(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 661 043**

(51) Int. CI.:

H04W 12/12 (2009.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 12/24 (2006.01)
H04W 12/04 (2009.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.10.2009 PCT/SE2009/051092**

(87) Fecha y número de publicación internacional: **12.08.2010 WO10090569**

(96) Fecha de presentación y número de la solicitud europea: **01.10.2009 E 09839778 (9)**

(97) Fecha y número de publicación de la concesión europea: **06.12.2017 EP 2394452**

(54) Título: **Unidad de red de un sistema de red de gestión de dispositivos para la protección de un mensaje de arranque y el dispositivo, método y programa de ordenador correspondientes**

(30) Prioridad:

05.02.2009 US 150118 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.03.2018

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

BARRIGA, LUIS;
DYSENIUS, PER-ANDERS y
LINDSTRÖM, MAGNUS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Unidad de red de un sistema de red de gestión de dispositivos para la protección de un mensaje de arranque y el dispositivo, método y programa de ordenador correspondientes

Campo técnico

La presente invención se refiere en general al campo de los sistemas de redes de comunicaciones con móviles o inalámbricas y, más específicamente, a los aparatos y a un método para proteger de forma segura un mensaje de arranque durante el arranque de un sistema de redes de gestión de dispositivos.

Antecedentes

Los dispositivos móviles deben configurarse con diversas estructuras para controlar y proporcionar diferentes funciones y servicios de soporte. Un método conocido de configuración de dispositivos móviles con datos relacionados con el servicio es a través de, por ejemplo, el servicio de mensajes cortos (SMS) o el protocolo de aplicaciones inalámbricas (WAP). Esta es una ruta unidireccional y para poder realizar un servicio bidireccional, asociación con móviles abierta (OMA) tiene protocolos, modelos de datos y políticas específicas para la gestión de los dispositivos (DM). Como ejemplo, *OMA DM versión 1.2.1 enabler release specifications* disponibles en la URL: http: //www.openmobilealiance.org, define cómo se establece y se mantiene una sesión de DM. Una de las funciones importantes de estas especificaciones incluye una especificación del arranque que describe los métodos para que un dispositivo esté dotado con la configuración OMA DM antes de iniciar una sesión de gestión. Las especificaciones técnicas de arranque OMA DM se describen en *OMA DM Bootstrap versión 1.2 .., OMA- TS-DM Bootstrap V1 2 1. Open Mobile Alliance, junio de 2008.*

El arranque es un proceso de aprovisionamiento de un cliente DM de un dispositivo móvil o inalámbrico al moverse el dispositivo desde un estado vacío no aprovisionado a un estado en el que puede iniciar una sesión de gestión a un servidor de DM y posteriormente a unos, por ejemplo, nuevos servidores de DM. Existen tres formas diferentes de realizar un proceso de arranque: arranque personalizado; arranque iniciado por el servidor y arranque desde una tarjeta inteligente.

En el proceso de arranque personalizado, los dispositivos se cargan con la información de arranque OMA DM durante la fabricación. Esto también se define como arranque de fábrica.

En el proceso de arranque iniciado por el servidor, un servidor está configurado para enviar información de arranque por medio de algún mecanismo de origen en el servidor, por ejemplo, origen en el servidor WAP. Para este proceso, el servidor debe recibir la dirección/número de teléfono del dispositivo de antemano.

En el proceso de arranque desde la tarjeta inteligente, la tarjeta inteligente (por ejemplo, el módulo de identidad del abonado (SIM) o SIM universal (USIM)) está insertado en el dispositivo y el cliente de DM se inicializa desde la tarjeta inteligente.

Sin embargo, existen diversos problemas y desventajas asociados con los sistemas que usan estos procesos. El proceso de arranque personalizado requiere que los parámetros básicos sean conocidos en el momento de la fabricación o en el momento de la venta del dispositivo. El proceso de arranque iniciado por el servidor especifica que la identidad del abonado móvil internacional (IMSI) se debe utilizar para codificar los parámetros básicos de DM cuando el servidor de DM realiza un arranque en el interfaz aéreo. Esto se hace enviando un SMS cifrado con los parámetros básicos al dispositivo. La clave utilizada para el cifrado es el IMSI, por ejemplo, sistema de red de segunda generación/tercera generación, o el número de serie electrónico (ESN) para el sistema de acceso múltiple por división de código (CDMA). Sin embargo, el IMSI o el ESN no han sido diseñados para ser secretos. Esto también significa que el mensaje de arranque que se transmitirá desde el servidor de DM al dispositivo estará débilmente protegido. Como resultado, un atacante puede crear su propio mensaje de arranque para arrancar un dispositivo que estaría bloqueado en un servidor malicioso de DM. Otro inconveniente es que un atacante puede tener acceso al mensaje de arranque que solo está protegido en su integridad. Dado que el mensaje de arranque puede contener credenciales tales como nombre de usuario y contraseña, el atacante puede suplantar el dispositivo

.La figura 1 ilustra una vista de alto nivel de un proceso de arranque iniciado por el servidor, como se define en las especificaciones citadas anteriormente *OMA DM Bootstrap versión 1.2.1, OMA-TS-DM Bootstrap VI _ 2 _I*. El escenario de la figura 1 que describe el arranque iniciado por el servidor, muestra un dispositivo 10, un usuario 11, una red 12 y un servidor DM (DMS) 13. En *OMA-TS-DM Bootstrap VI 2_1,* se describe que una vez que el usuario 11 adquiere el dispositivo 10 y lo personaliza, por ejemplo insertando una SIM, quedan habilitados los requisitos previos para el proceso de arranque. El DMS 13 es notificado o informado de la identidad, dirección o número de teléfono del dispositivo 10 por ejemplo por la red 12 la primera vez que el dispositivo 10 se registra en la red 12. Cuando esto sucede, puede enviarse una solicitud para arrancar el dispositivo 10 desde la red (central) 12 al DMS 13 con el número utilizado por el dispositivo 10. El DMS 13 ahora está en una posición en la que puede enviar un mensaje de arranque OMA DM. Este mensaje de arranque contiene la información para que el dispositivo 10 pueda iniciar una sesión de gestión con DMS 13 que envió el mensaje de arranque.

La débil protección del escenario de arranque descrito anteriormente, se deriva del hecho de que el mensaje de arranque, como se mencionó anteriormente, solo está protegido con una clave no secreta (IMSI o ESN) como se indica en la sección 5.7.2.3.1 en *OMA Device Management Security 1.2.1, OMA-TS-DM Security-V1 _ 2 _1, OMA, 2008*. Por lo tanto, ni IMSI ni ESN se consideran un secreto compartido desde el punto de vista de la seguridad. Las especificaciones similares de OMA también adolecen de las mismas debilidades de seguridad, tales como *Enable Release Definition for OMA Client Provisioning Specifications versión 1.2. OMA-ERELD-ClientProvisioning-V1_1; y Provisioning Bootstrap 1.1. OMA-WAP-ProvBoot-V1_1.*

Cabe mencionar que estas vulnerabilidades de seguridad son las razones por las cuales el grupo de seguridad (SA3) en el proyecto de asociación de tercera generación (3GPP) emitió una fuerte recomendación de no utilizar el método/proceso de arranque iniciado por el servidor como se indica en la respuesta *3GPP LS reply S3-080262*.

