(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 536 844**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.03.2012 E 12738008 (7)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2015 EP 2523421**

(54) Título: **Método y sistema de protección de la privacidad de comunicación de máquina a máquina y capa de capacidad del servicio de comunicación de máquina a máquina y dispositivo correspondiente**

(30) Prioridad:

11.03.2011 CN 201110059215

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.05.2015

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

JIN, LEI;
BIAN, YONGGANG;
ZHANG, YONGJING;
CHEN, XIANFENG;
LIN, QI y
MOU, LUNJIAN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y sistema de protección de la privacidad de comunicación de máquina a máquina y capa de capacidad del servicio de comunicación de máquina a máquina y dispositivo correspondiente

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de las comunicaciones y en particular, a un método y sistema de protección de la privacidad de comunicaciones de máquina a máquina, una entidad de gestión de servicio de comunicaciones de máquina a máquina y un dispositivo correspondiente.

ANTECEDENTES DE LA INVENCIÓN

Las comunicaciones de máquina a máquina (Machine-to-Machine Communications, M2M) es una aplicación basada en red y servicio que tiene como objetivo la interacción de máquina inteligente. En las comunicaciones de máquina a máquina M2M, un módulo de comunicaciones cableadas o inalámbricas y la lógica de procesamiento de aplicación están incorporadas en una máquina para realizar la comunicación de datos sin necesidad de intervención manual, con el fin de satisfacer los requisitos de informatización de un usuario en aspectos tales como supervisión, control y expedición de recogida de datos y de medición. La Figura 1-a ilustra una arquitectura típica del dispositivo M2M, en donde varios terminales M2M (a modo de ejemplo, un sensor y un microcontrolador) acceden a una entidad de gestión de servicio M2M (Capa de Capacidad de Servicio, SCL), directamente o a distancia por intermedio de una pasarela M2M y en varias aplicaciones de M2M (a modo de ejemplo, medición del consumo de electricidad y tráfico inteligente), los datos recogidos por los terminales M2M se adquieren o los terminales M2M se controlan y gestionan a distancia mediante una capacidad de servicio que se proporciona por la entidad de gestión de servicio M2M.

Un objetivo global del Instituto Europeo de Normalización de las Telecomunicaciones para las Comunicaciones de Máquina a Máquina (European Telecommunications Standards Institute for Machine-to-Machine Communications, ETSI M2M) es crear una normalización abierta para las comunicaciones de máquina a máquina M2M para favorecer el establecimiento de una futura red que integre varios dispositivos y servicios, para permitir a un servicio M2M tener interoperabilidad y para permitir que las aplicaciones M2M compartan un servicio básico y se pongan en práctica con independencia de una red. En la norma EISI M2M, una interfaz de programación de aplicación de la localización (Application Programming Interface, API), se define como una interfaz *mla* entre una aplicación M2M y la entidad de gestión de servicio M2M, de modo que en la aplicación de M2M, la información de la localización pueda adquirirse y se pueda suscribir un cambio de la información de la localización.

Una cuestión de protección de la privacidad está estrechamente relacionada con la información de la localización. La protección de la privacidad se refiere a que cuando se procesan los datos personales en las comunicaciones electrónicas, un usuario tenga permiso para especificar cuándo y dónde le está permitido a una tercera parte recoger información de la localización del usuario y está autorizado para suprimir el permiso para la tercera parte para la recogida de la información de la localización del usuario. Por lo tanto, la protección de la privacidad es una cuestión que debe considerarse para la localización en las comunicaciones hombre a hombre (Human to Human Communications, H2H). A modo de ejemplo, en una red del Proyecto de Asociación de la 3ª Generación (The 3rd-Generation Partenership Project, 3GPP), la protección de la privacidad se realiza por una entidad independiente tal como un registro de perfil de la privacidad (Privacy Profile Register, PPR) o un centro de localización móvil de pasarela (Gateway Mobile Location Center, GMLC) y es una clase de protección de la privacidad con una arquitectura centralizada. Su procedimiento de puesta en práctica es: después de que un cliente de servicio de localización externa (LoCation Service, LCS) inicie una orden de adquisición de la localización por intermedio de una interfaz Le o una interfaz OSA-LCS, siendo la orden de adquisición de la localización transferida a un centro de localización móvil de pasarela base (Home Gateway Mobile Location Center, HGMLC) o se envía, además, por el HGMLC a la entidad de PPR por intermedio de una interfaz Lpp para protección de la privacidad para comprobar si el cliente de LCS externo tiene permiso para localizar un equipo UE de usuario (User Equipment, UE). Si el cliente de LCS externo no tiene la autorización, se reenvía un mensaje al cliente de LCS externo y si el cliente de LCS externo tiene la autorización, se realiza, además, un proceso de localización de 3GPP. Un mecanismo de protección de la privacidad incluye un proceso de envío de una notificación de privacidad (es decir, una notificación de localización) al equipo de usuario UE o un proceso de realización de la autorización de la privacidad de UE. En el último proceso, el cliente de LCS externo tiene autorización para realizar la localización solamente después de que el usuario confirme (a modo de ejemplo, por intermedio de una interfaz de usuario del equipo UE), que está permitida la localización. Además, un permiso de privacidad diferente puede establecerse para un equipo UE en diferentes áreas de localización.

Para varios sectores industriales que utilizan M2M, a modo de ejemplo, vivienda inteligente, automóvil inteligente y medición del consumo de electricidad inteligente, se utiliza un dispositivo M2M como un dispositivo personal y una localización del dispositivo identifica la información de la localización de un usuario en gran medida. Por lo tanto, en el M2M, necesita resolverse una cuestión relativa a la protección de la privacidad que es similar a la planteada en el caso de H2H. El ETSI M2M utiliza un estilo denominado Restful basado en recursos. La capa de capacidad de servicio (Service Capability Layer, SCL) de un dispositivo, una pasarela y una entidad de gestión de servicio pueden

todos ellos gestionar los recursos en las capas SCLs. Lo que antecede pertenece a un sistema de gestión de recursos distribuidos. Dicho de otro modo, en una arquitectura del sistema M2M existente, ninguna entidad del centro que sea similar a las de PPR o GMLC en el H2H, es para poner en práctica una función de protección de la privacidad.

Sobre la base de la arquitectura del sistema M2M existente, en ETSI M2M, se introduce una función de derecho de acceso, que forma una arquitectura del sistema M2M ilustrada en la Figura 1-b. Sin embargo, numerosos dispositivos existen en un sistema M2M y no cada dispositivo tiene una interfaz de usuario (user interface, UI). Por lo tanto, la notificación de la privacidad o la autenticación no pueden realizarse directamente en cada dispositivo M2M como se realiza la notificación de la privacidad o la autenticación en los equipos de usuario UEs (todos estos equipos UEs tienen interfaces de usuario, a modo de ejemplo, unidades de presentación visual de teléfonos móviles) en 3GPP. Es decir, para una situación en la que un solo usuario tenga múltiples dispositivos en el sistema M2M (a modo de ejemplo, el usuario tiene un dispositivo A y un dispositivo B de MEM), se supone que el dispositivo A tiene una interfaz UI, mientras que el dispositivo B no tiene ninguna interfaz UI, en cuyo caso, la modificación de la privacidad o la autenticación puede realizarse en el dispositivo A. Para la protección de la privacidad para el dispositivo B, aunque se introduce una función de derecho de acceso, el dispositivo A sigue necesitando todavía encontrarse por intermedio de una interfaz mId primero y luego, se realiza la notificación de privacidad o autenticación en el dispositivo B. En otro aspecto de la idea inventiva, aun cuando una función de localización de 3GPP puede utilizarse por intermedio de una interfaz NTOE, esencialmente, cuando la función de derecho de acceso, es decir, una función de autenticación de acceso distribuida, se utiliza para procesar un mecanismo de protección de la privacidad, el dispositivo B necesita también encontrarse por intermedio de la interfaz mId en primer lugar. Después de que un SCL del dispositivo B procese la información recibida, si se encuentra que la función de localización de 3GPP necesita utilizarse para localizar el dispositivo B, la localización de 3GPP se utiliza por intermedio de la interfaz mId.

Una red subyacente de la interfaz mId puede ser una red cableada y puede ser también una red inalámbrica. Por lo tanto, una manera de encontrar el dispositivo A mediante la interfaz mId en primer lugar y luego, realizar la notificación de la privacidad o la autenticación para el dispositivo B o una manera de encontrar el dispositivo B por intermedio de la interfaz mId en primer lugar y luego, utilizar 3GPP para localizar el B en la técnica anterior, puede dar lugar a una carga de señalización adicional. La carga de señalización innecesaria puede dar lugar a una sobrecarga de la red y ocupar un canal de datos normal, lo que origina pérdidas de costes del operador. Para una red inalámbrica con una interfaz de aire, un problema de sobrecarga de señalización es más grave.

El documento US 2010/0197268 publicado con fecha 05/08/2010, da a conocer que el usuario puede configurar la estrategia del dispositivo para las preferencias/establecimiento de la privacidad del usuario en el servidor de gestión de estrategias operativas, de modo que, a modo de ejemplo, la información sensible (p.e., datos de geolocalización, el registro histórico del sitio web) no se comunica a la red sin la autorización del usuario.

SUMARIO DE LA INVENCIÓN

La presente invención da a conocer un método y sistema de protección de la privacidad de comunicaciones de máquina a máquina, una entidad de gestión de servicio de comunicaciones de máquina a máquina y un dispositivo correspondiente, con el fin de poner en práctica la protección de la privacidad para M2M y para reducir una sobrecarga de señalización al mismo tiempo.

Según un aspecto de la presente invención, un método de protección de la privacidad de comunicaciones máquina a máquina, según la reivindicación 1, incluye: después de recibir un mensaje de acceso a la localización, determinar, por una entidad de gestión de servicio M2M y en función de la información de la localización, una entidad que realice la inspección de la privacidad e iniciar operativamente, mediante la entidad de gestión de servicio M2M, la entidad que realiza la inspección de la privacidad para efectuar dicha inspección de la privacidad, en donde, la inspección de la privacidad consiste en que la entidad que realiza la inspección de la privacidad determine si una tercera parte que inicia una orden de adquisición de la localización, por intermedio de una aplicación de M2M, tiene autorización para acceder a un recurso de localización de un dispositivo M2M y/o localizar el dispositivo M2M;

en donde, la determinación de la entidad que realiza la inspección de la privacidad comprende:

la información de la localización que comprende la información de establecimiento de la privacidad está configurada utilizando una aplicación M2M, en la entidad de gestión de servicio M2M y la información de establecimiento de la privacidad indica si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en un servidor de localización del Proyecto de Asociación de la 3ª Generación 3GPP;

después de recibir la orden de adquisición de la localización, adquirir, por la entidad de gestión de servicio M2M, la información de establecimiento de la privacidad y determinar, en función de la información de establecimiento de la privacidad, si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en la localización de 3GPP.

En conformidad con otro aspecto de la presente invención, una entidad de gestión de servicio de comunicaciones de máquina a máquina, según la reivindicación 8, incluye: un módulo de determinación, configurado para, después de recibir un mensaje de acceso a la localización, determinar, en función de la información de la localización, una entidad que realice la inspección de la privacidad y un módulo de iniciación operativa, configurado para iniciar operativamente a la entidad que realiza la inspección de la privacidad para realizar la inspección de la privacidad; en donde la inspección de la privacidad es que la entidad que realiza la inspección de la privacidad determine si una tercera parte que inicia una orden de adquisición de la localización por intermedio de una aplicación de M2M tenga autorización para acceder a un recurso de localización de un dispositivo M2M y/o localizar el dispositivo M2M;

en donde la determinación de la entidad que realiza la inspección de la privacidad comprende: la información de la localización que comprende información del establecimiento de la privacidad está configurada utilizando una aplicación de M2M, en la entidad de gestión de servicio M2M y la información de establecimiento de privacidad indica si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en un servidor de localización del Proyecto de Asociación de la 3ª Generación 3GPP; después de recibir la orden de adquisición de la localización, adquirir, mediante la entidad de gestión de servicio M2M, la información de establecimiento de la privacidad y determinar, en función de la información de establecimiento de la privacidad, si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en la localización de 3GPP.

Según otro aspecto de la presente invención, un sistema de protección de la privacidad de las comunicaciones de máquina a máquina, según la reivindicación 15, incluye: una entidad de gestión de servicio de comunicaciones de máquina a máquina y un servidor de localización del Proyecto de Asociación de la 3ª Generación, en donde

la entidad de gestión de servicio de comunicaciones de máquina a máquina está configurada para, después de recibir un mensaje de acceso a la localización, determinar, en función de la información de la localización, una entidad que realice la inspección de la privacidad e iniciar operativamente la entidad que realiza la inspección de la privacidad para efectuar dicha inspección de la privacidad; en donde la inspección de la privacidad es que la entidad que realiza la inspección de la privacidad determine si una tercera parte que inicia una orden de adquisición de la localización, por intermedio de una aplicación M2M, tiene autorización para acceder a un recurso de la localización de un dispositivo M2M y/o localizar el dispositivo M2M; y

el servidor de localización del Proyecto de Asociación de la 3ª Generación está configurado para la recepción de una demanda de servicio de LCS enviada por la entidad de gestión de servicio de comunicaciones de máquina a máquina y para realizar la inspección de la privacidad; y

en donde la entidad de determinación que realiza la inspección de la privacidad comprende:

la información de la localización, que comprende información de establecimiento de la privacidad, está configurada utilizando una aplicación de M2M, en la entidad de gestión de servicio M2M y la información de establecimiento de la privacidad indica si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en un servidor de localización del Proyecto de Asociación de la 3ª Generación 3GPP;

después de recibir la orden de adquisición de la localización, adquirir, mediante la entidad de gestión de servicio M2M, la información de establecimiento de la privacidad y determinar, en función de la información de establecimiento de la privacidad, si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en la localización de 3GPP.

Puede deducirse de la presente invención que la entidad de gestión de servicio M2M determina, por anticipado, la entidad que realiza la inspección de la privacidad e inicia operativamente la entidad que realiza la inspección de la privacidad para realizar dicha inspección de la privacidad. Por lo tanto, con los métodos de la presente invención, se realice la interacción de mensajes en una interfaz mId, con lo que se reduce una sobrecarga de mensajes. De este modo, se reduce una carga de la red y en particular, para una red inalámbrica con una interfaz de aire, es mayor el beneficio que proporciona la reducción de una sobrecarga de señalización. Al mismo tiempo, se utiliza completamente una función de protección de la privacidad y un procedimiento de la localización del servidor de localización de 3GPP, lo que reduce la complejidad de una plataforma.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para describir las soluciones técnicas en las formas de realización de la presente invención con mayor claridad, se describen concisamente, a continuación, los dibujos adjuntos requeridos para describir las formas de realización de la técnica anterior. Evidentemente, los dibujos adjuntos en la descripción siguiente son solamente algunas formas de realización de la presente invención.

La Figura 1-a es un diagrama esquemático de una arquitectura del sistema M2M típica en la técnica anterior;

La Figura 1-b es un diagrama esquemático de una arquitectura del sistema M2M después de que ETSI M2M introduzca una función de derecho de acceso;

La Figura 2 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones máquina a máquina en conformidad con una forma de realización de la presente invención;

La Figura 3-a es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones máquinas a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 3-b es un diagrama estructural esquemático de un recurso de establecimiento de privacidad en conformidad con una forma de realización de la presente invención;

La Figura 4 es un diagrama de flujo esquemático de un método de protección de la privacidad de las comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 5 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina, en conformidad con otra forma de realización de la presente invención;

La Figura 6 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina, en conformidad con otra forma de realización de la presente invención;

La Figura 7 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina, en conformidad con otra forma de realización de la presente invención;

La Figura 8 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina, en conformidad con otra forma de realización de la presente invención;

La Figura 9 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con una forma de realización de la presente invención;

La Figura 10 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 11 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 12 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 13 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención,

La Figura 14 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 15 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 16 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 17 es un diagrama esquemático de una estructura lógica de un dispositivo de comunicaciones de máquina a máquina en conformidad con una forma de realización de la presente invención;

La Figura 18 es un diagrama esquemático de una estructura lógica de un dispositivo de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 19 es un diagrama esquemático de una estructura lógica de un dispositivo de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 20 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención;

La Figura 21 es un diagrama esquemático de una estructura lógica de un sistema de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con una forma de realización de la presente invención;

La Figura 22 es un diagrama esquemático de una estructura lógica de un sistema de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención; y

La Figura 23 es un diagrama esquemático de una estructura lógica de un sistema de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN DE LA INVENCIÓN

Las soluciones técnicas en las formas de realización de la presente invención están clara y completamente descritas, a continuación, haciendo referencia a los dibujos adjuntos en las formas de realización de la presente invención. Evidentemente, las formas de realización a describirse son solamente una parte y no la totalidad de las formas de realización de la presente invención.

La Figura 2 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con una forma de realización de la presente invención, en donde el método incluye principalmente las etapas siguientes:

S201: Después de recibir un mensaje de acceso a la localización, una entidad de gestión de servicio M2M de comunicaciones de máquina a máquina, determina, en función de la información de la localización, una entidad que realice la inspección de la privacidad, en donde el mensaje de acceso a la localización se refiere a un mensaje para adquirir, suprimir, crear o actualizar un recurso de localización en una entidad de gestión de servicio o un dispositivo M2M o un mensaje para la suscripción o no suscripción respecto a un recurso de localización.

Conviene señalar que una función de la entidad de gestión de servicio en la presente invención puede ponerse en práctica también mediante una plataforma o un sistema informático denominado *middleware*. Además, la entidad de gestión de servicio M2M (SCL) puede localizarse en una plataforma, una pasarela o algunos dispositivos M2M.

En esta forma de realización de la presente invención, la entidad de gestión de servicio M2M de las comunicaciones de máquina a máquina está situada en el mismo lugar que una entidad de gestión de servicio M2M en una arquitectura del sistema M2M ilustrada en la Figura 1-a y puede proporcionar una capacidad de servicio para varias aplicaciones de M2M (a modo de ejemplo, medición del consumo de electricidad y tráfico inteligente), con lo que se adquieren datos recogidos por un dispositivo M2M o el control y gestión a distancia de un dispositivo M2M. Una orden de adquisición de la localización puede iniciarse por una aplicación de M2M por intermedio de una interfaz de programación de aplicación de la localización (Application Programming Interface, API) de una interfaz mIa, a modo de ejemplo, una función de interfaz API de localización puede ser la de Recuperación *Retrieve* (URI de recursos de la localización, parámetros (deviceId)).

Conviene señalar que, en esta forma de realización de la presente invención, un “usuario” se refiere a un usuario al que pertenece un dispositivo (incluyendo un dispositivo M2M sin una interfaz de usuario o un equipo de usuario con una interfaz de usuario). Un equipo de usuario con una interfaz de usuario puede denominarse un “Dispositivo Notificado” en esta forma de realización de la presente invención. Este equipo de usuario con una interfaz de usuario no puede ser un dispositivo M2M peso soporta una manera de notificación y de autenticación tal como un mensaje corto o un mensaje multimedia. Este equipo de usuario con una interfaz de usuario puede ser también un dispositivo M2M y soporta una manera de acceso al recurso basado en URI y un modo de notificación y de autenticación tal como un mensaje corto o un mensaje multimedia. Este equipo de usuario con una interfaz de usuario recibe información, a modo de ejemplo, una demanda de notificación/autenticación, enviada por la entidad de gestión de servicio M2M. La información reenvía por este equipo de usuario con una interfaz de usuario es una respuesta de un usuario a la información enviada por la entidad de gestión de servicio M2M, a modo de ejemplo, permitiendo la adquisición de la localización y localizando un dispositivo M2M que pertenece al usuario.

En esta forma de realización de la presente invención, la determinación de la entidad que realiza la inspección de la privacidad incluye los casos siguientes:

Un primer caso puede ser que un usuario configure o establezca información de localización que incluya información de establecimiento de la privacidad en una entidad de gestión de servicio de M2M utilizando una aplicación de M2M, en donde la información de establecimiento de la privacidad indica si se realiza la inspección de la privacidad en la entidad de gestión de servicio M2M, un dispositivo M2M o un servidor de localización de 3GPP. Después de recibir la orden de adquisición de la localización, la entidad de gestión de servicio M2M puede adquirir la información de establecimiento de la privacidad y determinar, en función de la “información de establecimiento de la privacidad”, si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M (a modo de ejemplo, integrando una función del servidor de localización de 3GPP), el dispositivo M2M o el servidor de localización de 3GPP (separado de la entidad de gestión de servicio M2M).

