(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 672 340**

(51) Int. CI.:

***H04L 29/06*** (2006.01)
***H04W 12/06*** (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.11.2014 PCT/EP2014/075990**

(87) Fecha y número de publicación internacional: **09.07.2015 WO15101451**

(96) Fecha de presentación y número de la solicitud europea: **28.11.2014 E 14808906 (3)**

(97) Fecha y número de publicación de la concesión europea: **03.01.2018 EP 3090520**

(54) Título: **Sistema y método para asegurar las comunicaciones Máquina a Máquina**

(30) Prioridad:

**31.12.2013 EP 13306900**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**13.06.2018**

(73) Titular/es:

**GEMALTO SA (100.0%)**
**6, rue de la Verrerie**
**92190 Meudon, FR**

(72) Inventor/es:

**SMADJA, PHILIPPE;**
**DELSUC, JULIEN;**
**GANEM, HERVÉ y**
**ENNESSER, FRANÇOIS**

(74) Agente/Representante:

**CASANOVAS CASSA, Buenaventura**

DESCRIPCION

Sistema y método para asegurar las comunicaciones Máquina a Máquina

CAMPO TÉCNICO

La presente invención se refiere en general a sistemas y métodos para asegurar las comunicaciones en el internet de las cosas.

Particularmente, la presente invención se refiere a un método y sistema para asegurar el acceso a los recursos en Internet de las cosas.

TÉCNICA ANTERIOR

Muchas nuevas aplicaciones han comenzado a surgir con la expansión del despliegue de infraestructuras de red celular. El mercado de máquina a máquina (M2M) es un segmento especifico que ha ganado un considerable amplio uso. Se predice que este mercado de rápido crecimiento verá miles de millones de máquinas interconectadas en un futuro cercano.

Un sistema M2M tipico comprende un dispositivo M2M, un servidor M2M, una parte de red (que incluye entidades de función lógica tales como un elemento de red de una red de acceso, un elemento de red de una red central, ...). El servidor M2M almacena información de datos relacionados de dispositivos o grupos M2M para proporcionar servicios M2M. Por ejemplo, el dispositivo M2M es un contador de agua o electricidad, y el servidor M2M es un servidor de lectura y procesamiento para el contador de agua o electricidad, que almacena la información de configuración del contador de agua o electricidad y procesa los datos leidos de los medidores en consecuencia .

Los dispositivos M2M difieren de otros suscriptores de red ordinarios principalmente con respecto al uso de datos; generalmente, los dispositivos M2M no son accedidos o programados de manera flexible; y su software no está pensado para operar con la amplia variedad de servicios que un suscriptor humano puede manejar.

En el sistema M2M actual, los datos generados por el dispositivo M2M pueden enviarse directamente a un servidor M2M a través de la red. En otra realización, los datos generados por el dispositivo M2M se envían al servidor M2M a través de una puerta de enlace M2M. Una vez que los datos han llegado al servidor M2M, pueden ponerse a disposición o distribuirse a otras entidades de consumo (a las que se hace referencia como consumidores de recursos), como actuadores conectados o procesadores de datos.

Un inconveniente de la arquitectura M2M antes mencionada es que existen varios riesgos potenciales de seguridad. De hecho, los dispositivos M2M que están situados en lugares desprotegidos de acceso público pueden modificarse fraudulentamente o manipularse de modo inapropiado. Los terminales corruptos se pueden usar para atacar el sistema M2M y/o la red. Los perpetradores de dicho fraude pueden apuntar a un usuario de M2M (por ejemplo, a través de ataques de denegación de servicio, ataques de hombre en el medio, bloqueo de mensajes, etc.), y/o operadores de la Red Móvil Terrestre Pública (PLMN) (por ejemplo, por robo de servicio, etc.). Además, a diferencia de los terminales de propiedad personal, la naturaleza no supervisada de los dispositivos M2M complica la detección y denuncia de uso o modificación fraudulenta.

Una vez que los datos generados por el dispositivo M2M han llegado al servidor M2M, pueden estar disponibles o ser distribuidos a otras entidades de destino (denominadas aplicaciones de consumo de recursos), tales como procesadores de datos.

La arquitectura para el sistema M2M implica dos canales de comunicación distintos, tipicamente asociados a diferentes credenciales: uno desde el objeto al servidor M2M y otro desde el servidor M2M a una entidad de destino, en consecuencia no hay seguridad de extremo a extremo entre las entidades de destino y la fuente de los datos (el dispositivo M2M). La arquitectura suele ser típicamente en la que hay dos saltos de comunicaciones protegidos por credenciales diferentes. Los datos se revelan en el servidor M2M y pueden publicarse para otras entidades.

En este caso, el servidor M2M puede ser pirateado y/o utilizado de manera fraudulenta para rastrear los datos del usuario. En el caso de que el servidor M2M es operado por un proveedor de servicios M2M (estandarizado por ETSI TC M2M o la asociación oneM2M), la aplicación M2M debe confiar en este proveedor de servicios para manipular datos no cifrados que pueden ser confidenciales o privados.

El documento WO2011/163561, 29 Diciembre 2011 (2011-12-29), revela una interfaz de un servidor M2M con red de núcleo 3gpp. Existe una necesidad de una seguridad de extremo a extremo para las comunicaciones de máquina a máquina. Especificamente, existe la necesidad de proteger los datos transmitidos entre un dispositivo M2M y una entidad de destino a través de un servidor M2M.