Otra técnica anterior descrita en la solicitud de patente US 2008/0155071 propone un método y un sistema para el arranque de un dispositivo en una red de comunicaciones. En esta técnica anterior, un arranque iniciado por el servidor se utiliza para aprovisionar primero una tarjeta inteligente de un dispositivo que utiliza tecnología inalámbrica (OTA) para que el dispositivo pueda arrancar desde la tarjeta inteligente. Esto se realiza mediante la combinación de arranque por medio de la tarjeta inteligente con la función de detección automática del dispositivo 3GPP (ADD). La 3GPP ADD, que se define en la especificación técnica *3GPP TS 22.101,* permite la detección automática de un dispositivo cuando el dispositivo aparece en la red. Sin embargo, el método de esta técnica anterior todavía se basa en la falta de seguridad del arranque Iniciado por el Servidor especificado en la OMA DM actual como se describió anteriormente.

La técnica en relación con este campo técnico se describe, por ejemplo, en el documento normalizado 3GPP TS 33224, Nº V0.1.0 (2008-04), que describe un servicio iniciado por la red, en la que un operador puede actualizar la información sobre un dispositivo de manera segura, en el caso en el que el dispositivo no se haya puesto en contacto con el operador y no pueda ser activado de manera segura para realizar un arranque. En cambio, la información para la gestión del dispositivo se instala en el dispositivo de manera segura, en un instante fijo o durante un periodo predefinido

Compendio

Por lo tanto, es un objeto de las realizaciones de ejemplo de la presente invención abordar los problemas mencionados anteriormente y proporcionar aparatos y método que permitan la transmisión protegida de los mensajes de arranque desde un servidor DM a un dispositivo evitando que espías y/o atacantes suplanten el dispositivo y/o lo pirateen. La reivindicación 1 define una primera unidad de red de acuerdo con la invención, la reivindicación 4 define un dispositivo de acuerdo con la invención, la reivindicación 7 define un método de acuerdo con la invención y la reivindicación 10 define un programa de ordenador de acuerdo con la invención, con diversas realizaciones como se menciona en las reivindicaciones dependientes.

De acuerdo con un primer aspecto de las realizaciones de ejemplo de la presente invención, los problemas indicados anteriormente se resuelven por medio de una primera unidad de red de un sistema de red DM, para permitir la protección de un mensaje de arranque. La primera unidad de red comprende un receptor configurado para recibir un primer mensaje que comprende una solicitud para arrancar un dispositivo, el mensaje que comprende información que identifica el dispositivo y la información que identifica a un abonado. La primera unidad de red comprende además un transmisor configurado para enviar un segundo mensaje que comprende la información que identifica al abonado, a una segunda unidad de red, solicitando el segundo mensaje a la segunda unidad de red que proporcione a la primera unidad de red una clave de arranque que se base en la información que identifica al abonado. El receptor está configurado además para recibir desde la segunda unidad de red, un tercer mensaje que comprende la clave de arranque que se utilizará para la protección del mensaje de arranque. El tercer mensaje también comprende la información de activación que se transmite al dispositivo para activar la generación de la clave de arranque en el dispositivo.

Nada más recibir la información de activación desde la primera unidad de red, el dispositivo genera internamente la clave de arranque. Cuando tanto la primera unidad de red como el dispositivo están en posesión de la clave de arranque, la primera unidad de red protege, basándose en la clave de arranque, el mensaje de arranque y transmite el mensaje de arranque al dispositivo. De esta forma, un atacante no puede piratear o suplantar el dispositivo ya que la clave secreta de arranque es conocida solo por la red DM y el dispositivo.

De acuerdo con otro aspecto de las realizaciones de ejemplo de la presente invención, los problemas indicados anteriormente se resuelven mediante un método en una primera unidad de red de una red DM, para permitir la protección de un mensaje de arranque. El método comprende: recibir un primer mensaje que comprende una solicitud para arrancar un dispositivo, comprendiendo el primer mensaje información que identifica al dispositivo y a un abonado. El método comprende además, transmitir un segundo mensaje que comprende la información que identifica al abonado a una segunda unidad de red, solicitando a la segunda unidad de red que proporcione a la primera unidad de red una clave de arranque que se base en la información que identifica al abonado. El método comprende además, recibir desde la segunda unidad de red un tercer mensaje que comprende la clave de arranque, para permitir la protección del mensaje de arranque, comprendiendo el tercer mensaje además la

información de activación. El método comprende además, transmitir la información de activación al dispositivo para activar la generación de la clave de arranque en el dispositivo.

De acuerdo con otro aspecto más de las realizaciones de ejemplo de la presente invención, los problemas indicados anteriormente se resuelven por medio de un dispositivo capaz de comunicarse con una primera unidad de red de un sistema de red DM para permitir la protección de un mensaje de arranque. El dispositivo comprende medios para notificar a la primera unidad de información de red que identifica el dispositivo y un abonado. El dispositivo comprende además un receptor configurado para recibir desde la primera unidad de red, información de activación para activar la generación de la clave de arranque en el dispositivo. El receptor está configurado además para recibir un mensaje de arranque protegido basándose en la clave de arranque, y el dispositivo comprende medios para verificar y/o descifrar el mensaje de arranque de protección, protegido.

Una ventaja de las realizaciones de ejemplo de la presente invención es evitar que los atacantes pirateen un dispositivo y/o lo suplanten.

Otra ventaja de las realizaciones de ejemplo de la presente invención es asegurarse de utilizar una clave de arranque verdaderamente secreta que solo sea conocida por la red y por el dispositivo.

Además otras ventajas, objetivos y características de las realizaciones de la presente invención resultarán evidentes a partir de la siguiente descripción detallada junto con los dibujos que se adjuntan, prestando atención al hecho, sin embargo, de que los siguientes dibujos son solo ilustrativos, y pueden realizarse diversas modificaciones y cambios en las realizaciones específicas ilustradas como se describe dentro del alcance de las reivindicaciones adjuntas. Se debe entender además que los dibujos no están necesariamente dibujados a escala y que, a menos que se indique lo contrario, simplemente están destinados a ilustrar conceptualmente las estructuras y procedimientos descritos en este documento.

Breve descripción de los dibujos

La figura 1 es una vista de alto nivel según la técnica anterior de la señalización implicada durante un procedimiento de arranque iniciado por el servidor.

La figura 2 es un diagrama de flujo para habilitar el arranque seguro iniciado por el servidor de un dispositivo de acuerdo con una realización de ejemplo de la presente invención.

La figura 3 es otro diagrama de flujo para el arranque seguro iniciado por el servidor de un dispositivo de acuerdo con otra realización de ejemplo de la presente invención.

La figura 4 es un diagrama que ilustra un diagrama de flujo de un método para su uso en una primera unidad de red de acuerdo con las realizaciones de ejemplo de la presente invención.

La figura 5 ilustra un diagrama de bloques de una unidad de red de ejemplo de acuerdo con realizaciones de ejemplo de la presente invención.

La figura 6 ilustra un diagrama de bloques de un dispositivo de ejemplo de acuerdo con realizaciones de ejemplo de la presente invención.

Descripción detallada

En la siguiente descripción, con el propósito de explicación y no limitativo, se exponen detalles específicos tales como arquitecturas particulares, escenarios, técnicas, etc. con el fin de proporcionar una comprensión completa de la presente invención. Sin embargo, a partir de lo siguiente, será evidente que la presente invención y sus realizaciones se pueden poner en práctica en otras realizaciones aunque se aparten de estos detalles específicos.

