(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 368 683**

(51) Int. CI.:
H04W 4/00 (2009.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08735870 .1**
(96) Fecha de presentación: **07.04.2008**
(97) Número de publicación de la solicitud: **2140717**
(97) Fecha de publicación de la solicitud: **06.01.2010**

(54) Título: **MÉTODO Y SISTEMA PARA ACREDITACIÓN DE DISPOSITIVOS MÓVILES.**

(30) Prioridad:
20.04.2007 US 913090 P
30.11.2007 US 948352

(45) Fecha de publicación de la mención BOPI:
21.11.2011

(45) Fecha de la publicación del folleto de la patente:
21.11.2011

(73) Titular/es:
Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm, SE

(72) Inventor/es:
GEHRMANN, Christian

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

DESCRIPCIÓN

Método y sistema para acreditación de dispositivos móviles.

Campo técnico

La presente invención se refiere de manera general al aprovisionamiento de dispositivos móviles, y particularmente se refiere a facilitar sobre la activación en el aire de dispositivos móviles a través del uso de información de identidad de la suscripción preliminar mantenida en un directorio centralizado de dispositivo que es accesible por uno o más operadores de red.

Antecedentes

La fabricación, distribución, y activación eficiente de equipos son habilitadores clave para la explotación de manera efectiva de la gama de oportunidades de negocio proporcionadas por la continua revolución en las comunicaciones inalámbricas. Los planteamientos existentes para el “aprovisionamiento” del equipo de usuario con las credenciales de suscripción necesarias representan un impedimento para operaciones más eficientes.

Por ejemplo, un planteamiento convencional se basa en vender o distribuir de otro modo el equipo de usuario con los Módulos de Identidad de Abonado instalados, SIM. Cada SIM comprende un módulo de circuito resistente al sabotaje, comúnmente integrado en un factor de forma tipo tarjeta pequeña, en la que el módulo del circuito almacena la información de las credenciales para un operador de red específico. En otras palabras, el equipo de usuario está ligado a un operador de red particular en virtud del SIM pre programado, y el abonado llama o contacta de otro modo con el operador de red para proporcionar la información de facturación, etc. En respuesta, el operador de red marca ese SIM como activo en una o más bases de datos de abonado, haciendo por ello operativo el equipo de usuario.

Se han propuesto otros planteamientos para automatizar el proceso de aprovisionamiento, al menos parcialmente. Los ejemplos incluyen la Publicación de la US 2005/0079863 por Macaluso, que revela una forma de aprovisionamiento en el aire (comúnmente designada como aprovisionamiento “OTA” en la literatura relevante); la Publicación de la US 2007/0099599 por Smith, que trata el aprovisionamiento dinámico de los servicios inalámbricos y el aprovisionamiento inicial a través del acceso a una base de datos en internet; la Patente de U.S. Nº 6.980.660 por Hind, que revela los métodos para la inicialización de los dispositivos de comunicación inalámbricos que usan una base de datos de empresa; y la Patente de U.S. Nº 6.490.445 por Holmes, que revela el uso de la información temporal de acceso en el equipo inalámbrico, para permitir una forma de acceso restringido a la red para el aprovisionamiento en el aire. La EP 0 820 206 A revela un método para activar automáticamente una estación móvil en una red de comunicaciones inalámbricas en el aire. Un procesador OTAF en la red recibe un mensaje de registro desencadenado por la estación móvil que solicita la activación. La estación móvil solicita la activación en el aire transmitiendo en la petición de registro un valor ficticio serializado secuencialmente para el número de identificación móvil (un MIN ficticio), que se puede usar para determinar la dirección de encaminamiento de la red del procesador OTAF.

Como una proposición general, no obstante, parece que la complejidad del marco del problema general ha impedido los planteamientos pasados de dotar un sistema y método general que simplifique la fabricación, venta, y, a la larga, el registro de los dispositivos móviles con respecto al aprovisionamiento seguro en el aire.

Resumen

Los métodos y sistemas enseñados aquí dentro permiten a los fabricantes de dispositivos móviles pre configurar los dispositivos móviles para la suscripción con cualquier operador de red que tiene acceso a un servidor centralizado de directorio de dispositivos. En al menos una realización, los dispositivos móviles se aprovisionan con identificadores temporales de dispositivo, que también se contienen en un servidor centralizado de directorio de dispositivos que es accesible a cualquier número de operadores de red. Ventajosamente, a una estación móvil se la puede conceder acceso temporal a través de cualquier red de participación, y ese acceso se usa de esta manera para obtener las credenciales permanentes de la suscripción, a través de la cooperación con un servidor de credenciales asociado con el operador de red que emitirá las credenciales permanentes de la suscripción.

Por consiguiente, un método de facilitar la activación del dispositivo de comunicación móvil en el aire comprende, en un servidor centralizado del directorio de dispositivos, almacenar un registro del dispositivo que comprende la información de las credenciales de suscripción preliminar para un dispositivo móvil, y enviar al menos parte de la información de las credenciales de suscripción preliminar de manera segura a una parte inicial de aprovisionamiento, para usar en dotar inicialmente el dispositivo móvil. La parte inicial de aprovisionamiento puede ser, por ejemplo, un fabricante de dispositivos móviles. El método continúa con la recepción de un identificador del dispositivo para el dispositivo móvil a partir de un servidor de credenciales de un operador de red dado asociado con un usuario final previsto del dispositivo móvil, y vincular de esta manera la información de la dirección de la red del servidor de credenciales con el registro del dispositivo.

El método continúa con la recepción de una petición de validación desde un servidor de autenticación, sensible al

dispositivo móvil que intenta acceder a una red de comunicación inalámbrica usando la información de las credenciales de suscripción preliminar. En respuesta a la petición de valoración, el servidor de directorio envía un vector de autenticación basado en una clave secreta incluida en la información de las credenciales de suscripción preliminar al servidor de autenticación, si la información de las credenciales de suscripción preliminar para el dispositivo móvil es válida. El método también incluye el servidor de directorio que más tarde recibe una petición de la dirección del servidor de credenciales desde el dispositivo móvil, y que envía la información de la dirección de red para el servidor de credenciales al dispositivo móvil, como vinculada en el registro del dispositivo almacenado por el dispositivo móvil.

En otra realización, un sistema para facilitar la activación del dispositivo de comunicación móvil en el aire incluye un servidor centralizado del directorio de dispositivo. El servidor de directorio en esta realización comprende uno o más circuitos de procesamiento configurados para almacenar un registro del dispositivo que comprende la información de las credenciales de suscripción preliminar para un dispositivo móvil, y para enviar al menos parte de la información de las credenciales de suscripción preliminar de manera segura a una parte inicial de aprovisionamiento, para usar en dotar inicialmente el dispositivo móvil. El servidor de directorio se configura además para recibir un identificador de dispositivo para el dispositivo móvil desde un servidor de credenciales de un operador de red dado asociado con un usuario final previsto del dispositivo móvil, y de esta manera enlazar la información de la dirección de la red del servidor de credenciales al registro del dispositivo correspondiente.

Continuando, el servidor de directorio se configura para recibir una petición de validación desde un servidor de autenticación, sensible al dispositivo móvil que intenta acceder a una red de comunicación inalámbrica que usa la información de las credenciales de suscripción preliminar, y enviar un vector de autenticación basado en una clave secreta en la información de las credenciales de suscripción preliminar al servidor de autenticación, si es válida la información de las credenciales de suscripción preliminar para el dispositivo móvil. Aún más, el servidor de directorio se configura para recibir una petición de dirección del servidor de credenciales desde el dispositivo móvil, consecutiva al dispositivo móvil que consigue el acceso temporal a la red de comunicación inalámbrica a través del vector de autenticación, y para enviar de esta manera la información de la dirección de red para el servidor de credenciales al dispositivo móvil, como vinculada en el registro del dispositivo almacenado por el dispositivo móvil.