SUMARIO DE LA INVENCIÓN

El siguiente resumen de la invención se proporciona con el fin de proporcionar una comprensión básica de algunos aspectos y características de la invención. Este resumen no es una descripción general extensa de la invención y, como tal, no pretende identificar particularmente elementos clave o críticos de la invención o delimitar el alcance de la invención. Su único propósito es presentar algunos conceptos de la invención en una forma simplificada como preludio de la descripción más detallada que se presenta más adelante.

La presente invención aborda los inconvenientes de seguridad de la arquitectura M2M antes mencionados. La presente invención se refiere a un sistema y un método para asegurar comunicaciones M2M. Particularmente, la presente invención se refiere a un método y un sistema para proteger el tránsito de datos entre el dispositivo M2M (en general una aplicación de origen) y una entidad de destino (aplicación del consumidor), sobre una posible red no segura o no confiable.

Esta invención se refiere a la implementación de seguridad de extremo a extremo para la comunicación entre objetos en el dominio de Internet de las Cosas (o Internet de Objetos). El objetivo de la patente es lidiar con la configuración de un canal seguro de información autorizado entre la fuente de datos (dispositivo M2M, aplicación de origen u objeto) y los consumidores de datos (entidad de destino, aplicación del consumidor).

De acuerdo con la presente invención, el acceso a un dispositivo M2M (en general la aplicación de origen) por una entidad de destino (aplicación de consumidor) se controla mediante un servidor de autorización M2M. El servidor de autorización M2M es la entidad a cargo de gestionar los derechos de acceso para el dispositivo M2M y toma la decisión con respecto al acceso al recurso por parte de la entidad de destino. A través del servidor de autorización M2M, el usuario establecerá las políticas relacionadas con el acceso al recurso del dispositivo M2M y otorgará el consentimiento para que la entidad de destino acceda al recurso.

El servidor M2M está haciendo cumplir las decisiones tomadas por el servidor de autorización M2M y la concesión/denegación del acceso a la entidad de destino. En la presente invención, el servidor M2M juega el papel de Policy Enforcer y Data-Access Enabler que preferiblemente no tiene acceso para borrar los datos del dispositivo M2M (datos de la aplicación de origen). Los datos transferidos a través del servidor M2M se cifran entre la aplicación del consumidor y el dispositivo M2M; esto permite la seguridad de extremo a extremo entre la aplicación del consumidor y el dispositivo M2M (aplicación de origen). La seguridad puede reforzarse mediante el establecimiento de un canal de comunicación seguro entre el dispositivo M2M y el servidor M2M y otro canal de comunicación segura entre el servidor M2M y la aplicación del consumidor.

Cuando una aplicación de consumidor necesita comunicarse con un dispositivo M2M, la presente invención propone un método para asegurar los datos transferidos entre la aplicación del consumidor y el dispositivo M2M (en general la aplicación de origen). Para ello, la presente invención propone un método para encriptar y autorizar la comunicación entre la aplicación del consumidor y el dispositivo M2M utilizando el servidor M2M que se ejecuta como Data Access Enabler y Policy Enforcer.

Cuando la aplicación del consumidor desea recibir las credenciales para acceder al dispositivo M2M, autentica el servidor de autorización M2M. Cuando la autenticación es exitosa, el servidor de autorización M2M calcula un token de acceso y calcula o genera claves de sesión y una clave de autenticación. El token de acceso, la clave de autenticación y las claves de sesión se envían a la aplicación del consumidor.

Cuando la aplicación del consumidor desea acceder a los datos del dispositivo M2M, calcula los datos de autenticación utilizando la clave de autenticación y envía el token de acceso y los datos de autenticación al servidor M2M, el servidor M2M comprueba el token de acceso y utiliza los datos de autenticación para verificar si la aplicación del consumidor es válida (cumplimiento de política). El servidor M2M también realiza una gestión anti-repetición. Si todas las verificaciones son exitosas, el servidor M2M devuelve los datos encriptados solicitados.

Los aspectos de las realizaciones de la presente invención se refieren en general a un método para generar claves de sesión de cifrado. Estas claves de sesión se pueden generar de acuerdo con los siguientes pasos:

- cuando una aplicación de consumidor M2M recibe una solicitud para comunicarse con un dispositivo M2M, la aplicación de consumidor genera una datos de sesión única (preferiblemente datos aleatorios),
- la aplicación de consumidor solicita credenciales de seguridad del servidor de autorización M2M, esta solicitud comprende los datos criptográficos calculados sobre los datos de sesión únicos generados,
- al recibir esta solicitud, el servidor de autorización M2M devuelve las credenciales de seguridad. Las credenciales de seguridad pueden comprender las claves de sesión, una clave de autenticación y un token de acceso. El token de acceso puede comprender los datos criptográficos y en algunas realizaciones los índices de las claves de sesión y, en algunas otras realizaciones, las claves de sesión se cifran con una clave de dispositivo M2M compartida entre el servidor de autorización M2M y el dispositivo M2M. El contenido del token de acceso puede ser cifrado por el servidor de autorización M2M.
- a la recepción, la aplicación del consumidor elabora un mensaje de autenticación que comprende los datos de

sesión única y un contador de solicitudes del consumidor que se cifran con la clave de autenticación. Este mensaje de autenticación y el token de acceso se envían al servidor M2M.