Un segundo caso puede ser que el usuario no configure ni establezca la información de establecimiento de la privacidad en el primer caso en la entidad de gestión de servicio M2M. Después de recibir una orden de adquisición de la localización, para reducir una sobrecarga de mensajes y el retardo operativo, la entidad de gestión de servicio M2M determina, analizando la información de la localización que incluye la información de establecimiento de la privacidad tal como un modo de notificación y de autenticación, si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M (a modo de ejemplo, integración del servidor de localización de 3GPP), el

dispositivo M2M o el servidor de localización 3GPP (separado de la entidad de gestión de servicio M2M). A modo de ejemplo, si la entidad de gestión de servicio M2M, analizando la información de establecimiento de la privacidad en la información de la localización, que necesita enviarse una demanda de notificación/autenticación a un equipo de usuario (dispositivo Notificado), se determina que la inspección de la privacidad se realice en la entidad de gestión de servicio M2M; de no ser así, se determina que la inspección de la privacidad se realice en el dispositivo M2M; y a modo de otro ejemplo, si una tercera parte que inicia una orden de adquisición de la localización demanda que solamente se obtenga la información de la localización existente del dispositivo M2M y no necesita localizar el dispositivo M2M en tiempo real, puede determinarse que la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M. De este modo, se puede reducir también una sobrecarga de mensajes y el retardo operativo.

A modo de otro ejemplo, analizando la información del tipo de la localización en la información de la localización, si dicha información de localización se adquiere utilizando un servidor de localización (location server), a modo de ejemplo, un GMLC de elemento de red del protocolo 3GPP, la entidad de gestión de servicio M2M puede determinar, en función de la información del tipo de localización del dispositivo recogida con anterioridad o la información del tipo de localización del dispositivo demandada desde un dispositivo después de que se reciba la información de acceso a la localización, que la inspección de la privacidad se realice en la entidad de gestión de servicio M2M o en el servidor de localización.

Si la información de la localización se adquiere a través de un dominio de dispositivos provisto, a modo de ejemplo, de un GPS o un WSN para localización, la entidad de gestión de servicio puede determinar, en función de la información del tipo de localización de dispositivo recogida con anterioridad o de la información del tipo de localización del dispositivo demandada desde el dispositivo M2M después de que se reciba la orden de adquisición de la localización, que la inspección de la privacidad se realice en el dispositivo M2M. Además, la entidad de gestión de servicio M2M puede conocer, en función de la información de capacidad de localización del dispositivo recogida con anterioridad o de la información de capacidad de localización del dispositivo demandada desde el dispositivo M2M después de que se reciba la orden de adquisición de la localización, que en la localización de WSN, un nodo de referencia o un dispositivo de pasarela realiza una operación de localización y obtiene información de localización del dispositivo M2M. En este caso, el dispositivo M2M, en la Figura, puede ser el nodo de referencia o el dispositivo de pasarela, es decir, la inspección de la privacidad puede realizarse en el dispositivo M2M. La información de la localización, en este caso, puede ser información de localización exacta, a modo de ejemplo, longitud, latitud y altitud y puede ser una información de localización difusa, a modo de ejemplo, una ciudad, carretera, comunidad residencial y número de habitación y puede ser también una información de localización relativa, a modo de ejemplo, una distancia a la pasarela o al nodo de referencia en el WSN.

S202: La entidad de gestión de servicio M2M inicia operativamente a la entidad que realiza la inspección de la privacidad para que efectúe dicha inspección de la privacidad.

La inspección de la privacidad se refiere a que la entidad que realiza la inspección de la privacidad determine si una tercera parte que inicia una orden de adquisición de la localización, mediante una aplicación de M2M, tiene autorización para acceder a un recurso de localización del dispositivo M2M y/o localizar el dispositivo M2M.

En una forma de realización de la presente invención, puede determinarse, en función de la información de la localización, que una entidad que realiza la inspección de la privacidad es la entidad de gestión de servicio M2M y puede determinarse también, en función de la información de la localización, que la entidad que realiza la inspección de la privacidad es el dispositivo M2M. En este caso, la entidad de gestión de servicio M2M inicia operativamente la entidad que realiza la inspección de la privacidad, para realizar la inspección de la privacidad, que puede iniciar concretamente la inspección de la privacidad en una manera de acceso al recurso denominado Restful o mediante la interacción de señalización, a modo de ejemplo, señalización SIP o señalización interna privada.

En esta forma de realización, la entidad de gestión de servicio M2M tiene una función de inspección de la privacidad. Después de que se complete la inspección de la privacidad y se permita la localización, la entidad de gestión de servicio M2M puede enviar una demanda de servicio de LCS a un servidor de localización de 3GPP por intermedio de una interfaz Le (una interfaz entre un cliente de LCS y el servidor de localización de 3GPP) para procesar la protección de la privacidad y el proceso de localización en un lado de 3GPP. Además, en esta forma de realización, la entidad de gestión de servicio M2M integra una función de un servidor de localización, a modo de ejemplo, un servidor de localización de 3GPP, GMLC. Por lo tanto, después de que se complete la inspección de la privacidad y se permita la localización, la entidad de gestión de servicio M2M puede enviar una demanda de servicio de LCS a un elemento de red 3GPP por intermedio de una interfaz Lg/SLg (una interfaz entre el servidor de localización de 3GPP y el elemento de red de 3GPP) para procesar un procedimiento de localización.

En otra forma de realización de la presente invención, si se determina, en función de la información de localización, que la entidad que realiza la inspección de la privacidad es el dispositivo M2M, la entidad de gestión de servicio M2M inicia operativamente a la entidad que realiza la inspección de la privacidad para que efectúe dicha inspección de la privacidad, que incluye: la entidad de gestión de servicio M2M envía una demanda de inspección de la privacidad o una orden de adquisición de la localización al dispositivo M2M y la entidad de gestión de servicio M2M

recibe una respuesta desde el dispositivo M2M.

En otra forma de realización de la presente invención, si se determina, en función de la información de localización, que la entidad que realiza la inspección de la privacidad es un servidor de localización del Proyecto de Asociación de la 3ª Generación 3GPP, la entidad de gestión de servicio M2M inicia operativamente a la entidad que la realiza la inspección de la privacidad para que efectúe dicha inspección de la privacidad que incluye: La entidad de gestión de servicio M2M envía una demanda de servicio de LCS al servidor de localización de 3GPP y el servidor de localización de 3GPP realiza la inspección de la privacidad. En este caso, si el servidor de localización de 3GPP no tiene una función de inspección de la privacidad, el servidor de localización de 3GPP interacciona con un registro PPR por intermedio de una interfaz Lpp y el PPR realiza la inspección de la privacidad. En esta forma de realización, la entidad de gestión de servicio M2M envía una demanda de servicio de LCS en la que un mensaje de acceso a la localización se convierte al servidor de localización de 3GPP, que puede ser: La entidad de gestión de servicio M2M envía la demanda de servicio de LCS al servidor de localización de 3GPP por intermedio de la interfaz Le (la interfaz entre el cliente de LCS y el servidor de localización de 3GPP) y el servidor de localización envía la demanda de servicio de LCS al elemento de red de 3GPP para realizar el procedimiento de localización.

Puede deducirse de la forma de realización precedente de la presente invención que la entidad de gestión de servicio M2M determina, por anticipado, la entidad que realiza la inspección de la privacidad e inicia operativamente la entidad que realiza la inspección de la privacidad para que efectúe dicha inspección de la privacidad. Por lo tanto, con el método dado a conocer en esta forma de realización de la presente invención, se reduce la interacción de mensajes en una interfaz mId, con lo que se disminuye una sobrecarga de mensajes. De este modo, se reduce una carga de la red y en particular, para una red inalámbrica con una interfaz de aire, siendo mayor el beneficio que proporciona la reducción de una sobrecarga de señalización. Al mismo tiempo, una función de protección de la privacidad y un procedimiento de localización del servidor de localización de 3GPP se utiliza completamente, lo que reduce la complejidad de una plataforma.

Además del contenido básico precedente, la entidad de gestión de servicio M2M inicia operativamente la inspección de la privacidad, lo que incluye además: La entidad de gestión de servicio M2M envía una demanda de notificación y/o una demanda de autenticación a un dispositivo Notificado, el dispositivo Notificado reenvía una respuesta de notificación o autenticación (la respuesta de notificación es opcional) después de que se completen la presentación visual de la notificación y autenticación dentro del dispositivo Notificado y la entidad de gestión de servicio M2M recibe una respuesta a la demanda de notificación y/o a la demanda de autenticación.

Para reducir una sobrecarga y mejorar la eficiencia de la localización o mejorar la experiencia del usuario, la entidad de gestión de servicio M2M puede enviar una notificación combinada a un equipo de usuario en función de la información de establecimiento de la privacidad, en donde se utiliza la notificación combinada para notificar que la localización ha de realizarse en un grupo de dispositivos M2M. Es decir, un grupo de dispositivos de un usuario no está autorizado para localizarse en su totalidad y la entidad de gestión de servicio M2M combina estas notificaciones enviadas a cada uno de los dispositivos M2M, en el grupo, en un solo mensaje de notificación en conformidad con una función de notificación de grupo (group) que se permite en el establecimiento de la privacidad y envía simultáneamente la notificación combinada al dispositivo Notificado (es decir, al usuario) en un determinado punto temporal. La entidad de gestión de servicio M2M puede enviar también una demanda de autenticación combinada al equipo de usuario en función de la información de establecimiento de la privacidad, en donde la demanda de autenticación combinada se utiliza para demandar que se realice la localización en un grupo de dispositivos M2M. En consecuencia, el dispositivo Notificado necesita reenviar, para la notificación combinada, solamente una respuesta de notificación de usuario y reenviar, para la demanda de autenticación combinada, una sola respuesta de autenticación del usuario. Si la respuesta de autenticación es que el dispositivo M2M está autorizado para ser localizado, ésta es una función de asociación de dispositivos del mismo tipo dada a conocer en esta forma de realización de la presente invención, es decir, durante la autenticación, después de que el dispositivo Notificado permita a una tercera parte localizar un determinado dispositivos M2M del usuario, todos los dispositivos M2M que son del mismo tipo y son propiedad del usuario pueden localizarse posteriormente sin necesidad de autenticación, con el fin de reducir una sobrecarga y mejorar la experiencia del usuario. El usuario puede establecer la función de asociar dispositivos del mismo tipo cuando se establece la información de establecimiento de la privacidad y una plataforma habilita, en conformidad con una respuesta de autenticación posterior del usuario, la función de asociar dispositivos del mismo tipo, con el fin de reducir una sobrecarga de un mensaje de autenticación para el usuario.

En una forma de realización de la presente invención, si se determina, en función de la información de localización, que una entidad que realiza la inspección de la privacidad es una entidad de gestión de servicio M2M, cuando un resultado de la inspección de la privacidad es que el dispositivo M2M está autorizado para ser localizado, la entidad de gestión de servicio M2M envía una demanda de servicio de LCS a un elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP y recibe una respuesta de servicio de LCS del elemento de red de 3GPP; o la entidad de gestión de servicio M2M envía una demanda de servicio de LCS a un elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP y recibe un resultado de localización del dispositivo M2M por el elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP; o la entidad de gestión de servicio M2M envía una demanda de servicio de LCS al dispositivo M2M y recibe un resultado de localización de la localización del dispositivo M2M por el dispositivo M2M.

El elemento de red 3GPP tiene también una función de inspección de la privacidad. Por lo tanto, si la inspección de la privacidad ha sido realizada en la entidad de gestión de servicio M2M, cuando la entidad de gestión de servicio M2M envía la demanda de servicio de LCS al elemento de red de 3GPP, el elemento de red 3GPP puede realizar probablemente, de nuevo, la inspección de la privacidad. Sin embargo, la inspección de la privacidad realizada de nuevo por el elemento de red 3GPP no es obligatoria y esta inspección de la privacidad repetida suele causar una experiencia inadecuada para el usuario. En esta forma de realización de la presente invención, la demanda de servicio de LCS, enviada por la entidad de gestión de servicio M2M al elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP puede incluir un identificador de localización de la entidad de gestión de servicio M2M, en donde el identificador de localización se utiliza para dar instrucciones al elemento de red 3GPP para evitar que se realice de nuevo la inspección de la privacidad o la demanda de servicio de LCS enviada por la entidad de gestión de servicio M2M al elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP puede incluir un identificador que se utiliza para indicar que la entidad de gestión de servicio M2M ha realizado la inspección de la privacidad, a modo de ejemplo, un identificador que se añade modificando una interfaz Le existente e indica que se ha realizado la inspección de la privacidad en una plataforma M2M. Un registro del perfil de privacidad de 3GPP o GMLC determina si necesita continuarse la inspección de la privacidad, es decir, necesita añadirse un tipo de localización para los datos de privacidad de 3GPP y el elemento de red 3GPP determina si necesita realizarse de nuevo la inspección de la privacidad.

El dispositivo M2M está autorizado para ser localizado en diferentes áreas, es decir, áreas diferentes en donde está autorizada la localización pueden ser flexiblemente configuradas, por anticipado, en conformidad con los diferentes requisitos de la tercera parte, a modo de ejemplo, permitiendo a un colega profesional de un usuario localizar el usuario o un vehículo del usuario en una empresa en donde trabaja el usuario, permitiendo a un amigo de un usuario localizar el usuario o un vehículo del usuario en torno a un lugar de actividades de ocio o permitiendo a un miembro de la familia de un usuario localizar el usuario o un vehículo del usuario en todas las zonas exteriores a una empresa.

En otra forma de realización de la presente invención, si se determina, en función de la información de la localización, que la entidad que realiza la inspección de la privacidad es un dispositivo M2M, después de que la entidad de gestión de servicio M2M envíe una demanda de inspección de la privacidad o una orden de adquisición de la localización al dispositivo M2M, el método incluye además: La entidad de gestión de servicio M2M recibe un resultado de localización con respecto a la localización del dispositivo M2M o la entidad de gestión de servicio M2M recibe un resultado de la inspección de la privacidad que se realiza por el dispositivo M2M.

En esta forma de realización de la presente invención, el resultado de la inspección de la privacidad incluye principalmente: El dispositivo M2M está autorizado para ser localizado; el dispositivo M2M no está autorizado para ser localizado; el dispositivo M2M está autorizado para ser localizado y se envía una notificación a un equipo de usuario; una notificación se envía a un equipo de usuario y se requiere la autenticación del equipo de usuario, pero la localización está permitida cuando no se reenvía ninguna respuesta y se remite una notificación a un equipo de usuario y se permite la localización solamente después de que tenga un resultado satisfactorio la autenticación del equipo de usuario.

En una forma de realización de la presente invención en donde se determina, en conformidad con la información de localización, que una entidad que realiza la inspección de la privacidad es un dispositivo M2M o un servidor de localización del Proyecto de Asociación de la 3ª Generación 3GPP, la entidad de gestión de servicio M2M inicia operativamente a la entidad que realiza la inspección de la privacidad para que efectúe dicha inspección de la privacidad, lo que incluye, además: La entidad de gestión de servicio M2M envía una demanda de notificación y/o autenticación a un equipo de usuario o al dispositivo M2M y la entidad de gestión de servicio M2M recibe una respuesta de autenticación a la demanda de autenticación, en donde la respuesta de autenticación incluye información sobre si el dispositivo M2M está autorizado para ser localizado.

Para reducir una sobrecarga y mejorar la eficiencia de la localización o mejorar la experiencia del usuario, en la forma de realización en donde se determina que la entidad que realiza la inspección de la privacidad es el dispositivo M2M o el servidor de localización del Proyecto de Asociación de la 3ª Generación 3GPP, la entidad de gestión de servicio M2M puede enviar una notificación combinada al equipo de usuario o al dispositivo M2M en función de la información de establecimiento de la privacidad, en donde la notificación combinada se utiliza para notificar que ha de realizarse la localización en un grupo de dispositivos M2M. Esta última es una función de asociación de un grupo de dispositivos dado a conocer en esta forma de realización de la presente invención, es decir, un grupo de dispositivos de un usuario están autorizados para ser localizados en su totalidad y la entidad de gestión de servicio M2M combina estas notificaciones en un solo mensaje de notificación para una función de notificación de grupo (group) que está habilitada para el establecimiento de la privacidad y envía simultáneamente el mensaje de notificación a un dispositivo Notificado (es decir, al usuario) en un determinado punto temporal. La entidad de gestión de servicio M2M puede enviar también una demanda de autenticación combinada al equipo de usuario o al dispositivo M2M en función de la información de establecimiento de la privacidad, en donde la demanda de autenticación combinada se utiliza para demandar que se realice la localización en un grupo de dispositivos M2M. En consecuencia, el dispositivo Notificado necesita reenviar, para la notificación combinada, solamente una

respuesta de notificación del usuario y reenviar, para la demanda de autenticación combinada, una respuesta de autenticación del usuario. Si la respuesta de autenticación es que el dispositivo M2M está autorizado para ser localizado, la respuesta de autenticación puede incluir que un dispositivo M2M del mismo tipo que el dispositivo M2M esté autorizado directamente para ser localizado y una tercera parte no necesita enviar una demanda de autenticación de nuevo para la autenticación correspondiente. Esta última es una función de asociación de dispositivos del mismo tipo, dada a conocer en esta forma de realización de la presente invención, es decir, durante la autenticación, después de que el dispositivo Notificado permita a una tercera parte localizar un determinado dispositivo M2M del usuario, todos los dispositivos M2M que señal del mismo tipo y sean propiedad del usuario pueden posteriormente localizarse sin necesidad de autenticación, con el fin de reducir una sobrecarga y mejorar la experiencia del usuario.

La Figura 3-a es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención. En la forma de realización ilustrada en la Figura 3-a, sobre la base de la forma de realización ilustrada en la Figura 2, se describe la interacción de cada dispositivo como sigue:

S301: Una aplicación de M2M envía un mensaje de acceso a la localización a una entidad de gestión de servicio M2M.

A modo de ejemplo, utilizando una función de interfaz API de recuperación *Retrieve* (URI de recurso de localización, parámetros (deviceId)), el mensaje de acceso a la localización se envía a la entidad de gestión de servicio M2M por intermedio de una interfaz mIa para adquirir la más reciente información de localización o la información de localización existente de un dispositivo M2M.

S302: La entidad de gestión de servicio M2M analiza la información de la localización.

En esta forma de realización de la presente invención, la información de localización incluye el mensaje de acceso a la localización. Una finalidad principal de analizar la información de la localización por la entidad de gestión de servicio M2M es examinar si se realiza la inspección de la privacidad en la entidad de gestión de servicio M2M, el dispositivo M2M o un servidor de localización de 3GPP. Para un método de determinación, puede hacerse referencia concretamente a una parte relacionada de la etapa S201 representada en la Figura 2. En esta forma de realización, se supone que se determina que la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M.

S303: La entidad de gestión de servicio M2M realiza la inspección de la privacidad.

La entidad de gestión de servicio M2M realiza la inspección de la privacidad. Una base principal para la inspección es la privacidad del usuario que se establece por unario utilizando la aplicación de M2M y un proceso que es similar a un proceso de creación, recuperación, actualización, supresión (Create Retrieve Update Delete, CRUD) de un derecho de acceso en la norma ETSI M2M por intermedio de una interfaz tal como una interfaz día y una interfaz mIa. A modo de ejemplo el establecimiento de un sub-recurso de usuario de contacto contacUser, un sub-recurso de <Cliente> y un sub-recurso de área permitida areaAllowed, según se ilustra en la Figura 3-b, es definir el permiso para acceder a la información de localización en un sub-recurso de <derecho de acceso>/locPermissions.

Cuando se determina un mensaje de configuración de la privacidad utilizando la aplicación de M2M, el usuario especifica información de direccionamiento de un dispositivo Notificado por intermedio del sub-recurso contacUser y puede configurar concretamente un número de dispositivo, una dirección IP o una URI. Cuando una tercera parte inicia un mensaje de acceso a la localización y necesita notificar al usuario o dar instrucciones al usuario para realizar la autenticación, un mensaje de notificación o un mensaje de autenticación se envía al dispositivo Notificado enviando un mensaje corto/mensaje multimedia para la identidad del usuario userIdentity, realizando el acceso a un recurso del dispositivo Notificado por intermedio de una interfaz URI en una manera de recurso o utilizando una dirección IP configurada. Después de que el dispositivo Notificado reciba el mensaje de notificación o el mensaje de autenticación, el mensaje se convierte, en el dispositivo, en un mensaje que puede procesarse en una interfaz de usuario UI para la utilización del usuario.

El establecimiento del Atributo en el sub-recurso contacUser se define principalmente con los atributos siguientes:

Asociación: una función de asociar dispositivos del mismo tipo, lo que significa que durante la autenticación, después de que el sub-recurso contacUser permita a una aplicación de red NA localizar un determinado dispositivo del usuario, todos los dispositivos que sean del mismo tipo y sean propiedad del usuario pueden posteriormente localizarse sin necesidad de autenticación, con el fin de reducir una sobrecarga y mejorar la experiencia del usuario.