En una o más de las realizaciones anteriores, la información de las credenciales de suscripción preliminar, también conocida como identidades de suscripción preliminares, comprende parejas de claves secretas e Identidades Internacionales de Abonado Móvil Preliminares, abreviado como PIMSI. De esta manera, el directorio del dispositivo almacena, por ejemplo, un lote de PIMSI y pares de claves secretas, y los fabricantes de dispositivos proporcionan los dispositivos móviles, individuales con la PIMSI y los pares de claves secretas individuales.

Por supuesto, la presente invención no se limita a los rasgos y ventajas anteriores. Verdaderamente, aquellos expertos en la técnica reconocerán rasgos y ventajas adicionales tras la lectura de la siguiente descripción detallada, y tras ver los dibujos anexos.

Breve descripción de los dibujos

La Fig. 1 es un diagrama de bloques de una realización de al menos parte de un sistema para facilitar el aprovisionamiento en el aire de los dispositivos móviles, que incluye un servidor centralizado de directorio de dispositivo que proporciona información de las credenciales de suscripción preliminar a los servidores de aprovisionamiento inicial asociados con, por ejemplo, los fabricantes de los dispositivos.

La Fig. 2 es un diagrama de bloques de una realización de un elemento o estructura de datos de “registro del dispositivo”, que incluye un identificador de dispositivo temporal y una clave secreta.

La Fig. 3 es un diagrama de bloques de una realización de un dispositivo móvil.

La Fig. 4 es un diagrama de flujo lógico de una realización de la lógica de procesamiento que se puede implementar en un servidor centralizado del directorio de dispositivo, para generar y distribuir las identidades de suscripción preliminares para usar en dotar inicialmente los dispositivos móviles.

La Fig. 5 es un diagrama de flujo lógico de una realización de la lógica de procesamiento que se puede implementar en un servidor de aprovisionamiento inicial, para usar en dotar inicialmente los dispositivos móviles en base a la información recibida o asociada de otro modo con la información de las credenciales de suscripción preliminar almacenada en un servidor centralizado del directorio de dispositivo.

La Fig. 6 es un diagrama de bloques de una realización de uno o más servidores de credenciales que se acoplan de manera comunicativa con un servidor centralizado del directorio de dispositivo, y se asocia con uno o más operadores de red.

La Fig. 7 es un diagrama de flujo lógico de la lógica de procesamiento que se puede implementar en un servidor de credenciales, para provocar a un servidor centralizado de directorio del dispositivo asociar la información de las credenciales de suscripción preliminar particular contenida por el servidor centralizado de directorio del dispositivo para los dispositivos móviles particulares al servidor de credenciales.

La Fig. 8 es un diagrama de bloques que ilustra una realización de un sistema general para facilitar el aprovisionamiento en el aire de un dispositivo móvil, que incluye un servidor centralizado de directorio de dispositivo.

Descripción detallada

La Fig. 1 ilustra una realización de un servidor centralizado de directorio de dispositivo 10 ("servidor de directorio 10"), como se contempla aquí dentro para facilitar la activación en el aire de los dispositivos móviles. El término "dispositivo móvil" se debería interpretar ampliamente aquí dentro. Por medio de un ejemplo no limitativo, el término abarca los radioteléfonos celulares y otros tipos de estaciones móviles inalámbricas, y abarca las tarjetas de acceso de red, y otros módulos de comunicación inalámbrica. Igualmente, el término "activación" se debería interpretar ampliamente, y el término al menos se refiere a un método por el cual un abonado obtiene convenientemente y de manera segura las credenciales de suscripción permanentes (largo plazo) desde el operador de red asociado del abonado a través de un proceso de aprovisionamiento en el aire, incluso donde el abonado consigue el acceso temporal de red a través de otro operador de red.

La mejor apreciación de la flexibilidad y conveniencia del sistema y método de activación contemplado aquí dentro comienza con una comprensión más detallada del servidor de directorio 10, de acuerdo con los detalles ejemplo ilustrados en la figura. Incluye o se asocia con un almacén de datos 12, e incluye uno o más circuitos de procesamiento 14. Los circuitos de procesamiento 14 incluyen interfaces de comunicación 16 y los circuitos de procesamiento de suscripción preliminares 18 ("circuitos de procesamiento de suscripción 18"). Los circuitos de procesamiento 14 comprenden los componentes físicos, los componentes lógicos, o cualquier combinación de los mismos. Por ejemplo, los circuitos de procesamiento 14 pueden incluir uno o más circuitos basados en microprocesador, que se configuran para llevar a cabo las funciones descritas aquí dentro por medio de la ejecución de las instrucciones de programa almacenadas. Esas instrucciones se pueden integrar como un producto de programa de ordenador guardado, por ejemplo, en un medio legible por ordenador del almacén de datos 12, o se puede contener en otros dispositivos de memoria/almacenamiento incluidos en o asociados con el servidor de directorio 10.

Otra información almacenada en el servidor de directorio 10 incluye un lote 20 de registros de dispositivo 22. Los registros de dispositivo 22-1 hasta 22-N se ilustran, como un ejemplo. Como se muestra en la Fig. 2, en al menos una realización, cada registro de dispositivo 22 comprende la información de suscripción preliminar para un dispositivo móvil. En una realización, cada registro de dispositivo 22 incluye un identificador de dispositivo temporal 24 y una clave secreta 26. También, como se explicará más tarde, cada registro de dispositivo 22 se vincula con (por ejemplo, incluye o apunta a) la información de dirección de la red del servidor de credenciales 28. (Además, aunque no se ilustre explícitamente en el dibujo, el servidor de directorio 10 puede almacenar un Identificador de Dispositivo Público (PDI) en cada registro de dispositivo 22. En un ejemplo, el PDI se obtiene usando una función "para generar claves" en un sentido en el identificador de dispositivo temporal 24.)

De acuerdo con esta configuración básica, cada registro de dispositivo 22 representa las credenciales de suscripción temporales para un dispositivo móvil. El servidor de directorio 10 se configura en una o más realizaciones para generar los lotes 20 de los registros del dispositivo 22, el cual entonces se puede distribuir a cualquier número de partes implicadas en dotar inicialmente los dispositivos móviles. Típicamente, los registros del dispositivo 22 se distribuyen a uno o más fabricantes de dispositivos móviles. En al menos una realización aquí dentro, se generan distintos lotes 20 de los registros del dispositivo 22 para los distintos fabricantes. Por ejemplo, suponiendo que el identificador temporal del dispositivo 24 se genera como un número, por ejemplo, una Identidad Internacional de Abonado Móvil Preliminar (PIMSI), se pueden usar distintas gamas de números para los distintos fabricantes de dispositivos. Hacerlo así permite a los elementos de red implicados más tarde en la activación en el aire de un dispositivo móvil determinar el fabricante del dispositivo a partir de la gama de valor del identificador temporal del dispositivo 24 notificado por el dispositivo móvil.

Ahora, con referencia de nuevo a la Fig. 1, uno ve que el servidor de directorio 10 genera uno o más lotes 20 de registros de dispositivo 22, y distribuye los registros de dispositivo 22 a un servidor de aprovisionamiento inicial 30 (u otro sistema informático) en cada uno de uno o más fabricantes de dispositivos móviles. Particularmente, la Fig. 1 ilustra los servidores de aprovisionamiento inicial 30-1 hasta el 30-R, asociados con distintos fabricantes de dispositivos móviles 1 hasta R. Cada servidor de aprovisionamiento 30 recibe algún número de registros de dispositivo 22 desde el directorio de dispositivo 10, y carga todo o parte de un registro de dispositivo individual 22 en uno particular de los dispositivos móviles 32 que se aprovisiona inicialmente por él. Esta carga se puede integrar en el proceso de fabricación.