- a la recepción, el servidor M2M, en caso de que el token de acceso esté cifrado, descifra el contenido del token de acceso utilizando el algoritmo relacionado con la clave correspondiente. Si el token de acceso no está encriptado, la solicitud al servidor M2M puede ser transportada a través de un canal seguro como SSL/TLS. Desde la clave de autenticación del (descifrado) token de acceso, el servidor M2M descifra el mensaje de autenticación. A partir del mensaje de autenticación descifrado, el servidor M2M recalcula los datos criptográficos de los datos de sesión única y los compara con los datos criptográficos del token de acceso. Como solo la aplicación del consumidor conoce los datos de sesión única, esta comparación permite al servidor M2M tener la seguridad de que la aplicación para el consumidor es respaldada por el sistema de seguridad.

El servidor M2M puede ser capaz de comprobar la autenticidad del token de acceso o verificando una firma del token de acceso generado por el servidor de autorización M2M, o verificando en el token de acceso algunos datos de autenticación compartidos entre el servidor de autorización M2M y el servidor M2M o accediendo al servidor de autorización M2M.

El servidor M2M comprueba que el contador de solicitudes del consumidor del mensaje de autenticación descifrado sea mayor que el anterior almacenado en la base de datos del servidor M2M (gestión anti-reproducción). Si tiene éxito, almacena el nuevo contador de solicitudes del consumidor asociado al token de acceso en su base de datos.

Opcionalmente, el servidor M2M puede reforzar su decisión autenticándose en el servidor de autorización M2M. En este caso, el servidor M2M solicita una validación del token de acceso por parte del servidor de autorización M2M.

Todas estas verificaciones realizadas permiten que el servidor M2M sepa que la aplicación del consumidor está autorizada para acceder al recurso del dispositivo M2M. De esta forma, el servidor M2M no necesita tener conocimiento de las aplicaciones del consumidor autorizadas; delega esta gestión al servidor de autorización M2M. A continuación, el servidor M2M o devuelve los datos cifrados del Dispositivo ya recibidos o envía la solicitud al Dispositivo M2M.

Cuando el dispositivo M2M recibe una solicitud de la aplicación del consumidor a través del servidor M2M para acceder a sus recursos, el dispositivo M2M recupera las claves de sesión correspondientes a la solicitud. En una realización, el dispositivo M2M recibe del servidor M2M las claves de sesión cifradas con una clave de dispositivo M2M (compartida entre el servidor de autorización M2M y el dispositivo M2M). El dispositivo M2M descifra las claves de sesión. En otra realización, el dispositivo M2M recibe los identificadores de las claves de sesión, en este caso, el dispositivo M2M puede autenticarse al servidor de autorización M2M y solicita las claves de sesión al servidor de autorización M2M; si la autenticación del dispositivo M2M es exitosa, el servidor de autorización M2M devuelve las claves de sesión.

El dispositivo M2M descifra la solicitud de acceso, procesa la solicitud, elabora la correspondiente respuesta, cifra la respuesta con las claves de sesión y devuelve la respuesta cifrada a la aplicación del consumidor a través del servidor M2M. El dispositivo M2M también puede enviar de forma asíncrona datos cifrados al servidor M2M.

En caso de que el Dispositivo M2M no tenga posibilidad de conectarse de manera segura al Servidor de Autorización M2M, por cualquier razón, o el dispositivo M2M no se puede configurar para establecer la clave usada para encriptar las claves de sesión, el mismo Servidor M2M puede desempeñar el papel del Dispositivo M2M vis-a-vis con el servidor de autorización M2M para recuperar las claves de sesión de la autorización M2M o descifrar las claves de sesión cifradas dentro de esta clave de cifrado del servidor M2M de las claves de sesión. Al finalizar, el servidor M2M descifra la solicitud y cifra la respuesta. En este caso, la seguridad de extremo a extremo es parcial porque el servidor M2M debe obtener y gestionar datos claros desde el dispositivo M2M. Sin embargo, esta situación es bastante común, por ejemplo, cuando el servidor M2M es una puerta de enlace que habilita la conectividad entre WAN y LAN y cuando el dispositivo M2M no se puede configurar para autenticarse de forma segura al servidor de autorización M2M. También es el caso cuando el servidor M2M tiene que realizar operaciones en los datos del dispositivo M2M (agregación de múltiples fuentes, etc.)

La presente invención tal como se describe en este documento permite realizar seguridad entre una aplicación de consumidor y el dispositivo M2M. El servidor M2M es una entidad que habilita el acceso a los recursos y aplica la política de seguridad sin tener ninguna información sobre la aplicación del consumidor solicitante y sin tener ninguna información sobre el solicitante. Esto permite la delegación de autorización a una entidad externa confiable (el servidor de autorización M2M).

Con la presente invención, solo las aplicaciones de consumidores autorizadas tienen derecho a acceder de forma segura al servidor M2M para la aplicación de políticas y al dispositivo M2M para el cifrado de datos. El servidor M2M y el dispositivo M2M no abarcan ninguna información del usuario sino que delegan la administración del usuario y el control de acceso al servidor de autorización M2M externo. El servidor M2M y el dispositivo M2M no abarcan ningún conocimiento sobre la aplicación del consumidor solicitante, sino que delegan la administración de la aplicación del consumidor y el control de acceso al servidor de autorización externo. Dichos sistemas y métodos de la presente

invención mejoran la seguridad de la información transferida entre una aplicación del consumidor y un dispositivo M2M proporcionando medios eficientes para un canal de comunicación seguro.