Grupo: una función de asociar un grupo de dispositivos, lo que significa que algunos dispositivos del usuario son localizados por una aplicación en su totalidad, pero una función de la privacidad combina estas notificaciones del usuario en un solo mensaje de notificación en conformidad a la circunstancia de que la función de notificación de grupo esté habilitada en el establecimiento de la privacidad y envía simultáneamente las notificaciones al usuario en un determinado punto temporal.

areaPermitted: información de la autorización para la determinación de la privacidad. La información de establecimiento de la privacidad permitida en áreas se utiliza para permitir al dispositivo M2M ser localizado en diferentes áreas. La entidad de gestión de servicio M2M puede recibir la información de establecimiento de la privacidad permitida en esa área. Con respecto a la utilización areaPermitted del 3GPP, para un dispositivo localizado del usuario, solamente puede establecerse un área fija en donde esté autorizada la localización. En M2M, diferentes áreas en donde está autorizada la localización, pueden autorizarse flexiblemente en conformidad con una aplicación de red (Network Application, NA). A un compañero profesional del usuario le está permitido localizar al usuario o un vehículo del usuario en una empresa en donde trabaja el usuario, a un amigo del usuario le está permitido localizar al usuario o un vehículo del usuario en torno a un lugar de actividades de ocio o un miembro de la familia del usuario está autorizado para localizar al usuario o un vehículo del usuario en todas las áreas exteriores a una empresa.

Conviene señalar que el establecimiento de la privacidad puede realizarse también por intermedio de una interfaz privada además de configurarse por el usuario utilizando la aplicación de M2M por intermedio de una interfaz tal como una interfaz día y una interfaz mIa. En algunos casos, después de que un usuario firme un contrato con un operador o un proveedor de servicios de M2M, el establecimiento de la privacidad que se incluye en el contrato puede configurarse en un recurso relacionado con la privacidad por intermedio de una interfaz privada.

S304: La entidad de gestión de servicio M2M envía una demanda de notificación y/o una entidad de autenticación a un equipo de usuario, en donde el equipo de usuario puede referirse a un dispositivo con una interfaz de usuario.

Si la entidad de gestión de servicio M2M encuentra, analizando el mensaje de acceso a la localización, que el usuario necesita notificarse y realizar la autenticación, según se describió con anterioridad, los resultados de la notificación y de la autenticación del usuario se reenvían por el equipo de usuario (dispositivo Notificado). Por lo tanto, la entidad de gestión de servicio M2M envía la demanda de notificación y/o la demanda de autenticación al dispositivo Notificado.

S305: El equipo de usuario reenvía una respuesta de notificación o una respuesta de autenticación.

Después de que se completen la presentación visual de la notificación y la autenticación en el interior del equipo de usuario (dispositivo Notificado), el equipo de usuario (dispositivo Notificado) reenvía la respuesta de notificación o la respuesta de autenticación, en donde la respuesta de notificación es opcional.

S306: La entidad de gestión de servicio M2M envía una demanda de servicio de LCS a un servidor de localización de 3GPP.

Conviene señalar que, en esta forma de realización, la entidad de gestión de servicio M2M integra el servidor de localización de 3GPP o una función del servidor de localización de 3GPP. Por lo tanto, la entidad de gestión de servicio M2M puede enviar también la demanda de servicio de LCS a un elemento de red de 3GPP por intermedio de una interfaz Lg/Slg (una interfaz entre el servidor de localización de 3GPP y el elemento de red 3GPP).

S307: El servidor de localización de 3GPP reenvía un resultado de la localización a la entidad de gestión de servicio M2M.

En esta forma de realización de la presente invención, para un dispositivo M2M que esté localizado por intermedio de una interfaz Le con la ayuda de un elemento de red 3GPP, un resultado de localización de un plano de usuario SUPL/plano de control se adquiere en conformidad con un procedimiento de localización de 3GPP, en donde una tecnología de localización incluye, a modo de ejemplo, una tecnología OTDOA, CellID, AGPS o un sistema de procesamiento global (Global Positioning System, GPS). Un 3GPP PPR o GMLC determina si necesita continuarse la inspección de la privacidad. El elemento de red 3GPP proporciona el resultado de la localización para el servidor de localización de 3GPP y luego, el servidor de localización de 3GPP reenvía el resultado de la localización a la entidad de gestión de servicio M2M.

S308: La entidad de gestión de servicio M2M reenvía el resultado de la localización a la aplicación de M2M.

La Figura 4 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención. En esta forma de realización, un servidor de localización 3GPP está separado de una entidad de gestión de servicio M2M. En la forma de realización ilustrada en la Figura 4, sobre la base de la forma de realización representada en la Figura 2, la interacción de cada dispositivo se describe como sigue:

S401: Una aplicación de M2M envía un mensaje de acceso a la localización a una entidad de gestión de servicio M2M.

A modo de ejemplo, utilizando un recurso de función de interfaz API de recuperación *Retrieve* (URI de recurso de

localización, parámetros (deviceId)), el mensaje de acceso de la localización se envía a la entidad de gestión de servicio M2M por intermedio de una interfaz mIa para adquirir la más reciente información de localización o información de localización existente de un dispositivo M2M.

S402: La entidad de gestión de servicio M2M analiza la información de la localización.

En esta forma de realización de la presente invención, la información de la localización incluye el mensaje de acceso a la localización. Una finalidad principal de analizar la información de localización por la entidad de gestión de servicio M2M es determinar si la inspección de la privacidad se realiza en un servidor de localización de 3GPP o en el dispositivo M2M. Se supone que la entidad de gestión de servicio M2M puede determinar, en función de la información en el mensaje de acceso a la localización, a modo de ejemplo, la información del tipo de localización (es decir, si se adopta una manera de localización de 3GPP u otra manera de localización, a modo de ejemplo, localización wsn), de que la inspección de la privacidad se realiza en el servidor de localización de 3GPP.

S403: La entidad de gestión de servicio M2M envía una demanda de servicio de LCS al servidor de localización de 3GPP.

En esta forma de realización, la entidad de gestión de servicio M2M envía la demanda de servicio de LCS al servidor de localización 3GPP, que puede ser: La entidad de gestión de servicio M2M envía la demanda de servicio de LCS al servidor de localización 3GPP por intermedio de una interfaz Le (una interfaz entre un cliente de LCS y el servidor de localización de 3GPP) y el servidor de localización envía la demanda de servicio de LCS a un elemento de red 3GPP. Después de recibir la demanda de servicio de LCS (LCS service request), el servidor de localización 3GPP realiza la inspección de la privacidad (S404).

S405: El servidor de localización 3GPP envía una respuesta de servicio de LCS de la demanda de servicio de LCS a la entidad de gestión de servicio M2M.

Si el servidor de localización 3GPP realiza satisfactoriamente la operación de localización, la respuesta de servicio de LCS incluye información de la localización del dispositivo M2M.

S406: La entidad de gestión de servicio M2M reenvía la respuesta de servicio de LCS a la aplicación de M2M.

La Figura 5 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención, en donde el método incluye principalmente las etapas siguientes:

S501: Después de recibir un mensaje de acceso a la localización, la entidad de gestión de servicio de comunicaciones de máquina a máquina M2M determina, en función de la información de localización, una entidad que realiza la inspección de la privacidad.

Se determina que se realiza la inspección de la privacidad en la entidad de gestión de servicio M2M, en un servidor de localización de 3GPP o en un dispositivo M2M. Para un método de determinación específico, puede hacerse referencia a una parte relacionada de la etapa S201 en la forma de realización representada en la Figura 2. A modo de ejemplo, si la información de la localización se adquiere por intermedio de un dominio de dispositivos provisto, a modo de ejemplo, de WSN para localización, la entidad de gestión de servicio M2M puede determinar, en función de la información de capacidad de localización del dispositivo recogida con anterioridad o de la información de capacidad de localización del dispositivo demandada desde un dispositivo después de que se reciba el mensaje de acceso a la localización, que la inspección de la privacidad se realice en el dispositivo M2M (M2M device). Además, la entidad de gestión de servicio M2M puede conocer, en función de la información de capacidad de localización del dispositivo recogida con anterioridad o de la información de capacidad de localización del dispositivo demandada desde el dispositivo después de que se reciba el mensaje de acceso a la localización, que se realiza una operación de localización en un dominio de dispositivos con un dispositivo, a modo de ejemplo, siendo un nodo de referencia o un dispositivo de pasarela y una localización de un nodo en la información de la localización puede obtenerse a este respecto. En este caso, el dispositivo M2M en la Figura puede ser el nodo de referencia o el dispositivo de pasarela, es decir, la inspección de la privacidad puede realizarse en el dispositivo M2M.

S502: Si en la etapa S501, se determina que la entidad que realiza la inspección de la privacidad es el dispositivo M2M, la entidad de gestión de servicio M2M envía una demanda de inspección de la privacidad o el mensaje de acceso a la localización al dispositivo M2M y recibe una respuesta de autenticación desde el dispositivo M2M.

De forma opcional, el dispositivo M2M reenvía, además, una respuesta de notificación y la entidad de gestión de servicio M2M recibe la respuesta de notificación.

De forma opcional, el dispositivo M2M reenvía, además, un resultado de la inspección de la privacidad que se realiza por el dispositivo M2M y la entidad de gestión de servicio M2M recibe el resultado de la inspección de la privacidad que se realiza por el dispositivo M2M, que incluye principalmente los casos siguientes:

si la entidad de gestión de servicio M2M necesita entrar en contacto con un servidor de localización con el fin de localizar el dispositivo M2M en un proceso de localización posterior, el dispositivo M2M necesita reenviar el resultado de la inspección de la privacidad, a modo de ejemplo, con la autorización de la localización, a la entidad de gestión de servicio M2M; y

si la entidad de gestión de servicio M2M realiza un análisis sintáctico o conversión cuando recibe el mensaje de acceso a la localización, a modo de ejemplo, la conversión del mensaje de acceso a la localización en un mensaje de demanda de inspección de la privacidad y después de que se realice la autenticación por el dispositivo M2M, a una tercera parte no le está permitido localizar el servicio M2M, puesto que el dispositivo M2M necesita notificar un resultado de que “una tercera parte no está autorizada para localizar el dispositivo M2M” a la entidad de gestión de servicio M2M y luego, la entidad de gestión de servicio M2M notifica una respuesta para una aplicación de M2M.

En esta forma de realización de la presente invención, el resultado de la inspección de la privacidad incluye cualquiera o alguna combinación de lo que sigue: el dispositivo M2M está autorizado para su localización; el dispositivo M2M no está autorizado para su localización; el dispositivo M2M está autorizado para su localización y se envía una notificación a un dispositivo M2M con una interfaz de usuario; se envía una notificación a un dispositivo M2M con una interfaz de usuario y el dispositivo M2M con una interfaz de usuario necesita realizar la autenticación; se envía una notificación a un dispositivo M2M con una interfaz de usuario y está autorizada la localización solamente después de que se realice la autenticación por el dispositivo M2M con una interfaz de usuario de forma satisfactoria y así sucesivamente.

S503: La entidad de gestión de servicio M2M recibe un resultado de la localización con respecto a la localización del dispositivo M2M.

Si la entidad de gestión de servicio M2M envía una demanda de inspección de la privacidad al dispositivo M2M, antes de que la entidad de gestión de servicio M2M reciba el resultado de la inspección de la privacidad que se realiza por el dispositivo M2M, el método incluye además: La entidad de gestión de servicio M2M envía un mensaje de acceso a la localización o una demanda de servicio de LCS al dispositivo M2M. Más concretamente, si antes de que la entidad de gestión de servicio M2M reciba el resultado de la inspección de la privacidad que se realiza por el dispositivo M2M, la entidad de gestión de servicio M2M envía el mensaje de acceso a la localización al dispositivo M2M y el propio dispositivo M2M pone en práctica una función de localización, y por lo tanto, la entidad de gestión de servicio M2M no necesita entregar de nuevo el mensaje de acceso a la localización; y si antes de que la entidad de gestión de servicio M2M recibe el resultado de la inspección de la privacidad que se realiza por el dispositivo M2M, la entidad de gestión de servicio M2M envía la demanda de inspección de la privacidad al dispositivo M2M, el mensaje de acceso a la localización o la demanda de servicio de LCS necesita enviarse al dispositivo M2M. Si el mensaje de acceso a la localización se entrega o la demanda de servicio de LCS se entrega, se determina en función de si la entidad de gestión de servicio M2M realiza un análisis sintáctico y convierte una demanda de la aplicación de M2M.

La Figura 6 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención, en donde el método incluye principalmente las etapas siguientes:

S601: Un dispositivo de comunicaciones de máquina a máquina M2M recibe un mensaje de acceso a la localización o una demanda de inspección de la privacidad, en donde el mensaje de acceso a la localización o la demanda de inspección de la privacidad se envían por una entidad de gestión de servicio M2M.

En esta forma de realización, el mensaje de acceso a la localización o la demanda de inspección de la privacidad que se recibe por el dispositivo M2M de comunicaciones de máquina a máquina se envían cuando la entidad de gestión de servicio M2M determina que la inspección de la privacidad se realiza en el dispositivo M2M.

S602: El dispositivo M2M reenvía una respuesta para la inspección de la privacidad a la entidad de gestión de servicio M2M.

La respuesta para la inspección de la privacidad puede ser, a modo de ejemplo, la autorización a una tercera parte localizar el dispositivo M2M y de forma opcional, el dispositivo M2M reenvía, además, una respuesta de notificación.

De forma opcional, el dispositivo M2M reenvía una respuesta de autenticación para la inspección de la privacidad a la entidad de gestión de servicio M2M, que incluye, además: el dispositivo M2M reenvía un resultado de la realización de la inspección de la privacidad a la entidad de gestión de servicio M2M.

Para reducir una sobrecarga o mejorar la experiencia del usuario, el dispositivo M2M necesita reenviar, para una notificación combinada, solamente una respuesta de notificación de un usuario y reenviar, para una demanda de autenticación combinada, una respuesta de autenticación del usuario. Si la respuesta de autenticación es que el dispositivo M2M tiene autorización para ser localizado, la respuesta de autenticación puede incluir que un dispositivo

M2M del mismo tipo que el dispositivo M2M está directamente autorizado para ser localizado y una tercera no necesita enviar una demanda de autenticación para realizar de nuevo la autenticación. Esta última es una función de asociación de dispositivos del mismo tipo dada a conocer en esta forma de realización de la presente invención, es decir, durante la autenticación, después de que un dispositivo Notificado permita a una tercera parte localizar un determinado dispositivo M2M del usuario, todos los dispositivos M2M que son del mismo tipo y son propiedad del usuario pueden ser posteriormente localizados sin necesidad de autenticación, con el fin de reducir una sobrecarga y mejorar la experiencia del usuario.

En esta forma de realización de la presente invención, el resultado de la inspección de la privacidad incluye cualquiera o alguna combinación de lo que sigue: el dispositivo M2M está autorizado para ser localizado; el dispositivo M2M no está autorizado para ser localizado; el dispositivo M2M está autorizado para ser localizado y se envía una notificación a un dispositivo M2M con una interfaz de usuario; se envía una notificación a un dispositivo M2M con una interfaz de usuario y el dispositivo M2M con una interfaz de usuario necesita realizar la autenticación; se envía una notificación a un dispositivo M2M con una interfaz de usuario y la localización está autorizada solamente después de que se realice la autenticación por el dispositivo M2M con una interfaz de usuario de forma satisfactoria y así sucesivamente.

S603: Si el dispositivo M2M está autorizado para ser localizado, el dispositivo M2M adquiere la información de localización del dispositivo M2M.

En esta forma de realización, el dispositivo M2M adquiere información de la localización del dispositivo M2M, que incluye: el dispositivo M2M adquiere la información de localización del dispositivo M2M utilizando su propio sistema de posicionamiento global (Global Positioning System, GPS), el dispositivo M2M adquiere la información de la localización del dispositivo M2M dese un elemento de red base de 3GPP o el dispositivo M2M adquiere la información de la localización del dispositivo M2M por intermedio de WSN. Más concretamente, para un dispositivo cuya información de localización se adquiere en un dominio de dispositivos del dispositivo M2M, se adquiere un resultado de localización en conformidad con un procedimiento de localización de WSN, en donde una tecnología de localización incluye las tecnologías de RSSI, TOA, TDOA, AOA o una tecnología de localización que está basada en el número de saltos operativos y la conectividad en lugar del alcance operativo.

Además, si un nodo de referencia o un dispositivo de pasarela realiza un procedimiento de localización, el nodo de referencia o el dispositivo de pasarela necesitan crear, en una manera de acceso de recursos Restful, un recurso de localización en el dispositivo M2M para memorizar la información de localización o especificar, mediante un recurso de anuncio (announce resource), una función de URI de un lugar en donde está situada la información de la localización. Como alternativa, la entidad de gestión de servicio M2M mantiene una función URI del nodo de referencia y adquiere directamente la información de la localización a partir de un recurso de localización del nodo de referencia cuando recibe un mensaje de acceso a la localización desde una aplicación de red NA. A modo de ejemplo, el dispositivo de pasarela o un determinado nodo de referencia en una WSN tiene una función de GPS y en una red inalámbrica WSN a pequeña escala, otro dispositivo M2M puede utilizar información de la localización adquirida por el sistema GPS como su propia información de localización.

Si un dispositivo M2M localizado, el nodo de referencia o el dispositivo de pasarela está conectado a 3GPP, se puede adquirir una localización de dispositivo por intermedio de una demanda de localización iniciada por un terminal móvil 3GPP en un procedimiento de demanda de localización originada móvil (Mobile Originated Location Request, MO-LR) (este procedimiento no implica la inspección de la privacidad en 3GPP). Para asegurar todavía más la privacidad, un identificador de aplicación M2M que indica que la aplicación de M2M como una tercera parte inicia la localización que necesita realizarse cuando el dispositivo M2M localizado o el nodo de referencia inicia una demanda de servicio de LCS.

La Figura 7 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención. En la forma de realización ilustrada en la Figura 7, sobre la base de las formas de realización ilustradas en la Figura 5 y en la Figura 6, la interacción de cada dispositivo se describe como sigue:

S701: Una aplicación de M2M envía un mensaje de acceso a la localización a una entidad de gestión de servicio M2M.

A modo de ejemplo, utilizando una función de API de recuperación *Retrieve* (URI de recurso de localización, parámetros (deviceId)), el mensaje de acceso a la localización se envía a la entidad de gestión de servicio M2M por intermedio de una interfaz mIa para adquirir la más reciente información de localización o la información de localización existente de un dispositivo M2M.

S702: La entidad de gestión de servicio M2M analiza un mensaje de localización.

En esta forma de realización de la presente invención, el mensaje de localización incluye el mensaje de acceso a la localización. Una finalidad principal de analizar el mensaje de localización por la entidad de gestión de servicio M2M

es determinar si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M, en un servidor de localización de 3GPP o un dispositivo M2M. Para un método de determinación, puede hacerse referencia concretamente a una parte relacionada de la etapa S201 ilustrada en la Figura 2. En esta forma de realización, se supone que se determina que la inspección de la privacidad se realiza en el dispositivo M2M.

S703: La entidad de gestión de servicio M2M envía una demanda de inspección de la privacidad o un mensaje de acceso a la localización al dispositivo M2M.

S704: El dispositivo M2M realiza la inspección de la privacidad.

S705: El dispositivo M2M reenvía una respuesta de autenticación a la entidad de gestión de servicio M2M.

La respuesta de autenticación reenviada por el dispositivo M2M es una respuesta de autenticación para la inspección de la privacidad, a modo de ejemplo, puede ser: autorizar a una tercera parte para localizar el dispositivo M2M. De forma opcional, el dispositivo M2M reenvía, además, una respuesta de notificación y también de forma opcional, el dispositivo M2M reenvía, además, un resultado de la inspección de la privacidad que se realiza por el dispositivo M2M y la entidad de gestión de servicio M2M recibe el resultado de la inspección de la privacidad que se realiza por el dispositivo M2M.

S706: El dispositivo M2M localiza al dispositivo M2M.

Si el resultado de la inspección de la privacidad es positivo, a modo de ejemplo, el dispositivo M2M está autorizado para ser localizado, el dispositivo M2M adquiere la información de localización del dispositivo M2M.

S707: El dispositivo M2M reenvía una respuesta de localización a la entidad de gestión de servicio M2M.

Si la información de la localización del dispositivo M2M se adquiere, la respuesta de localización reenviada incluye información de localización adquirida.

S708: La entidad de gestión de servicio M2M reenvía la respuesta de localización a la aplicación de M2M.

Si el dispositivo M2M adquiere la información de la localización del dispositivo M2M, la respuesta de localización reenviada por la entidad de gestión de servicio M2M incluye la información de localización adquirida del dispositivo M2M.

La Figura 8 es un diagrama de flujo esquemático de un método de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención, en donde el método incluye principalmente las etapas siguientes:

S801: Una entidad de gestión de servicio M2M de comunicaciones máquina a máquina convierte un mensaje de acceso a localización recibido en señalización de localización que es identificable para un elemento de red 3GPP o PPR.

