositivo de la infraestructura del sistema es un registro de localización de visitantes localizado en una zona, y el segundo dispositivo de la infraestructura del sistema es un registro de localización local situado en la misma zona.

9. El método de la Reivindicación 6, en el que el, al menos un segmento de la información de autenticación de sesión recibida está cifrado usando una inter-clave que está compartida por una pluralidad de zonas y que se usa por un dispositivo de la infraestructura del sistema distinto de una estación móvil en una zona en la pluralidad de zonas para cifrar al menos la información de autenticación de sesión para el transporte a otro dispositivo de la infraestructura del sistema distinto de una estación móvil en otra zona en la pluralidad de zonas.

10. El método de la Reivindicación 9, en el que, el primer dispositivo de la infraestructura del sistema es un registro de localización de visitantes localizado en una zona, y el segundo dispositivo de la infraestructura de la infraestructura del sistema es un registro de localización local en una zona diferente.

11. El método de la Reivindicación 1, en el que el método está realizado en una cualquiera de las estaciones base y un sitio base.

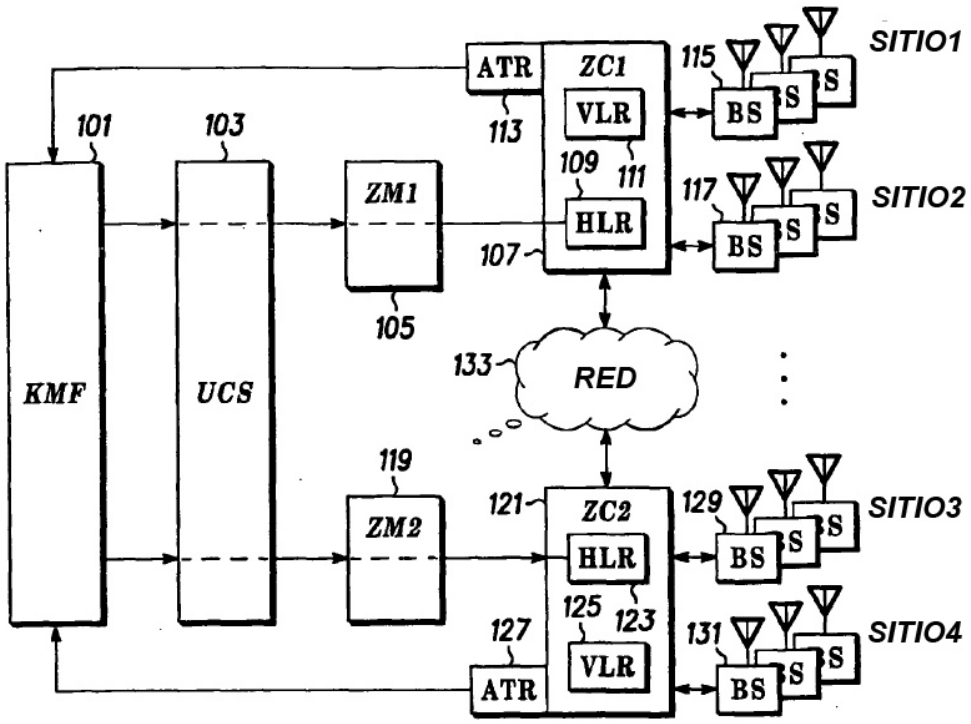
ATR
ZC1
VLR
HLR
113
109
111
115
117
SITIO1
SITIO2
101
103
ZM1
105
107
KMF
UCS
133
RED
119
ZM2
121
ZC2
HLR
125
123
127
VLR
ATR
129
131
SITIO3
SITIO4
BS

FIG. 1

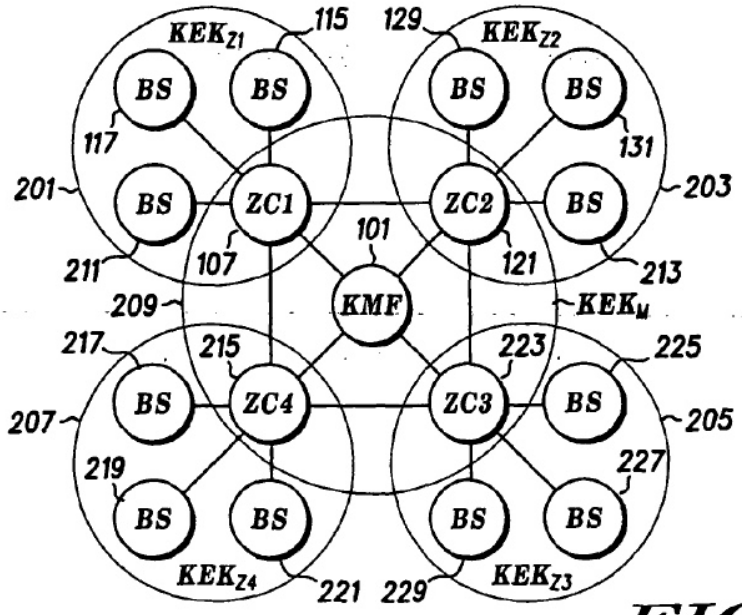
KEKZ1
KEKZ2
KEKZ4
KEKZ3
KEKM
115
129
117
131
201
203
ZC1
ZC2
107
101
121
211
213
209
KMF
217
215
223
225
ZC4
ZC3
207
205
219
227
221
229
BS