Las realizaciones de ejemplo de la presente invención se describen en este documento a modo de referencia en escenarios de ejemplo en particular. En concreto, la invención se describe en un contexto general no limitativo en relación con el escenario de arranque iniciado por el servidor en un sistema de red de gestión de dispositivos (DM) que comprende el servidor DM (DMS) que interactúa con una arquitectura genérica de arranque (GBA) de acuerdo con especificaciones de instalación GBA en las especificaciones técnicas 3GPP TS 33.223. El DMS se denominará en adelante como una primera unidad de red. Sin embargo, se ha de tener en cuenta que la primera unidad de red puede ser cualquier unidad de red o nodo adecuado capaz de ejecutar las realizaciones de ejemplo de la presente invención. Dicha unidad de red puede, por ejemplo, estar representada por un proxy DM en lugar de un DMS.

Con referencia a la figura 2, se ilustra un diagrama de flujo para habilitar el arranque seguro iniciado por el servidor de un dispositivo en un sistema de red, de acuerdo con una realización de ejemplo de la presente invención. Las entidades que se muestran son: el dispositivo 20, una entidad de red (o entidades) 21 (por ejemplo, un registro de ubicación de origen), una primera unidad de red 22 y una segunda unidad de red 23. Como se ilustrará y describirá más adelante, también se pueden usar nodos/funciones adicionales con fines de arranque seguro de un dispositivo.

Como se muestra en la figura 2, el dispositivo 20 notifica a la red 21 su disponibilidad (S21). Esto puede ser realizado por el usuario/abonado al conectar el dispositivo 20 que intenta conectarse a la red 21. Por medio, por ejemplo, de los métodos conocidos de detección automática de dispositivos (ADD), como se describe en *3GPP TS 22.101*, o los procedimientos conocidos iniciados por el usuario como se describe en *GBA Push 3GPP TS 33.223,* la red 21 detecta la presencia/disponibilidad del dispositivo 20 (S22). Tras la conexión a la red 21, el dispositivo 20 envía la información que identifica el dispositivo, es decir, su identidad, por ejemplo, el IMEI y también envía la información que identifica al abonado, por ejemplo, el IMSI/ESN. En la solicitud de arranque (S23) la red 21 solicita a la primera unidad de red 22 que arranque el dispositivo 20. En la solicitud de arranque (S23), la red 21 (por ejemplo, HLR) incluye la información que identifica el dispositivo (IMEI) y la información que identifica el abonado, es decir, el IMSI/ESN, MSISDN, etc. Cuando la primera unidad de red 22 recibe la solicitud, y basándose en la información que identifica el dispositivo y el usuario/abonado, la primera unidad de red 22 determina si se puede usar GBA PUSH hacia el dispositivo. Si es así, la primera unidad de red 22 transmite un mensaje (S24) a la segunda unidad de red 23 solicitando a la segunda unidad de red 23 que proporcione a la primera unidad de red 22 una clave de arranque. La segunda unidad de red 23 que es parte del subsistema de GBA comprende una función de servidor de arranque (BSF) y un servidor de abonado doméstico (HSS).

Se debe mencionar que si la primera unidad de red 22 determinó que GBA PUSH puede usarse hacia el dispositivo, una función de aplicación de red (NAF) de la primera unidad de red 22 está configurada para contactar con la BSF usando los procedimientos GBA PUSH para solicitar, usando el mensaje (S24), al menos una información de activación y una clave de arranque. La información de activación corresponde a la información (GPI) GBA PUSH. El mensaje (S24) también comprende la identidad de la NAF. Sin embargo, es preciso tener en cuenta que la primera unidad de red 22 está configurada para seleccionar un método para iniciar el dispositivo 20, estando entonces GBA PUSH basada en uno de los seguros. Se debe seleccionar GBA PUSH, basándose en la información que identifica el dispositivo y el abonado, entonces la NAF de la primera unidad de red 22 gestiona el proceso de arranque seguro. A continuación se describe el caso en el que se puede usar GBA PUSH hacia el dispositivo 20, es decir, el mensaje de solicitud (S24) llega a la segunda unidad de red 23.

Con referencia de nuevo a la figura 2, cuando la segunda unidad de red (23) recibe el mensaje de petición (S24), genera la clave de arranque (S25) y envía o entrega la clave de arranque y al menos la GPI a la primera unidad de red (22) en un mensaje de respuesta (S26) denominado aquí como respuesta GPI. Ahora que la primera unidad de red 22 está en posesión de la respuesta de GPI, transmite o reenvía la información de activación, es decir, la parte de GPI en la respuesta de GPI al dispositivo 20 (S27). La primera unidad de red 22 también puede almacenar la clave de arranque antes de transmitir la GPI al dispositivo 20. La GPI o la información de activación se pueden transmitir a través de SMS, WAP, HTTP, inserción de SIP o cualquier portador adecuado para transportar la información de activación para activar la generación de la clave de arranque en el dispositivo 20. Tras la recepción de la GPI, el dispositivo 20 genera la clave de arranque (S28) usando los procedimientos normalizados adecuados.

En *GBA Push 3GPP TS 33.223,* se describe que la GPI está protegida. Esto se conoce como protección de integridad de GPI y protección de confidencialidad de GPI. Y que en GBA la clave de arranque se denomina Ks_NAF y esta clave también se conoce como material clave o material de claves. Ks_NAF se describe en *3GPP TS 33.220 V8.5.0* a la que se hace referencia en la técnica anterior anteriormente mencionada *GBA Push 3GPP TS 33.223.* A lo largo de la descripción, se utilizará una clave de arranque para denominar Ks_NAF o material clave o de claves.

Con referencia de nuevo a la figura 2, cuando el dispositivo 20 genera la clave de arranque (S28) almacena la clave de arranque Posteriormente, la primera unidad de red 22 puede realizar un arranque seguro protegiendo y transmitiendo un mensaje de arranque que está protegido basándose en la clave de arranque (S29). La primera unidad de red 22 puede proteger directamente el mensaje de arranque utilizando la clave de arranque o puede derivar otras claves usando la clave de arranque y usar estas claves para proteger el mensaje de arranque. Obsérvese que si la primera unidad de red 22 ha cifrado el mensaje de arranque antes de transmitirlo al dispositivo 20, el dispositivo 20 necesita primero descifrar el mensaje de arranque y luego verificar el mensaje. La clave de arranque puede en lugar delMSI/ESN, utilizarse para la protección de la integridad y/o se puede usar para la protección de la confidencialidad. Tras el arranque satisfactorio y seguro del dispositivo, las sesiones de DM pueden comenzar entre el dispositivo 20 y la primera unidad de red 22. Obsérvese que la clave de arranque también se puede utilizar como clave maestra para generar claves que se puedan usar para proteger una o más sesiones de DM entre el dispositivo 20 y la primera unidad de red 22, por ejemplo, la autenticación, después de la verificación/descifrado satisfactorios del mensaje de arranque.