En un caso en el que numerosos dispositivos M2M acceden al 3GPP un sistema M2M y necesita realizarse la localización mediante una función de localización de 3GPP, la entidad de gestión de servicio M2M introduce una función de protección de la privacidad poseída por un GMLC y un cliente de LCS externo, es decir, la conversión de un mensaje de acceso a la localización enviado por una aplicación de M2M por intermedio de una interfaz mIa en una señalización de localización de red base que es identificable para 3GPP. La interfaz mIa soporta también el aprovisionamiento en el cliente de LCS externo para configurar datos relacionados con la privacidad que incluyen una clase de privacidad (privacy class). Además, la configuración de privacidad puede ponerse en práctica también por intermedio de una interfaz privada.

S802: Interacción con el elemento de red 3GPP o PPR para adquirir información de localización de un dispositivo M2M.

En esta forma de realización, la entidad de gestión de servicio M2M tiene una interfaz Lg y puede conectarse a 3GPP para reutilizar una capacidad de localización del elemento de red 3GPP; tiene una función de inspección de la privacidad y reutiliza una función de un GMLC existente y soporta una interfaz Lpp para intercambiar un mensaje de inspección de la privacidad con PPR y puede soportar múltiples interfaces Lpp.

La Figura 9 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con una forma de realización de la presente invención. Para facilitar la descripción, solamente una parte relacionada con la forma de realización de la presente invención es objeto de ilustración. En esta forma de realización de la presente invención, la entidad de gestión de servicio M2M está situada en el mismo lugar que una entidad de gestión de servicio M2M en una arquitectura del sistema M2M ilustrada en la Figura 1-a y puede proporcionar una capacidad de servicio para varias aplicaciones de M2M (a modo

de ejemplo, medición del consumo de electricidad y tráfico inteligente), adquiriendo, de este modo, datos recogidos por un dispositivo M2M o controlando y gestionando a distancia un dispositivo M2M. Un módulo/unidad funcional puede ser un módulo/unidad de software, un módulo/unidad de hardware o una combinación de un módulo/unidad de software y un módulo/unidad de hardware y un módulo de determinación 901 y un módulo de iniciación operativa 902 se incluyen a este respecto, en donde:

el módulo de determinación 901 está configurado para, después de recibir un mensaje de acceso de localización, determinar, en función de la información de localización, una entidad que realice la inspección de la privacidad; y

el módulo de iniciación operativa 902 está configurado para iniciar operativamente a la entidad que realiza la inspección de la privacidad o para realizar la inspección de la privacidad, en donde la entidad que realiza la inspección de la privacidad se determina por el propio módulo de determinación 901.

Más concretamente, si el módulo de determinación 901 determina, en función de la información de localización, que la entidad que realiza la inspección de la privacidad es una entidad de gestión de servicio M2M, el módulo de iniciación operativa 902 inicia operativamente a la entidad de gestión de servicio M2M para realizar la inspección de la privacidad. Si el módulo de determinación 901 determina, en función de la información de localización, que la entidad que realiza la inspección de la privacidad es el dispositivo M2M, el módulo de iniciación operativa 902 incluye una primera unidad de envío 1001 y una primera unidad de recepción 1002. Según se ilustra en la Figura 10, otra forma de realización de la presente invención da a conocer una entidad de gestión de servicio de comunicaciones de máquina a máquina, en donde la primera unidad de envío 1001 está configurada para enviar una demanda de inspección de la privacidad o el mensaje de acceso a la localización al dispositivo M2M y la primera unidad de recepción 1002 está configurada para recibir una respuesta del dispositivo M2M. Si el módulo de determinación 901 determina, en función con la información de la localización, que la entidad que realiza la inspección de la privacidad es un servidor de localización del Proyecto de Asociación de la 3ª Generación 3GPP el módulo de iniciación operativa 902 incluye una unidad de envío de demanda de servicio de LCS 1101. Según se ilustra en la Figura 11, otra forma de realización de la presente invención da a conocer una entidad de gestión de servicio de comunicaciones de máquina a máquina, en donde la unidad de envío de demanda de servicio de LCS 1101 está configurada para enviar una demanda de servicio de LCS al servidor de localización de 3GPP y el servidor de localización de 3GPP realiza la inspección de la privacidad.

Conviene señalar que, en la forma de realización precedente de la entidad de gestión de servicio de comunicaciones de máquina a máquina, la división de cada módulo funcional es solamente para fines ilustrativos. En una aplicación real, la función precedente puede ponerse en práctica por diferentes módulos funcionales en función de un requerimiento operativo, a modo de ejemplo, un requerimiento de configuración de hardware correspondiente o una consideración por conveniencia de la puesta en práctica del software. Es decir, una estructura interna de la entidad de gestión de servicio de comunicaciones de máquina a máquina se divide en diferentes módulos funcionales para poner en práctica la totalidad o parte de las funciones descritas con anterioridad. Además, en una aplicación real, los módulos funcionales correspondientes en esta forma de realización pueden ponerse en práctica por el hardware correspondiente y pueden realizarse también por el software correspondiente de ejecución de hardware también correspondiente. A modo de ejemplo, el módulo de determinación puede ser hardware, a modo de ejemplo, un dispositivo de determinación, que determina, en función de la información de localización, después de recibir el mensaje de acceso a la localización, la entidad que realiza la inspección de la privacidad y puede ser también un procesador general u otro dispositivo de hardware que sea capaz de ejecutar un programa informático correspondiente para poner en práctica la función precedente. A modo de otro ejemplo, el módulo de iniciación operativa puede ser hardware, a modo de ejemplo, un dispositivo de iniciación operativa que realice una función de iniciación operativa de la entidad que realiza la inspección de la privacidad para realizar dicha inspección de la privacidad y puede ser también un procesador general u otro dispositivo de hardware que sea capaz de ejecutar un programa informático correspondiente para poner en práctica la función precedente.

Si el módulo de determinación 901 determina, en función de la información de la localización, que la entidad que realiza la inspección de la privacidad es la entidad de gestión de servicio M2M, una entidad de gestión de servicio de comunicaciones de máquina a máquina incluye, además, un primer módulo transceptor 1201, un segundo módulo transceptor 1202 o un tercer módulo transceptor 1203. Según se ilustra en la Figura 12, otra forma de realización de la presente invención da a conocer una entidad de gestión de servicio de comunicaciones de máquina a máquina en donde:

el primer módulo transceptor 1201 está configurado para, cuando un resultado de la inspección de la privacidad es que el dispositivo M2M está autorizado para ser localizado, enviar una demanda de servicio de LCS a un elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP y recibir un resultado obtenido de inspección de la privacidad que se realiza por el elemento de red 3GPP;

el segundo módulo transceptor 1202 está configurado para, cuando un resultado de la inspección de la privacidad es que el dispositivo M2M está autorizado para ser localizado, enviar una demanda de servicio de LCS a un elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP y recibir un resultado de la localización de la localización del dispositivo M2M por el elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP; y

el tercer módulo transceptor 1203 está configurado para, cuando un resultado de la inspección de la privacidad es que el dispositivo M2M está autorizado para ser localizado, enviar una demanda de servicio de LCS al dispositivo M2M y recibir un resultado de localización con respecto a la localización del dispositivo M2M por el dispositivo M2M. En el primer módulo transceptor 1201 ilustrado en la Figura 12, la demanda de servicio de LCS incluye un identificador de localización de la entidad de gestión de servicio M2M, en donde el identificador de localización se utiliza para dar instrucciones al elemento de red 3GPP para evitar la inspección de la privacidad que ha de realizarse de nuevo o la demanda de servicio LCS que incluye un identificador de indicación que se utiliza para indicar que la entidad de gestión de servicio M2M ha realizado la inspección de la privacidad y el elemento de red 3GPP determina si necesita realizarse de nuevo la inspección de la privacidad.

La entidad de gestión de servicio de comunicaciones de máquina a máquina que se ilustra en la Figura 9 o en la Figura 12 puede incluir, además un primer módulo de recepción de resultados 1301 o un segundo módulo de recepción de resultados 1302. Según se ilustra en la Figura 13, otra forma de realización de la presente invención da a conocer una entidad de gestión de servicio de comunicaciones de máquina a máquina, en donde:
el primer módulo de recepción de resultados 1301 está configurado para recibir un resultado de localización de la localización del dispositivo M2M; y

el segundo módulo de recepción de resultados 1302 está configurado para recibir un resultado de la inspección de la privacidad que se realiza por el dispositivo M2M.

En la entidad de gestión de servicio de comunicaciones de máquina a máquina, que se ilustra en cualquiera de las Figuras 9 a 13, la entidad que realiza la inspección de la privacidad está configurada, además, para enviar una notificación a un equipo de usuario; la entidad que realiza la inspección de la privacidad está configurada, además, para enviar una demanda de autenticación al equipo de usuario y la entidad que realiza la inspección de la privacidad está configurada, además, para recibir una respuesta de autenticación a la demanda de autenticación, en donde la respuesta de autenticación incluye información sobre si el dispositivo M2M está autorizado para ser localizado.

Para reducir una sobrecarga y mejorar la eficiencia de localización o mejorar la experiencia del usuario, en la entidad de gestión de servicio de comunicaciones de máquina a máquina, según se ilustra en cualquiera de las Figuras 9 a 13, la entidad que realiza la inspección de la privacidad puede enviar, además, una notificación combinada al equipo de usuario en función de la información de establecimiento de la privacidad, en donde la notificación combinación se utiliza para notificar que la localización ha de realizarse en un grupo de dispositivos M2M. Es decir, un grupo de dispositivos de un usuario están todos ellos autorizados para ser localizados y la entidad de gestión de servicio M2M combina estas notificaciones en un solo mensaje de notificación en conformidad con una función de notificación de grupo (group) que está habilitada para el establecimiento de la privacidad y envía simultáneamente las notificaciones a un dispositivo Notificado (es decir, al usuario) en un determinado punto temporal. La entidad que realiza la inspección de la privacidad puede enviar también una demanda de autenticación combinada al equipo de usuario en función de la información de establecimiento de la privacidad, en donde la demanda de autenticación combinada se utiliza para demandar que se realice la localización en un grupo de dispositivos M2M. En consecuencia, el dispositivo Notificado necesita reenviar, para la notificación combinada, solamente una respuesta de notificación remitida por el usuario y reenviar, para la demanda de autenticación combinada, una sola respuesta de autenticación remitida por el usuario. Si la respuesta de autenticación es que el dispositivo M2M está autorizado para ser localizado, esta última es una función de asociación de dispositivos del mismo tipo dada a conocer en esta forma de realización de la presente invención, es decir, durante la autenticación, después de que el dispositivo Notificado autorice a una tercera parte a localizar un determinado dispositivo M2M del usuario, siendo todos los dispositivos M2M del mismo tipo y siendo propiedad del usuario que pueden posteriormente localizarse sin necesidad de autenticación, con el fin de reducir una sobrecarga y mejorar la experiencia del usuario. El usuario puede establecer la función de asociar dispositivos del mismo tipo cuando se establece la información de establecimiento de la privacidad y una plataforma habilita, en conformidad con una posterior respuesta de autenticación del usuario, la función de asociar dispositivos de mismo tipo, con el fin de reducir una sobrecarga de un mensaje de autenticación para el usuario.

La entidad de gestión de servicio de comunicaciones de máquina a máquina, ilustrada en cualquiera de las Figuras 9 a 13, incluye, además, un primer módulo de recepción de información de establecimiento operativo 1401 y/o un segundo módulo de recepción de información de establecimiento operativo 1402. Según se ilustra en la Figura 14, otra forma de realización de la presente invención da a conocer una entidad de gestión de servicio de comunicaciones de máquina a máquina, en donde:

el primer módulo de recepción de información de establecimiento operativo 1401 está configurado para recibir información de establecimiento de privacidad de localización directa, en donde la información de establecimiento de privacidad de localización directa se utiliza para permitir directamente que se realice la localización en un dispositivo M2M del mismo tipo que el dispositivo M2M y

el segundo módulo de recepción de información de establecimiento operativo 1402 está configurado para recibir

información de establecimiento de privacidad en área permitida, en donde la información de establecimiento de la privacidad en área permitida se utiliza para permitir a las partes de demanda de servicio de LCS diferentes localizar el dispositivo M2M en áreas diferentes. La entidad de gestión de servicio de comunicaciones de máquina a máquina, según se ilustra en cualquiera de las Figuras 9 a 14, puede incluir, adema, un módulo de adquisición de información de localización 1501. Según se ilustra en la Figura 15, otra forma de realización de la presente invención da a conocer una entidad de gestión de servicio de comunicaciones de máquina a máquina, en donde el módulo de adquisición de información de la localización 1501 está configurado para adquirir información de localización, en donde dicha información de localización incluye información de establecimiento de la privacidad e información del tipo de localización.

La entidad de gestión de servicio de comunicaciones de máquina a máquina, ilustrada en la Figura 15 puede incluir una primera unidad de adquisición 1601, una segunda unidad de adquisición 1602, una tercera unidad de adquisición 1603 o una cuarta unidad de adquisición 1604. Según se ilustra en la Figura 16, otra forma de realización de la presente invención da a conocer una entidad de gestión de servicio de comunicaciones de máquina a máquina, en donde:

la primera unidad de adquisición 1601 está configurada para realizar la adquisición utilizando información de capacidad adquirida comunicada por un dispositivo M2M;
la segunda unidad de adquisición 1602 está configurada para realizar la adquisición utilizando datos de usuario que se adquieren por intermedio de una interfaz Rg en 3GPP;

la tercera unidad de adquisición 1603 está configurada para realizar la adquisición por intermedio de una interfaz de datos de usuario general que se define en OMA SUPM; y

la cuarta unidad de adquisición 1604 está configurada para realizar la adquisición utilizando la información de configuración del usuario que se adquiere por intermedio de una interfaz de programación de aplicación API.

La Figura 17 es un diagrama esquemático de una estructura lógica de un dispositivo de comunicaciones de máquina a máquina según una forma de realización de la presente invención. Para facilitar la descripción, solamente se ilustra una parte relacionada con la forma de realización de la presente invención. El dispositivo de comunicaciones de máquina a máquina ilustrado en la Figura 17 incluye:

un módulo de recepción 1701, configurado para recibir un mensaje de acceso de localización o una demanda de inspección de la privacidad, en donde el mensaje de acceso de la localización o la demanda de inspección de la privacidad se envía por una entidad de gestión de servicio M2M; y

un módulo de reenvío 1702, configurado para reenviar una respuesta de autenticación para la inspección de la privacidad a la entidad de gestión de servicio M2M.

El dispositivo de comunicaciones de máquina a máquina ilustrado en la Figura 17 puede incluir, además, un módulo de adquisición de información de localización 1801. Según se ilustra en la Figura 18, otra forma de realización de la presente invención da a conocer un dispositivo de comunicaciones de máquina a máquina. El módulo de adquisición de información de localización 1801 está configurado para adquirir información de la localización del dispositivo M2M si la respuesta de autenticación es que el dispositivo M2M está autorizado para ser localizado.

El módulo de adquisición de información 1801 ilustrado en la Figura 17 puede incluir, además, una primera unidad de adquisición 1901, una segunda unidad de adquisición 1902 o una tercera unidad de adquisición 1903. Según se ilustra en la Figura 19, otra forma de realización de la presente invención da a conocer un dispositivo de comunicaciones de máquina a máquina, en donde:

la primera unidad de adquisición 1901 está configurada para adquirir información de localización del dispositivo M2M utilizando su propio sistema de posicionamiento global GPS;

la segunda unidad de adquisición 1902 está configurada para adquirir la información de localización del dispositivo M2M desde un elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP y más concretamente, la segunda unidad de adquisición 1902 está configurada para adquirir información de localización por intermedio de un procedimiento de localización MO-LR en donde un identificador de localización de una parte de demanda de servicio de LCS o una entidad de gestión de servicio o una indicación que indica que la información de localización se utiliza para comunicaciones de M2M que están incluidas; y

la tercera unidad de adquisición 1903 está configurada para adquirir la información de localización del dispositivo M2M utilizando una red de sensores inalámbrica WSN y más concretamente, la tercera unidad de adquisición 1903 está configurada a este respecto, con una función de protección de la privacidad de la entidad de gestión de servicio enviando un mensaje de acceso a la localización o una orden de inspección de la privacidad a un nodo de referencia en conformidad con una URI configurada de nodo de referencia.

La Figura 20 es un diagrama esquemático de una estructura lógica de una entidad de gestión de servicio de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención. Para facilitar la descripción, solamente se ilustra una parte relacionada con la forma de realización de la presente invención. La entidad de gestión de servicio de comunicaciones de máquina a máquina, ilustrada en la Figura 20, incluye:

un módulo de conversión 2001, configurado para convertir un mensaje de acceso de localización recibido en señalización de localización que es identificable para un elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP o un registro de perfil de privacidad PPR; y

un módulo de adquisición 2002, configurado para interaccionar con el elemento de red 3GPP o el registro de perfiles de privacidad PPR para adquirir información de localización de un dispositivo M2M.

La Figura 21 es un diagrama esquemático de una estructura lógica de un sistema de protección de la privacidad de comunicaciones de máquina a máquina según una forma de realización de la presente invención. Para facilitar la Escritura de Constitución, solamente se ilustra una parte relacionada con la forma de realización de la presente invención. El sistema ilustrado en la Figura 21 incluye una entidad de gestión de servicio de comunicaciones de máquina a máquina 2101 y un dispositivo de comunicaciones de máquina a máquina 2102, en donde:

la entidad de gestión de servicio de comunicaciones de máquina a máquina 2101 está configurada para, después de recibir un mensaje de acceso a la localización, determinar, en función de la información de localización, una entidad que realiza la inspección de la privacidad e iniciar operativamente la entidad que realiza la inspección de la privacidad para que efectúe dicha inspección de la privacidad; y

el dispositivo de comunicaciones de máquina a máquina 2102 está configurado para recibir un mensaje de acceso a la localización o una demanda de inspección de la privacidad, en donde el mensaje de acceso a la localización o la demanda de inspección de la privacidad se envía por la entidad de gestión de servicio de comunicaciones de máquina a máquina 2101 y para reenviar una respuesta de autenticación para la inspección de la privacidad a la entidad de gestión de servicio de comunicaciones de máquina a máquina.

La Figura 22 es un diagrama esquemático de una estructura lógica de un sistema de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención. Para facilitar la descripción, solamente se ilustra una parte relacionada con la forma de realización de la presente invención. El sistema ilustrado en la Figura 22 incluye una entidad de gestión de servicio de comunicaciones de máquina a máquina 2201 y un servidor de localización del Proyecto de Asociación de la 3ª Generación 2202, en donde:

la entidad de gestión de servicio de comunicaciones de máquina a máquina 2201 está configurada para, después de recibir un mensaje de acceso a la localización, determinar, en función de la información de localización una entidad que realice la inspección de la privacidad e iniciar operativamente la entidad que realiza la inspección de la privacidad para realizar dicha inspección de la privacidad; y

el servidor de localización del Proyecto de Asociación de la 3ª Generación 2202 está configurado para recibir una demanda de servicio de LCS enviada por la entidad de gestión de servicio de comunicaciones de máquina a máquina 2201 y para realizar la inspección de la privacidad.

La Figura 23 es un diagrama esquemático de una estructura lógica de un sistema de protección de la privacidad de comunicaciones de máquina a máquina en conformidad con otra forma de realización de la presente invención. Para facilitar la descripción, solamente se ilustra una parte relacionada con la forma de realización de la presente invención. El sistema ilustrado en la Figura 23 incluye una entidad de gestión de servicio de comunicaciones de máquina a máquina 2301 y un elemento de red 2302 o un registro de perfiles de la privacidad 2303 en una red del Proyecto de Asociación de la 3ª Generación, en donde:

la entidad de gestión de servicio de comunicaciones de máquina a máquina 2301 incluye un módulo de conversión 23011 y un módulo de adquisición 23012;

el módulo de conversión 23011 está configurado para convertir un mensaje de acceso a la localización recibido en señalización de localización que es identificable para el elemento de red 2302 o el registro de perfiles de la privacidad 2303 en la red del Proyecto de Asociación de la 3ª Generación;

el módulo de adquisición 23012 está configurado para interaccionar con el elemento de red del Proyecto de Asociación de la 3ª Generación 2302 o el registro de perfiles de la privacidad 2303 para adquirir información de la localización de un dispositivo de comunicaciones de máquina a máquina; y

el elemento de red 2302 o el registro de perfiles de la privacidad 2303 en la red del Proyecto de Asociación de la 3ª Generación está configurado para adquirir la información de la localización del dispositivo de comunicaciones de

máquina a máquina y proporcionar la información de la localización del dispositivo de comunicaciones de máquina a máquina para la entidad de gestión de servicio de comunicaciones de máquina a máquina 2301.

Conviene señalar que el contenido tal como intercambio de información entre cada módulo/unidad de los aparatos y los procesos de ejecución está basado en las mismas ideas inventivas de las formas de realización del método de la presente invención y por lo tanto, da lugar a los mismos efectos técnicos que las formas de realización del método de la presente invención. Para conocer más detalles, puede hacerse referencia a la descripción en las formas de realización del método de la presente invención, que no se describen aquí de nuevo.