FIG. 2

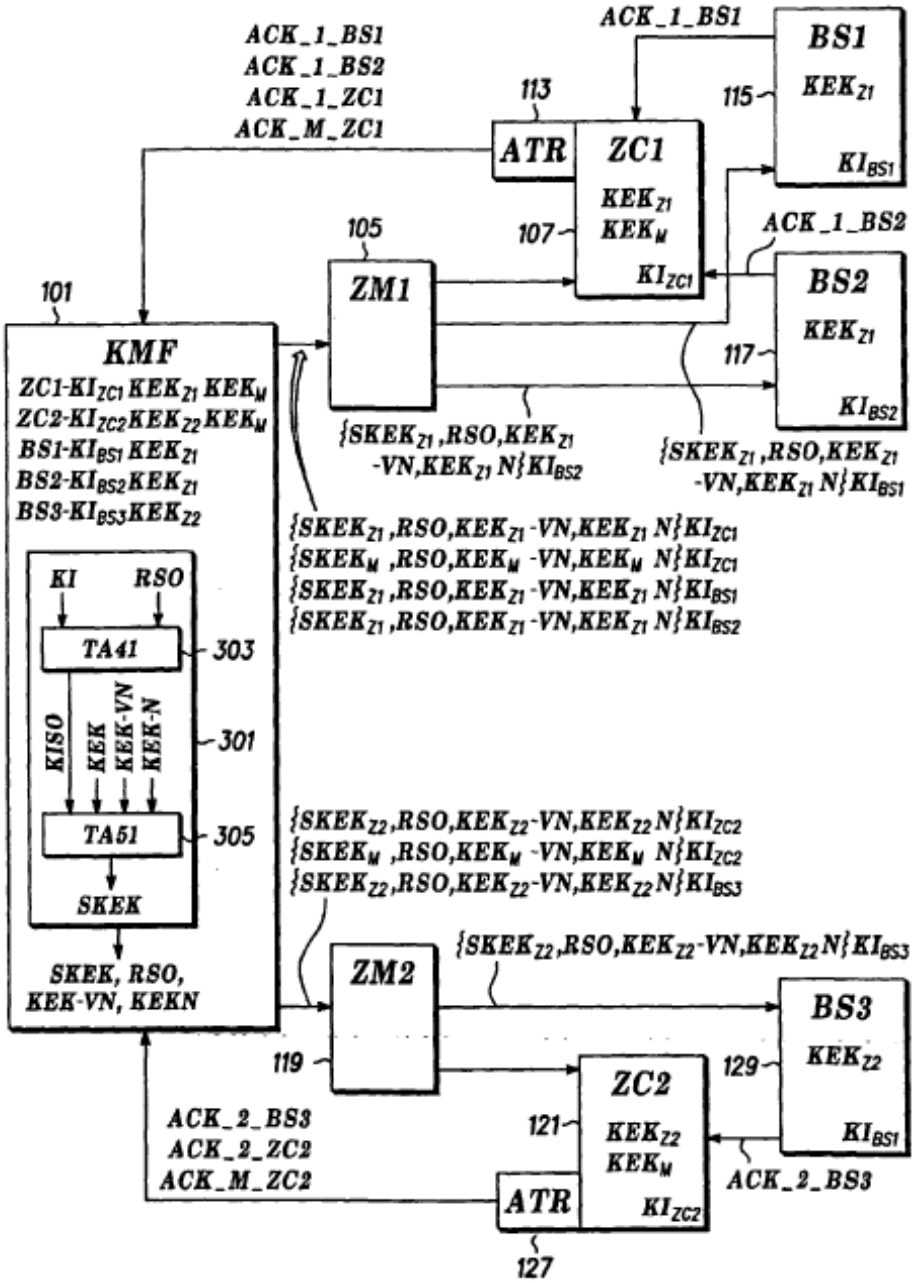
ACK_1_BS1
ACK_1_BS2
ACK_1_ZC1
ACK_M_ZC1
ACK_1_BS1
BS1
KEKZ1
KIBS1
115
113
ATR
ZC1
KEKZ1
KEKM
KIZC1
107
105
ZM1
ACK_1_BS2
BS2
KEKZ1
KIBS2
117
101
KMF
ZC1-KIZC1 KEKZ1 KEKM
ZC2-KIZC2 KEKZ2 KEKM
BS1-KIBS1 KEKZ1
BS2-KIBS2 KEKZ1
BS3-KIBS3 KEKZ2
{SKEKZ1,RSO,KEKZ1 -VN,KEKZ1 N}KIBS2
{SKEKZ1,RSO,KEKZ1 -VN,KEKZ1 N}KIBS1
{SKEKZ1,RSO,KEKZ1 -VN,KEKZ1 N}KIZC1
{SKEKM,RSO,KEKM -VN,KEKM N}KIZC1
{SKEKZ1,RSO,KEKZ1 -VN,KEKZ1 N}KIBS1
{SKEKZ1,RSO,KEKZ1 -VN,KEKZ1 N}KIBS2
KI
RSO
TA41
303
KISO
KEK
KEK-VN
KEK-N
301
TA51
305
SKEK
SKEK, RSO,
KEK-VN, KEKN
{SKEKZ2,RSO,KEKZ2 -VN,KEKZ2 N}KIZC2
{SKEKM,RSO,KEKM -VN,KEKM N}KIZC2
{SKEKZ2,RSO,KEKZ2 -VN,KEKZ2 N}KIBS3
{SKEKZ2,RSO,KEKZ2 -VN,KEKZ2 N}KIBS3
ZM2
BS3
KEKZ2
KIBS1
129
119
ZC2
KEKZ2
KEKM
KIZC2
121
ACK_2_BS3
ACK_2_ZC2
ACK_M_ZC2
ATR
127
ACK_2_BS3

FIG. 3

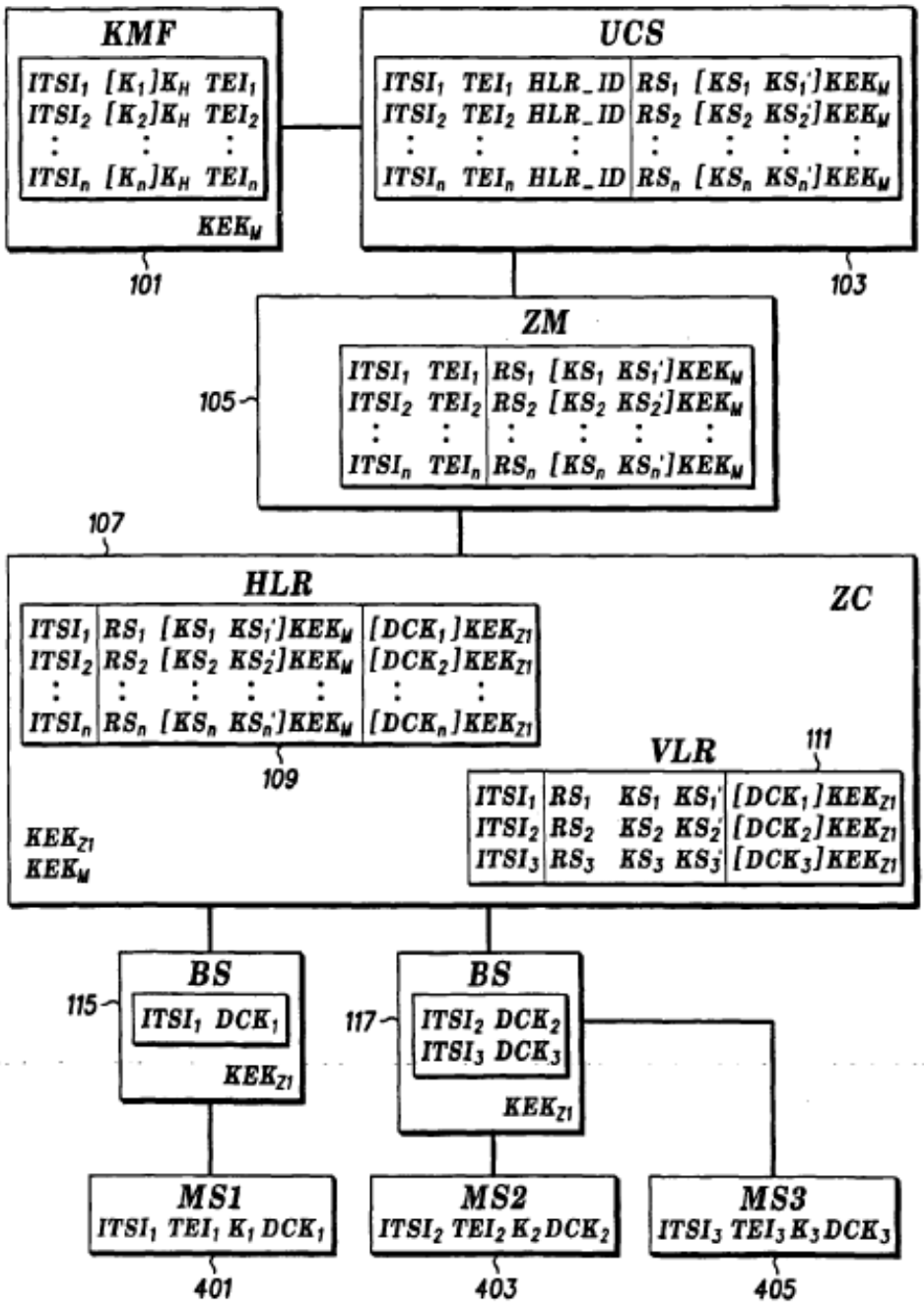
KMF
ITSI1 [K1]KH TEI1
ITSI2 [K2]KH TEI2
ITSIn [Kn]KH TEIn
KEKM
101
UCS
ITSI1 TEI1 HLR_ID RS1 [KS1 KS1']KEKM
ITSI2 TEI2 HLR_ID RS2 [KS2 KS2']KEKM
ITSIn TEIn HLR_ID RSn [KSn KSn']KEKM
103
ZM
105
ITSI1 TEI1 RS1 [KS1 KS1']KEKM
ITSI2 TEI2 RS2 [KS2 KS2']KEKM
ITSIn TEIn RSn [KSn KSn']KEKM
107
HLR
ITSI1 RS1 [KS1 KS1']KEKM [DCK1]KEKZ1
ITSI2 RS2 [KS2 KS2']KEKM [DCK2]KEKZ1
ITSIn RSn [KSn KSn']KEKM [DCKn]KEKZ1
109
ZC
VLR
111
ITSI1 RS1 KS1 KS1' [DCK1]KEKZ1
ITSI2 RS2 KS2 KS2' [DCK2]KEKZ1
ITSI3 RS3 KS3 KS3' [DCK3]KEKZ1
KEKZ1
KEKM
BS
115
ITSI1 DCK1
KEKZ1
BS
117
ITSI2 DCK2
ITSI3 DCK3
KEKZ1
MS1
ITSI1 TEI1 K1 DCK1
401
MS2
ITSI2 TEI2 K2 DCK2
403
MS3
ITSI3 TEI3 K3 DCK3
405