La presente invención se refiere a la implementación de seguridad de extremo a extremo para la comunicación entre objetos en el dominio de Internet de las Cosas (o Internet de los Objetos). El objetivo de la patente es lidiar con la configuración de un canal seguro de información autorizado entre la fuente de datos (dispositivo M2M) y los consumidores de datos (entidad consumidora). De acuerdo con la presente invención, el acceso a un dispositivo M2M por una entidad consumidora (aplicación del consumidor) se controla mediante un servidor de autorización M2M. El servidor de autorización M2M es la entidad a cargo de gestionar los derechos de acceso para el dispositivo M2M y toma la decisión con respecto al acceso al recurso por parte de la entidad del consumidor (aplicación del consumidor). El servidor M2M es una entidad que aplica la decisión y permite el acceso al dispositivo M2M. Cuando una aplicación del consumidor necesita comunicarse con un dispositivo M2M, la presente invención propone un método para autorizar a una aplicación del consumidor a acceder a un dispositivo M2M y para encriptar la comunicación entre la aplicación del consumidor y el dispositivo M2M. El servidor de autorización M2M calcula las credenciales de seguridad que se envían a la aplicación del consumidor. La aplicación del consumidor accede al servidor M2M para recuperar el recurso del dispositivo M2M. El servidor M2M aplica la decisión del servidor de autorización M2M comprobando la solicitud de acceso, y en caso de éxito accede al dispositivo M2M (o en algunas realizaciones al propio servidor M2M). El dispositivo M2M recupera de forma segura la clave de cifrado de solicitud y la clave de cifrado de respuesta o descifrando las claves de sesión cifradas recibidas, o accediendo de forma segura al servidor de autorización M2M. El dispositivo M2M proporciona los datos cifrados al servidor M2M para su posterior entrega a la aplicación del consumidor.

Para lograr estas y otras ventajas, y de acuerdo con el propósito de la invención tal como se describe ampliamente, la invención propone un método. Un método para asegurar comunicaciones de máquina a máquina entre una aplicación del consumidor M2M y un proveedor de recursos M2M en donde cuando es una iniciada una solicitud de acceso:

- enviar una solicitud de credenciales de valores desde la aplicación del consumidor a un servidor de autorización M2M,
- recibir del servidor de autorización M2M a la aplicación del consumidor las credenciales de valores generadas que comprende un token de acceso, claves de cifrado de sesión y una clave de autenticación,
- transmitir desde la aplicación del consumidor M2M el token de acceso y un mensaje de autenticación al proveedor de recursos M2M para autenticar la aplicación del consumidor,
- transmitir la solicitud de acceso desde la aplicación del consumidor al proveedor del recursos M2M, comprendiendo dicha solicitud de acceso un parámetro de solicitud encriptado con las claves de sesión para acceder o controlar los recursos,
- autenticación por el proveedor del recursos de la aplicación del consumidor como una autorizada del mensaje de autenticación y el contenido del token de acceso,
- recuperar por parte del proveedor de recursos las claves de sesión del contenido del token de acceso,
- descifrar por el proveedor de recursos el parámetro de solicitud cifrada con las claves de sesión
- enviar, desde el proveedor de recursos, la respuesta cifrada del parámetro de solicitud a la aplicación del consumidor.

En otro aspecto de la presente invención, el proveedor de recursos es un dispositivo M2M o un servidor M2M.

En otro aspecto de la presente invención, la generación del token de acceso comprende los siguientes pasos:

- generación de datos de la sesión por parte de la aplicación del consumidor, dichos datos de sesión identifican de manera única la transacción en curso entre la aplicación del consumidor y el proveedor del recurso,
- cálculo de datos criptográficos a partir de los datos de sesión generados,
- agregar los datos criptográficos a la solicitud de credenciales de valores,
- el token de acceso generado por el servidor de autorización M2M comprende los datos criptográficos de la solicitud de credenciales de valores, información para recuperar claves de sesión y una clave de autenticación generada.

En otro aspecto de la presente invención, el token de acceso se cifra con una clave compartida entre el servidor de autorización M2M y el proveedor de recursos.

En otro aspecto de la presente invención, la información para recuperar las claves de sesión comprende o un índice asociado a las claves de sesión en una base de datos del servidor de autorización M2M, o claves de sesión cifradas con una clave compartida entre el servidor de autorización M2M y el proveedor de recursos.

En otro aspecto de la presente invención, la autenticación de la aplicación del consumidor por el proveedor de recursos comprende los siguientes pasos:

- cifrar los datos de la sesión con la clave de autenticación, por parte de la aplicación del consumidor,

- enviar el token de acceso y los datos de la sesión cifrada desde la aplicación del consumidor al servidor M2M,
- Desde la clave de autenticación del token de acceso, descifrar los datos de la sesión cifrada,
- a partir de los datos de la sesión descifrada, cálculo de los datos criptográficos,
- Si la comparación de los datos criptográficos calculados con los datos criptográficos del token de acceso es exitosa, la aplicación del consumidor es autenticada.

En otro aspecto de la presente invención, el proveedor del recurso verifica la autenticidad del token de acceso o a partir de una firma calculada por el servidor de autorización M2M, o de un dato de autenticación añadido por el servidor de autorización M2M al token de acceso.