Los expertos en esta técnica pueden entender que la totalidad o parte de las etapas de los métodos en las formas de realización pueden ponerse en práctica mediante un programa informático que proporciona instrucciones a un hardware pertinente. El programa puede memorizarse en un soporte de memorización legible por ordenador y el soporte de memorización puede incluir una memoria de solamente lectura (ROM, Read Only Memory), una memoria de acceso aleatorio (RAM, Random Access Memory), un disco magnético o un disco compacto, etc.

El método y sistema de protección de la privacidad de comunicaciones de máquina a máquina, la entidad de gestión de servicio de comunicaciones de máquina a máquina y el dispositivo relacionado en conformidad con las formas de realización de la presente invención se describen en detalle en la exposición precedente. Realizaciones concretas, a modo de ejemplo, se utilizan para ilustrar principios y modos de puesta en práctica de la presente invención. Las descripciones precedentes sobre las formas de realización se utilizan simplemente como ayuda a entender los métodos e ideas básicas de la presente invención. En conclusión, el contenido de esta especificación no debe interpretarse como una limitación a la presente invención.

REIVINDICACIONES

1. Un método de protección de la privacidad de las comunicaciones de máquina a máquina, M2M, que comprende:

después de recibir un mensaje de acceso a la localización, la determinación (S201), por una entidad de gestión de servicio M2M y en conformidad con la información de localización, una entidad que realiza una inspección de la privacidad; y

iniciar operativamente (S202), por la entidad de gestión de servicio M2M, la entidad que realiza la inspección de la privacidad para efectuar una inspección de la privacidad; caracterizado por cuanto que la inspección de la privacidad comprende que la entidad que realiza la inspección de la privacidad determine si una tercera parte que inicia una orden de adquisición de localización por intermedio de una aplicación M2M, tenga el permiso para acceder a un recurso de localización de un dispositivo M2M y/o de localizar el dispositivo M2M;

y por cuanto que la determinación de la entidad que realiza la inspección de la privacidad comprende:

la información de localización que comprende información de establecimiento de privacidad que está configurada utilizando una aplicación M2M, en la entidad de gestión de servicio M2M y la información de establecimiento de privacidad indica si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en un servidor de localización de Proyecto de Asociación de la 3ª Generación (3GPP);

después de recibir la orden de adquisición de localización, adquirir, por la entidad de gestión de servicio M2M, la información de establecimiento de privacidad y determinar, en función de la información de establecimiento de la privacidad, si la inspección de privacidad se realiza, o no, en la entidad de gestión de servicio M2M o en el servidor de localización de 3GPP.

2. El método según la reivindicación 1, en donde si se determina, en función de la información de localización, que la entidad que realiza la inspección de la privacidad es la entidad de gestión de servicio M2M, iniciar operativamente, mediante la entidad de gestión de servicio M2M, la entidad de gestión de servicio M2M para realizar la inspección de la privacidad.

3. El método según la reivindicación 2, en donde cuando un resultado de la inspección de la privacidad es que un dispositivo M2M está autorizado para ser localizado, enviar, por la entidad de gestión de servicio M2M, una demanda del Servicio de Localización, LCS, a un elemento de red 3GPP y recibir una respuesta de servicio LCS del elemento de red 3GPP; o

enviar, por la entidad de gestión de servicio M2M, una demanda de servicio LCS a un dispositivo M2M y recibir un resultado de localización sobre la localización del dispositivo M2M por el dispositivo M2M; o

enviar, por la entidad de gestión de servicio M2M, una demanda de servicio LCS a un elemento de red de Proyecto de Asociación de la 3ª Generación 3GPP y recibir un resultado de localización de la localización del dispositivo M2M por el elemento de red.

4. El método según la reivindicación 3, en donde la demanda de servicio de LCS comprende un identificador de localización de la entidad de gestión de servicio M2M; o

la demanda de servicio de LCS comprende un identificador de indicación que se utiliza para indicar que el elemento de red 3GPP determina si se realiza, o no, la inspección de la privacidad.

5. El método según la reivindicación 1, en donde si se determina, en función de la información de localización, que la entidad que realiza la inspección de la privacidad es el servidor de localización 3GPP, la iniciación operativa, por la entidad de gestión de servicio M2M, de la entidad que realiza la inspección de la privacidad para realizar dicha inspección de la privacidad, comprende:

enviar, por la entidad de gestión de servicio M2M, una demanda de servicio de LCS al servidor de localización 3GPP y realizar, por el servidor de localización 3GPP, la inspección de la privacidad.

6. El método según la reivindicación 1, en donde antes de la determinación, en función de la información de localización, de una entidad que realice la inspección de la privacidad, el método comprende, además:

adquirir, por la entidad de gestión de servicio M2M, la información de localización, en donde la información de localización comprende información del establecimiento de la privacidad e información del tipo de localización.

7. El método según la reivindicación 6, en donde la adquisición, por la entidad de gestión de servicio M2M, de la información de localización consiste concretamente en:

realizar la adquisición utilizando la información de capacidad adquirida informada por un dispositivo M2M; o

realizar la adquisición utilizando datos de usuarios que se adquieren a partir de una interfaz Rg en el Proyecto de Asociación de la 3ª Generación, 3GPP; o

realizar la adquisición, por intermedio de una interfaz de datos de usuario general que se define en la Gestión del Perfil de Usuario de Servicio SUPM de la Alianza Móvil Abierta, OMA; o

efectuar una adquisición utilizando la información de configuración de usuario que se adquiere por intermedio de una interfaz de programación de aplicación API.

8. Una entidad de gestión de servicio de comunicaciones de máquina a máquina, M2M, que comprende:

un módulo de determinación (901), configurado para, después de recibir un mensaje de acceso a la localización, determinar, en función de la información de localización, una entidad que realice la inspección de la privacidad; y

un módulo de iniciación operativa (902), configurado para iniciar operativamente a la entidad que realiza la inspección de la privacidad para efectuar la inspección de la privacidad; caracterizado por cuanto que la inspección de la privacidad es que la entidad que realiza la inspección de la privacidad determine si una tercera parte que inicia una orden de adquisición de localización, por intermedio de una aplicación de M2M, tiene permiso, o no, para acceder a un recurso de localización de un dispositivo M2M y/o localizar el dispositivo M2M;

y por cuanto que la determinación de la entidad que realiza la inspección de la privacidad comprende: la información de localización que comprende información del establecimiento de la privacidad que está configurada utilizando una aplicación de M2M, en la entidad de gestión de servicio M2M y la información de establecimiento de privacidad indica si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en un servidor de localización del Proyecto de Asociación de la 3ª Generación, 3GPP; después de recibir la orden de adquisición de la localización, adquirir, por la entidad de gestión de servicio M2M, la información del establecimiento de la privacidad y determinar, en función de la información de establecimiento de la privacidad, si se realiza la inspección de la privacidad en la entidad de gestión de servicio M2M o en un servidor de localización 3GPP.

9. La entidad de gestión de servicio de comunicaciones máquina a máquina según la reivindicación 8, en donde si el módulo de determinación determina, en función de la información de localización, que la entidad que realiza la inspección de la privacidad es la entidad de gestión de servicio M2M, el módulo de iniciación operativa inicia la entidad de gestión de servicio M2M para realizar la inspección de la privacidad.

10. La entidad de gestión de servicio de comunicaciones de máquina a máquina según la reivindicación 9, que comprende, además, un primer módulo transceptor (1201), un segundo módulo transceptor (1202) o un tercer módulo transceptor (1203);

el primer módulo transceptor (1201) está configurado para, cuando un resultado de la inspección de la privacidad es que un dispositivo M2M esté autorizado para su localización, enviar una demanda de servicio de LCS a un elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP y recibir una respuesta de servicio de LCS del elemento de red de 3GPP;

el segundo módulo transceptor (1202) está configurado para, cuando un resultado de la inspección de la privacidad es que un dispositivo M2M esté autorizado para su localización, enviar una demanda de servicio de LCS a un elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP y para recibir un resultado de la localización del dispositivo M2M mediante el elemento de red del Proyecto de Asociación de la 3ª Generación 3GPP; y

el tercer módulo transceptor (1203) está configurado para, cuando un resultado de la inspección de la privacidad es que un dispositivo M2M esté autorizado para su localización, enviar una demanda de servicio de LCS al dispositivo M2M y para recibir un resultado de localización del dispositivo M2M mediante el dispositivo M2M.

11. La entidad de gestión de servicio de comunicaciones de máquina a máquina según la reivindicación 10, en donde la demanda de servicio de LCS comprende un identificador de localización de la entidad de gestión de servicio M2M; o

la demanda de servicio de LCS comprende un identificador de indicación y el elemento de red 3GPP determina si realizar, o no, la inspección de la privacidad.

12. La entidad de gestión de servicio de comunicaciones de máquina a máquina según la reivindicación 8, en donde si el módulo de determinación (901) determina, en función de la información de localización, que la entidad que realiza la inspección de la privacidad es un servidor de localización de Proyecto de Asociación de la 3ª Generación 3GPP, el módulo de iniciación operativa comprende:

una unidad de envío de demanda de servicio de LCS, configurada para enviar una demanda de servicio de LCS al servidor de localización 3GPP y el servidor de localización 3GPP realiza la inspección de la privacidad.

13. La entidad de gestión de servicio de comunicaciones de máquina a máquina según la reivindicación 8, que comprende, además:

un módulo de adquisición de información de localización (1501), configurado para adquirir la información de localización, en donde la información de localización comprende información de establecimiento de privacidad e información del tipo de localización.

14. La entidad de gestión de servicio de comunicaciones de máquina a máquina según la reivindicación 13, en donde el módulo de adquisición de información de localización (1501) comprende:

una primera unidad de adquisición (1601), configurada para realizar la adquisición utilizando la información de capacidad adquirida comunicada por un dispositivo M2M; o

una segunda unidad de adquisición (1602), configurada para realizar la adquisición utilizando datos de usuario que se adquieren a partir de una interfaz Rg en la red 3GPP; o

una tercera unidad de adquisición (1603), configurada para realizar la adquisición por intermedio de un interfaz de datos de usuario general que se define en OMA SUPM; o

una cuarta unidad de adquisición (1604), configurada para realizar la adquisición utilizando información de configuración de usuario que se adquiere por intermedio de la interfaz de programación de aplicación API.

15. Un sistema de protección de privacidad de las comunicaciones de máquina a máquina, M2M, que comprende una entidad de gestión de servicio de comunicaciones de máquina a máquina y un servidor de localización del Proyecto de Asociación de la 3ª Generación; en donde

la entidad de gestión de servicio de comunicaciones de máquina a máquina está configurada para, después de recibir un mensaje de acceso a la localización, determinar, en función de la información de la localización, una entidad que realice la inspección de la privacidad e iniciar operativamente la entidad que realiza la inspección de la privacidad para efectuar la inspección de la privacidad; caracterizada por cuanto que la inspección de la privacidad es que la entidad que realiza la inspección de la privacidad determine si una tercera parte que inicia una orden de adquisición de la localización, por intermedio de una aplicación M2M, tiene permiso, o no, para acceder a un recurso de localización de un dispositivo M2M y/o localizar el dispositivo M2M; y

el servidor de localización de Proyecto de Asociación de la 3ª Generación está configurado para recibir una demanda de servicio de LCS enviada por la entidad de gestión de servicio de comunicaciones de máquina a máquina y para realizar la inspección de la privacidad; y

en donde, la determinación de la entidad que realiza la inspección de la privacidad comprende:

la información de localización que comprende información del establecimiento de la privacidad está configurada utilizando una aplicación M2M, en la entidad de gestión de servicio M2M y la información de establecimiento de la privacidad indica si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en un servidor de localización del Proyecto de Asociación de la 3ª Generación 3GPP;

después de recibir la orden de adquisición de localización, adquirir, mediante la entidad de gestión de servicio M2M, la información de establecimiento de la privacidad y determinar, en función de la información de establecimiento de la privacidad, si la inspección de la privacidad se realiza en la entidad de gestión de servicio M2M o en la localización de 3GPP.

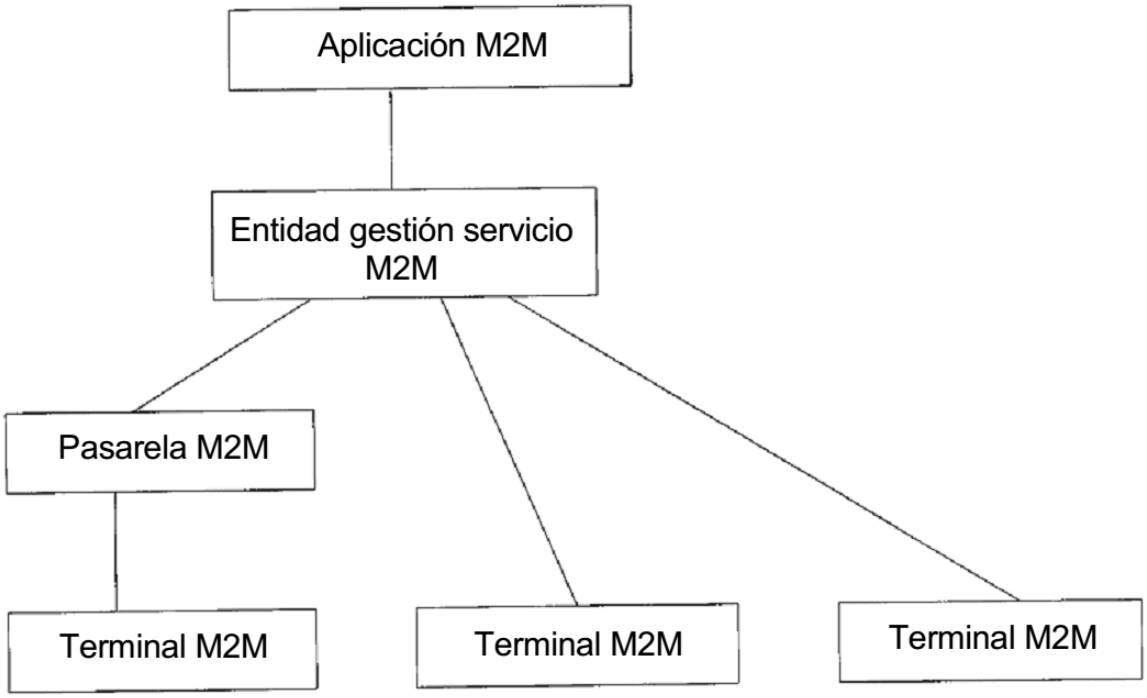
Aplicación M2M
Entidad gestión servicio M2M
Pasarela M2M
Terminal M2M
Terminal M2M
Terminal M2M

FIG. 1-a

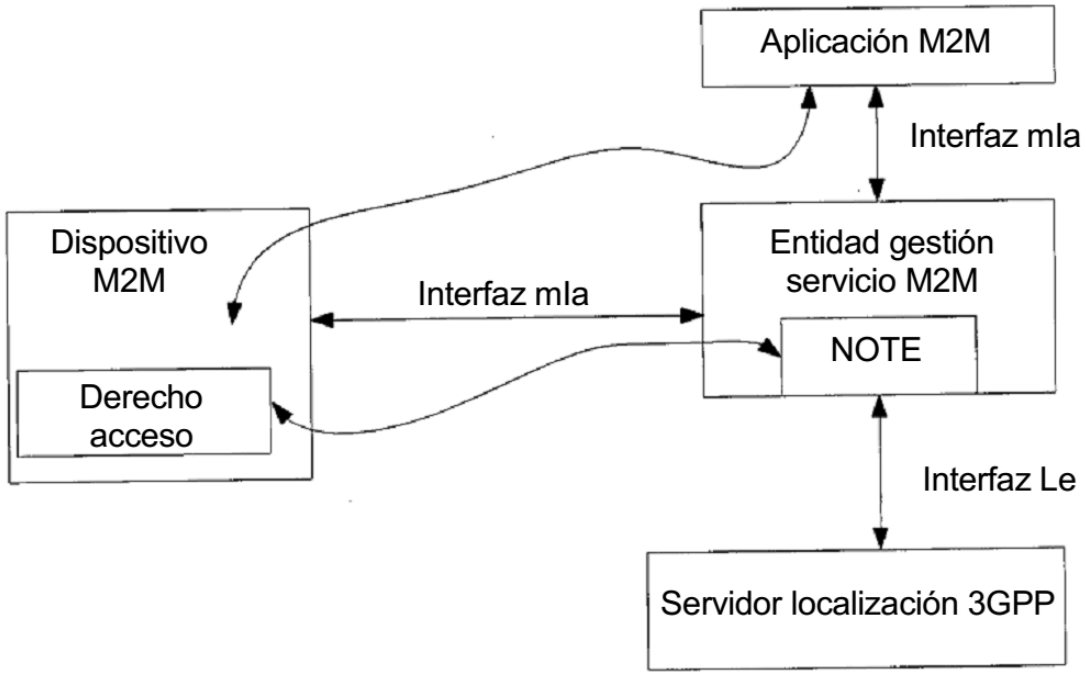
Aplicación M2M
Interfaz mIa
Dispositivo M2M
Interfaz mIa
Entidad gestión servicio M2M
NOTE
Derecho acceso
Interfaz Le
Servidor localización 3GPP

FIG. 1-b

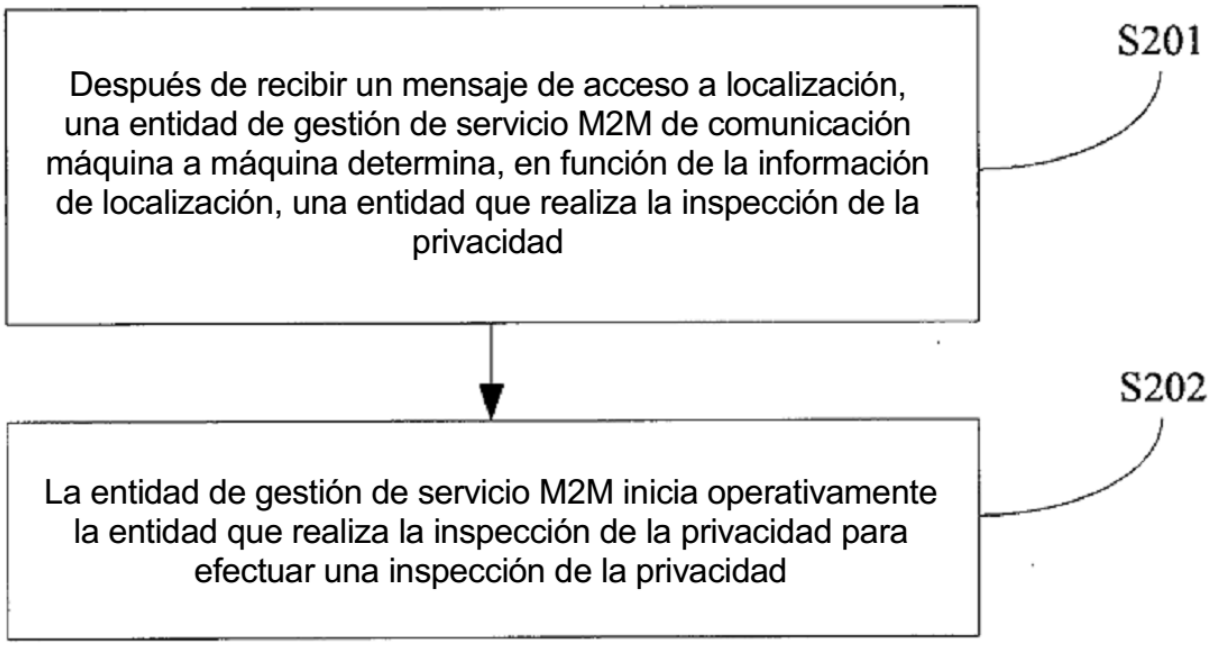
Después de recibir un mensaje de acceso a localización, una entidad de gestión de servicio M2M de comunicación máquina a máquina determina, en función de la información de localización, una entidad que realiza la inspección de la privacidad
S201
La entidad de gestión de servicio M2M inicia operativamente la entidad que realiza la inspección de la privacidad para efectuar una inspección de la privacidad
S202