Preferentemente, como se muestra en la Fig. 3, cada dispositivo móvil 32 incluye circuitos del sistema 40 (procesadores, circuitos de interfaz de usuario, etc.), circuitos de comunicación 42 (celular, WLAN, WiFi, etc.), y un módulo de confianza 44, tal como se configura de acuerdo con las implementaciones ARM ® TrustZone®, el Módulo de Confianza Móvil (MTM), o Módulo de Plataforma de Confianza (TPM). En una o más realizaciones, el módulo de confianza 44 incluye, por ejemplo, un procesador seguro 46, la memoria segura 48, y un motor de cifrado 50. Se pueden usar otros entornos de procesamiento seguro, y los detalles de la arquitectura segura que se ilustran se deberían interpretar como que limitan las enseñanzas presentadas aquí dentro.

En cualquier caso, un servidor de aprovisionamiento inicial 30 de esta manera carga en un dispositivo móvil dado 32, todo o parte de un registro de dispositivo 22, donde ese registro de dispositivo 22 también se contiene por el servidor de directorio 10. De esta manera, un intento más tarde del abonado para activar el dispositivo móvil 32 se puede basar en la verificación de la información del registro del dispositivo según se almacena en el dispositivo móvil 32 frente a la información del registro de dispositivo correspondiente según se almacena en el servidor de directorio 10.

Las Fig. 4 y 5 resumen el proceso anterior, en el que, en la Fig. 4, el servidor de directorio 10 genera las identidades de suscripción preliminares (Bloque 100) (por ejemplo, genera los registros de dispositivo 22 que comprende pares de PIMSI 24 y claves secretas 26). El servidor de directorio 10 entonces distribuye las identidades de suscripción preliminares a los fabricantes de dispositivos móviles (Bloque 102). Esa operación puede ser un "empuje" desde el servidor de directorio 10, o una "atracción" desde el servidor de directorio 10, con todas de tales transferencias sujetas a la verificación apropiada de seguridad, etc. Las comunicaciones entre el servidor de directorio 10 y los servidores de aprovisionamiento iniciales 30 puede estar basada en Internet, o basada en alguna otra conectividad de red.

A pesar de todo, el servidor de directorio 10 genera los registros de dispositivo individuales 22, cada uno que incluye un identificador de dispositivo temporal 24 y una clave secreta (designada como "K_p") como una par. Como se señala, el identificador temporal 24 puede comprender una PIMSI. En al menos una realización, la PIMSI es igual al número IMSI de UMTS/GSM, de manera que se pueden usar los procedimientos de autenticación del terminal móvil estándar para la PIMSI. El servidor de directorio 10 envía de esta manera los pares PIMSI/K_p a los servidores de aprovisionamiento iniciales 30 como los registros del dispositivo 22. Por ejemplo, se envían múltiples registros del dispositivo 22 como la $PIMSI_1/K_{p1}$, $PIMSI_2/K_{p2}$,…, y así sucesivamente. El servidor de directorio 10 también puede enviar su información de la dirección de red, o el servidor de aprovisionamiento inicial 30 se puede configurar con esa información.

La Fig. 5 ilustra que el servidor de aprovisionamiento inicial 30 de un fabricante del dispositivos móviles dado soporta el aprovisionamiento de los dispositivos móviles individuales 32 que usan la información de la suscripción preliminar recibida desde el servidor de directorio 10 (Bloque 104). El servidor de aprovisionamiento inicial 30 también puede cargar en cada dispositivo móvil 32 la información de la dirección de red para el servidor de directorio 10, junto con un listado de operadores de red que soportan el uso de la información de suscripción preliminar (Bloque 106). (Este listado de esta manera permite al dispositivo móvil 32 seleccionar más tarde un operador de red apropiado, suponiendo que múltiples operadores de red proporcionan cobertura en la ubicación del móvil, para llevar a cabo el aprovisionamiento en el aire del dispositivo móvil 32 con las credenciales de suscripción permanentes.)

En más detalle, se puede configurar el servidor de aprovisionamiento inicial 30 para generar un par de claves pública/privada, indicado como PuK/PrK, usando procesamiento seguro. En tales realizaciones, la información de la suscripción preliminar para el registro del dispositivo 22-x de esta manera incluiría PuK_x, PrK_x, K_{px}, y el identificador del dispositivo temporal 24 (por ejemplo, la $PIMSI_x$). El procesador de aprovisionamiento inicial 30 carga esta información en el módulo de confianza 44 del dispositivo móvil 32. El servidor de aprovisionamiento inicial 30 también carga, como se mencionó, un listado de operadores de red que soportan el uso de la información de suscripción preliminar, por ejemplo un listado de operadores de red que aceptará el uso de las PIMSI para conseguir el acceso de red temporal. El servidor de aprovisionamiento inicial también puede cargar la información de la dirección de red para el servidor de directorio 10.

Más generalmente, se debería entender que, en una o más realizaciones, el módulo de confianza 44 del dispositivo móvil 32 se proporciona con el identificador de dispositivo temporal 24 (por ejemplo, la $PIMSI_x$) la clave secreta K_{px}, y el par de claves pública/privada PuK_x, PrK_x (para usar más tarde en la activación en el aire del dispositivo móvil 32), y que todos de tales valores se pueden proporcionar por el servidor de aprovisionamiento inicial 30, o ese uno o más de ellos se puede autogenerar por el dispositivo móvil 32. Por ejemplo, en al menos una realización, el dispositivo móvil 32 se configura para generar el par de claves pública/privada PuK_x, PrK_x. La información de aprovisionamiento también incluye de manera general un listado de operadores de red que soporta el acceso de red de comunicación inalámbrica temporal a través del uso del identificador de dispositivo temporal 24, y puede incluir opcionalmente la información de la dirección de red para el servidor de directorio 10.

En algún momento posterior, se vende un dispositivo móvil dado 32 a o se dirige de otro modo para la asociación con un abonado de un operador de red dado. Como una ilustración ejemplo, la Fig. 6 representa tres servidores de credenciales 60-1, 60-2, y 60-3 distintos, que pueden representar elementos de acreditación de tres operadores de red distintos. Los servidores de credenciales ilustrados 60 se acoplan de manera comunicativa al servidor de directorio 10, y de esta manera son capaces de indicar al servidor de directorio 10 cuáles de los registros del dispositivo 22 contenidos por el servidor de directorio 10 van a ser asociados con o vinculados de otro modo a cuáles de los servidores de credenciales 60.

La Fig. 7 ilustra una realización ejemplo, en la que el servidor de credenciales 60-x de un operador de red dado comunica con el servidor de directorio 10, por ejemplo, a través de una conexión de Internet u otra red. Particularmente, el servidor de credenciales 60-x obtiene o se dota de otro modo con los datos del abonado (Bloque 110). Por ejemplo, un sistema de ventas u otro ordenador dota al servidor de credenciales 60-x con los detalles del abonado para los PDI particulares, donde los PDI corresponden a los registros de dispositivo individuales 22 en el

servidor de directorio 10. El servidor de credenciales 60-x de esta manera puede recibir los registros de abonado, donde cada registro de abonado incluye detalles para un abonado particular, junto con un PDI y la dirección del servidor de directorio 10 que contiene el registro del dispositivo 22 correspondiente a ese PDI.

De esta manera, un PDI correspondiente a un identificador de dispositivo temporal particular 24 se asocia con o se vincula de otro modo a los datos para un abonado particular en el servidor de credenciales 60-x. Estos datos de la suscripción, que funcionan como credenciales de suscripción, también pueden incluir los valores de suscripción secretos, como una "clave maestra" de UMTS. En cualquier caso, el procesamiento continúa con el servidor de credenciales 60-x que envía la información del PDI al servidor de directorio 10 (Bloque 112). El recibo de esa información del PDI hace que el servidor de directorio 10 asocie o vincule de otro modo los registros del dispositivo 22 correspondientes a la información del PDI recibido con el servidor de credenciales 60-x.