FIG. 4

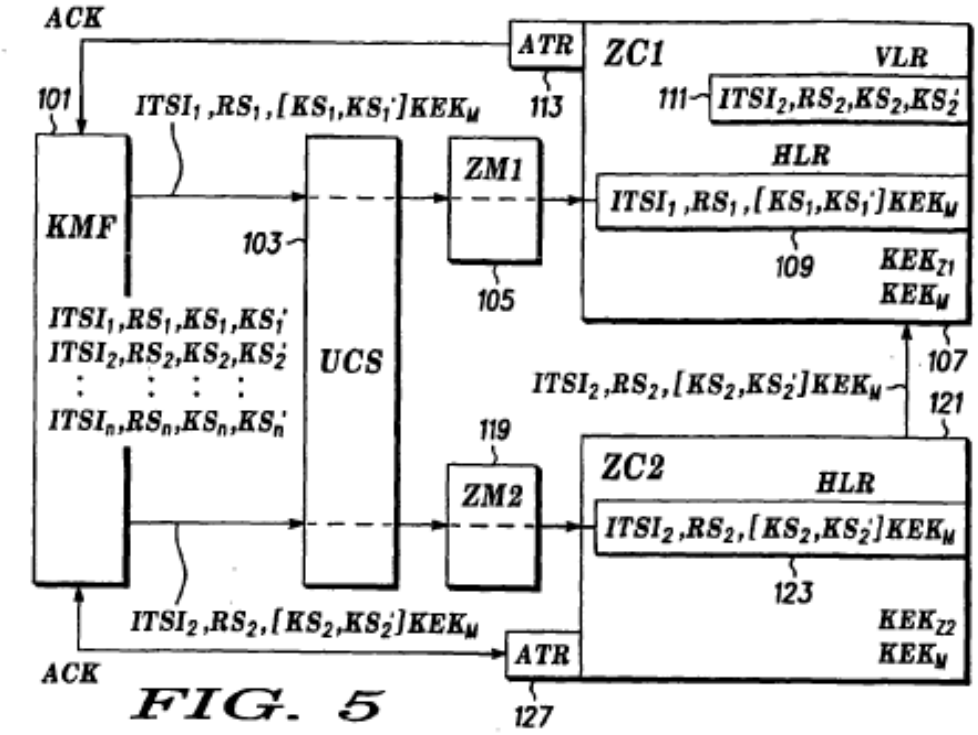
ACK
ATR
ZC1
VLR
101
ITSI1,RS1,[KS1,KS1']KEKM
113
111
ITSI2,RS2,KS2,KS2'
HLR
KMF
103
ZM1
ITSI1,RS1,[KS1,KS1']KEKM
105
109
KEKZ1
KEKM
ITSI1,RS1,KS1,KS1'
ITSI2,RS2,KS2,KS2'
UCS
ITSI2,RS2,[KS2,KS2']KEKM
107
121
119
ZM2
ZC2
HLR
ITSI2,RS2,[KS2,KS2']KEKM
123
KEKZ2
KEKM
ITSI2,RS2,[KS2,KS2']KEKM
ATR
ACK
127

FIG. 5

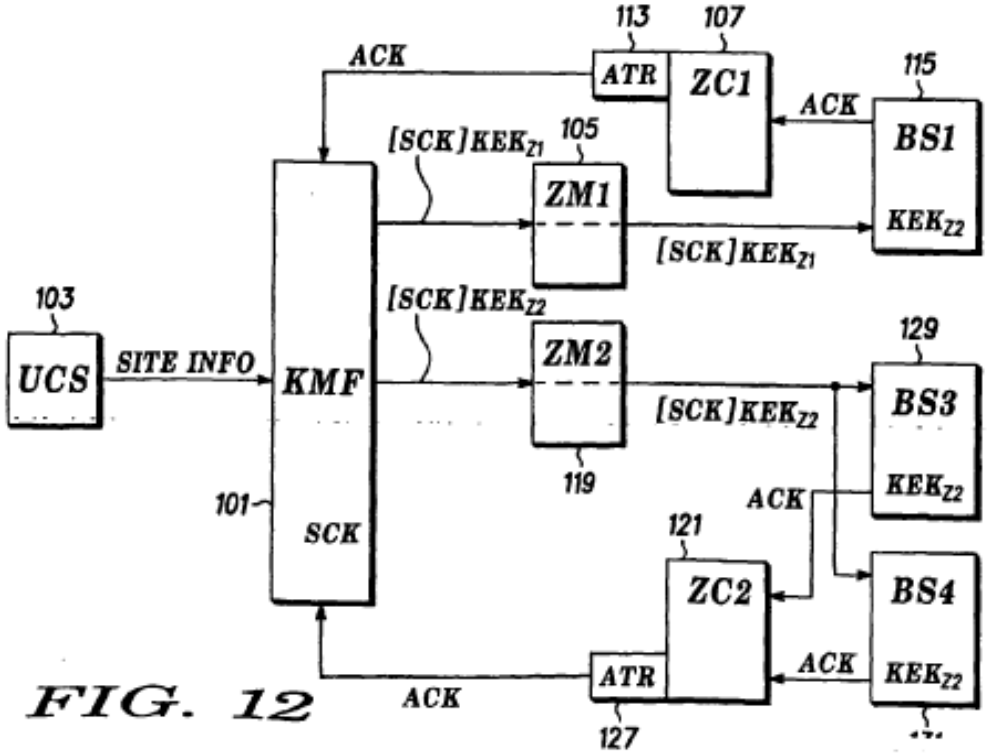
113
107
ACK
ATR
ZC1
115
ACK
BS1
[SCK]KEKZ1
105
ZM1
KEKZ2
[SCK]KEKZ1
103
[SCK]KEKZ2
129
UCS
SITE INFO
KMF
ZM2
BS3
[SCK]KEKZ2
119
ACK
101
SCK
121
ZC2
BS4
ACK
ATR
KEKZ2
ACK
127