Con referencia a la figura 3, se ilustra un diagrama de flujo para habilitar el arranque seguro iniciado por el servidor de un dispositivo en un sistema de red, de acuerdo con otra realización de ejemplo de la presente invención. De manera similar a la figura 2, el sistema de red comprende un dispositivo 30, una red 31 (por ejemplo, HLR), una primera unidad de red 32 (por ejemplo, DMS con una NAF) y una segunda unidad de red 33 que comprende una BSF 33A y un HSS 33B. La figura 3 también representa un usuario 30A. En (S31A), tras la conexión a la red 31, el dispositivo 30 envía la información que identifica el dispositivo, IMEI, y también envía la información que identifica al usuario/abonado (por ejemplo IMSI). Como se mencionó anteriormente, esto se puede hacer usando algún tipo de procedimiento ADD y/o procedimiento iniciado por el usuario. Debe mencionarse que un usuario/abonado 30A

puede notificar alternativamente a la red 31 acerca del IMEI y del IMSI (S31B). Esto puede ser realizado por un vendedor en una consola de punto de venta o por el propio usuario final por medio de un interfaz web o usando, por ejemplo, tonos DMTF.

En (S32), cuando la red 31 ha detectado el dispositivo/usuario/abonado identificado por, por ejemplo, por IMSI/ESN, MSISDN e IMEI, la red 31 envía una solicitud para arrancar el dispositivo 30, a la primera unidad de red 32 (por ejemplo, DMS (NAF)) e incluye en la solicitud el IMEI, IMSI (o ESN) y MSISDN. Como se mencionó anteriormente, la primera unidad de red 32 o la NAF de la primera unidad de red 32 primero determina basándose en el dispositivo y en la información del usuario/abonado si se puede utilizar GBA PUSH hacia el dispositivo 30. Si es así, la parte NAF de la primera unidad de red 32 envía una solicitud GPI (S33) utilizando procedimientos GBA PUSH, a la BSF 33A de la segunda unidad de red 33, para solicitar una respuesta GPI. La solicitud (S33) comprende la información que identifica al abonado, por ejemplo, el IMSI y al menos la identidad de la NAF (DMS_NAS_Id). Cuando la BSF 33A recibe la solicitud, procesa la solicitud (S34) e identifica al usuario/abonado. A partir de entonces, la BSF 33A envía una solicitud (S35) al HSS 33B de la segunda unidad de red 33, solicitando al HSS 33B un vector de autenticación (AV) para el dispositivo 30. En la solicitud AV (S35), se indica el IMPI. En (S36), el HSS 33B devuelve el AV solicitado en una respuesta AV. La BSF 33A luego genera (S37) una clave de arranque que es una clave de arranque DMS NAF y almacena la clave. La BSF 33A envía (S38) una respuesta GPI que comprende la clave de arranque y al menos una GPI que comprende parámetros GPI, a la primera unidad de red 32. La primera unidad de red 32 almacena la clave de arranque (S39) y prepara un paquete GPI que comprende la información de activación (es decir, GPI) antes de enviar el paquete GPI al dispositivo 30 (S40). Como se mencionó anteriormente, puede usarse cualquier portador adecuado para transportar la GPI al dispositivo 30, por ejemplo, GPI sobre WAP PUSH o SMS o SIP, etc. El MSISDN se puede usar para direccionar el dispositivo 30.

Cuando el dispositivo 30 recibe la GPI, el dispositivo 30 genera internamente la clave de arranque DMS NAF (S41) y el dispositivo 30 almacena la clave de arranque (S42). A partir de ahí, un mensaje de arranque está protegido por la primera unidad de red 32 basándose en la clave de arranque, y transmite el mensaje de arranque protegido al dispositivo 30 (no mostrado). El dispositivo luego verifica y/o descifra el mensaje de arranque. Si la verificación y/o el descifrado son satisfactorios, comienzan las sesiones de DM entre el dispositivo y la primera unidad de red (no mostrada). De esta manera, solo la primera unidad de red y el dispositivo conocen la clave de arranque, lo que impide que los espías y los atacantes se apropien del dispositivo o lo suplanten.

De forma similar a la realización de ejemplo descrita anteriormente, tanto la primera unidad de red como el dispositivo pueden usar la clave de arranque para generar claves adicionales. La primera unidad de red usa las claves adicionales para proteger el mensaje de arranque y el dispositivo puede usar las claves adicionales para verificar y/o descifrar el mensaje de arranque

Con referencia a la figura 4, se ilustran las etapas principales del método o procedimiento, en una primera unidad de red, para habilitar la protección de un mensaje de arranque de acuerdo con las realizaciones de ejemplo descritas previamente de la presente invención. Como se muestra en la figura 4, las etapas principales del método comprenden:

(401) recibir, un primer mensaje (es decir, una solicitud para arrancar un dispositivo) que comprende la información que identifica el dispositivo y la información que identifica a un abonado;

…(402) transmitir un segundo mensaje (por ejemplo, una solicitud GPI) que comprende la información que identifica al abonado, a una segunda unidad de red, solicitando a la segunda unidad de red que proporcione a la primera unidad de red una clave de arranque basándose en la información que identifica al abonado;

(403) recibir, desde la segunda unidad de red, un tercer mensaje (por ejemplo, respuesta GPI) que comprende la clave de arranque y una información de activación (es decir, GPI), para habilitar la protección del mensaje de arranque;

(404) transmitir la información de activación al dispositivo para activar la generación de la clave de arranque internamente en el dispositivo.

Ya se han descrito etapas adicionales del método y funciones de la primera unidad de red y por lo tanto, no se repetirán.

Con referencia a la figura 5, se ilustra un diagrama de bloques de una primera unidad de red de ejemplo 500, por ejemplo, un DMS, de un sistema de red DM, para habilitar la protección de un mensaje de arranque, de acuerdo con las realizaciones de ejemplo descritas previamente de la presente invención. Como se muestra en la figura 5, la primera unidad de red 500 comprende un receptor 510 (RX) configurado para recibir un primer mensaje que comprende una solicitud para arrancar un dispositivo. El primer mensaje comprende la información que identifica el dispositivo y el abonado. La primera unidad de red 500 comprende además un transmisor 520 (TX) configurado para transmitir un segundo mensaje (por ejemplo, solicitud GPI) que comprende la información que identifica al abonado, a una segunda unidad de red (por ejemplo, BSF + HSS), solicitando a la segunda unidad de red que proporcione la clave de arranque. El receptor 510 de la primera unidad 500 de red está configurado además para

recibir un tercer mensaje (es decir, respuesta GPI) que comprende la clave de arranque para habilitar la protección del mensaje de arranque. El tercer mensaje comprende además una información de activación (es decir, GPI). El transmisor 520 de la primera unidad de red 500 está configurado además para transmitir la información de activación al dispositivo para activar la generación de la clave de arranque en el dispositivo. La primera unidad de red 500 comprende además medios de almacenamiento 530 para almacenar la clave de arranque. La primera unidad de red 500 comprende además una lógica/unidad de procesamiento 540 configurada para determinar si GBA PUSH puede usarse hacia el dispositivo y está configurada además para generar claves adicionales basadas en la clave de arranque, y para proteger el mensaje de arranque. Los medios de almacenamiento 530 y la lógica/unidad de procesamiento 540 se muestran como parte de un sistema de procesamiento 550, aunque esto no sea necesario.

Aunque la figura 5 muestra componentes de ejemplo de la primera unidad de red 500, en otras ejecuciones, la primera unidad de red 500 puede contener menos, diferentes o adicionales componentes de los que se muestran en la figura 5. En otras ejecuciones, uno o más componentes de la unidad 500 pueden realizar las tareas descritas como realizadas por uno o más de otros componentes de la primera unidad de red 500.