El servidor de directorio 10 por lo tanto se configura para recibir un PDI desde el servidor de credenciales 60-x, y, en respuesta, enlazar el registro del dispositivo 22 correspondiente al PDI con el servidor de credenciales 60-x. Como ejemplo, el PDI es una generación de claves en un sentido de una PIMSI, y el directorio del dispositivo 10 procesa el PDI para obtener la PIMSI correspondiente, y entonces usa la PIMSI recuperada para indexar en uno o más lotes 20 de registros de dispositivo almacenados 22, para identificar el registro de dispositivo 22 que encaja con la PIMSI recuperada.

Una vez que se identifica el registro del dispositivo correcto 22, el servidor de directorio 10 lo enlaza al servidor de credenciales 60-x, por ejemplo, almacena la información de la dirección de red para el servidor de credenciales 60-x en el registro del dispositivo identificado 22, o hace que el registro del dispositivo 22 "apunte" al servidor de credenciales 60-x. Para cada uno de tales registros enlazados del PDI del dispositivo 22, el servidor de credenciales 60-x recibe una segunda clave secreta al servidor de credenciales 60-x desde el servidor de directorio 60-x (Bloque 114). Esa segunda clave secreta se denota como K_t para indicar su estado temporal. El servidor de directorio 10 deriva a partir de la clave secreta K_p del registro de dispositivo implicado 22. Por ejemplo, $K_t = F(K_p)$, donde "F" indica una función de un sentido adecuada criptográficamente fuerte. El servidor de credenciales 60-x almacena esta clave temporal K_t con el resto de los datos del abonado asociados con el PDI dado.

En el contexto del registro de abonado preliminar anterior, los fabricantes de dispositivos móviles dados pueden enviar los PDI y la información de la dirección del directorio del dispositivo correspondiente directamente a los operadores de red. Por ejemplo, un servidor de aprovisionamiento inicial 30 u otro sistema informático del fabricante se puede acoplar de manera comunicativa a los servidores de credenciales 60 de uno o más operadores de red. Tales comunicaciones permiten a los fabricantes de dispositivos móviles enlazar dispositivos móviles particulares 32 a los operadores de red particulares anterior a cualquier venta al por menor.

Adicionalmente o alternativamente, los dispositivos móviles individuales 32 se envían a sus respectivos compradores. Los PDI y las asociaciones de directorios de dispositivo para esos dispositivos móviles 32 se proporcionan a esos compradores, tal como en forma escrita o electrónica acompañando a los dispositivos móviles en sí mismos. De esta manera, una vez que un usuario final compra u obtiene de otra manera un dispositivo móvil particular 32, ese usuario final registra el PDI y la información del directorio del dispositivo de ese dispositivo móvil 32 con el servidor de credenciales 60 que pertenece a un operador de red de su elección.

La Fig. 8 ilustra una realización de este registro de usuario final como parte de una metodología general contemplada aquí dentro. Como se ilustra en el Paso 1, un servidor de directorio 10 proporciona un par de claves PIMSI/secreta ($PIMSI_x/K_{px}$) a un servidor de aprovisionamiento inicial 30. Los datos proporcionados hacen coincidir un registro de dispositivo 22 almacenado dentro del servidor de directorio 10.

En el Paso 2, el servidor de aprovisionamiento inicial 30 genera un par de claves pública/privada, PuK_x/PrK_x, y dota inicialmente un dispositivo móvil individual 32-x cargándolo con la información de la dirección de red PuK_x/PrK_x, K_{px}, $PIMSI_x$, para el servidor de directorio 10, y un listado de operadores de red que participan. Alternativamente, el dispositivo móvil 32-x autogenera la PuK_x/PrK_x, más que esos valores sean generados por el servidor de aprovisionamiento inicial 30.

En el Paso 3, un usuario final u otro abonado asociado con el dispositivo móvil 32-x presenta los datos del registro de abonado al servidor de credenciales 60. Como ejemplo, el servidor de credenciales 60 recibe la información de la identidad del abonado y de la facturación, junto con el PDI_x, y la dirección de red u otra información de identificación para un servidor de directorio 10.

En el Paso 4, el servidor de credenciales 60 presenta el PDI_x, al servidor de directorio 10, haciendo por ello que el servidor de directorio 10 procese el PDI_x e identifique el registro de dispositivo correspondiente 22-x, y enlace ese registro de dispositivo 22-x al servidor de credenciales de presentación 60.

En el Paso 5, el servidor de directorio 10 devuelve una clave secreta temporal K_{tx}, al servidor de credenciales 60.

En el Paso 6, el dispositivo móvil 32-x contacta una red de comunicación inalámbrica 70 y la dota con su identificador de dispositivo temporal 24, por ejemplo, con la $PIMSI_x$. Más concretamente, el dispositivo móvil 32-x se puede configurar para intentar registrarse con la red de comunicación inalámbrica 70 usando los procedimientos de

registro GSM/UMTS estándar en los que proporciona su $PIMSI_x$ a la red 70 como parte del registro. Además, el dispositivo móvil 32-x se puede configurar para determinar que la red 70 es apropiada para tales intentos de registro, en base a su listado almacenado de operadores de red que soportan el uso de los identificadores de dispositivo temporales 24 como una base para conseguir las credenciales de suscripción de largo plazo a través de aprovisionamiento en el aire.

También, como parte del Paso 6, la red 70 pasa la $PIMSI_x$ obtenida a partir del dispositivo móvil 32-x a un servidor de autenticación 72. El servidor de autenticación 72 puede ser, por ejemplo, un Registro de Localización de Visitantes (VLR) y/o Registro de Localización Local (HLR) asociado con la red 70 o con una red local de un operador de red asociado con el dispositivo móvil 32.

En el Paso 7, el servidor de autenticación 72 reconoce la $PIMSI_x$ como un identificador temporal, y pasa la $PIMSI_x$ al servidor de directorio 10 apropiado. En una o más realizaciones, el servidor de autenticación 72 se configura para determinar la información de la dirección de red para el servidor de directorio 10 a partir de la $PIMSI_x$ recibida desde el dispositivo móvil 32-x.

En el Paso 8, el servidor de directorio 10 encuentra el registro de datos correcto 22-x correspondiente a la $PIMSI_x$ según se recibe desde el servidor de autenticación 72. Como parte de este procesamiento, el servidor de directorio 10 puede determinar la validez de la $PIMSI_x$ comprobando si la $PIMSI_x$ está bloqueada, expirada, o ha sido usada de otro modo más de un número permitido de veces. De esta manera, si la $PIMSI_x$ existe dentro del(de los) lote(s) 20 de los registros de dispositivo 22 almacenados en el servidor de directorio 10 y es válida, el servidor de directorio 10 calcula un vector de autenticación temporal para el dispositivo móvil 32-x y devuelve el vector de autenticación al servidor de autenticación 72.

En una o más realizaciones, el directorio del dispositivo 10 se configura para derivar el vector de autenticación usando la clave secreta K_{px} almacenada en el registro de dispositivo 22-x para el dispositivo móvil 32-x. En este sentido, el directorio del dispositivo 10 se puede configurar para generar el vector de autenticación usando los procedimientos estandarizados del Proyecto de Cooperación de 3ª Generación (3GPP), tal como el algoritmo MILENAGE. Hacerlo así aumenta la interoperabilidad. A pesar de todo, el Paso 8 se muestra que continúa a través del vector de autenticación 72, que indica que el vector de autenticación se pasa de nuevo a la red 70.