FIG. 12

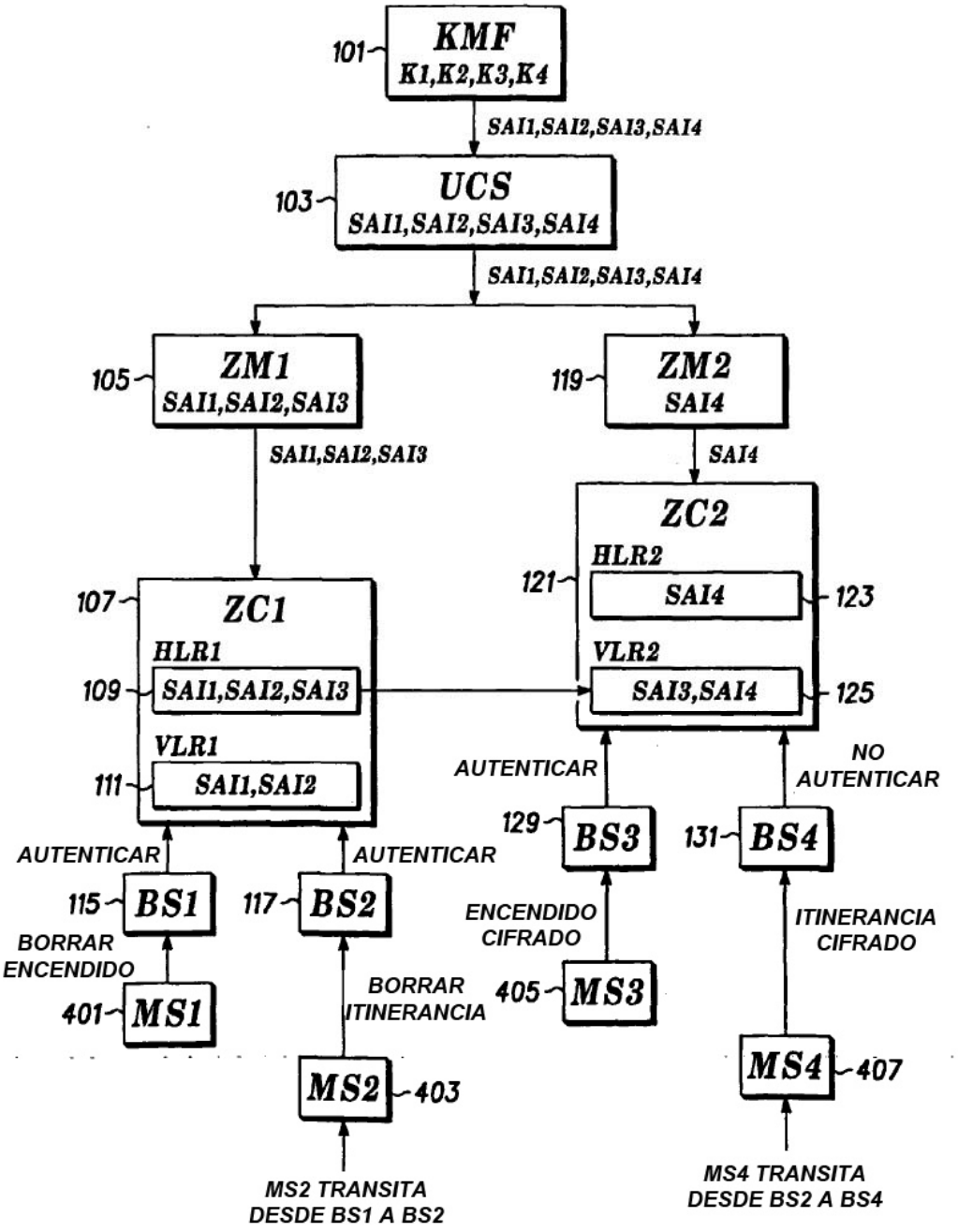
101
KMF
K1,K2,K3,K4
SAI1,SAI2,SAI3,SAI4
103
UCS
SAI1,SAI2,SAI3,SAI4
SAI1,SAI2,SAI3,SAI4
105
ZM1
SAI1,SAI2,SAI3
119
ZM2
SAI4
SAI1,SAI2,SAI3
SAI4
ZC2
HLR2
121
SAI4
123
VLR2
SAI3,SAI4
125
107
ZC1
HLR1
109
SAI1,SAI2,SAI3
VLR1
111
SAI1,SAI2
AUTENTICAR
NO AUTENTICAR
129
BS3
131
BS4
AUTENTICAR
AUTENTICAR
115
BS1
117
BS2
ENCENDIDO CIFRADO
ITINERANCIA CIFRADO
BORRAR ENCENDIDO
BORRAR ITINERANCIA
405
MS3
401
MS1
MS2
403
MS4
407
MS2 TRANSITA DESDE BS1 A BS2
MS4 TRANSITA DESDE BS2 A BS4

FIG. 6

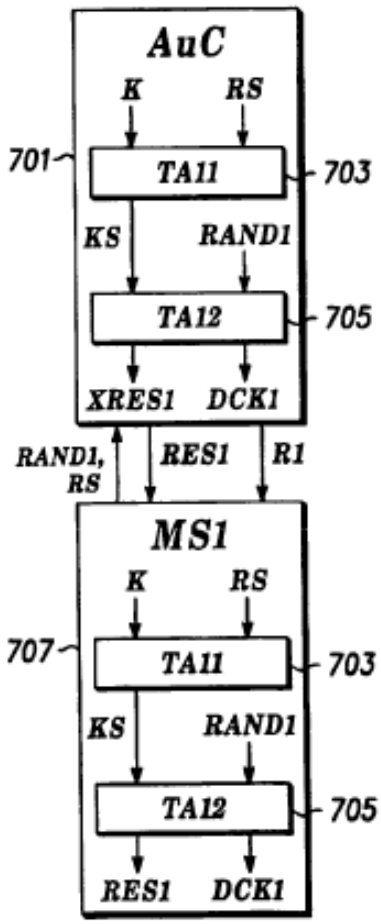
AuC
K
RS
701
TA11
703
KS
RAND1
TA12
705
XRES1
DCK1
RAND1,
RS
RES1
R1
MS1
K
RS
707
TA11
703
KS
RAND1
TA12
705
RES1
DCK1

FIG. 7

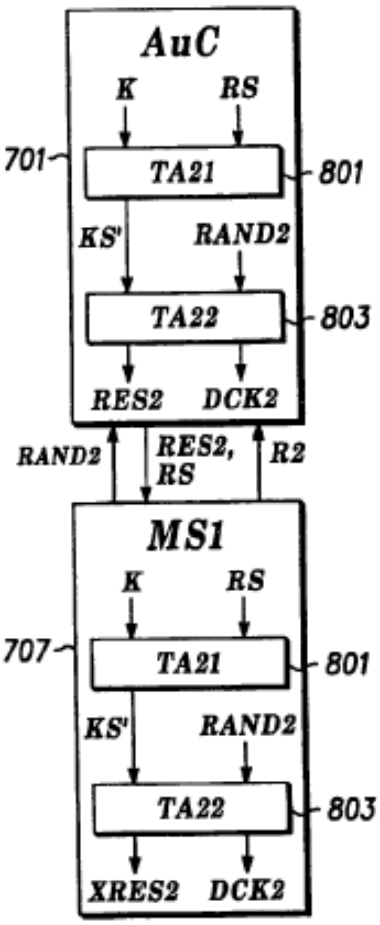
AuC
K
RS
701
TA21
801
KS'
RAND2
TA22
803
RES2
DCK2
RAND2
RES2,
RS
R2
MS1
K
RS
707
TA21
801
KS'
RAND2
TA22
803
XRES2
DCK2