Con referencia a la figura 6, se ilustra un diagrama de componentes de ejemplo del dispositivo 600 de acuerdo con algunas realizaciones de ejemplo de la presente invención. Como se ilustra, el dispositivo 600 comprende un transceptor 610 que comprende medios para notificar a una primera unidad de red (de la figura 5) del sistema de red DM de la información que identifica el dispositivo y el abonado para habilitar la protección de un mensaje de arranque. Los medios para la notificación pueden verse como un transmisor del transceptor 610. El transceptor 610 comprende además un receptor configurado para recibir de la primera unidad de red la información de activación (es decir, GPI) para activar la generación de una clave de arranque internamente en el dispositivo. El receptor del transceptor 610 está configurado además para recibir un mensaje de arranque protegido como la primera unidad de red protegida basándose en la clave de arranque. También se muestra una antena 620 conectada al transceptor 610. El dispositivo 600 comprende además medios para verificar y/o descifrar el mensaje de arranque protegido. La unidad/medios de procesamiento 630 del dispositivo 600 está configurada para generar la clave de arranque y para realizar la verificación/descifrado del mensaje de arranque protegido. El dispositivo 600 puede incluir varias antenas (solo se muestra una antena 620) una memoria o medios de almacenamiento 640 para almacenar la clave de arranque, un(os) dispositivo(s) de entrada 650, un(os) dispositivo(s) de salida 660 y un bus 670. Aunque la figura 6 muestra componentes de ejemplo del dispositivo 600, en otras ejecuciones, el dispositivo 600 puede contener menos, diferentes o adicionales componentes que los representados en la figura 6.

La presente invención y sus realizaciones de ejemplo se pueden realizar de muchas maneras. Por ejemplo, una realización de la presente invención incluye medios interpretables por ordenador que tienen instrucciones de programa almacenadas en los mismos que son ejecutables por un ordenador de la primera unidad de red para llevar a cabo las etapas del método de las realizaciones de ejemplo de la presente invención como se describieron previamente.

Aunque la invención se ha descrito en términos de varias realizaciones preferidas, se contempla que las alternativas, modificaciones, permutaciones y equivalencias de las mismas resultarán evidentes para los expertos en la materia al leer las especificaciones y tras el estudio de los dibujos. Por lo tanto, se pretende que el alcance de la invención incluya tales alternativas, modificaciones, permutaciones y equivalencias que caigan dentro de las definiciones de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Una primera unidad de red (500, 22, 32) de una gestión de dispositivos, DM, sistema de red, para proteger un mensaje de arranque, comprendiendo la primera unidad de red (500, 22, 32):

- un receptor (510) configurado para recibir desde una entidad de red (21, 31), cuando la entidad de red detecta un dispositivo, un primer mensaje que comprende una solicitud para arrancar un dispositivo detectado (600, 20, 30), comprendiendo dicho primer mensaje la información que identifica el dispositivo (600, 20, 30) y la información que identifica a un abonado;

- un transmisor (520) configurado para enviar un segundo mensaje que comprende la información que identifica a dicho abonado a una segunda unidad de red (23, 33), solicitando dicho segundo mensaje a la segunda unidad de red que proporcione a la primera unidad de red (500, 22, 32) una clave de arranque basada en la información que identifica al abonado, en la que:

- dicho receptor (510) está configurado además para recibir, desde la segunda unidad de red (23, 33), un tercer mensaje que comprende dicha clave de arranque, para proteger el mensaje de arranque, comprendiendo dicho tercer mensaje además la información de activación,

- la primera unidad de red comprende además medios de almacenamiento (530) configurados para almacenar la clave de arranque,

- la primera unidad de red está configurada para proteger, basándose en la clave de arranque, el mensaje de arranque,

- el transmisor (520) está configurado además para transmitir el mensaje de arranque protegido al dispositivo detectado (600,20,30),

- dicho transmisor (520) está configurado además para transmitir la información de activación al dispositivo (detectado 600, 20, 30) para activar la generación de la clave de arranque en el dispositivo detectado (600, 20, 30);

- la primera unidad de red está adaptada para establecer una sesión DM entre el dispositivo 'detectado (600, 20, 30) y la primera unidad de red.

2. La primera unidad de red (500, 22, 32) de acuerdo con la reivindicación 1, en la que dicho transmisor (520) está configurado para transmitir la información de activación en una información genérica de arranque originada en el servidor, GPI, mensaje, y en la que dicho receptor (510) está configurado para recibir dicho tercer mensaje que comprende la clave de arranque en un mensaje de respuesta GPI.

3. La primera unidad de red (500) de acuerdo con cualquiera de las reivindicaciones 1-2 que está configurada además para usar la clave de arranque como una clave maestra para generar claves adicionales para proteger al menos un mensaje durante al menos una sesión de DM entre el dispositivo (600) y el sistema de red de DM, después de verificar el mensaje de arranque.

4. Un dispositivo (600, 20, 30) para la comunicación con una primera unidad de red (500, 22, 32) de una gestión de dispositivos, DM, sistema de red, para proteger un mensaje de arranque, comprendiendo el dispositivo (600, 20, 30):

- medios (610) para notificar a la primera unidad de red (500, 22, 32) la información que identifica el dispositivo y la información que identifica a un abonado, después de haber notificado a una entidad de red (21, 31) la disponibilidad del dispositivo,

- un receptor (610) configurado para recibir, desde la primera unidad de red (500, 22, 32), la información de activación para activar la generación de una clave de arranque en el dispositivo, en el que:

- el dispositivo está adaptado para generar una clave de arranque al recibir la información de activación,

- dicho receptor (610) está configurado además para recibir un mensaje de arranque protegido, estando dicho mensaje de arranque protegido basado en la clave de arranque; y

- el dispositivo comprende medios (630) para verificar y descifrar el mensaje de arranque protegido, y

- el dispositivo está adaptado para establecer una sesión de DM entre el dispositivo y la primera unidad de red después de verificar y descifrar el mensaje de arranque protegido.

5. El dispositivo (600, 20, 30) de acuerdo con la reivindicación 4, en el que dicho receptor (610) está configurado para recibir la información de activación en una arquitectura de arranque genérica, GBA, información originada en el servidor, GPI, mensaje.

6. El dispositivo (600, 20, 30) de acuerdo con la reivindicación 4 o 5, que comprende además medios de almacenamiento (640) configurados para almacenar la clave de arranque.

7. Un método en una primera unidad de red (500, 22, 32) de un sistema de red de gestión de dispositivos, DM, sistema de red, para proteger un mensaje de arranque, comprendiendo el método

- (401) recibir, desde una entidad de red (21, 31), cuando la entidad de red detecta un dispositivo (600, 20, 30), un primer mensaje que comprende una solicitud para arrancar un dispositivo detectado, comprendiendo dicho primer mensaje la información que identifica dicho dispositivo y la información que identifica a un abonado;

- (402) transmitir un segundo mensaje que comprende la información que identifica a dicho abonado a una segunda unidad de red (23, 33), solicitando dicho segundo mensaje a la segunda unidad de red que proporcione a la primera unidad de red una clave de arranque basada en la información que identifica al abonado;

- (403) recibir, desde la segunda unidad de red (23, 33), un tercer mensaje que comprende dicha clave de arranque, para proteger el mensaje de arranque, comprendiendo dicho tercer mensaje además la información de activación;

- almacenar la clave de arranque en dicha primera unidad de red (500, 21, 31)

-protegiendo, basándose en la clave de arranque,

- transmitir el mensaje de arranque al dispositivo detectado después de proteger el mensaje de arranque,

- (404) transmitir dicha información de activación al dispositivo detectado, para activar la generación de la clave de arranque en el dispositivo, y

- establecer una sesión DM entre el dispositivo detectado (600, 20, 30) y la primera unidad de red.