En el Paso 9, la red 70 usa el vector de autenticación para conceder acceso temporal, por ejemplo, acceso de paquetes de datos temporales, al dispositivo móvil 32-x. Como ejemplo, el vector de autenticación es válido durante una cantidad limitada de tiempo, por ejemplo, un minuto, y/o es válido para una cantidad muy limitada de transferencia de datos.

En el Paso 10, el dispositivo móvil 32-x usa su acceso temporal para comunicar con el servidor de directorio 10. En este sentido, se señaló que la información de la dirección de red para el servidor de directorio 10 se puede incluir como parte de la información de aprovisionamiento inicial del dispositivo. De esta manera, el dispositivo móvil 32-x puede usar esa información almacenada para contactar el servidor de directorio apropiado 10 después de conseguir el acceso temporal. Aunque el diagrama aparece para mostrar la comunicación directamente entre el dispositivo móvil 32-x y el servidor de directorio 10, aquellos expertos en la técnica apreciarán que el enlace puede ser indirecto, y, en general, incluye una conexión en el aire que se soporta por la red 70 de acuerdo con el vector de autenticación temporal. Con su enlace comunicativo al servidor de directorio 10, el dispositivo móvil 32-x solicita que el servidor de directorio 10 le dote con la información de la dirección del servidor de credenciales vinculado al servidor de directorio 10 a su $PIMSI_x$.

En el Paso 11, el servidor de directorio 10 devuelve la información de la dirección del servidor de credenciales al dispositivo móvil 32-x.

En el Paso 12, el dispositivo móvil 32-x genera una nueva clave temporal K_{tx}. En al menos una realización, el dispositivo móvil 32-x deriva K_{tx} de su clave secreta K_{px}.

En el Paso 13, el dispositivo móvil 32-x envía una petición de credenciales al servidor de credenciales 60, ya identificado por la información de la dirección del servidor de credenciales devuelta al dispositivo móvil 32-x desde el directorio del dispositivo 10. (De nuevo, tales comunicaciones generalmente son indirectas, con al menos una parte del enlace soportado por una conexión en el aire hecha a través de la red 70.) En una realización, esta petición se protege usando la clave temporal K_{tx}, y, posiblemente, un Código de Autenticación del Mensaje (MAC). En otra realización, la conexión se protege por la clave temporal K_{tx} y un protocolo de seguridad de transporte, tal como TLS. A pesar de todo, en al menos una realización, la petición incluye la clave pública del dispositivo móvil PuK_x, y el PDI_x correspondiente a las $PIMSI_x$ de los dispositivos móviles.

En el Paso 14, el servidor de credenciales 60 crea las credenciales de suscripción permanente (largo plazo) para el dispositivo móvil 32. Por ejemplo, si puede generar un Módulo de Identidad de Abonado de Componentes Lógicos (SSIM) u otra forma de información de autorización basada en programas informáticos. Tales datos pueden incluir tanto las credenciales SIM como los parámetros SSIM. Los parámetros SSIM pueden incluir algoritmos SIM que tienen aplicabilidad específica para el operador de red asociado con el servidor de credenciales 60.

En el Paso 15, el servidor de credenciales 60 cifra las credenciales de suscripción permanente usando la clave pública del dispositivo móvil 32, PuK_x, y las envía al dispositivo móvil 32. En otra realización, el servidor de credenciales usa la clave temporal K_{tx}, para cifrar las credenciales de suscripción permanentes. Hacerlo así, no obstante, eleva una implicación de seguridad posible porque K_{tx} se deriva a partir de la clave secreta K_{px}, que también se contiene en el servidor de directorio 10.

En el Paso 16, el dispositivo móvil recibe las credenciales de suscripción permanentes cifradas, las descifra, y las instala, por ejemplo, dentro de su módulo de confianza 44. Este proceso puede incluir cualquier SIM necesario u otra actualización de programas informáticos. A pesar de ello, el dispositivo móvil 32 se aprovisiona ahora con las credenciales de suscripción permanentes, dando acceso al dispositivo móvil 32 a las redes de comunicación inalámbrica local y de visitantes dentro de cualesquiera límites establecidos por esas credenciales.

Una idea básica pero no limitativa que se realiza por la adaptación anterior es que a los fabricantes de dispositivos móviles se les permiten dotar inicialmente los dispositivos móviles 32 de tal manera que pueden ser activados más tarde (dotados permanentemente) usando la activación en el aire a través de cualquier número de operadores de red participantes. Esta adaptación permite de esta manera a un dispositivo móvil 32 conseguir acceso de red de comunicación inalámbrica temporal usando la información de la identidad de suscripción preliminar, y luego usar ese acceso para obtener la dirección de y la conexión a un servidor de credenciales que le dotará con información de suscripción permanente. En pocas palabras, un número potencialmente grande de operadores de red distintos puede estar de acuerdo con participar en la adaptación descrita, y enlazar de manera comunicativa sus respectivas redes de comunicación inalámbricas al servidor de directorio 10 (o a cualquiera en una serie de servidores de directorio 10 distintos).

De esta manera, se presenta aquí dentro un sistema y método para facilitar la activación del dispositivo de comunicación móvil en el aire. No obstante, se entenderá que la descripción anteriormente mencionada y los dibujos que se acompañan representan ejemplos no limitativos de los métodos, sistemas, y aparatos individuales enseñados aquí dentro. Como tal, la presente invención no se limita por la descripción anterior y los dibujos anexos. En su lugar, la presente invención se limita solamente por las siguientes reivindicaciones y sus equivalentes legales.

REIVINDICACIONES

1. Un método de facilitar la activación del dispositivo de comunicación móvil en el aire que comprende, en un servidor centralizado de directorio de dispositivos (10):

almacenar un registro de dispositivo (22-1;…; 22-N) que comprende la información de las credenciales de suscripción preliminares para un dispositivo móvil (32-1;…; 32-M);

enviar al menos parte de la información de las credenciales de suscripción preliminares de manera segura a una parte de aprovisionamiento inicial (30-1; …; 30-R), para usar en dotar inicialmente el dispositivo móvil;

recibir un identificador de dispositivo para el dispositivo móvil desde un servidor de credenciales (60-1; 60-2; 60-3) de un operador de red dado asociado con un usuario final previsto del dispositivo móvil, y vincular de la misma manera la información de la dirección de red del servidor de credenciales con el registro del dispositivo;

recibir una petición de validación desde un servidor de autenticación, sensible al dispositivo móvil que intenta acceder a una red de comunicación inalámbrica que usa la información de las credenciales de suscripción preliminar;

enviar un vector de autenticación al servidor de autenticación que se basa en una clave secreta incluida en la información de las credenciales de suscripción preliminar, si la información de las credenciales de suscripción preliminar para el dispositivo móvil es válida;

recibir una petición de la dirección del servidor de credenciales desde el dispositivo móvil, consecutiva a que el dispositivo móvil consiga el acceso temporal a la red de comunicación inalámbrica a través del vector de autenticación; y

enviar la información de la dirección de red para el servidor de credenciales al dispositivo móvil, ya enlazado en el registro del dispositivo almacenado por el dispositivo móvil.

2. El método de la reivindicación 1, en el que almacenar el registro del dispositivo comprende almacenar una Identidad Internacional de Abonado Móvil, PIMSI, y la clave secreta para el dispositivo móvil.

3. El método de la reivindicación 2, en el que recibir el identificador del dispositivo para el dispositivo móvil desde el servidor de credenciales del operador de red dado asociado con el usuario final previsto del dispositivo móvil comprende recibir un Identificador de Dispositivo Público, PDI, que se deriva de la Identidad Internacional de Abonado Móvil Preliminar, PIMSI, del dispositivo móvil, y que además comprende la identificación del registro del dispositivo para el dispositivo móvil desde el Identificador de Dispositivo Público, PDI, y vincular el registro del dispositivo a la información de la dirección de red del servidor de credenciales.