FIG. 8

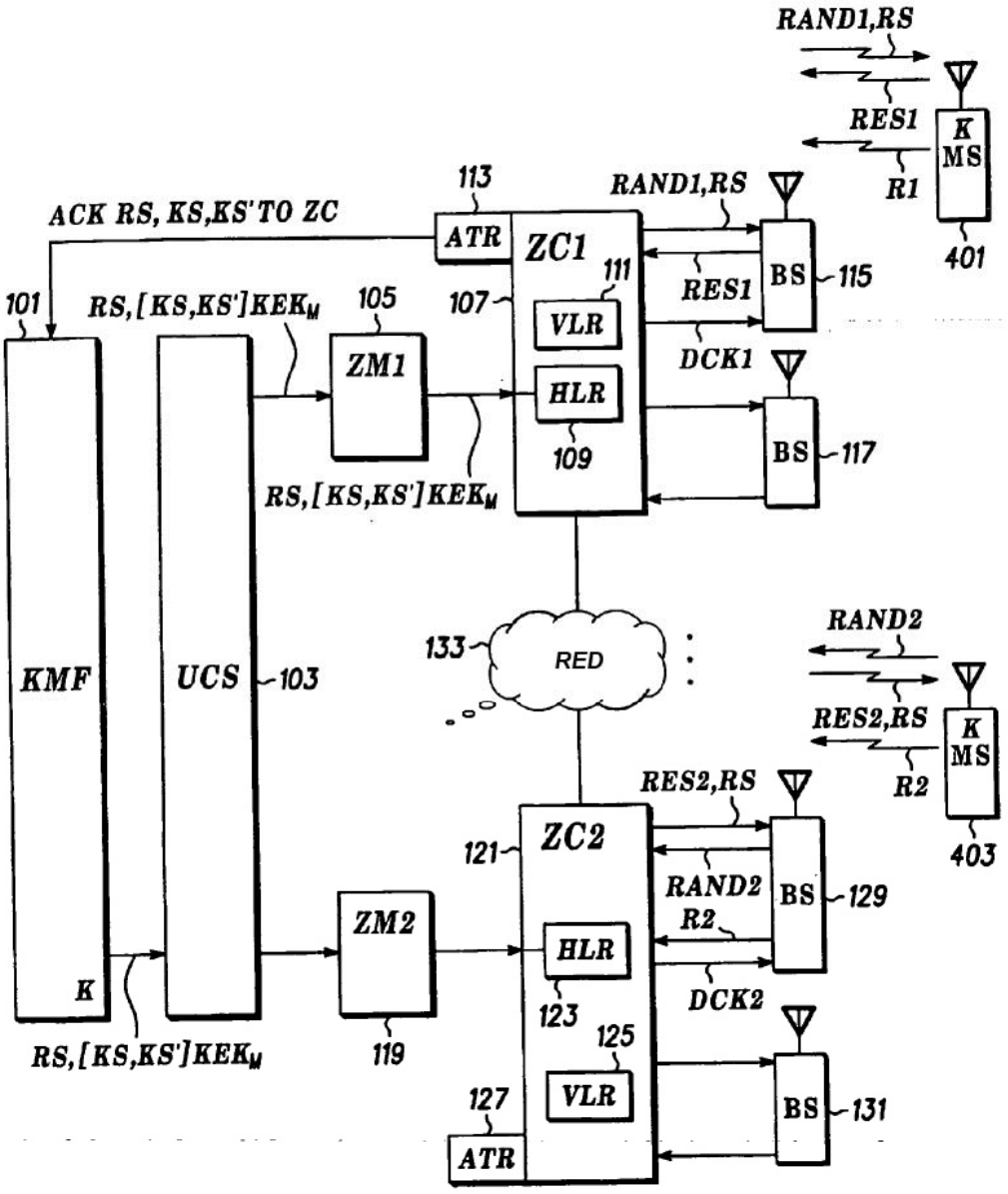
RAND1,RS
RES1
R1
K
MS
401
113
ATR
ZC1
111
VLR
HLR
109
107
RAND1,RS
RES1
BS
115
DCK1
BS
117
ACK RS, KS,KS'TO ZC
101
RS,[KS,KS']KEK$_M$
105
ZM1
RS,[KS,KS']KEK$_M$
KMF
UCS
103
133
RED
RAND2
RES2,RS
R2
K
MS
403
RES2,RS
121
ZC2
RAND2
R2
BS
129
DCK2
ZM2
HLR
123
125
VLR
127
ATR
BS
131
K
RS,[KS,KS']KEK$_M$
119

FIG. 9

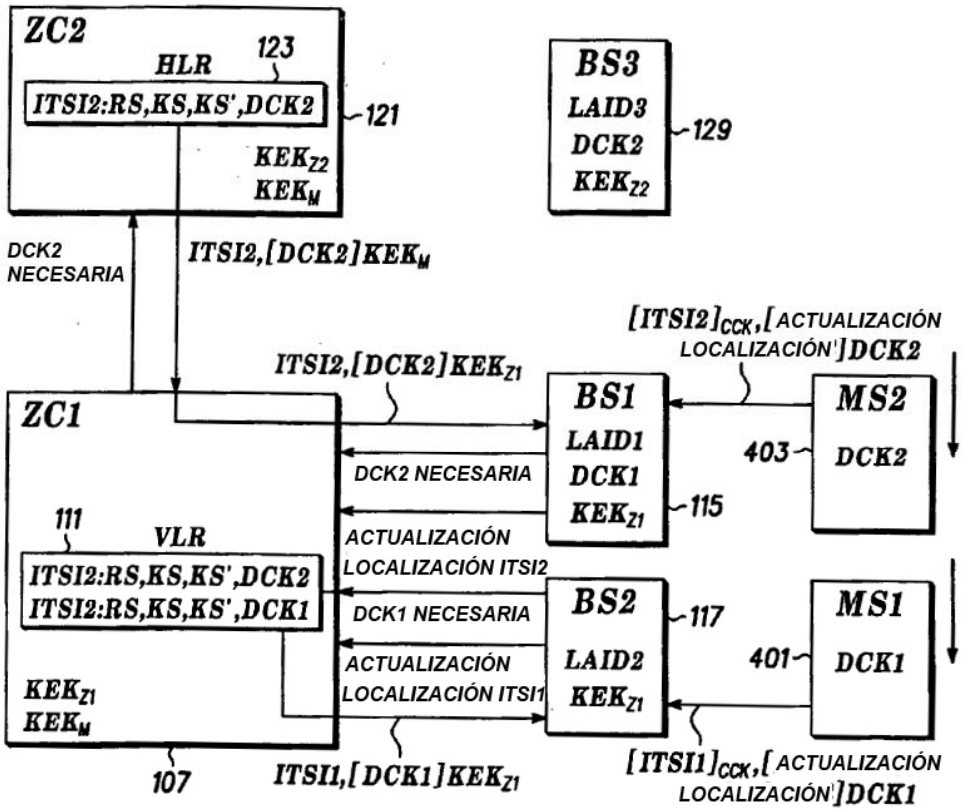
ZC2
HLR
123
ITSI2:RS,KS,KS',DCK2
121
KEK$_{Z2}$
KEK$_M$
BS3
LAID3
DCK2
KEK$_{Z2}$
129
DCK2 NECESARIA
ITSI2,[DCK2]KEK$_M$
[ITSI2]$_{CCK}$,[ACTUALIZACIÓN LOCALIZACIÓN']DCK2
ITSI2,[DCK2]KEK$_{Z1}$
ZC1
BS1
LAID1
DCK1
KEK$_{Z1}$
115
MS2
403
DCK2
DCK2 NECESARIA
111
VLR
ITSI2:RS,KS,KS',DCK2
ITSI2:RS,KS,KS',DCK1
ACTUALIZACIÓN LOCALIZACIÓN ITSI2
DCK1 NECESARIA
BS2
117
LAID2
KEK$_{Z1}$
MS1
401
DCK1
ACTUALIZACIÓN LOCALIZACIÓN ITSI1
KEK$_{Z1}$
KEK$_M$
107
ITSI1,[DCK1]KEK$_{Z1}$
[ITSI1]$_{CCK}$,[ACTUALIZACIÓN LOCALIZACIÓN']DCK1