8. El método de acuerdo con la reivindicación 7, en el que dicha transmisión (404) de la información de activación comprende transmitir dicha información de activación en una arquitectura de arranque genérica, información originada en el servidor, GPI, mensaje, y en el que dicha recepción (403) del tercer mensaje comprende recibir dicho tercer mensaje en un mensaje de respuesta GPI.

9. El método de acuerdo con cualquiera de las reivindicaciones 7-8 que comprende además el uso de la clave de arranque como una clave maestra para generar claves adicionales para proteger al menos un mensaje durante al menos una sesión DM entre el dispositivo y el sistema de red DM, después de la verificación del mensaje de arranque.

10. Un programa de ordenador que comprende instrucciones de programa para hacer que un ordenador realice el método de cualquiera de las reivindicaciones del método 7 - 9 cuando dicho programa se ejecuta en un ordenado

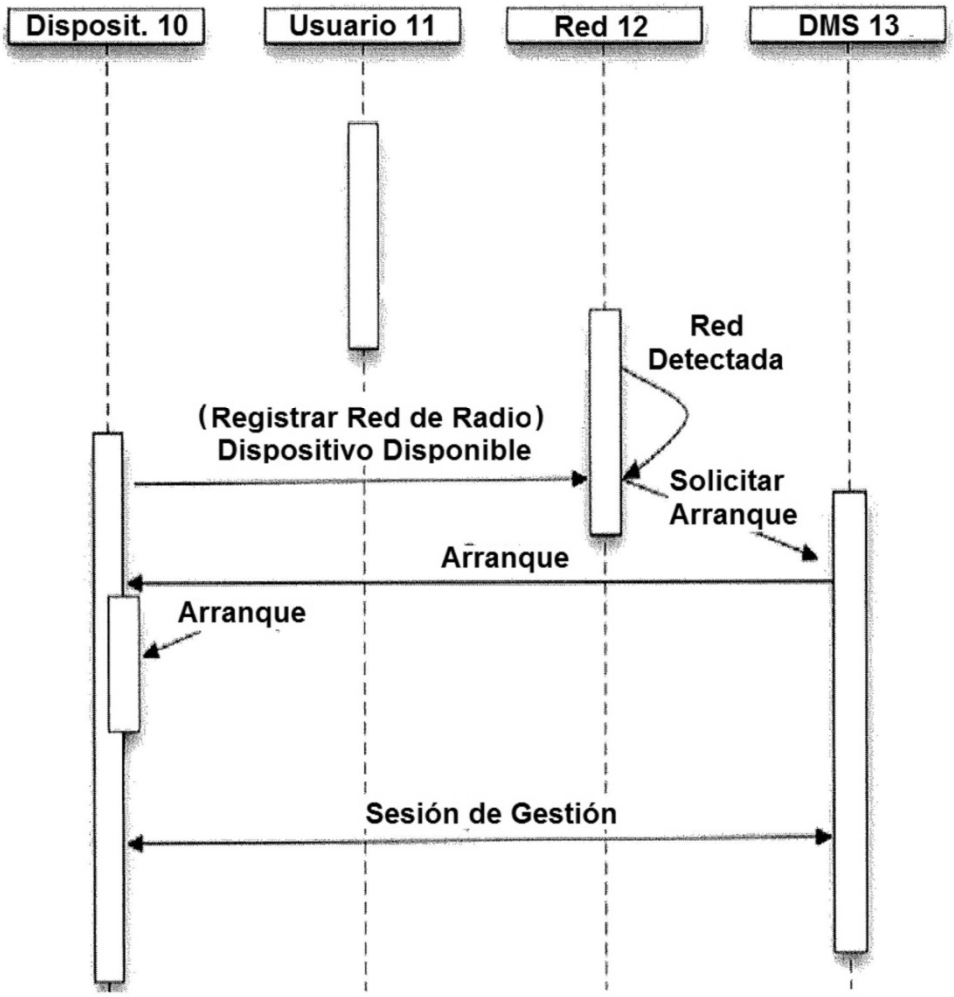
Disposit. 10
Usuario 11
Red 12
DMS 13
Red
Detectada
(Registrar Red de Radio)
Dispositivo Disponible
Solicitar
Arranque
Arranque
Arranque
Sesión de Gestión

FIGURA 1

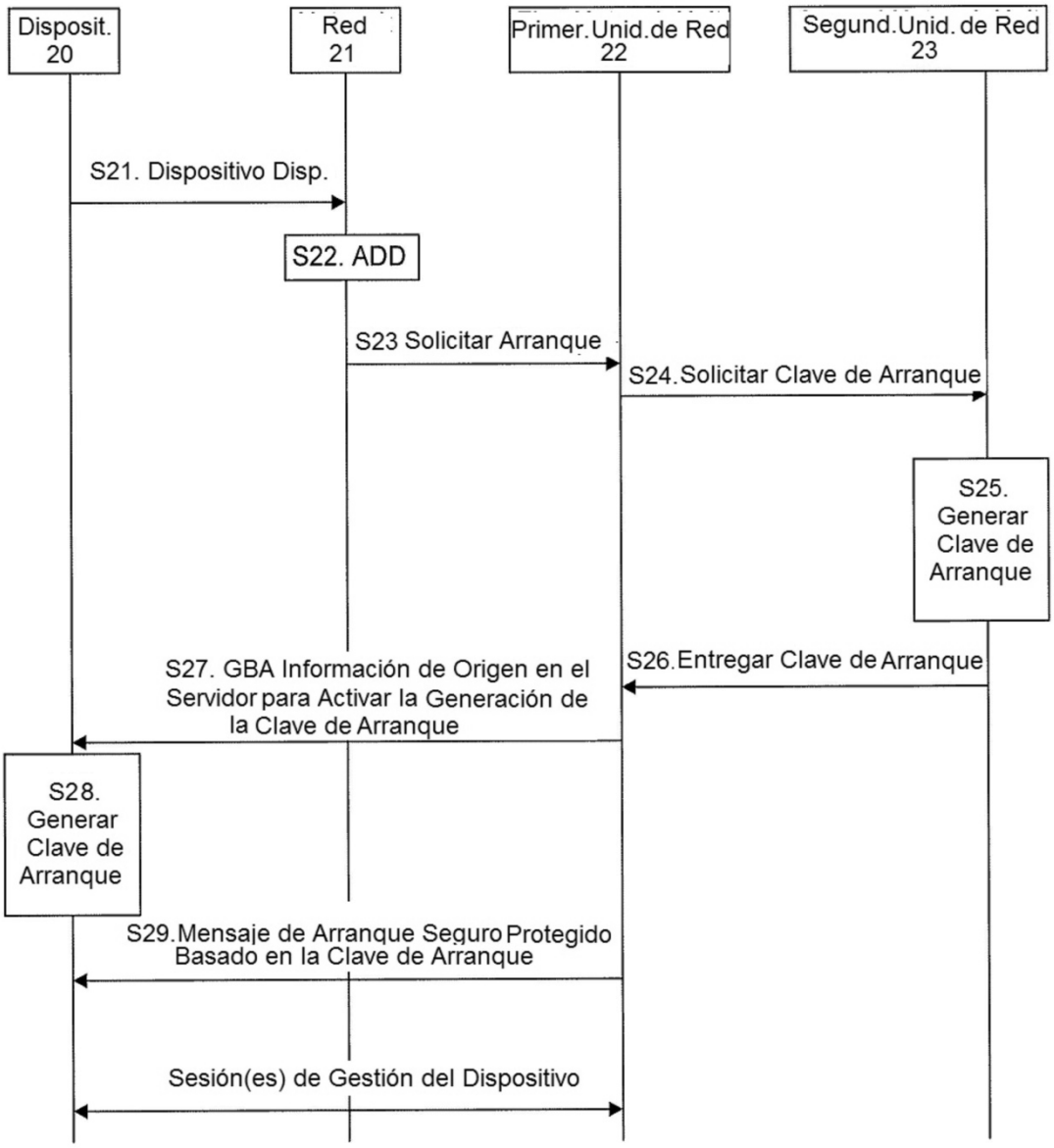
Disposit. 20
Red 21
Primer.Unid.de Red 22
Segund.Unid. de Red 23
S21. Dispositivo Disp.
S22. ADD
S23 Solicitar Arranque
S24.Solicitar Clave de Arranque
S25. Generar Clave de Arranque
S26.Entregar Clave de Arranque
S27. GBA Información de Origen en el Servidor para Activar la Generación de la Clave de Arranque
S28. Generar Clave de Arranque
S29.Mensaje de Arranque Seguro Protegido Basado en la Clave de Arranque
Sesión(es) de Gestión del Dispositivo