4. El método de la reivindicación 2, que además comprende dotar inicialmente un módulo de confianza del dispositivo móvil con la Identidad Internacional del Abonado Móvil Preliminar, PIMSI, la clave secreta, y un par de claves pública/privada, y dotar además el dispositivo móvil con la información de la dirección de red para el servidor centralizado de directorio de dispositivo y un listado de operadores de red que soportan el acceso de red de comunicación inalámbrica temporal a través del uso de la Identidad Internacional de Abonado Móvil Preliminar, PIMSI.

5. El método de la reivindicación 4, que además comprende conseguir el acceso temporal a la red de comunicación inalámbrica por el dispositivo móvil en base al dispositivo móvil que proporciona la Identidad Internacional del Abonado Móvil Preliminar, PIMSI, a la red de comunicación inalámbrica, y la red de comunicación inalámbrica que envía la Identidad Internacional de Abonado Móvil Preliminar, PIMSI, al servidor de autenticación para transferir al servidor centralizado de directorio del dispositivo.

6. El método de la reivindicación 5, que además comprende conseguir el acceso al servidor de credenciales del operador de la red dado por el dispositivo móvil, en base al dispositivo móvil que recibe la información de la dirección de red para el servidor de credenciales desde el servidor centralizado de directorio de dispositivo, y enviar una petición de credenciales desde el dispositivo móvil al servidor de credenciales, dicha petición de credenciales que incluye la clave pública del par de claves pública/privada almacenada en el dispositivo móvil, y dicha petición de credenciales protegida por una clave temporal derivada de la clave secreta almacenada en el dispositivo móvil.

7. El método de la reivindicación 6, que además comprende, en el servidor de credenciales, verificar la petición de credenciales desde el dispositivo móvil, y generar un Módulo de Identidad de Abonado de Componentes Lógicos, SSIM, y enviar el SSIM al dispositivo móvil en forma cifrada usando la clave pública del dispositivo móvil, para usar por el dispositivo móvil en la instalación de las credenciales de suscripción permanentes para el operador de red dado.

8. El método de la reivindicación 2, que además comprende, en el servidor centralizado de directorio de dispositivo, derivar una segunda clave secreta desde la clave secreta, y enviar la segunda clave secreta para el almacenamiento en el servidor de credenciales en asociación con los datos de abonado del usuario final, para usar

más tarde en proteger la información del Módulo de Identidad de Abonado de Componentes Lógicos, SSIM, generada por el servidor de credenciales y enviada en el aire al dispositivo móvil.

9. Un sistema para facilitar la activación del dispositivo de comunicación móvil en el aire que incluye un servidor centralizado de directorio de dispositivos (10) que comprende uno o más circuitos de procesamiento configurados para:

almacenar un registro de dispositivo (22-1; …; 22-N) que comprende la información de las credenciales de suscripción preliminares para un dispositivo móvil (32-1; …; 32-M);

enviar al menos parte de la información de las credenciales de suscripción preliminares de manera segura a una parte de aprovisionamiento inicial (30-1; …; 30-R), para usar en dotar inicialmente el dispositivo móvil;

recibir un identificador de dispositivo para el dispositivo móvil desde un servidor de credenciales (60-1; 60-2; 60-3) de un operador de red dado asociado con un usuario final previsto del dispositivo móvil, y vincular de la misma manera la información de la dirección de red del servidor de credenciales con el registro del dispositivo;

recibir una petición de validación desde un servidor de autenticación, sensible al dispositivo móvil que intenta acceder a una red de comunicación inalámbrica que usa la información de las credenciales de suscripción preliminar;

enviar un vector de autenticación al servidor de autenticación que se basa en una clave secreta incluida en la información de las credenciales de suscripción preliminar, si la información de las credenciales de suscripción preliminar para el dispositivo móvil es válida; y

recibir una petición de la dirección del servidor de credenciales desde el dispositivo móvil, consecutiva a que el dispositivo móvil consiga el acceso temporal a la red de comunicación inalámbrica a través del vector de autenticación, y enviar de la misma manera la información de la dirección de red para el servidor de credenciales al dispositivo móvil, como vinculada en el registro del dispositivo almacenado por el dispositivo móvil.

10. El sistema de la reivindicación 9, en el que el servidor centralizado de directorio del dispositivo se configura para almacenar, como el registro del dispositivo, una Identidad Internacional del Abonado Móvil Preliminar, PIMSI, la clave secreta para el dispositivo móvil.

11. El sistema de la reivindicación 10, en el que el servidor centralizado de directorio del dispositivo incluye un interfaz de comunicación configurado para comunicar directamente o indirectamente con el servidor de credenciales, y recibir, como el identificador del dispositivo para el dispositivo móvil, un Identificador de Dispositivo Público, PDI, que se deriva de la Identidad Internacional del Abonado Móvil Preliminar, PIMSI, del dispositivo móvil, y en el que el servidor centralizado de directorio de dispositivo se configura para identificar el registro del dispositivo para el dispositivo móvil a partir del Identificador de Dispositivo Público, PDI, y vincular el registro del dispositivo a la información de la dirección de red del servidor de credenciales.

12. El sistema de la reivindicación 10, que además comprende un servidor de aprovisionamiento inicial para el suministro de un módulo de confianza del dispositivo móvil con la Identidad Internacional del Abonado Móvil Preliminar, PIMSI, y la clave secreta, y para dotar además el dispositivo móvil con la información de la dirección de red para el servidor centralizado de directorio de dispositivo, y un listado de operadores de red que soporta el acceso de red de comunicación inalámbrica temporal a través del uso de la Identidad Internacional de Abonado Móvil Preliminar, PIMSI.

13. El sistema de la reivindicación 12, en el que el servidor de aprovisionamiento inicial se configura además para dotar el módulo de confianza del dispositivo móvil con el par de claves pública/privada para usar más tarde en la activación en el aire del dispositivo móvil.

14. El sistema de 12, en el que el servidor de autenticación se acopla de manera comunicativa a la red de comunicación inalámbrica y se configura para recibir la Identidad Internacional del Abonado Móvil Preliminar, PIMSI, y para recibir de esa manera un vector de autenticación para la estación móvil en respuesta a la transferencia de la Identidad Internacional de Abonado Móvil Preliminar, PIMSI, al servidor centralizado de directorio del dispositivo para la verificación, y devolver el vector de autenticación a la red de comunicación inalámbrica para conceder el acceso temporal al dispositivo móvil.

15. El sistema de la reivindicación 14, en el que el servidor centralizado de directorio del dispositivo se configura para recibir una petición de la dirección del servidor de credenciales desde el dispositivo móvil después de que al dispositivo móvil se le concede acceso temporal en base al vector de autenticación, y devolver la información de la dirección de red del servidor de credenciales, ya vinculado al registro del dispositivo del dispositivo móvil.

16. El sistema de la reivindicación 15, en el que el dispositivo móvil se configura para recibir la información de la dirección de red para el servidor de credenciales desde el directorio del dispositivo centralizado, y de esa manera enviar una petición de credenciales para la suscripción permanente de las credenciales al servidor de credenciales,

dicha petición de credenciales que incluye la clave pública del par de claves pública/privada almacenadas en el dispositivo móvil, y dicha petición de credenciales protegida por una clave temporal derivada a partir de la clave secreta del dispositivo móvil.

17. El sistema de la reivindicación 16, en el que el servidor de credenciales se configura para verificar la petición de credenciales a partir del dispositivo móvil y de esa manera generar un Módulo de Identidad de Abonado de Componentes Lógicos, SSIM, y se configura además para enviar el SSIM al dispositivo móvil en forma cifrada ya protegida por la clave pública del dispositivo móvil, para usar por el dispositivo móvil en la instalación de las credenciales de suscripción permanentes para el operador de red dado.