En otro aspecto de la presente invención, los datos de autenticación comprenden un valor incrementado de un contador que se usa para realizar una gestión anti-repetición, el proveedor de recursos M2M verifica si el valor del contador recibido en los datos de autenticación es mayor que un valor del contador guardado previamente, si esta verificación es exitosa, el proveedor de recursos M2M guarda el valor del contador entrante y elimina el guardado anteriormente.

En otro aspecto de la presente invención:

- cuando la autenticación de la aplicación del consumidor es exitosa, el proveedor de recursos M2M se autentica al servidor de autorización M2M,
- Si la autenticación es exitosa, recupera las claves de sesión.

En otro aspecto de la presente invención, la solicitud de acceso comprende también los datos de la sesión encriptados con la clave de autenticación de sesión y el token de acceso.

En otro aspecto de la presente invención, un dispositivo M2M encripta continuamente datos con las claves de sesión para enviarlo al proveedor de recursos M2M para su almacenamiento.

En otro aspecto de la presente invención, el token de acceso comprende el identificador único de recursos (URL) y la lista de parámetros de consultas autorizadas por la aplicación del consumidor, si el parámetro de solicitud cifrado está en la lista de acceso autorizado, se procesa el parámetro de consulta cifrado por el proveedor de recursos.

En otro aspecto de la presente invención, durante la autenticación de la aplicación del consumidor por el servidor M2M, se verifica la vida útil del token de acceso.

En otro aspecto de la presente invención, cuando se alcanza la vida útil del token de acceso

- generación de, respectivamente, nuevos datos de la sesión y/o un nuevo token de acceso,
- las claves de sesión y/o la clave de autenticación se renuevan o mantienen.

La presente invención también se refiere a un sistema de comunicaciones M2M, que comprende una aplicación del consumidor. Dicha aplicación del consumidor está configurada para comunicarse con un dispositivo M2M mediante un servidor M2M a través de una red de acceso, donde los mensajes de solicitud de acceso transitan entre la aplicación del consumidor y el dispositivo M2M, durante esta comunicación está asegurada por un servidor de autorización M2M de acuerdo con el método de la presente invención.

## BREVE DESCRIPCIÓN DE LOS DIBUJOS

La siguiente descripción detallada se comprenderá mejor con los dibujos, en los cuales:

FIG. 1 ilustra las diferentes entidades involucradas en un proceso de seguridad de tránsito de datos entre una aplicación del consumidor y un dispositivo M2M.
FIG. 2 es un diagrama de flujo lógico de acuerdo con una realización ejemplar de esta invención durante el establecimiento de un proceso de seguridad entre la aplicación del consumidor y un servidor M2M.
FIG. 3 es un diagrama de flujo lógico de acuerdo con una realización ejemplar de esta invención durante el establecimiento de un proceso de seguridad entre la aplicación del consumidor y un dispositivo M2M.

## DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN DE LA INVENCIÓN

La presente invención no es especifica para cualquier implementación particular de hardware o software, y está en un nivel conceptual por encima de las características especificas de la implementación. Debe entenderse que pueden producirse otras diversas realizaciones y variaciones de la invención sin apartarse del espíritu o alcance de la invención. Lo siguiente se proporciona para ayudar a comprender la implementación práctica de realizaciones particulares de la invención.

Los mismos elementos han sido designados con los mismos números de referencia en los diferentes dibujos. Para

mayor claridad, solo aquellos elementos y pasos que son útiles para la comprensión de la presente invención se han mostrado en los dibujos, y serán descritos.

Además, los mecanismos de comunicación de datos entre las partes y su entorno tampoco han sido detallados, ya que aquí la presente invención es de nuevo compatible con los mecanismos habituales.

Además, las líneas de conexión mostradas en las diversas figuras contenidas en este documento pretenden representar relaciones funcionales ejemplares y/o acoplamientos físicos entre los diversos elementos. Cabe señalar que muchas alternativas o relaciones funcionales adicionales o conexiones físicas pueden estar presentes en un sistema práctico. Además, las diversas entidades en la FIG. 1 puede comunicarse a través de cualquier medio de comunicación adecuado (incluido Internet), utilizando cualquier protocolo de comunicación adecuado.

Además, cuando se dice que una acción se realiza por un dispositivo, de hecho se ejecuta mediante un microprocesador en este dispositivo controlado por códigos de instrucciones grabados en una memoria de programa en dicho dispositivo. Una acción también se asigna a una aplicación del consumidor o software. Esto significa que el microprocesador ejecuta parte de los códigos de instrucción que componen la aplicación del consumidor o el software.

La referencia, a lo largo de toda la memoria descriptiva, a "una realización" o "la realización" significa que una característica, estructura o característica particular descrita en conexión con una realización se incluye en al menos una realización del tema descrito. Así, la aparición de las frases "en una realización" o "en la realización" en varios lugares a lo largo de la memoria descriptiva no se refieren necesariamente a la misma realización. Además, las características, estructuras o características particulares se pueden combinar de cualquier manera adecuada en una o más realizaciones.