FIG. 10

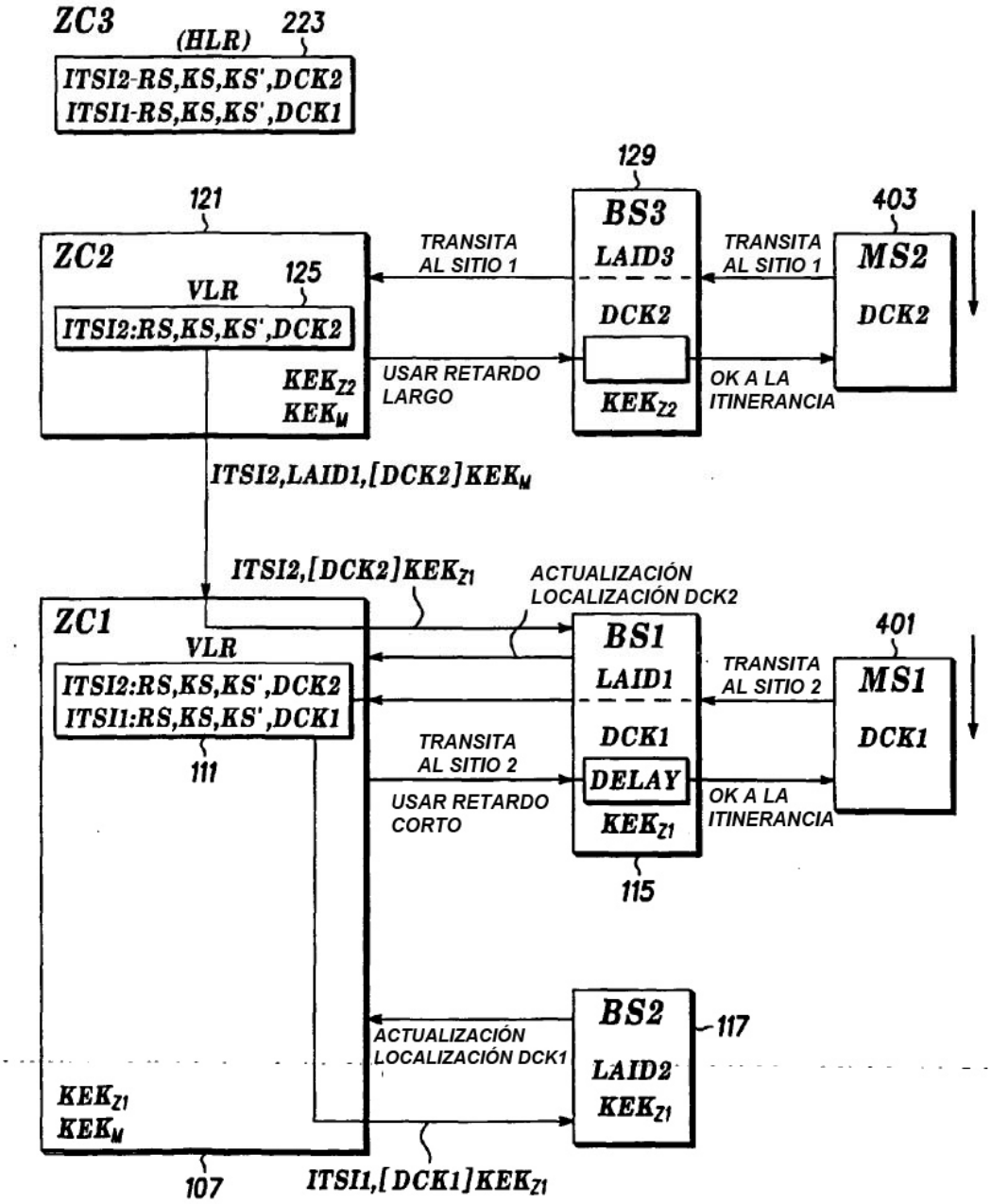
ZC3
(HLR)
223
ITSI2-RS,KS,KS',DCK2
ITSI1-RS,KS,KS',DCK1
129
121
BS3
LAID3
DCK2
KEKZ2
403
ZC2
VLR
125
ITSI2:RS,KS,KS',DCK2
KEKZ2
KEKM
TRANSITA AL SITIO 1
TRANSITA AL SITIO 1
MS2
DCK2
USAR RETARDO LARGO
OK A LA ITINERANCIA
ITSI2,LAID1,[DCK2]KEKM
ITSI2,[DCK2]KEKZ1
ACTUALIZACIÓN LOCALIZACIÓN DCK2
401
ZC1
VLR
ITSI2:RS,KS,KS',DCK2
ITSI1:RS,KS,KS',DCK1
111
BS1
LAID1
DCK1
DELAY
KEKZ1
115
TRANSITA AL SITIO 2
TRANSITA AL SITIO 2
MS1
DCK1
USAR RETARDO CORTO
OK A LA ITINERANCIA
BS2
117
LAID2
KEKZ1
ACTUALIZACIÓN LOCALIZACIÓN DCK1
KEKZ1
KEKM
107
ITSI1,[DCK1]KEKZ1

FIG. 11

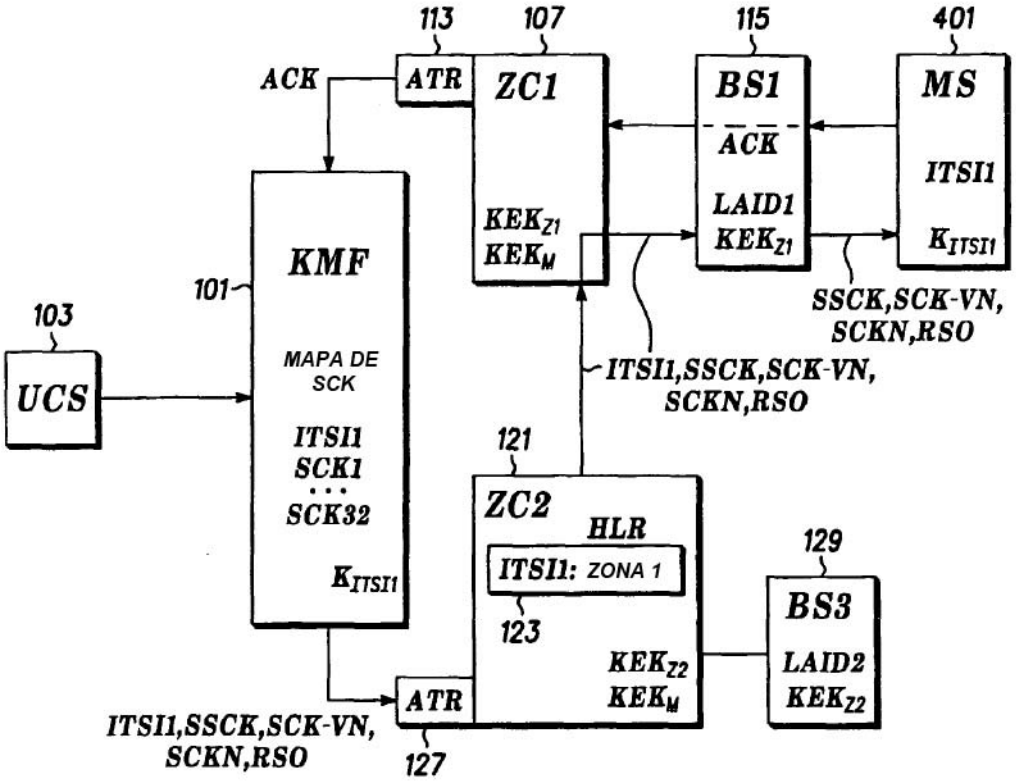
113
107
115
401
ACK
ATR
ZC1
BS1
MS
ACK
ITSI1
LAID1
KEKZ1
KEKM
KEKZ1
KITSI1
SSCK,SCK-VN,
SCKN,RSO
101
KMF
103
UCS
MAPA DE
SCK
ITSI1
SCK1
SCK32
KITSI1
ITSI1,SSCK,SCK-VN,
SCKN,RSO
121
ZC2
HLR
ITSI1: ZONA 1
123
129
BS3
LAID2
KEKZ2
KEKZ2
KEKM
ATR
ITSI1,SSCK,SCK-VN,
SCKN,RSO
127