18. El sistema de la reivindicación 9, en el que el servidor centralizado de directorio del dispositivo se configura para derivar una segunda clave secreta a partir de la clave secreta, y enviar la segunda clave secreta para el almacenamiento en el servidor de credenciales en asociación con los datos del abonado del usuario final, para usar más tarde en la protección de la información del Módulo de Identidad de Abonado de Componentes Lógicos, SSIM, generada por el servidor de credenciales y enviada en el aire al dispositivo móvil.

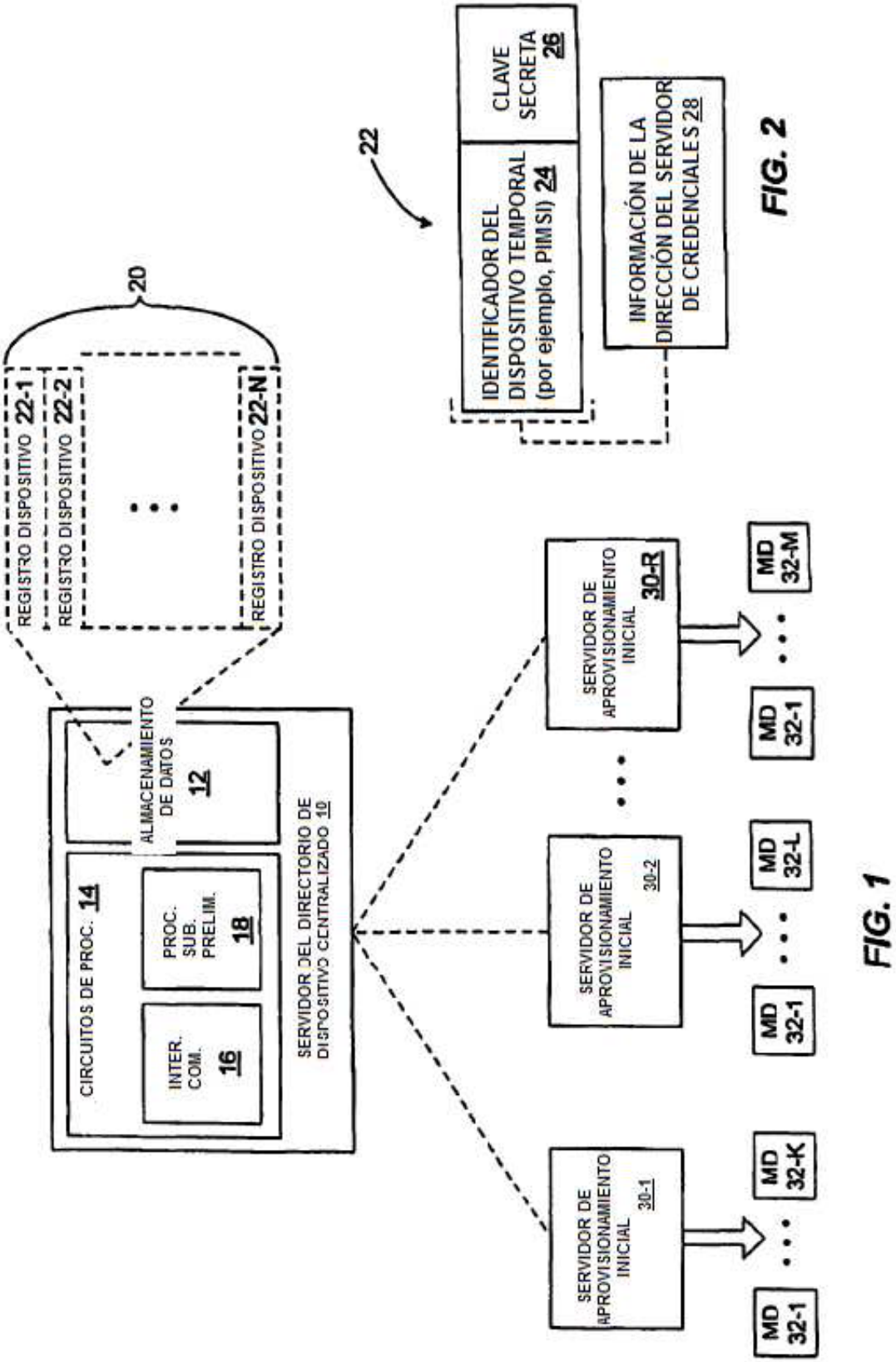
SERVIDOR DEL DIRECTORIO DE DISPOSITIVO CENTRALIZADO 10
CIRCUITOS DE PROC. 14
INTER. COM. 16
PROC. SUB. PRELIM. 18
ALMACENAMIENTO DE DATOS 12
20
REGISTRO DISPOSITIVO 22-1
REGISTRO DISPOSITIVO 22-2
REGISTRO DISPOSITIVO 22-N
22
IDENTIFICADOR DEL DISPOSITIVO TEMPORAL (por ejemplo, PIMSI) 24
CLAVE SECRETA 26
INFORMACIÓN DE LA DIRECCIÓN DEL SERVIDOR DE CREDENCIALES 28
SERVIDOR DE APROVISIONAMIENTO INICIAL 30-1
SERVIDOR DE APROVISIONAMIENTO INICIAL 30-2
SERVIDOR DE APROVISIONAMIENTO INICIAL 30-R
MD 32-1
MD 32-K
MD 32-L
MD 32-M