La comunicación Máquina a Máquina (M2M) es una forma de comunicación de datos que involucra a una o más entidades que no requieren interacción o intervención humana explícita en el proceso de comunicación. La comunicación Máquina a Máquina (M2M) permite que un servicio de comunicación inteligente sea usado de forma segura y conveniente entre un ser humano y un objeto o entre un objeto y otro objeto de forma ubicua. En consecuencia, la comunicación M2M permite que un objeto (un sensor, actuador, puerta de enlace...) realice una tarea que puede ser demasiado arriesgada para que un humano la realice manualmente, una tarea que puede durar largo tiempo o una tarea que puede requerir seguridad. La comunicación M2M se puede aplicar a los campos de la telemática, deportes, navegación, instrumentos de medición inteligentes, máquinas expendedoras automáticas, servicios de seguridad y similares. Las comunicaciones M2M se han implementado en redes inteligentes, redes domésticas, cuidado de la salud, entornos de redes vehiculares...

Un ejemplo de sistema de comunicación M2M en el que se pueden implementar las diversas realizaciones ejemplares descritas aquí se describe a continuación con respecto a la FIG. 1. Para simplificar la discusión, en la FIG. 1 solo se muestra una de cada entidad. Se entiende, sin embargo, que las realizaciones de la tecnología pueden incluir más de una de cada entidad. Adicionalmente, algunas realizaciones de la tecnología pueden incluir menos que todas las entidades mostradas en la FIG. 1.

El sistema de comunicación M2M incluye una pluralidad de objetos aquí denominados dispositivos M2M 10. En un escenario de comunicación M2M típico como se muestra en la FIG. 1, los datos se intercambian entre un servidor M2M 12 que ejecuta una aplicación del consumidor M2M y el dispositivo M2M 10 a través de una red de acceso 13.

El dispositivo M2M 10 ejecuta la/s aplicación/es del consumidor M2M usando capacidades de servicio M2M y funciones de dominio de red. Los dispositivos M2M 10 pueden conectarse a la red de acceso 13 o directamente o a través de una puerta de enlace M2M 11. Una red de área M2M 15 proporciona conectividad entre el dispositivo M2M 10 y la puerta de enlace M2M 11. Este dispositivo M2M 10 está etiquetado como dispositivo oculto ya que se conectan a la red de acceso 13 a través de la puerta de enlace M2M 11.

La puerta de enlace M2M 11 ejecuta aplicaciones del consumidor M2M utilizando capacidades de servicio M2M. La puerta de enlace M2M actúa como un proxy entre los dispositivos M2M y la red de acceso 13. La red de área M2M 15 es una red de dispositivos para comunicaciones M2M, (por ejemplo, ZigBee, 6lowPAN, etc.). La red de área M2M 15 puede denominarse red capilar. Una red local, como una red de área local (LAN) o una red de área personal (PAN), etc., pueden formar la red de área M2M 15.

El dispositivo M2M 10 puede ser un sensor o medidor que puede estar dispuesto para capturar un evento tal como temperatura, nivel de inventario u otro parámetro adecuado que se retransmite a una aplicación del consumidor M2M que está preparada para traducir el evento capturado en información significativa. El dispositivo M2M 10 puede ser, por ejemplo, un ordenador portátil, un teléfono inteligente, una tableta, un contador de servicios, un controlador de un sistema de calefacción, ventilación y aire acondicionado (HVAC), medidores inteligentes M2M, dispositivos de monitoreo del entorno o un servidor que proporcione datos y similares.

El servidor 12 de M2M es un dispositivo informático que permite aplicar el acceso de una aplicación del consumidor

18 a los dispositivos M2M a través de la red de acceso 13. El servidor M2M 12 puede comprender una base de datos para almacenar datos de los dispositivos M2M.

La aplicación del consumidor 18 se ejecuta en un dispositivo de usuario 14 o en una infraestructura remota. La aplicación del consumidor es una aplicación del consumidor que obtiene y consume recursos en nombre de un usuario. Como se usa en este documento, los términos "dispositivo de usuario" pueden incluir, pero no limitarse a, teléfonos celulares, teléfonos inteligentes, PCs y miniordenadores, ya sean de sobremesa, portátil u otros, así como dispositivos móviles tales como computadoras de mano, PDAs, cámaras de video, decodificadores, dispositivos media personales (PMD), dispositivos o módulos habilitados para M2M, tarjetas informatizadas o complementos, o cualquier combinación de los anteriores.

La red de acceso 13 puede soportar múltiples tecnologías diferentes de acceso por radio. Se pueden usar diversos ejemplos de sistemas de comunicación inalámbrica y redes de acceso que pueden implementar la presente invención. La red de acceso 13 puede referirse a cualquier tipo de datos, telecomunicaciones u otra red que incluye, sin verse limitada a, redes de datos (incluyendo MANs, PANs, WANs, LANs, WLANs, micronets, piconets, internets e intranets), redes coaxiales de fibra híbrida (HFC), redes satelitales, redes celulares y redes de telecomunicaciones. Dichas redes o partes de las mismas pueden utilizar una o más topologías diferentes (por ejemplo, anillo, bus, estrella, bucle, etc.), medios de transmisión (p. ej., cable con cable/RF, RF inalámbrico, onda milimétrica, óptica, etc.) y/o protocolos de comunicación o de red (p. ej., SONET, DOCSIS, IEEE Std. 802.3, 802.11, ATM, X.25, Frame Relay, 3GPP, 3GPP2, WAP, SIP, UDP, FTP, RTP/RTCP, H.323, etc.).