FIG. 13

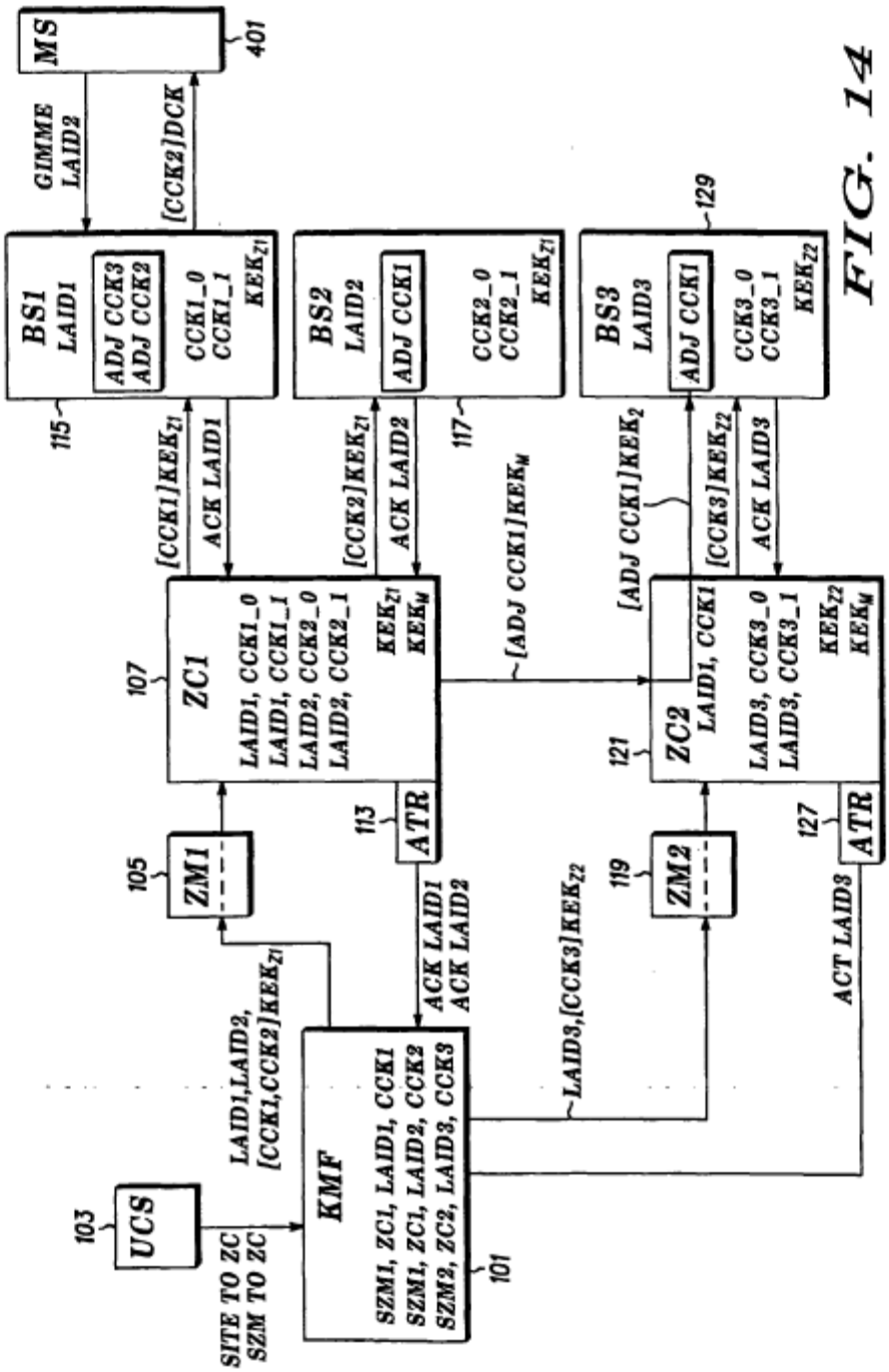
MS
401
GIMME
LAID2
[CCK2]DCK
BS1
LAID1
ADJ CCK3
ADJ CCK2
CCK1_0
CCK1_1
KEK_Z1
115
BS2
LAID2
ADJ CCK1
CCK2_0
CCK2_1
KEK_Z1
117
BS3
LAID3
ADJ CCK1
CCK3_0
CCK3_1
KEK_Z2
129
[CCK1]KEK_Z1
ACK LAID1
[CCK2]KEK_Z1
ACK LAID2
[ADJ CCK1]KEK_W
[ADJ CCK1]KEK_Z
[CCK3]KEK_Z2
ACK LAID3
107
ZC1
LAID1, CCK1_0
LAID1, CCK1_1
LAID2, CCK2_0
LAID2, CCK2_1
KEK_Z1
KEK_W
121
ZC2
LAID1, CCK1
LAID3, CCK3_0
LAID3, CCK3_1
KEK_Z2
KEK_W
105
ZM1
113
ATR
119
ZM2
127
ATR
LAID1,LAID2,
[CCK1,CCK2]KEK_Z1
ACK LAID1
ACK LAID2
LAID3,[CCK3]KEK_Z2
ACT LAID3
103
UCS
SITE TO ZC
SZM TO ZC
KMF
SZM1, ZC1, LAID1, CCK1
SZM1, ZC1, LAID2, CCK2
SZM2, ZC2, LAID3, CCK3
101

FIG. 14

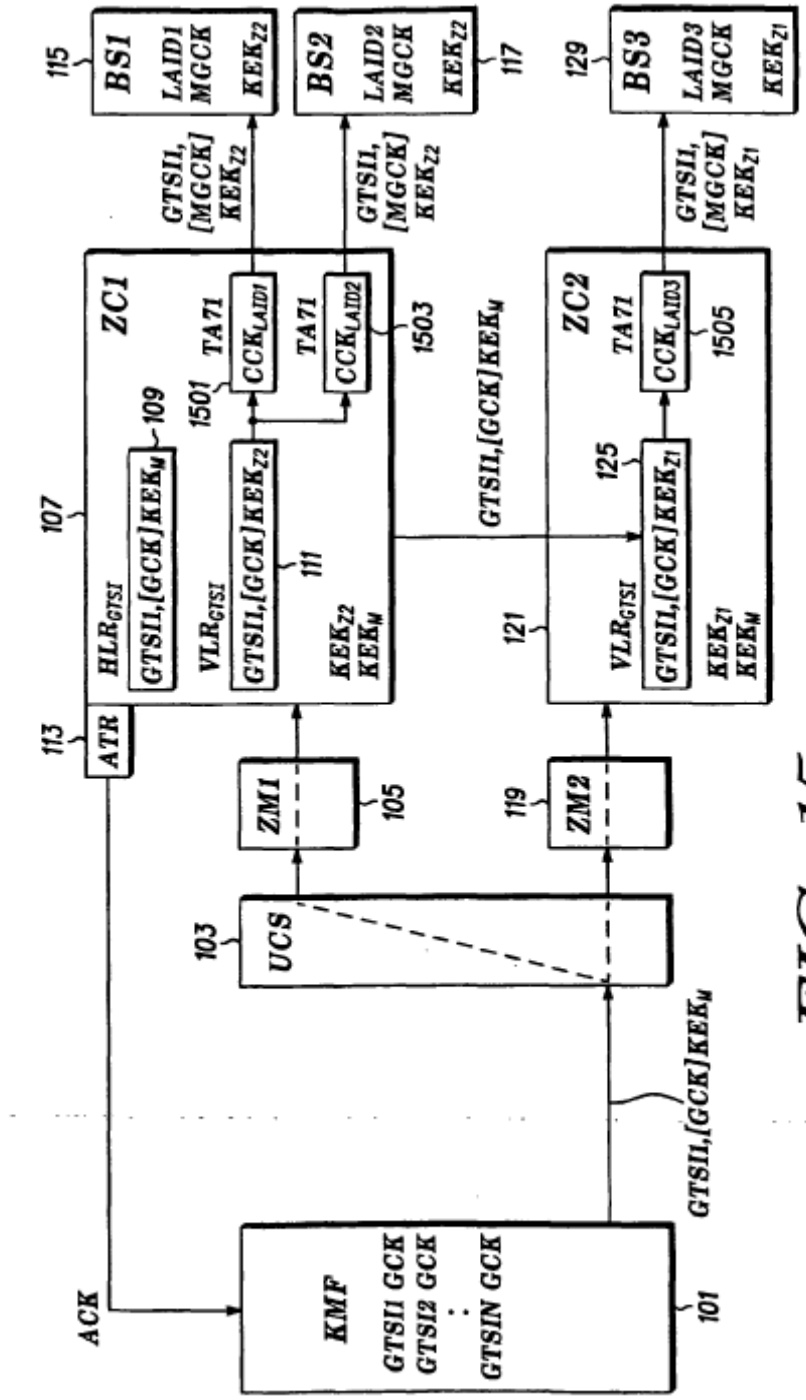
KMF
GTSI1 GCK
GTSI2 GCK
GTSIN GCK
101
ACK
GTSI1,[GCK]KEK_M
UCS
103
ZM1
105
ZM2
119
ATR
113
ZC1
107
HLR_GTSI
GTSI1,[GCK]KEK_M
109
VLR_GTSI
GTSI1,[GCK]KEK_Z2
111
KEK_Z2
KEK_M
TA71
1501
CCK_LAID1
CCK_LAID2
1503
GTSI1,[GCK]KEK_M
ZC2
121
VLR_GTSI
GTSI1,[GCK]KEK_Z1
125
KEK_Z1
KEK_M
TA71
CCK_LAID3
1505
BS1
LAID1
MGCK
KEK_Z2
115
BS2
LAID2
MGCK
KEK_Z2
117
BS3
LAID3
MGCK
KEK_Z1
129
GTSI1,[MGCK]KEK_Z2
GTSI1,[MGCK]KEK_Z2
GTSI1,[MGCK]KEK_Z1