FIG. 1

FIG. 2

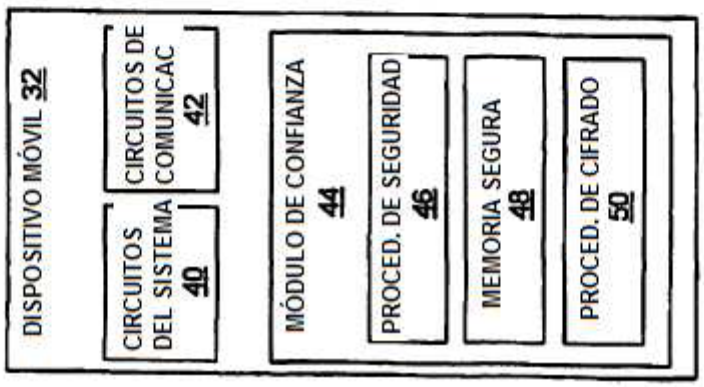

FIG. 3

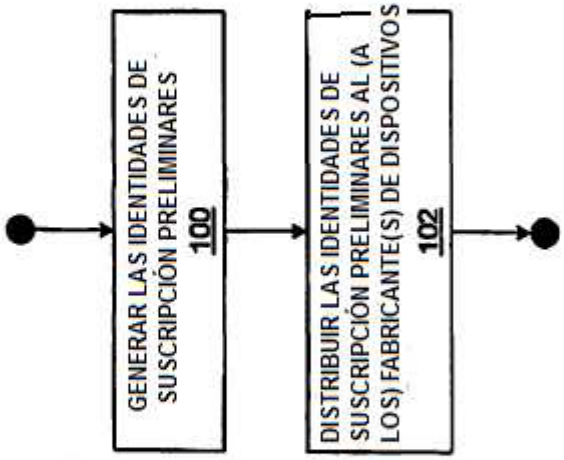

FIG. 4

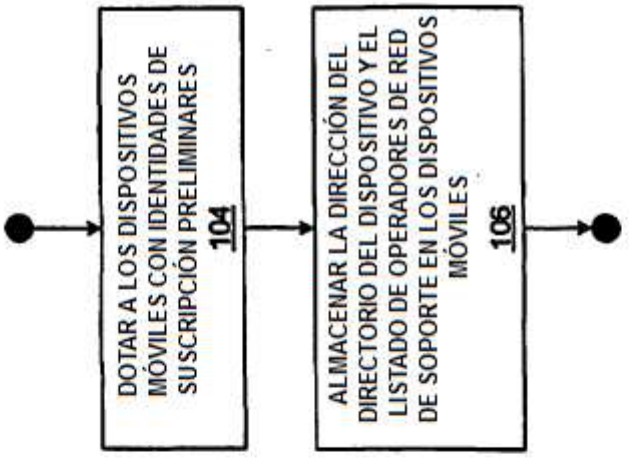

FIG. 5

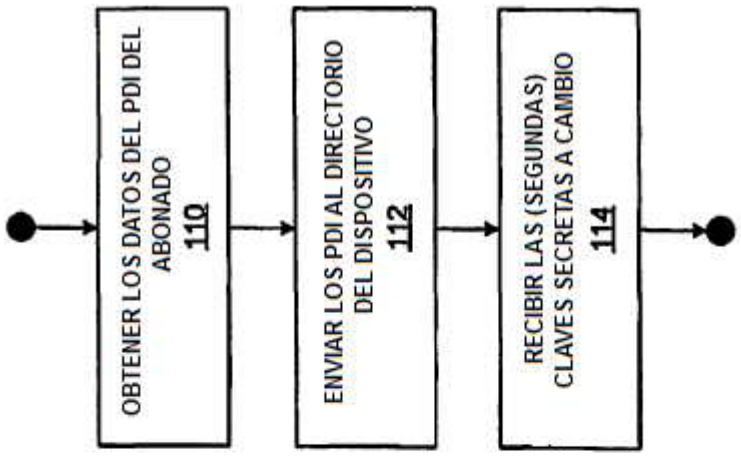
OBTENER LOS DATOS DEL PDI DEL ABONADO
110
ENVIAR LOS PDI AL DIRECTORIO DEL DISPOSITIVO
112
RECIBIR LAS (SEGUNDAS) CLAVES SECRETAS A CAMBIO
114

FIG. 7

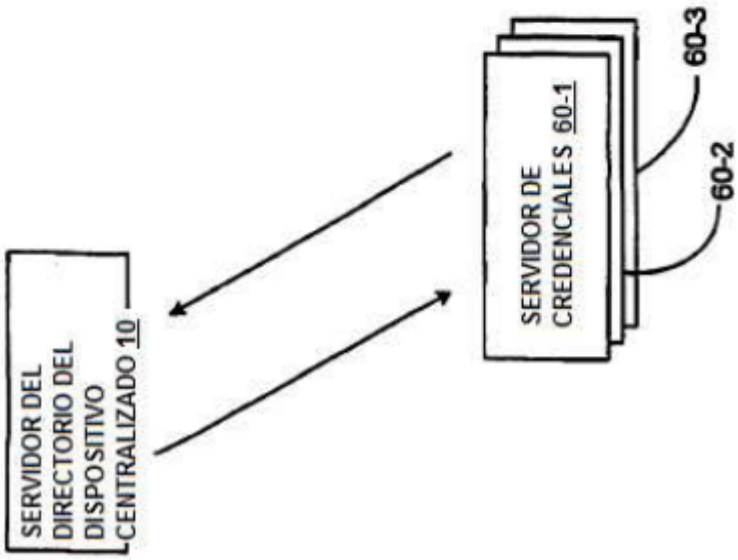
SERVIDOR DEL DIRECTORIO DEL DISPOSITIVO CENTRALIZADO 10
SERVIDOR DE CREDENCIALES 60-1
60-2
60-3

FIG. 6

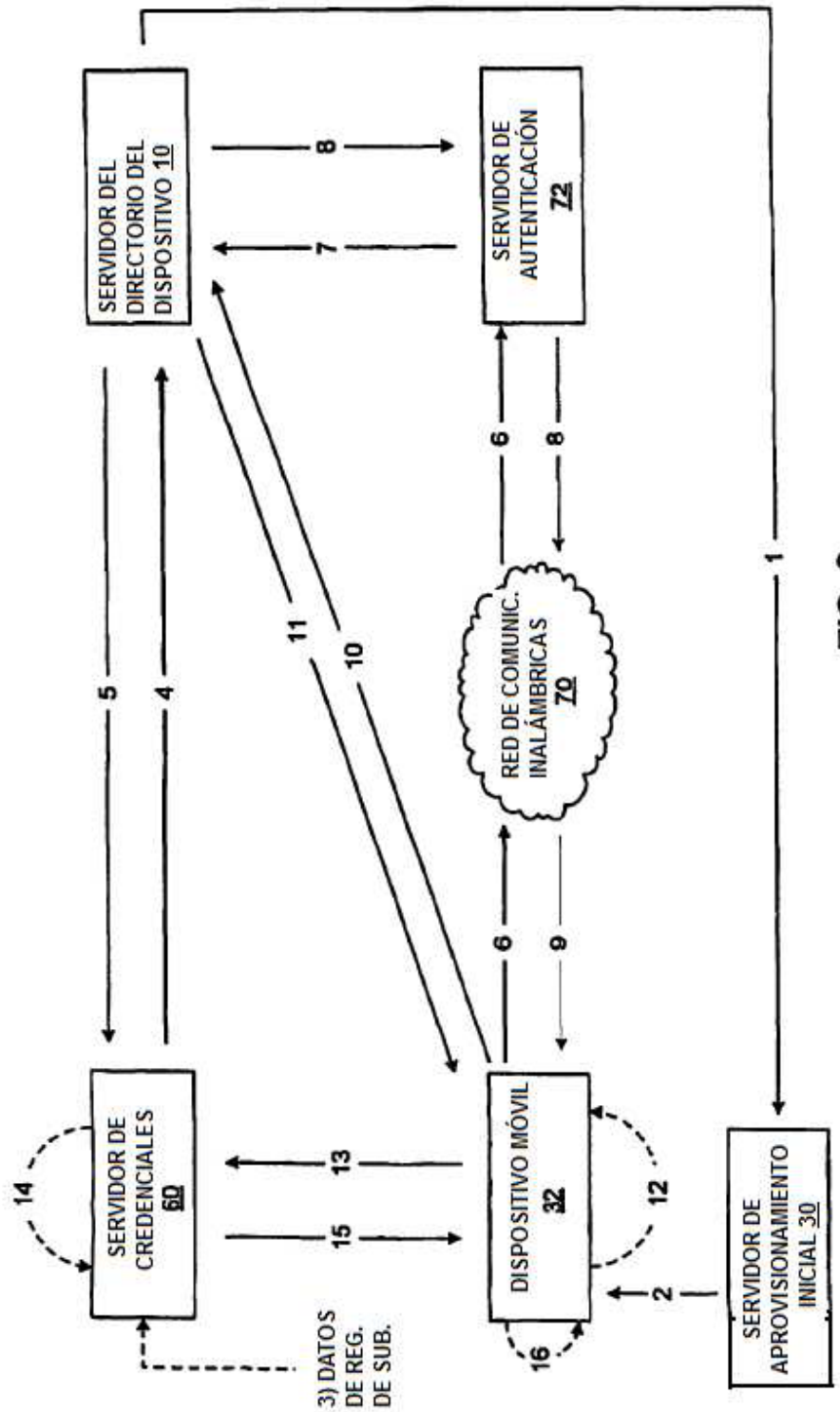
SERVIDOR DEL DIRECTORIO DEL DISPOSITIVO 10
SERVIDOR DE AUTENTICACIÓN 72
RED DE COMUNIC. INALÁMBRICAS 70
SERVIDOR DE CREDENCIALES 60
DISPOSITIVO MÓVIL 32
SERVIDOR DE APROVISIONAMIENTO INICIAL 30
3) DATOS DE REG. DE SUB.
1
2
4
5
6
7
8
9
10
11
12
13
14
15
16

FIG. 8