FIGURA 2

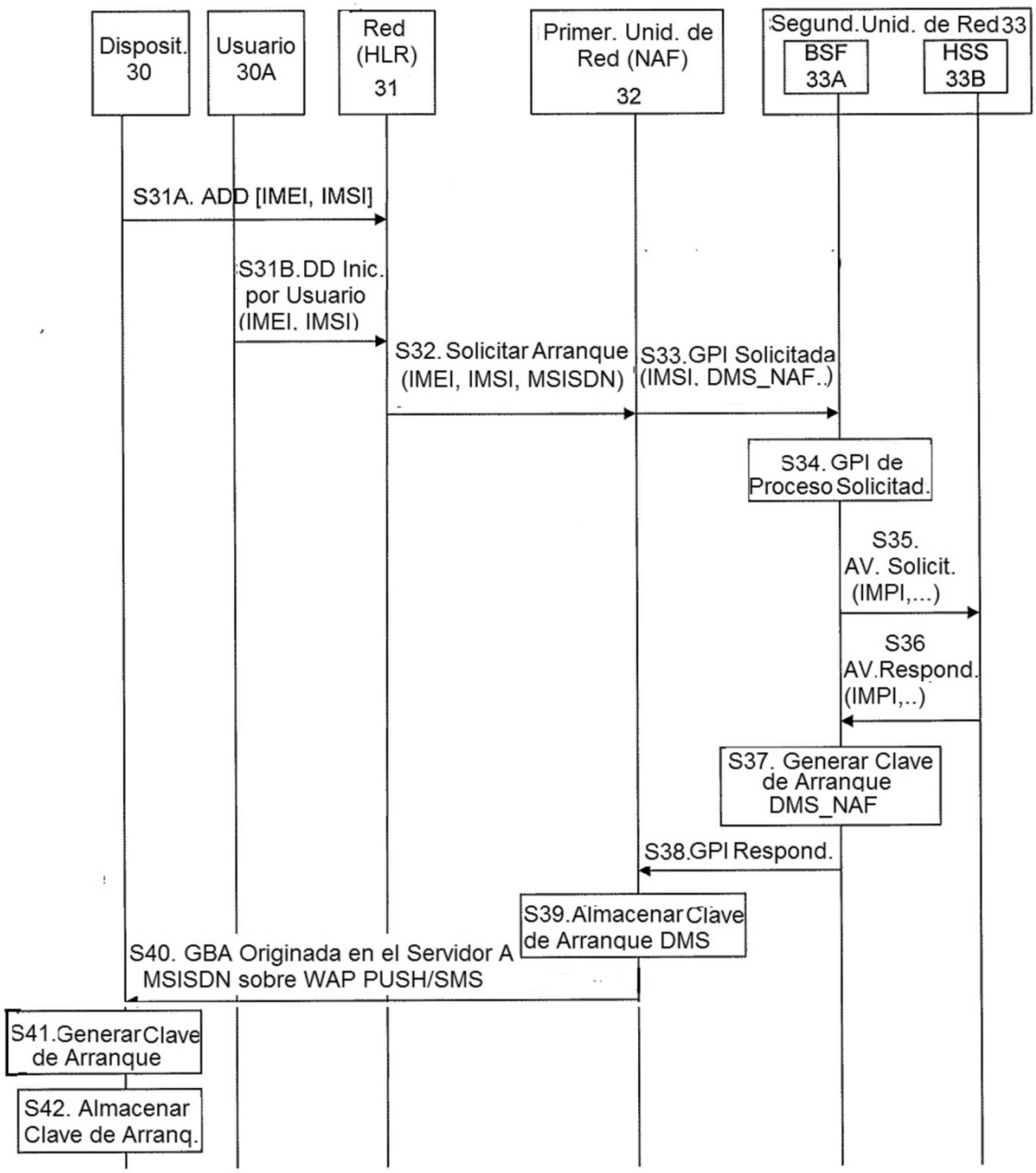
Disposit. 30
Usuario 30A
Red (HLR) 31
Primer. Unid. de Red (NAF) 32
Segund. Unid. de Red 33
BSF 33A
HSS 33B
S31A. ADD [IMEI, IMSI]
S31B. DD Inic. por Usuario (IMEI, IMSI)
S32. Solicitar Arranque (IMEI, IMSI, MSISDN)
S33. GPI Solicitada (IMSI, DMS_NAF..)
S34. GPI de Proceso Solicitad.
S35. AV. Solicit. (IMPI,...)
S36 AV. Respond. (IMPI,..)
S37. Generar Clave de Arranque DMS_NAF
S38. GPI Respond.
S39. Almacenar Clave de Arranque DMS
S40. GBA Originada en el Servidor A MSISDN sobre WAP PUSH/SMS
S41. Generar Clave de Arranque
S42. Almacenar Clave de Arranq.