Los sistemas de comunicaciones M2M como se muestran en la FIG. 1 comprenden un servidor de autorización M2M 16. El servidor de autorización M2M 16 gestiona la seguridad de la comunicación entre las entidades involucradas. El servidor de autorización M2M 16 realiza la autenticación del dispositivo M2M 10 y del servidor M2M 12 antes del establecimiento de la sesión. El servidor de autorización M2M 16 puede realizar funciones relacionadas con la seguridad de la sesión tales como el cifrado del tráfico al recibir una solicitud de seguridad y devolver credenciales de seguridad. El servidor de autorización M2M 16 es la entidad encargada de gestionar los derechos de acceso del usuario a un recurso del dispositivo M2M 10. El servidor de autorización M2M 16 es también la entidad encargada de tomar la decisión con respecto al acceso al recurso para un usuario 17. En una realización, el usuario tiene que autorizar al servidor de autenticación M2M a emitir las credenciales de seguridad a la aplicación del consumidor.

A través del servidor de autorización M2M 16, se establecen las políticas relacionadas con el acceso al recurso del dispositivo M2M. La configuración de las políticas puede comprender las fases de inscripción al servidor de autorización M2M 16 para las siguientes entidades:

- aplicación del consumidor,
- dispositivo M2M,
- usuario, y/o
- servidor M2M.

Las políticas pueden definir la siguiente información:

- la URL del servidor M2M incluyendo la referencia del dispositivo M2M (dirección del punto final). Esta URL de recurso será única en la comunicación M2M,
- el propietario (usuario) del recurso,
- los materiales clave definidos entre el servidor de autorización M2M y el servidor M2M 12 y entre el servidor de autorización M2M 16 y el dispositivo M2M 10. Los materiales clave pueden comprender:
- material de clave de cifrado compartido relevante para el servidor M2M 12 para el cifrado del token de acceso
- o una credencial de autenticación utilizada para autenticar el dispositivo M2M 10 al servidor de autorización M2M 16, y/o una clave de cifrado utilizada para encriptar las claves de sesión.
- credencial de autenticación que se puede usar para autenticar el servidor M2M 12 al servidor de autorización M2M 16
- algoritmos de generación de claves. El algoritmo de generación de claves es preferiblemente un generador aleatorio. Los algoritmos de generación de claves usados en este documento son bien conocidos por el versado en la materia y no necesitan ser descritos más. Los materiales clave se utilizan para lograr una comunicación segura de extremo a extremo entre la aplicación del consumidor 17 y el dispositivo M2M 10.

El propósito de estos procesos de inscripción y de las políticas de información definidas es permitir que la aplicación del consumidor use los dispositivos M2M expuestos por el servidor M2M de acuerdo con los derechos definidos.

Cualquier forma adecuada de proceso de inscripción entre estas entidades puede implementarse tal como reconocería un experto en la materia.

Se puede suponer que antes de que fluyan los procesos, como se describe en las FIG. 2 y FIG. 3, se configuran; el servidor de autorización M2M 16 realiza una autenticación del usuario. Esa etapa de autenticación del usuario se encuentra fuera del alcance de la presente invención.

Se puede asumir además que durante un proceso de personalización, se puede crear un material de clave de cifrado compartida $K_s$. La clave de material de clave de cifrado compartida $K_s$ puede ser una clave simétrica que se puede derivar de una clave maestra y un parámetro predefinido. El parámetro predefinido puede ser un identificador único del servidor M2M. Esta clave compartida es generada por el servidor de autorización 16 o por cualquier sistema de confianza. El servidor de autorización M2M 16 comparte la clave de material de clave de cifrado compartida $K_s$ creada, con el servidor M2M 12.

En otra realización, el material de clave de cifrado compartido $K_s$ es definido por el propietario del servidor M2M y se introduce en el servidor de autorización M2M durante la fase de inscripción del servidor M2M.

En otra realización, el token de acceso se cifra utilizando la clave pública del servidor M2M. El servidor M2M usará la clave privada correspondiente para recuperar el token de acceso. Esta realización puede ser relevante cuando el servidor M2M pueda generar dinámicamente un par de claves, solicitar certificado de clave pública a una autoridad de certificación y enviar el certificado al servidor de autorización para el registro de la clave pública (después de la validación del certificado de servidor M2M).

En otra realización, la clave compartida $K_s$ es nula, lo que significa que el token de acceso no está cifrado, en este caso, el canal de comunicación entre la aplicación del consumidor 18 y el servidor M2M 12 es preferiblemente un canal seguro como TLS.

Se puede implementar cualquier forma adecuada de generar y compartir la clave compartida entre estas entidades, como reconocería un experto en la materia. La forma en que se genera y comparte la clave compartida $K_s$ entre las entidades está fuera del alcance de la presente invención.

Se puede suponer además que las comunicaciones, entre el servidor de autorización M2M 16, la aplicación del consumidor 18, el dispositivo M2M 10, y el servidor M2M 12 se encaminan preferiblemente a través de un canal seguro y un protocolo que está fuera del alcance de la presente invención. En la realización en la que el token de acceso no está encriptado, se recomienda confiar en un canal seguro para este enlace de comunicación.

En la presente invención descrita aquí, se supone que los algoritmos de encriptación pueden usar estándares de cifrado de datos tales como, p. ej., RSA con una clave de al menos 1024 bits, estándar de cifrado de datos triple (DES), estándar de cifrado avanzado de 128 bits (AES), un algoritmo de encriptación de flujo RC4 que utiliza un tamaño mínimo de clave de 128 bits, etc. Se puede implementar cualquier otra forma adecuada de estándares de cifrado como reconocería un experto en la materia.