FIG. 2

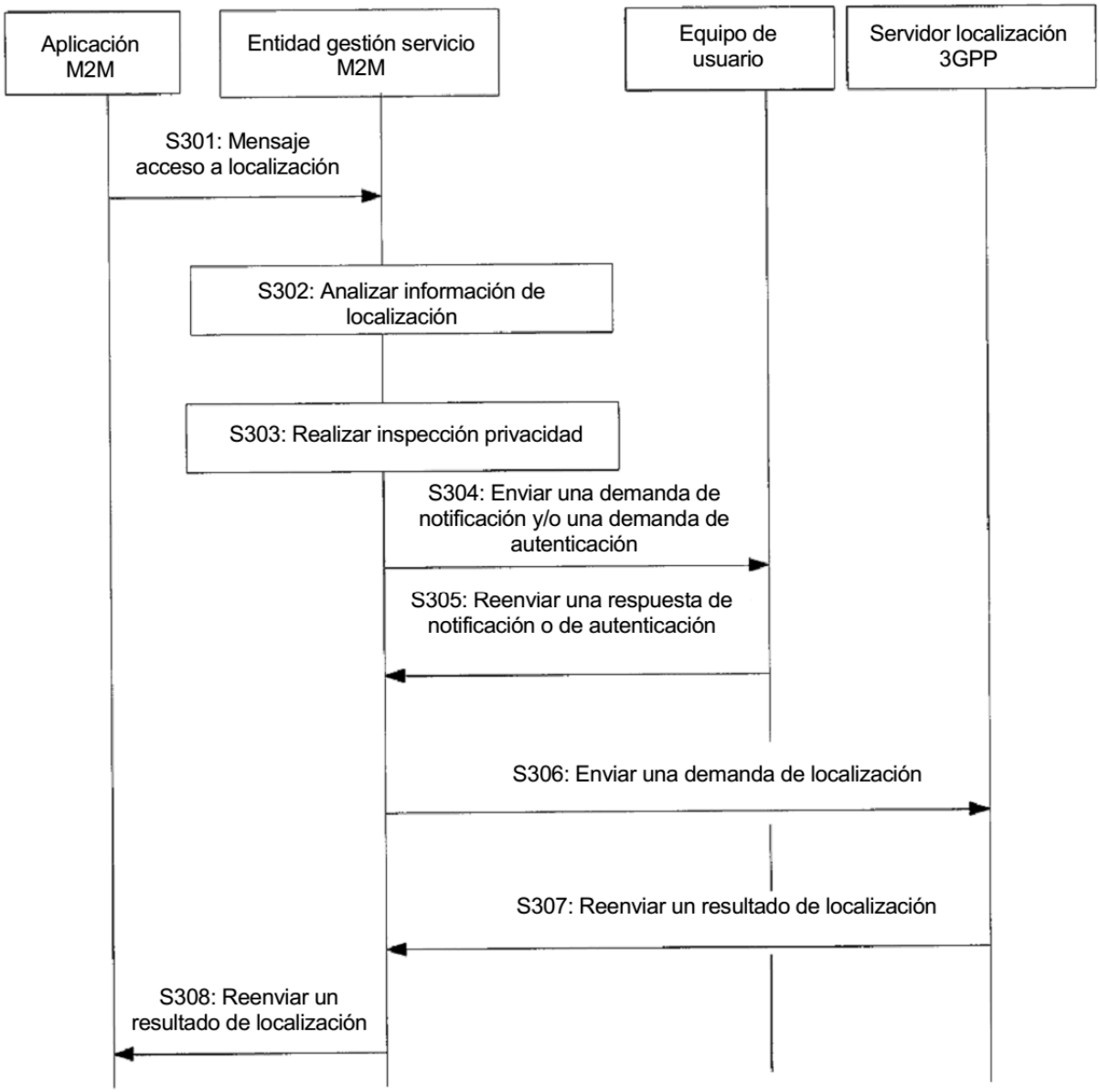
Aplicación M2M
Entidad gestión servicio M2M
Equipo de usuario
Servidor localización 3GPP
S301: Mensaje acceso a localización
S302: Analizar información de localización
S303: Realizar inspección privacidad
S304: Enviar una demanda de notificación y/o una demanda de autenticación
S305: Reenviar una respuesta de notificación o de autenticación
S306: Enviar una demanda de localización
S307: Reenviar un resultado de localización
S308: Reenviar un resultado de localización

FIG. 3-a

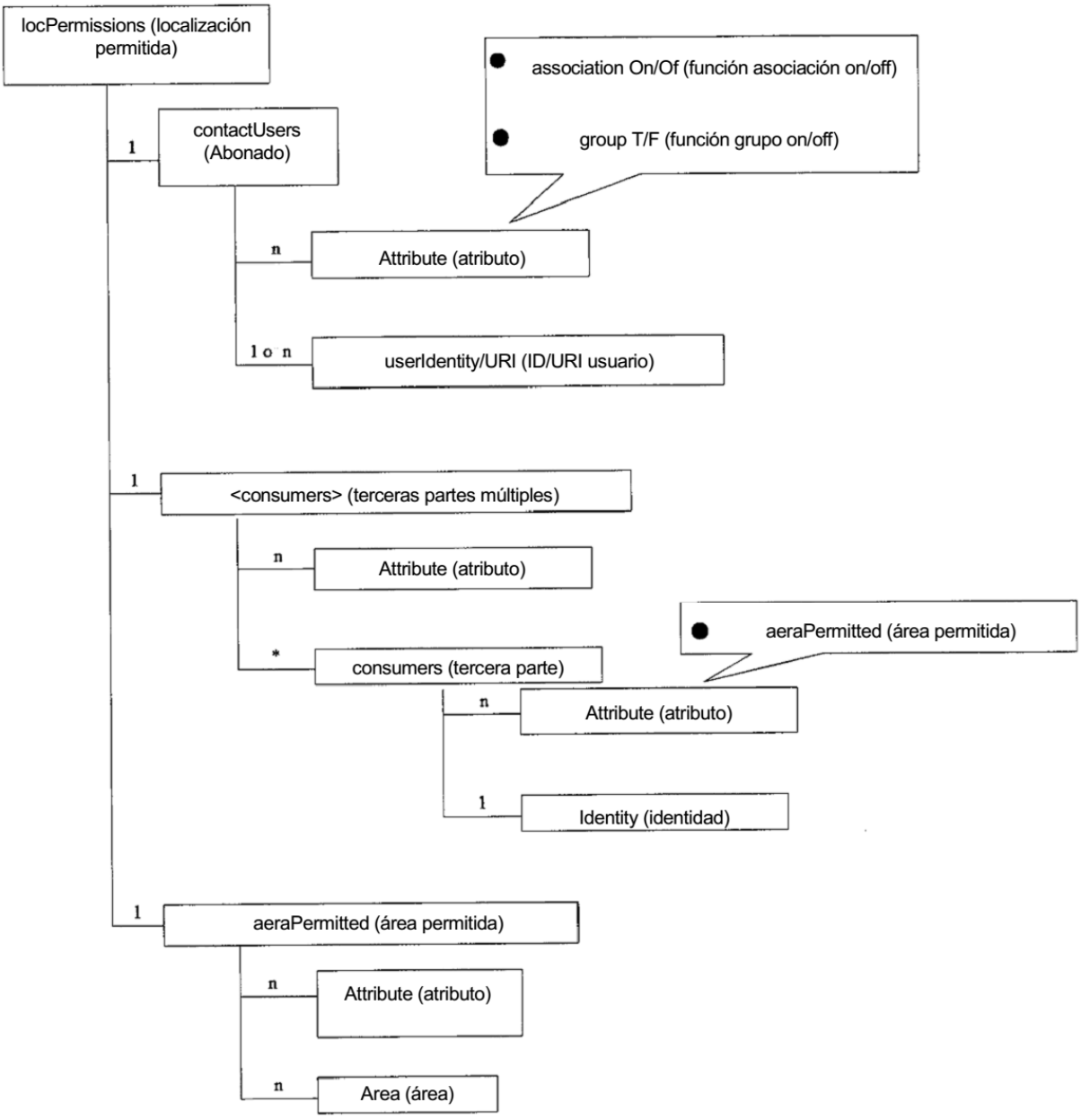
locPermissions (localización permitida)
association On/Of (función asociación on/off)
group T/F (función grupo on/off)
1
contactUsers (Abonado)
n
Attribute (atributo)
1 o n
userIdentity/URI (ID/URI usuario)
1
<consumers> (terceras partes múltiples)
n
Attribute (atributo)
aeraPermitted (área permitida)
*
consumers (tercera parte)
n
Attribute (atributo)
1
Identity (identidad)
1
aeraPermitted (área permitida)
n
Attribute (atributo)
n
Area (área)

FIG. 3-b

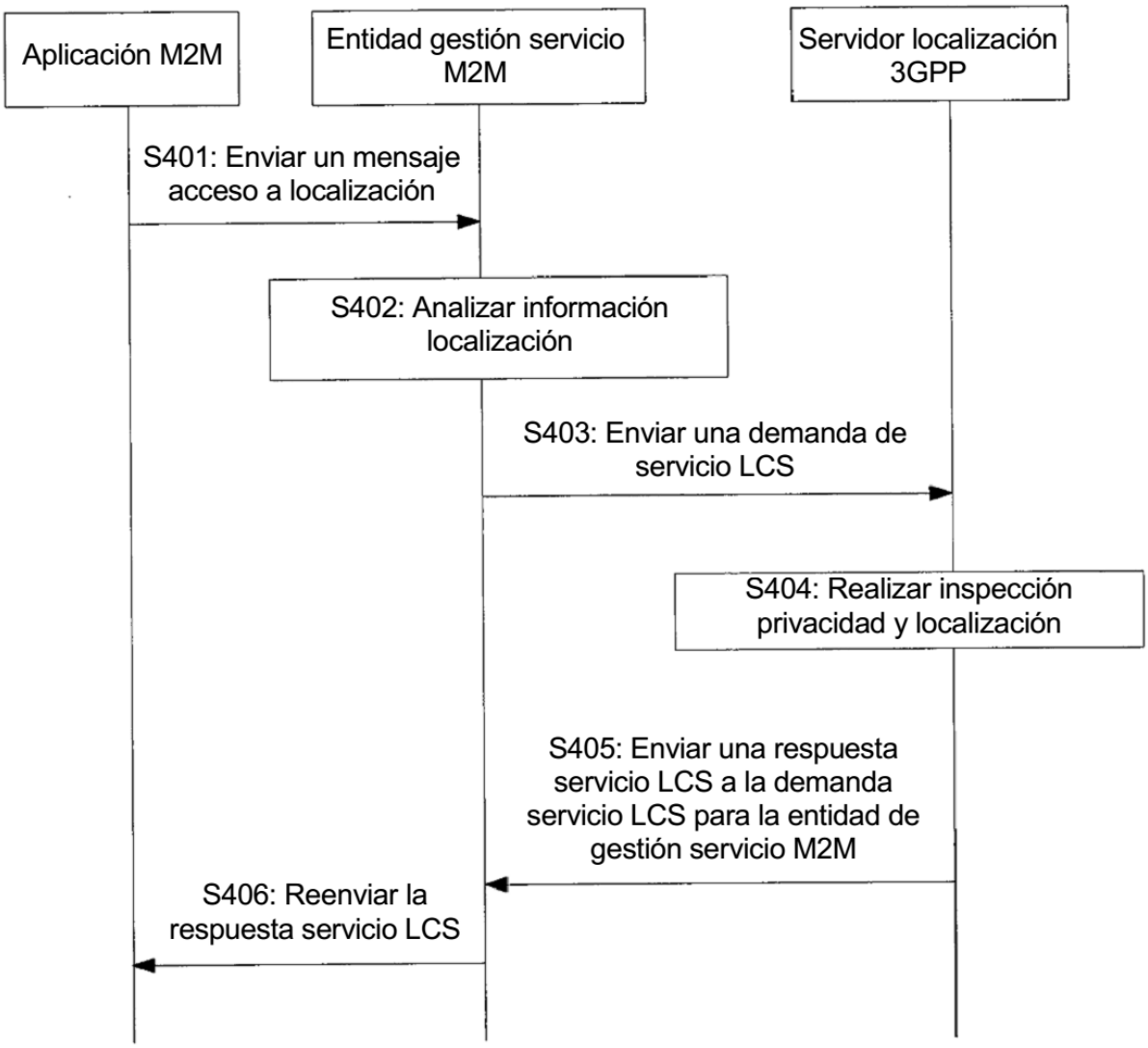
Aplicación M2M
Entidad gestión servicio M2M
Servidor localización 3GPP
S401: Enviar un mensaje acceso a localización
S402: Analizar información localización
S403: Enviar una demanda de servicio LCS
S404: Realizar inspección privacidad y localización
S405: Enviar una respuesta servicio LCS a la demanda servicio LCS para la entidad de gestión servicio M2M
S406: Reenviar la respuesta servicio LCS

FIG. 4

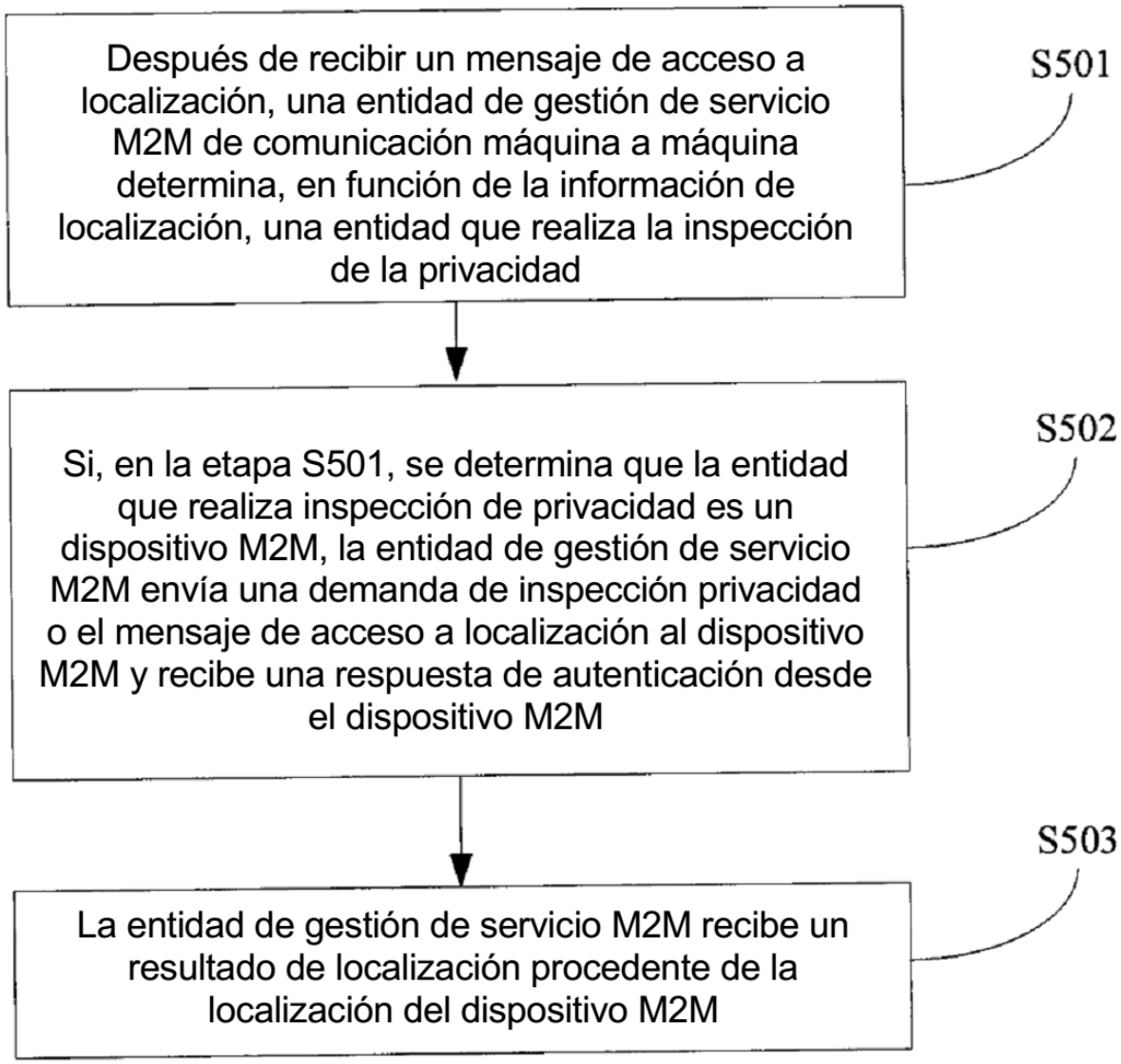
Después de recibir un mensaje de acceso a localización, una entidad de gestión de servicio M2M de comunicación máquina a máquina determina, en función de la información de localización, una entidad que realiza la inspección de la privacidad
S501
Si, en la etapa S501, se determina que la entidad que realiza inspección de privacidad es un dispositivo M2M, la entidad de gestión de servicio M2M envía una demanda de inspección privacidad o el mensaje de acceso a localización al dispositivo M2M y recibe una respuesta de autenticación desde el dispositivo M2M
S502
La entidad de gestión de servicio M2M recibe un resultado de localización procedente de la localización del dispositivo M2M
S503

FIG. 5

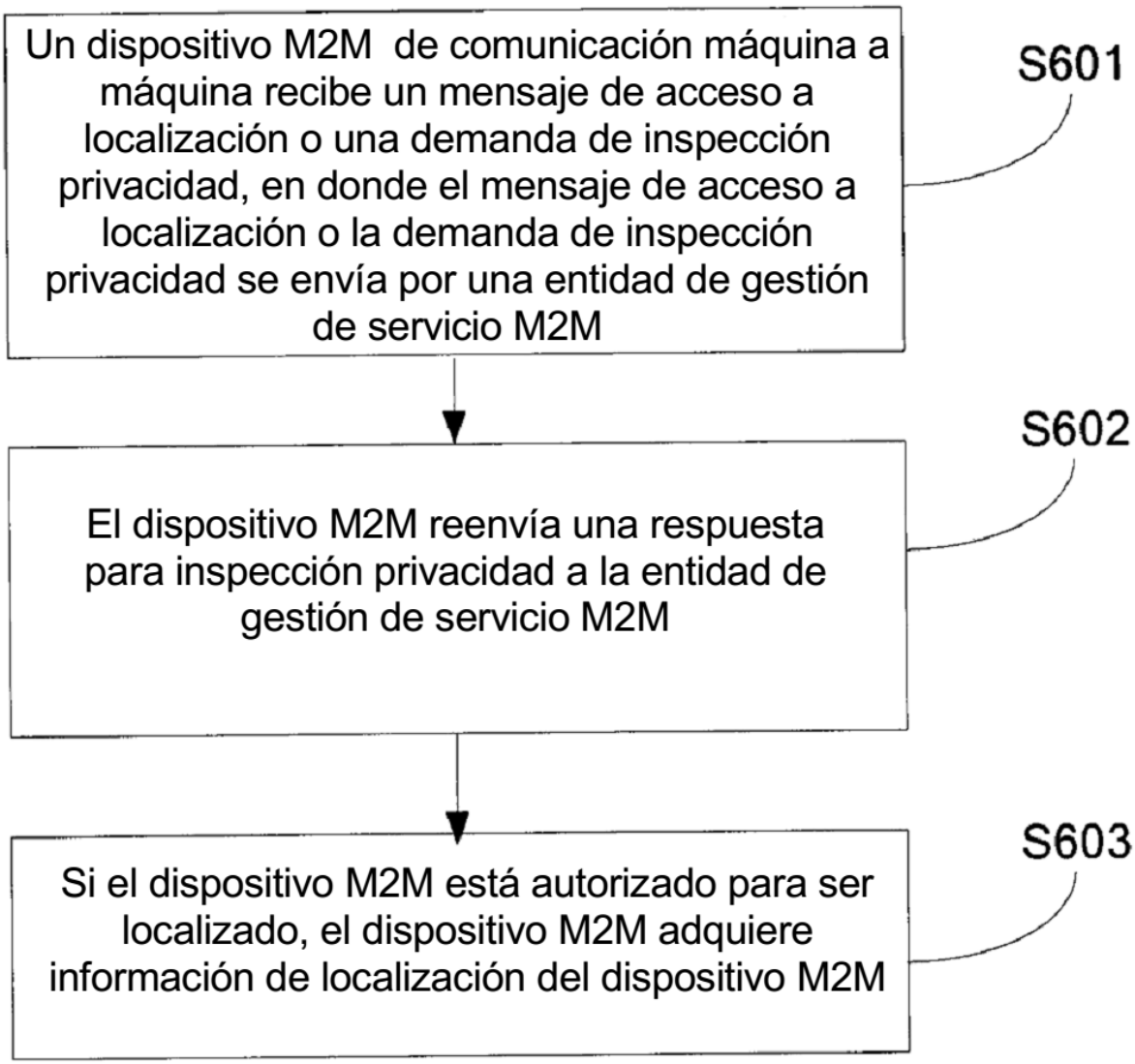
Un dispositivo M2M de comunicación máquina a máquina recibe un mensaje de acceso a localización o una demanda de inspección privacidad, en donde el mensaje de acceso a localización o la demanda de inspección privacidad se envía por una entidad de gestión de servicio M2M
S601
El dispositivo M2M reenvía una respuesta para inspección privacidad a la entidad de gestión de servicio M2M
S602
Si el dispositivo M2M está autorizado para ser localizado, el dispositivo M2M adquiere información de localización del dispositivo M2M
S603