FIG. 15

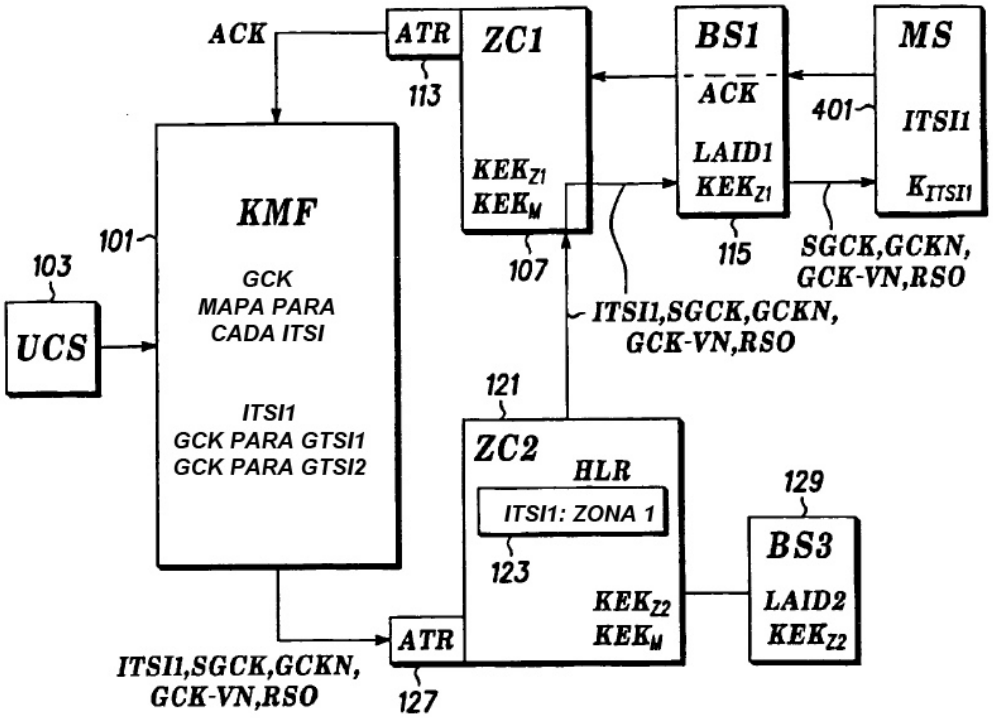
ACK
ATR
ZC1
113
BS1
ACK
LAID1
KEKZ1
401
MS
ITSI1
KITSI1
KMF
GCK
MAPA PARA
CADA ITSI
ITSI1
GCK PARA GTSI1
GCK PARA GTSI2
101
103
UCS
KEKZ1
KEKM
107
115
SGCK,GCKN,
GCK-VN,RSO
ITSI1,SGCK,GCKN,
GCK-VN,RSO
121
ZC2
HLR
ITSI1: ZONA 1
123
129
BS3
LAID2
KEKZ2
KEKZ2
KEKM
ATR
ITSI1,SGCK,GCKN,
GCK-VN,RSO
127

FIG. 16

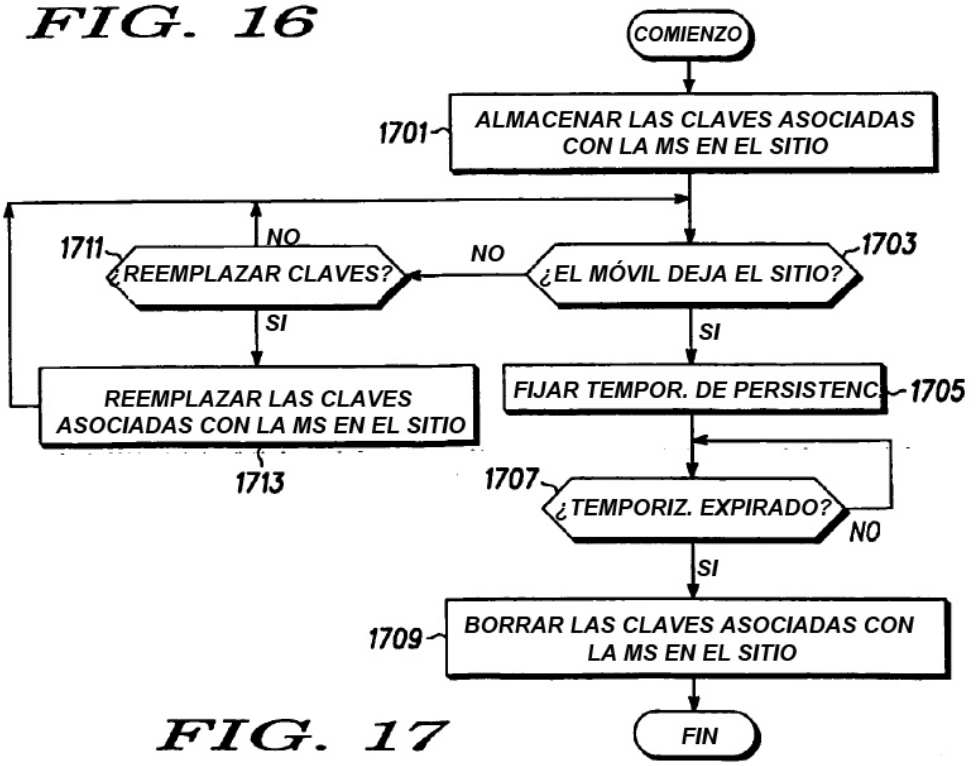
COMIENZO
1701
ALMACENAR LAS CLAVES ASOCIADAS
CON LA MS EN EL SITIO
1711
NO
¿REEMPLAZAR CLAVES?
NO
¿EL MÓVIL DEJA EL SITIO?
1703
SI
SI
REEMPLAZAR LAS CLAVES
ASOCIADAS CON LA MS EN EL SITIO
1713
FIJAR TEMPOR. DE PERSISTENC.
1705
1707
¿TEMPORIZ. EXPIRADO?
NO
SI
1709
BORRAR LAS CLAVES ASOCIADAS CON
LA MS EN EL SITIO
FIN

FIG. 17