FIGURA 3

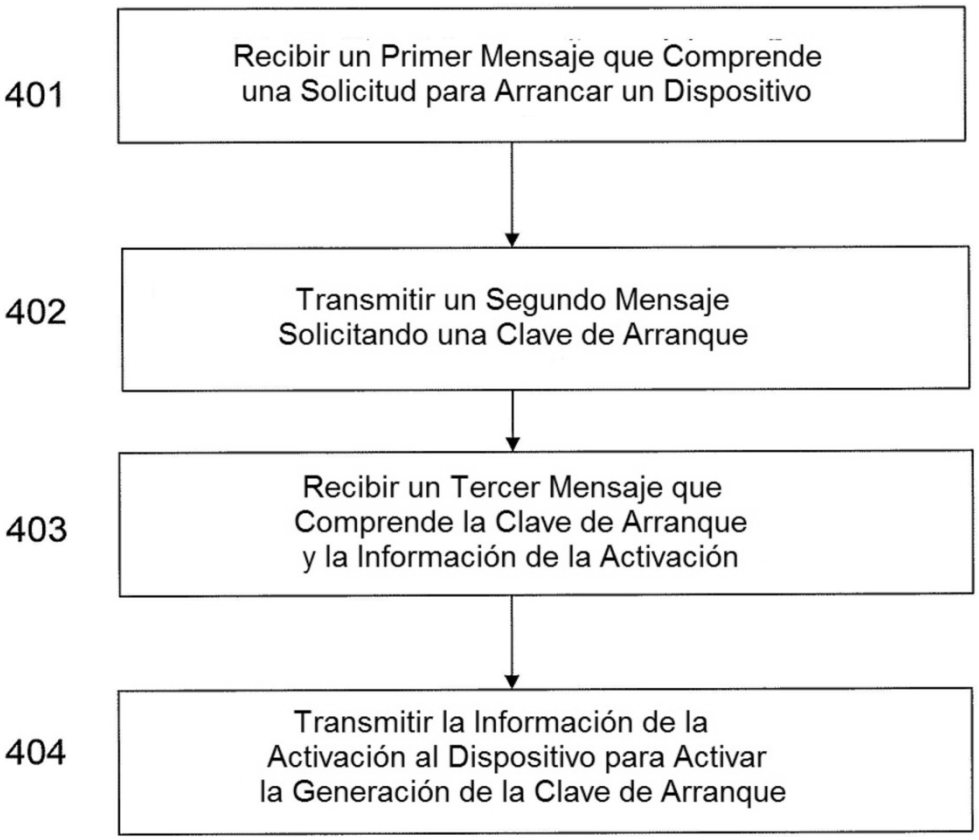
401
Recibir un Primer Mensaje que Comprende una Solicitud para Arrancar un Dispositivo
402
Transmitir un Segundo Mensaje Solicitando una Clave de Arranque
403
Recibir un Tercer Mensaje que Comprende la Clave de Arranque y la Información de la Activación
404
Transmitir la Información de la Activación al Dispositivo para Activar la Generación de la Clave de Arranque

FIGURA 4

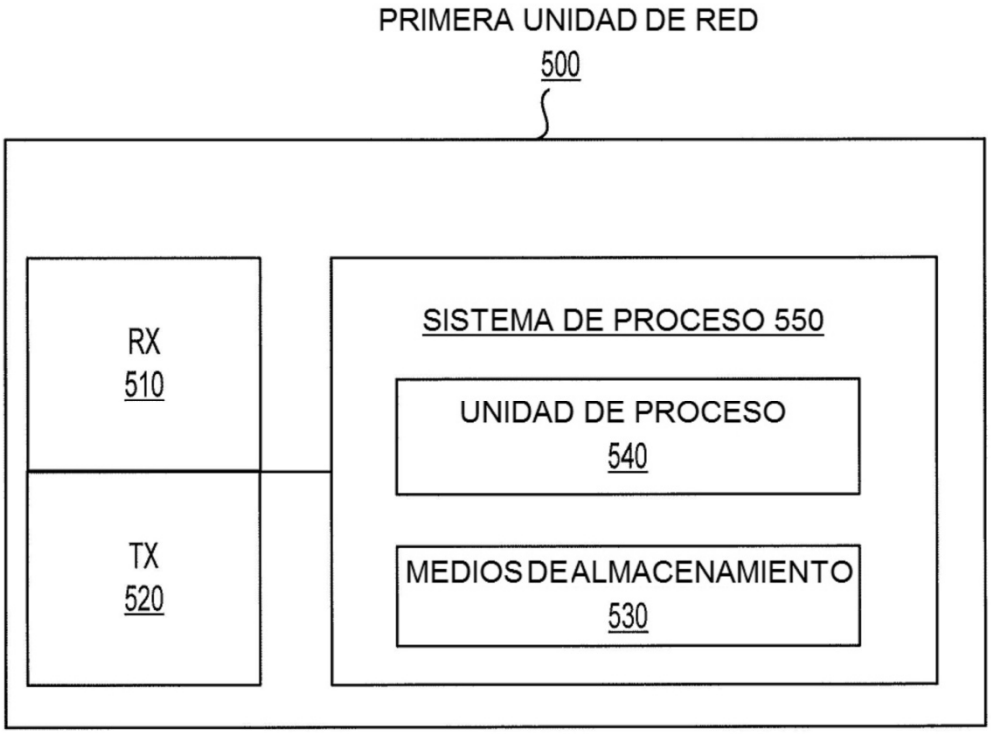
PRIMERA UNIDAD DE RED
500
RX
510
TX
520
SISTEMA DE PROCESO 550
UNIDAD DE PROCESO
540
MEDIOS DE ALMACENAMIENTO
530

FIGURA 5

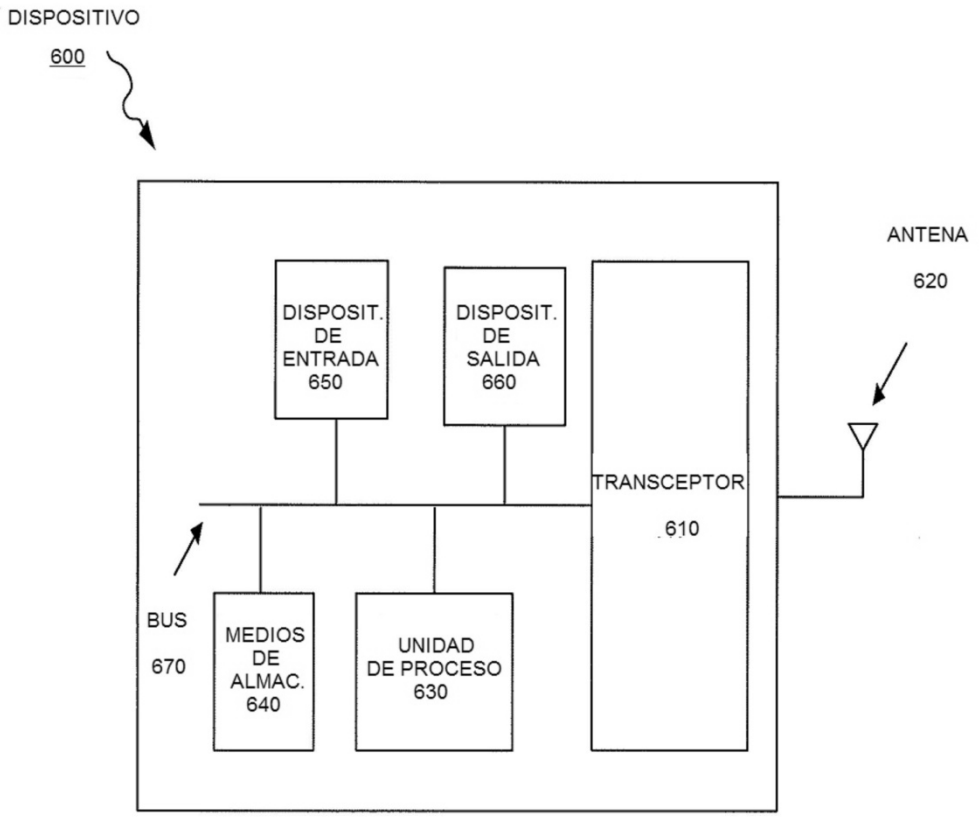
DISPOSITIVO
600
ANTENA
620
DISPOSIT. DE ENTRADA 650
DISPOSIT. DE SALIDA 660
TRANSCEPTOR
610
BUS
670
MEDIOS DE ALMAC. 640
UNIDAD DE PROCESO 630

FIGURA 6