FIG. 6

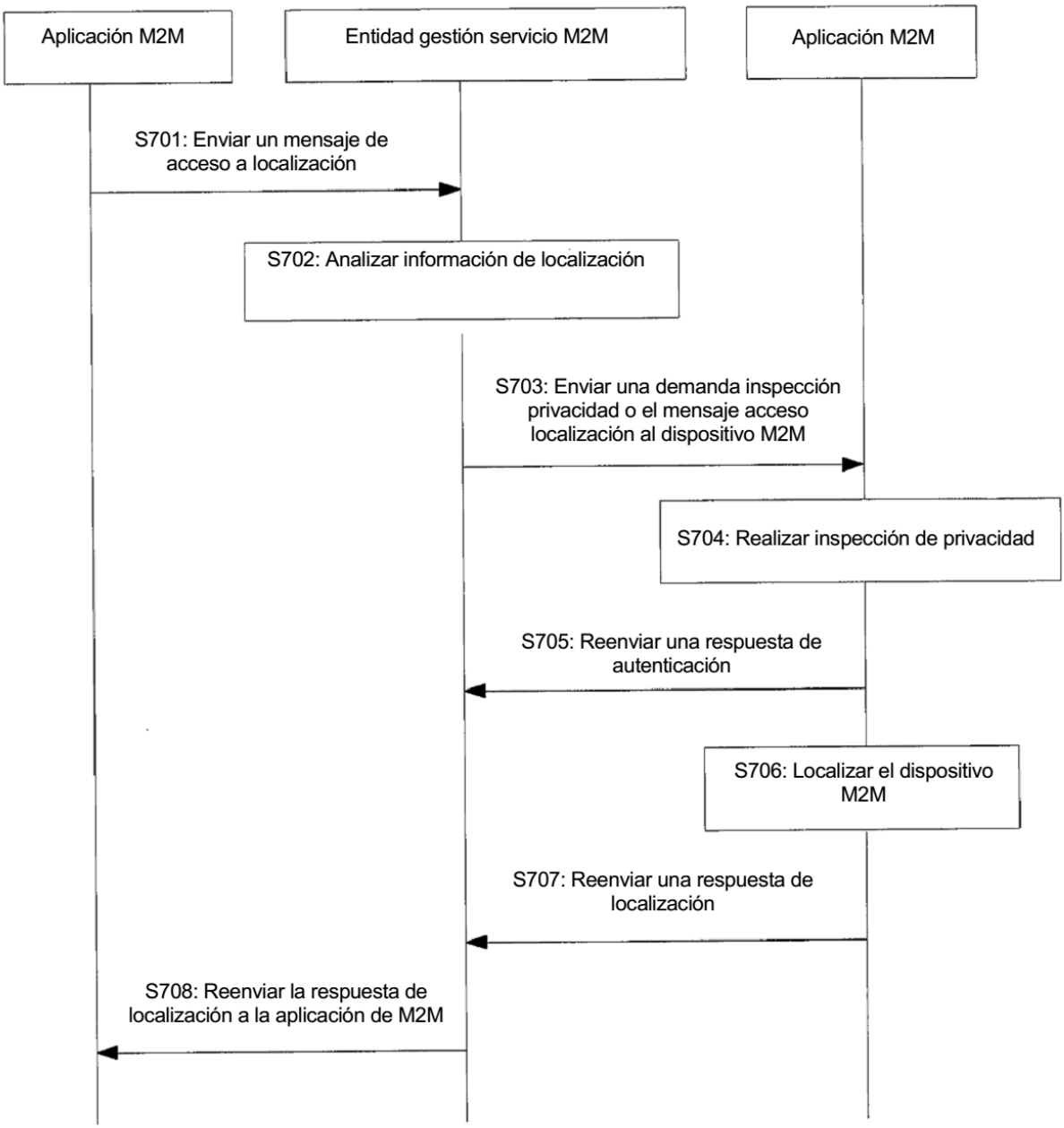
Aplicación M2M
Entidad gestión servicio M2M
Aplicación M2M
S701: Enviar un mensaje de acceso a localización
S702: Analizar información de localización
S703: Enviar una demanda inspección privacidad o el mensaje acceso localización al dispositivo M2M
S704: Realizar inspección de privacidad
S705: Reenviar una respuesta de autenticación
S706: Localizar el dispositivo M2M
S707: Reenviar una respuesta de localización
S708: Reenviar la respuesta de localización a la aplicación de M2M

FIG. 7

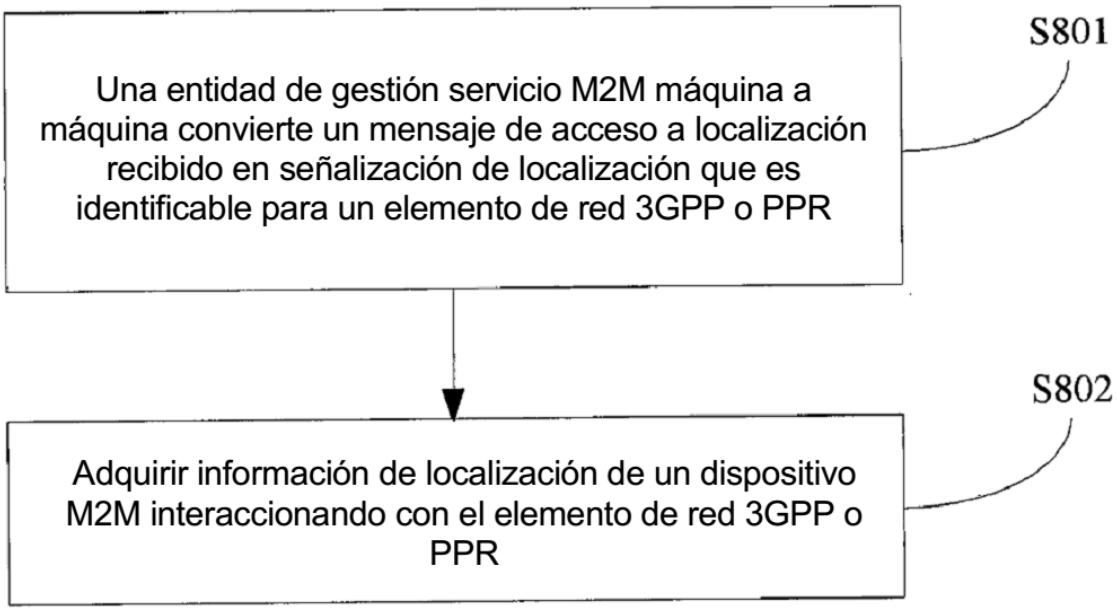
S801
Una entidad de gestión servicio M2M máquina a máquina convierte un mensaje de acceso a localización recibido en señalización de localización que es identificable para un elemento de red 3GPP o PPR
S802
Adquirir información de localización de un dispositivo M2M interaccionando con el elemento de red 3GPP o PPR

FIG. 8

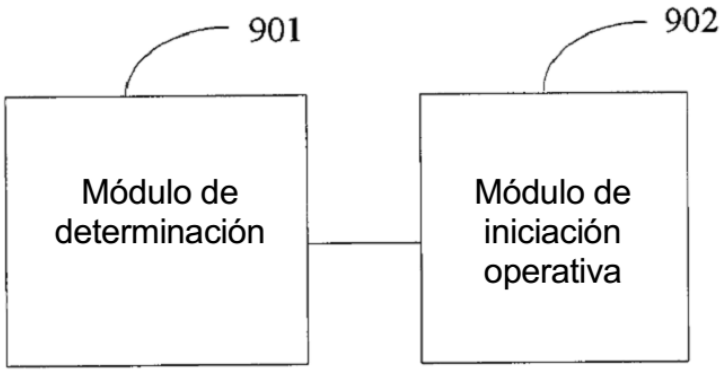
901
902
Módulo de determinación
Módulo de iniciación operativa

FIG. 9

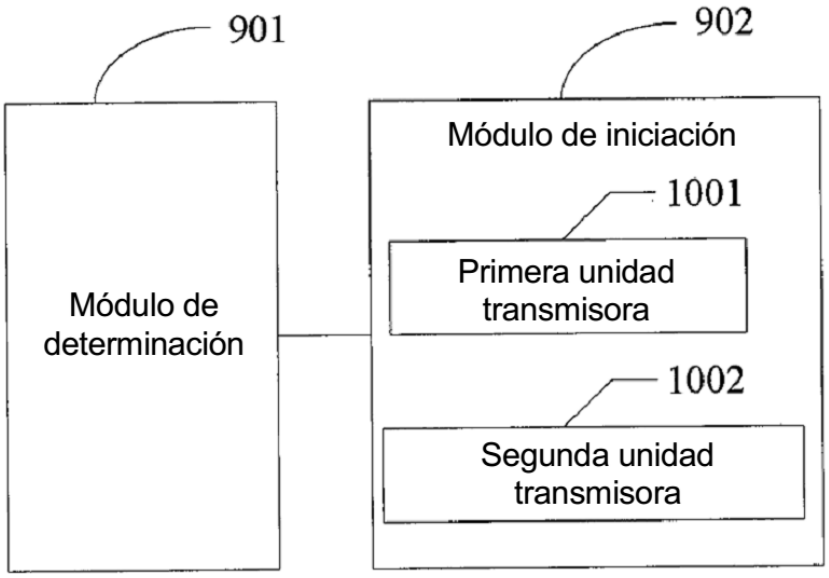
901
902
Módulo de iniciación
1001
Primera unidad transmisora
Módulo de determinación
1002
Segunda unidad transmisora

FIG. 10

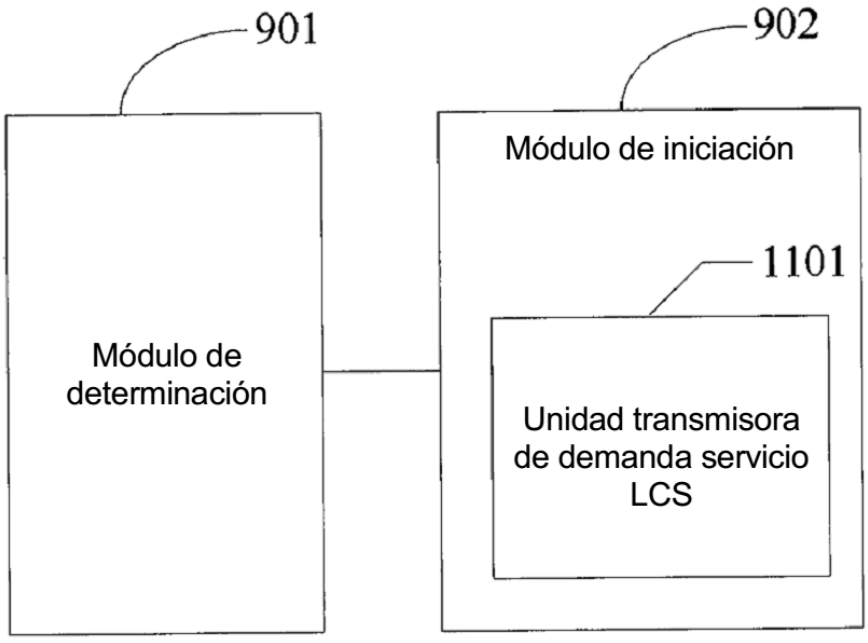
901
902
Módulo de iniciación
1101
Módulo de determinación
Unidad transmisora de demanda servicio LCS

FIG. 11

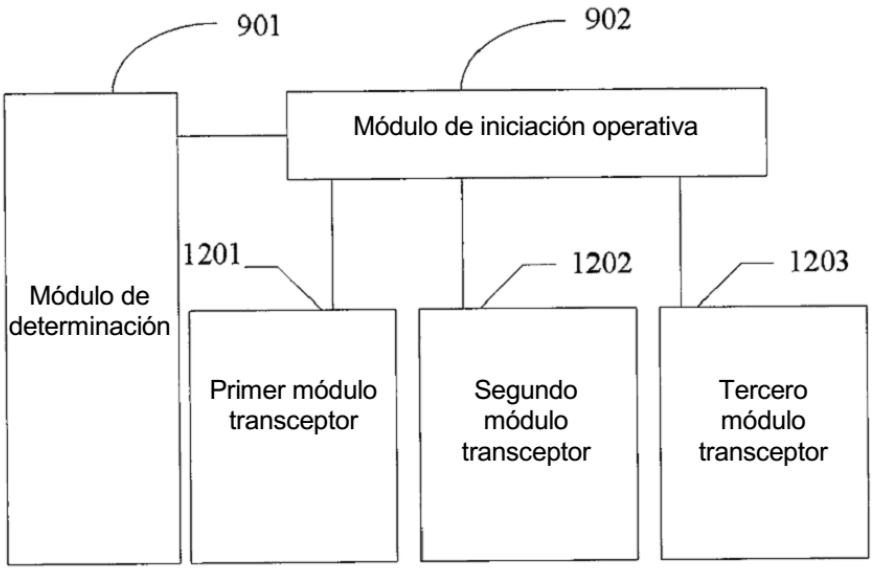
901
902
Módulo de iniciación operativa
Módulo de determinación
1201
1202
1203
Primer módulo transceptor
Segundo módulo transceptor
Tercero módulo transceptor

FIG. 12

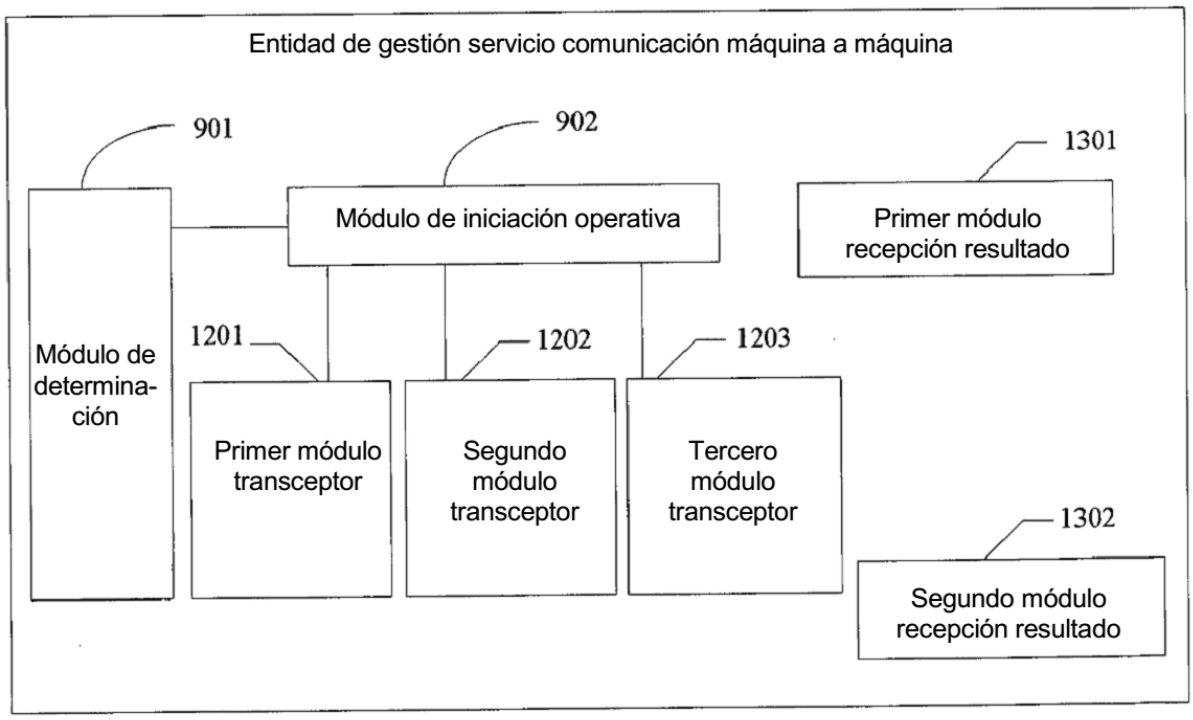
Entidad de gestión servicio comunicación máquina a máquina
901
902
1301
Módulo de iniciación operativa
Primer módulo recepción resultado
Módulo de determina-ción
1201
1202
1203
Primer módulo transceptor
Segundo módulo transceptor
Tercero módulo transceptor
1302
Segundo módulo recepción resultado

FIG. 13

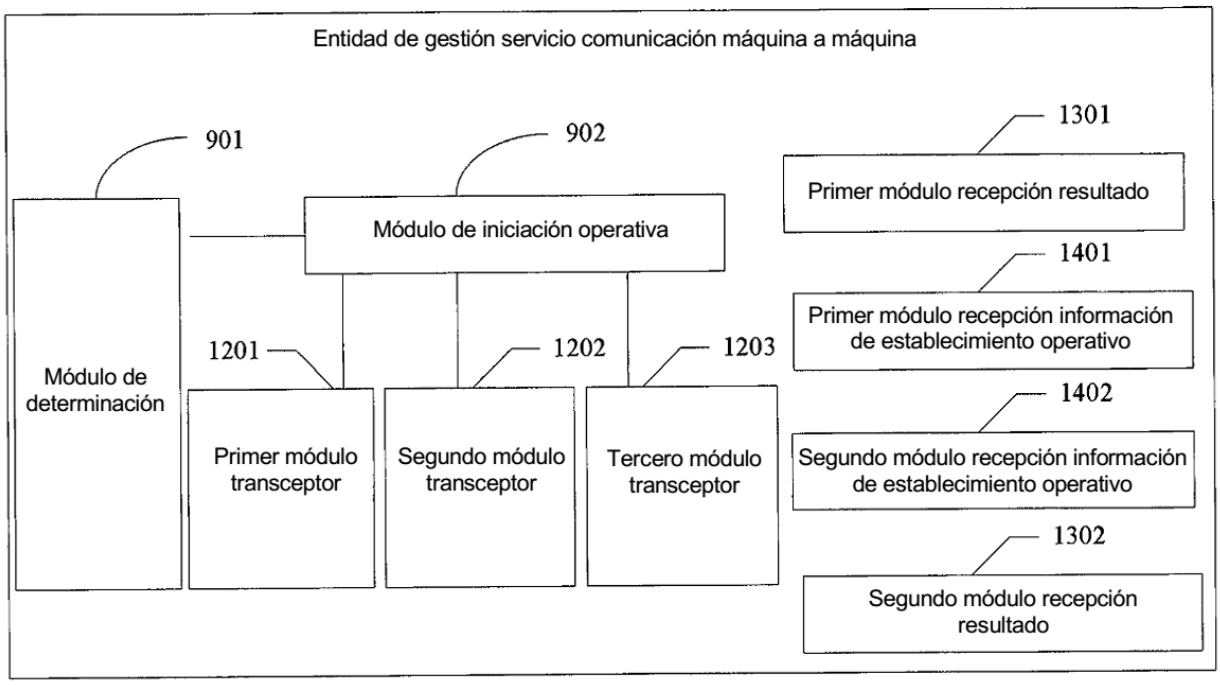
Entidad de gestión servicio comunicación máquina a máquina
901
902
1301
Primer módulo recepción resultado
Módulo de iniciación operativa
1401
Primer módulo recepción información de establecimiento operativo
Módulo de determinación
1201
1202
1203
Primer módulo transceptor
Segundo módulo transceptor
Tercero módulo transceptor
1402
Segundo módulo recepción información de establecimiento operativo
1302
Segundo módulo recepción resultado

FIG. 14

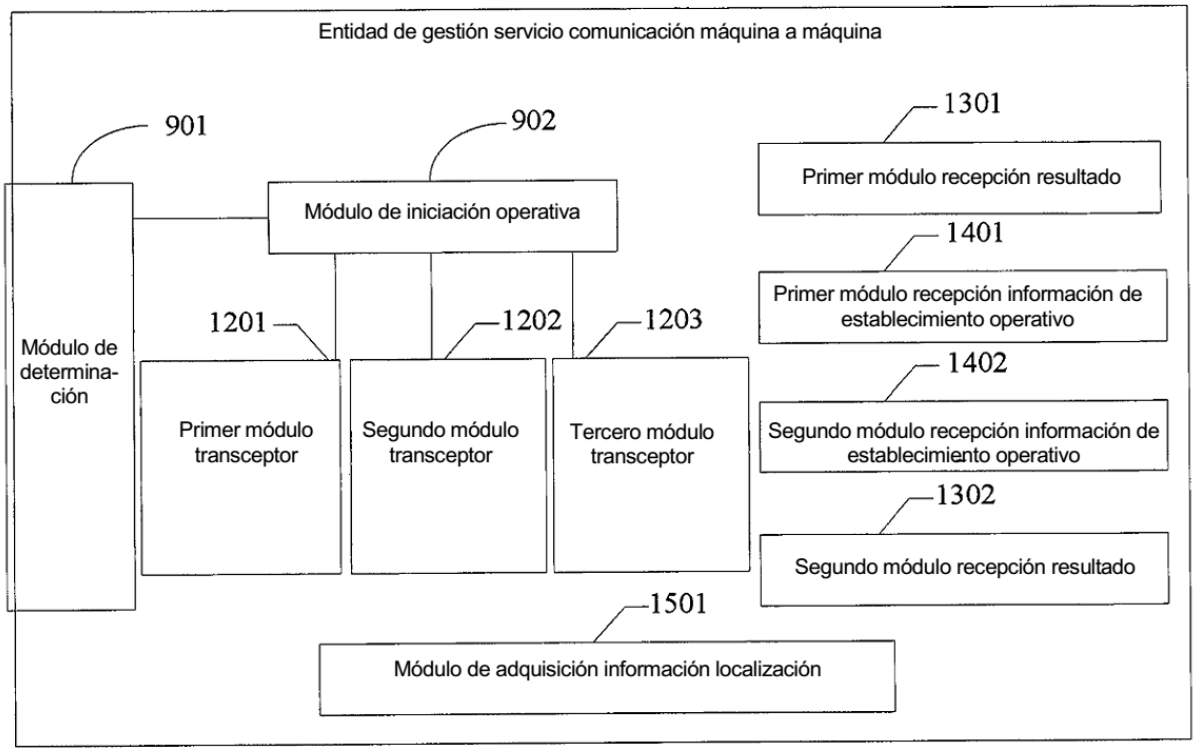
Entidad de gestión servicio comunicación máquina a máquina
901
902
1301
Primer módulo recepción resultado
Módulo de iniciación operativa
1401
Primer módulo recepción información de establecimiento operativo
Módulo de determina-ción
1201
1202
1203
Primer módulo transceptor
Segundo módulo transceptor
Tercero módulo transceptor
1402
Segundo módulo recepción información de establecimiento operativo
1302
Segundo módulo recepción resultado
1501
Módulo de adquisición información localización

FIG. 15

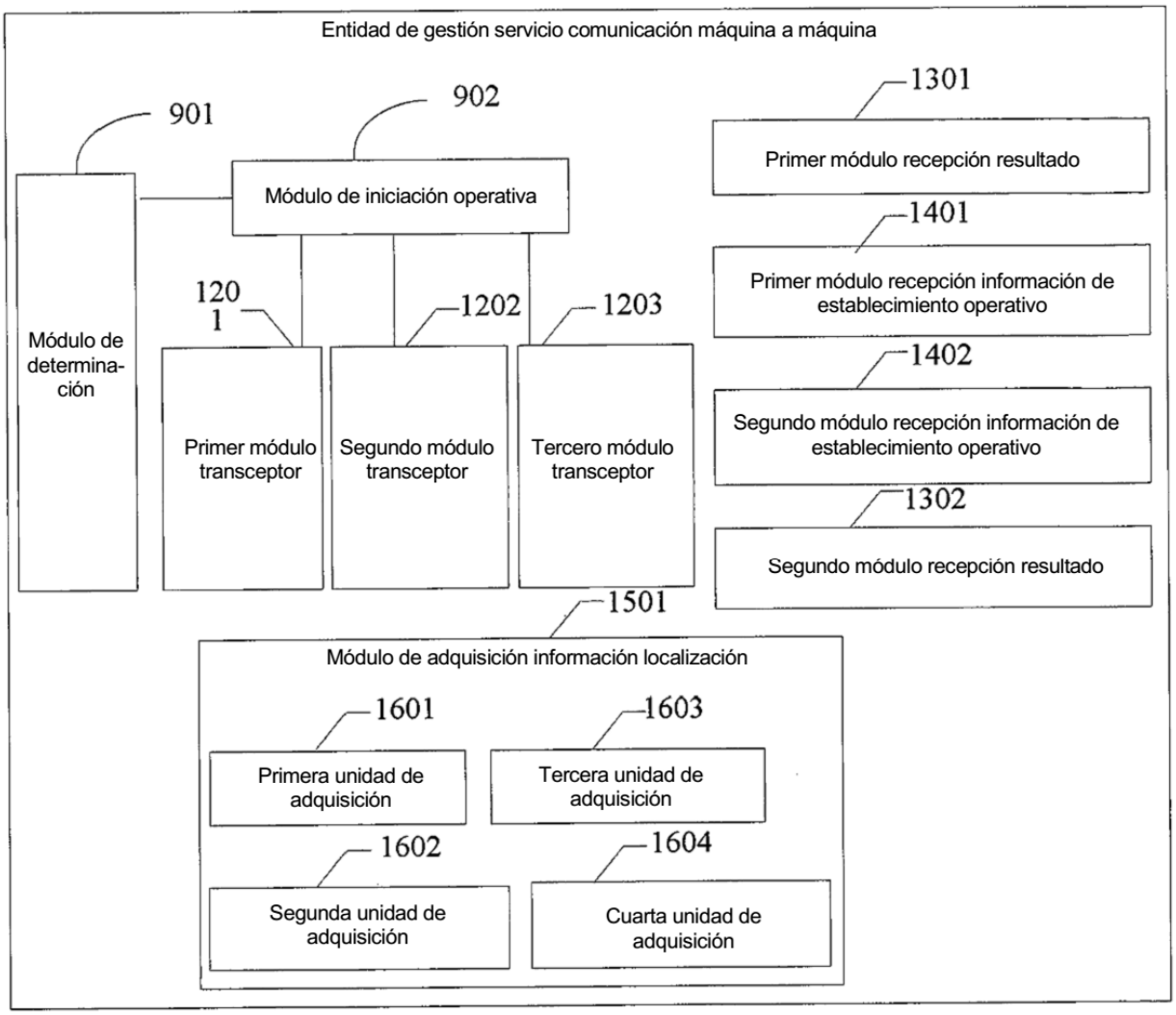
Entidad de gestión servicio comunicación máquina a máquina
901
902
1301
Módulo de determina-ción
Módulo de iniciación operativa
Primer módulo recepción resultado
1401
Primer módulo recepción información de establecimiento operativo
120 1
1202
1203
Primer módulo transceptor
Segundo módulo transceptor
Tercero módulo transceptor
1402
Segundo módulo recepción información de establecimiento operativo
1302
Segundo módulo recepción resultado
1501
Módulo de adquisición información localización
1601
1603
Primera unidad de adquisición
Tercera unidad de adquisición
1602
1604
Segunda unidad de adquisición
Cuarta unidad de adquisición

FIG. 16

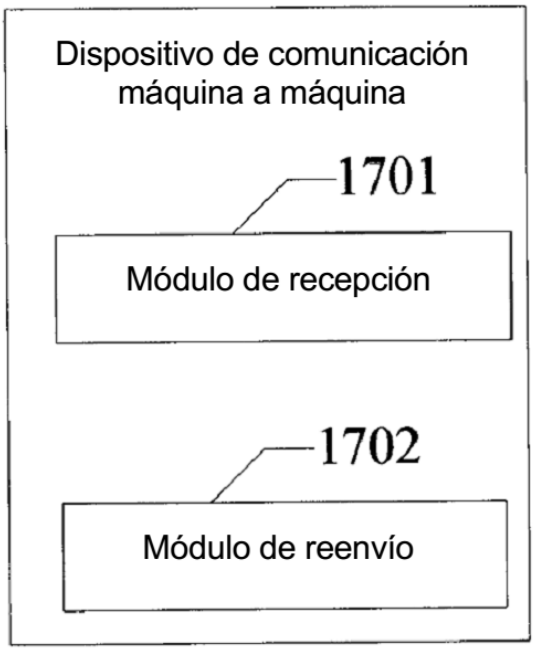
Dispositivo de comunicación máquina a máquina
1701
Módulo de recepción
1702
Módulo de reenvío

FIG. 17

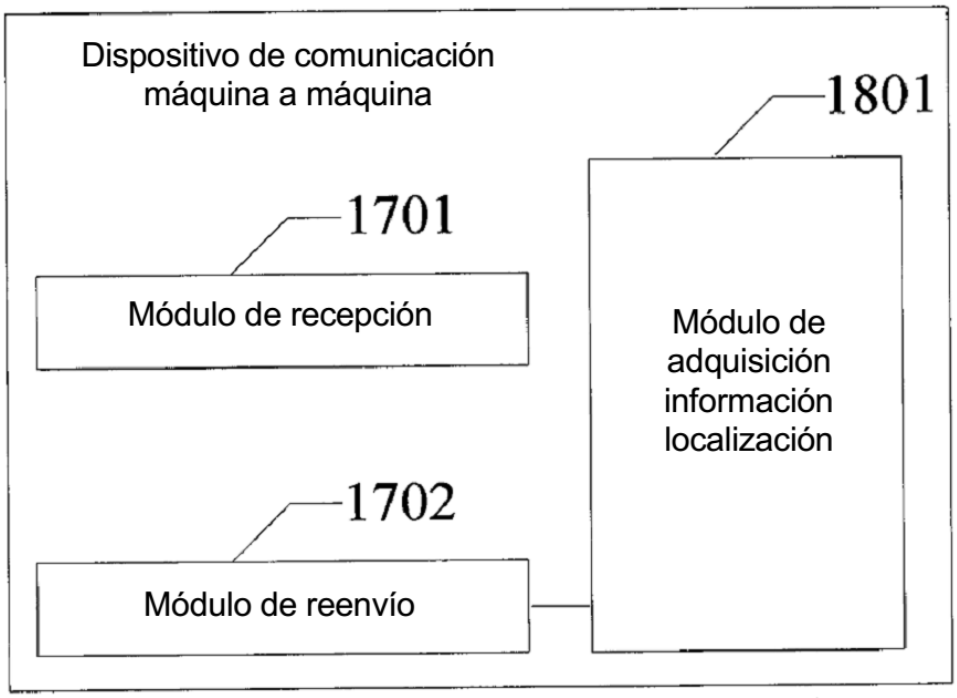
Dispositivo de comunicación máquina a máquina
1801
1701
Módulo de recepción
Módulo de adquisición información localización
1702
Módulo de reenvío

FIG. 18

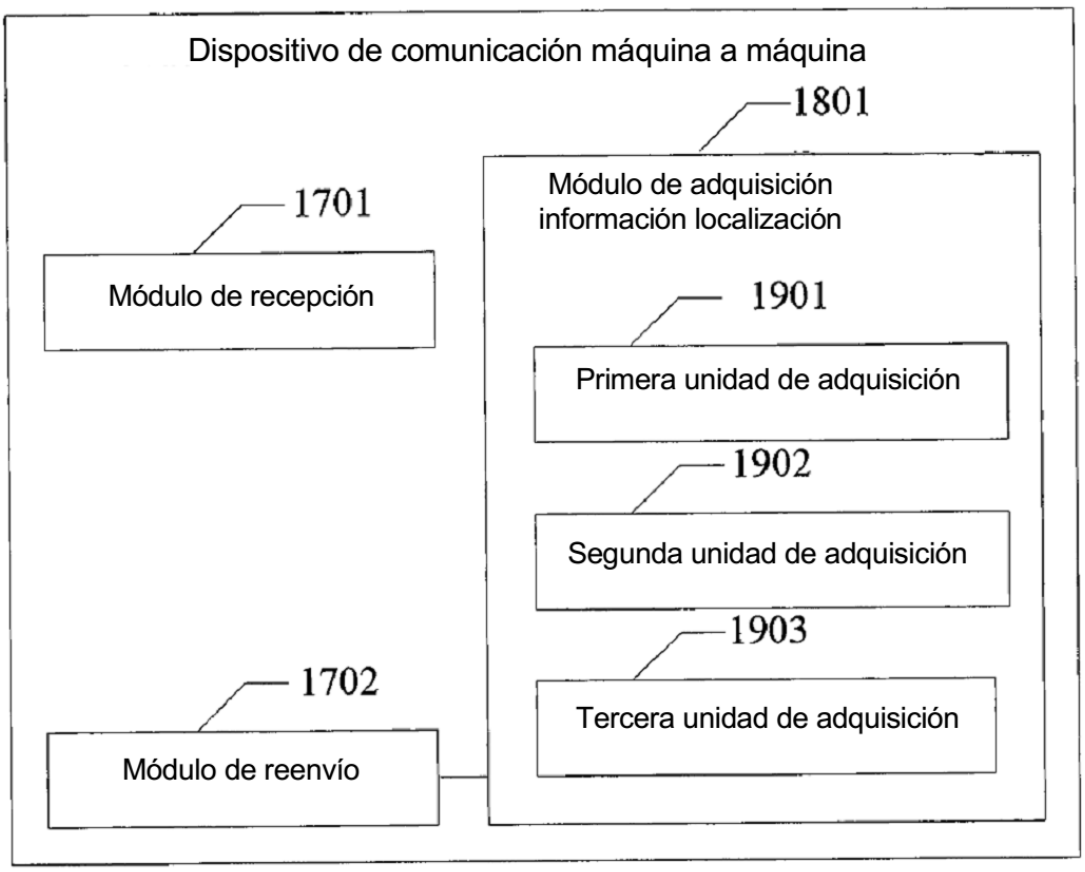
Dispositivo de comunicación máquina a máquina
1801
Módulo de adquisición información localización
1701
Módulo de recepción
1901
Primera unidad de adquisición
1902
Segunda unidad de adquisición
1903
Tercera unidad de adquisición
1702
Módulo de reenvío

FIG. 19

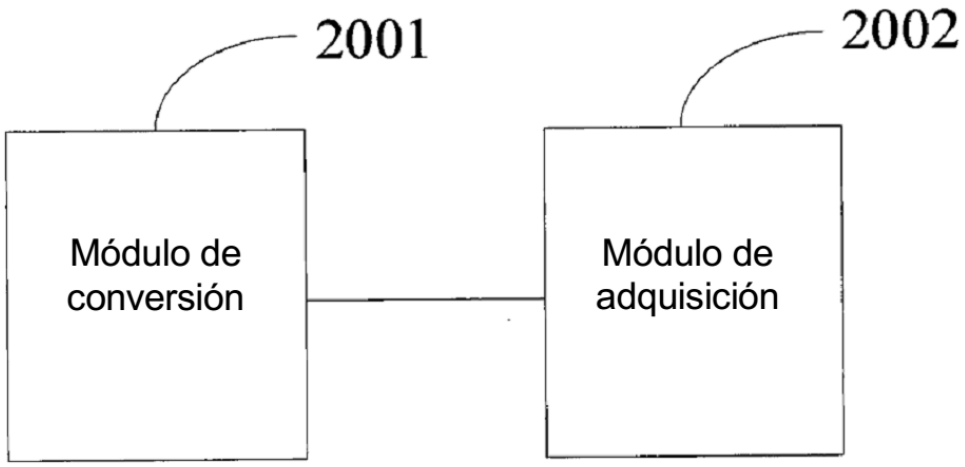
2001
2002
Módulo de conversión
Módulo de adquisición

FIG. 20

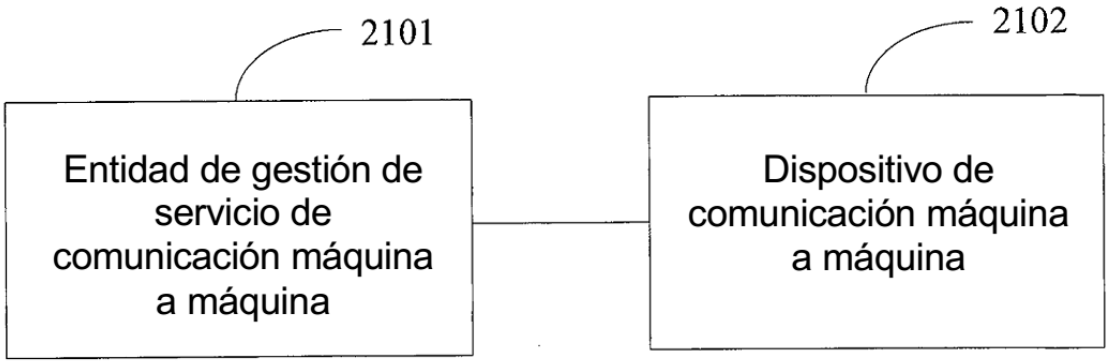
2101
2102
Entidad de gestión de servicio de comunicación máquina a máquina
Dispositivo de comunicación máquina a máquina

FIG. 21

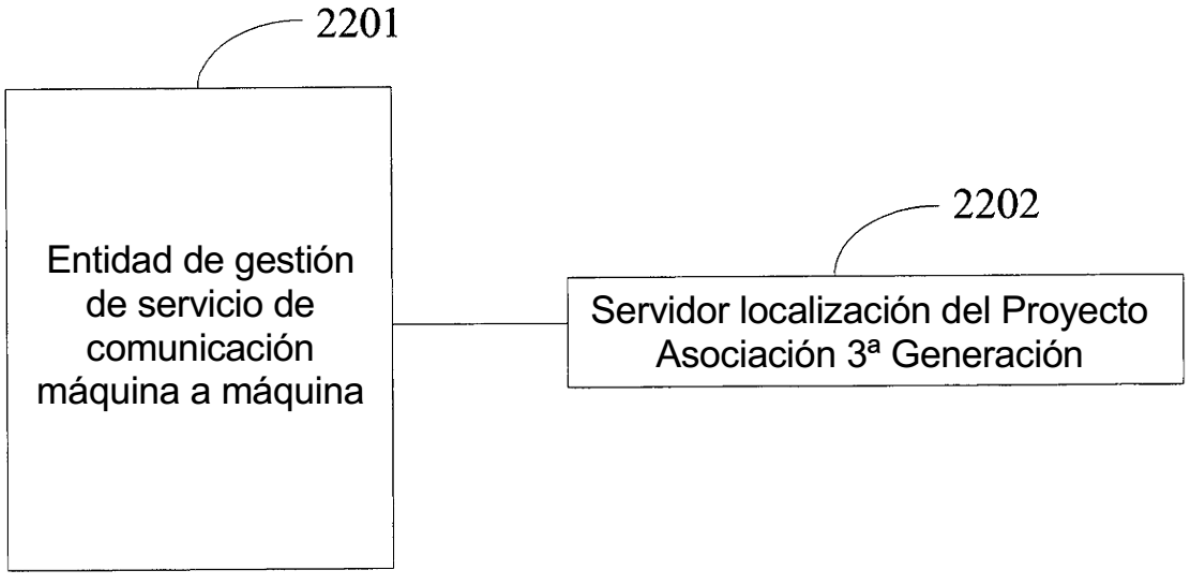
2201
2202
Entidad de gestión de servicio de comunicación máquina a máquina
Servidor localización del Proyecto Asociación 3ª Generación

FIG. 22

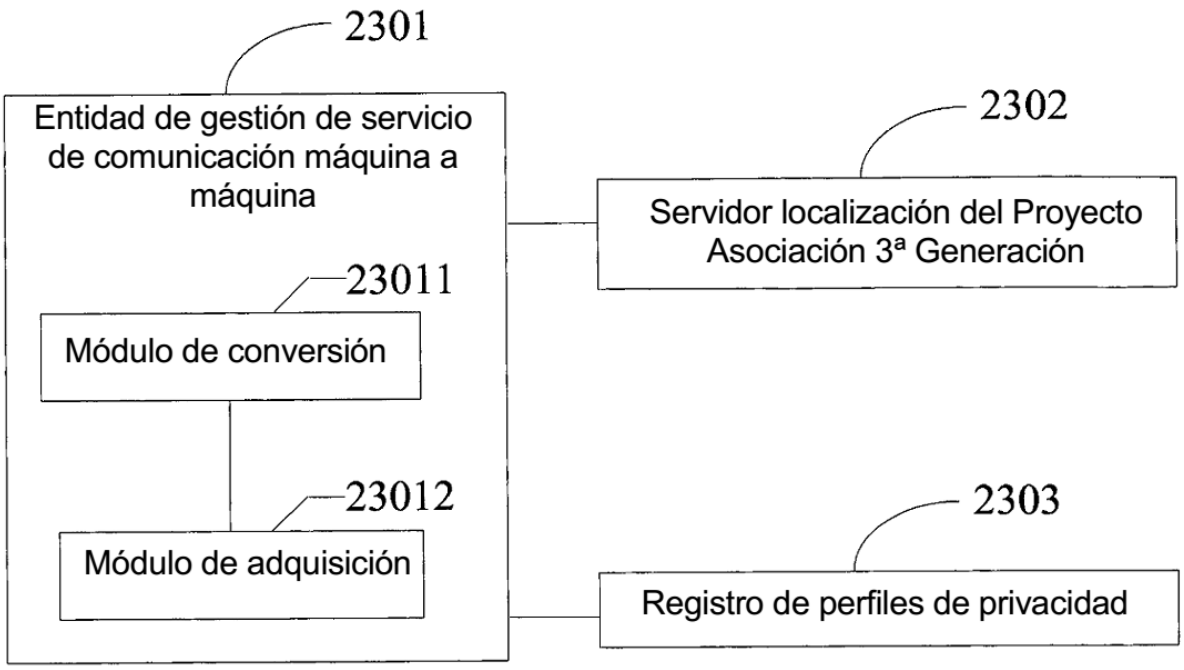
2301
Entidad de gestión de servicio de comunicación máquina a máquina
23011
Módulo de conversión
23012
Módulo de adquisición
2302
Servidor localización del Proyecto Asociación 3ª Generación
2303
Registro de perfiles de privacidad

FIG. 23