La FIG. 2 ilustra un diagrama de flujo ejemplar para asegurar el tránsito de datos entre la aplicación del consumidor 18 y el servidor de M2M 12. En este ejemplo ilustrado, el servidor M2M juega el papel de un dispositivo M2M vis a vis con el servidor de autorización M2M. En esta realización, el servidor M2M es un proveedor de recursos implementado por una puerta de enlace. El servidor M2M permite la transferencia de datos entre la aplicación del consumidor y el dispositivo M2M a través de la puerta de enlace. En este caso, el flujo de proceso entre el usuario 17 y el servidor M2M 12 se representa con flechas etiquetadas a las que se asignan los respectivos números. Se entiende que el flujo se realiza de forma secuencial de arriba hacia abajo según lo indiquen los números crecientes. Sin embargo, debe tenerse en cuenta que puede haber varias instancias de este protocolo ejecutándose en paralelo sin un orden especificado.

La Fig. 2 es un diagrama de flujo que representa un conjunto de funciones 20 que pueden llevarse a cabo de acuerdo con una realización de la presente invención. El conjunto de funciones 20 se puede realizar para proporcionar a la aplicación del consumidor 18 y al servidor M2M 12 credenciales de valores que permitan asegurar el tránsito de datos entre la aplicación del consumidor 18 y el servidor M2M 12. El conjunto de funciones 20 se muestra dentro de los pasos 21 a 37. Una descripción de estos pasos sigue a continuación.

En la etapa 21, al recibir una entrada de un usuario para solicitar un acceso a los recursos de los dispositivos M2M 10, el dispositivo de usuario 14 inicia la ejecución de la aplicación del consumidor 18. Cuando se lanza la aplicación del consumidor 18, se puede visualizar un teclado gráfico en el dispositivo de usuario 14. Puede comprender selectores de área que permiten al usuario 17 introducir un parámetro para acceder o controlar el dispositivo M2M 10. La aplicación del consumidor 18 elabora una solicitud de acceso correspondiente a los parámetros seleccionados por el usuario 17.

Entonces, la aplicación del consumidor 18 genera una solicitud de credenciales de valores. Para eso, en el paso 22, la aplicación del consumidor 18 genera datos de sesión (SDATA). Estos datos de sesión es una pieza de datos utilizada para autenticar la aplicación del consumidor al servidor de autorización M2M. Los datos de la sesión pueden ser, con frecuencia, una cadena larga y aleatoriamente generada para disminuir la probabilidad de obtener una válida por medio de una búsqueda forzada.

En la etapa 23, a partir del SDATA generado, la aplicación del consumidor 18 puede calcular datos criptográficos. Los datos criptográficos se pueden calcular mediante cualquier algoritmo que impida la recuperación de la

información inicial. Este tipo de algoritmos son preferiblemente una función de una sola dirección.

En una realización, los datos criptográficos se calculan aplicando funciones de hasheado o algoritmos de hasheado (p. ej., un hash MD5 o SHA...) al SDATA. Un algoritmo de hasheado transformará el SDATA en una cadena de identificador de longitud fija (a menudo llamado resumen).

En otra realización, los datos criptográficos pueden calcularse aplicando una operación MAC (Código de Autenticación de Mensaje), una operación HMAC (Hash MAC) o una operación de firma en los datos de sesión SDATA. Esas diversas realizaciones ejemplares son bien conocidas por los expertos en la materia y no necesitan ser descritas más aún.

En la etapa 24, la aplicación del consumidor 18 envía una solicitud de las credenciales de valores para acceder a los recursos del dispositivo M2M. Esta solicitud comprende los datos criptográficos. Al recibirla, el servidor de autorización M2M 16 puede solicitar una autenticación del usuario 17 para autorizar a la aplicación del consumidor a que recupere las credenciales para acceder a los recursos del dispositivo M2M. Este paso de autenticación de usuario está fuera del alcance de la presente invención.

En una realización, el servidor de autorización M2M verifica el consentimiento del usuario antes de procesar la solicitud desde la aplicación del consumidor 18 recibida en el paso 24. Por ejemplo, el usuario puede hacer clic en un formulario de validación que se muestra en su dispositivo de usuario y/o puede introducir su contraseña para dar su consentimiento.

Tras la recepción de esta solicitud, en el paso 25, el servidor de autorización M2M 16 genera claves de sesión y una clave de autenticación $K_{auth}$. Las claves de sesión comprenden una clave de encriptación de solicitud $K_{enc}$ y una clave de encriptación de respuesta $K_{res}$. Estas claves se generan a partir de materiales clave. La clave de cifrado de solicitud $K_{enc}$ se usa para proteger la confidencialidad de los mensajes enviados por la aplicación del consumidor 18 al dispositivo de M2M 10 a través del servidor M2M 12. La clave de cifrado de respuesta $K_{res}$ se usa para proteger la confidencialidad del mensaje enviado por el dispositivo M2M a la aplicación del consumidor 18. La clave $K_{auth}$ permite autenticar la aplicación del consumidor 18 al servidor M2M 12.

El servidor de autorización M2M 16 almacena las claves de sesión y la clave de autenticación $K_{auth}$ en su base de datos. Un índice o un identificador es asignado a las claves de sesión. El servidor de autorización 16 genera también un token de acceso asociado. Este token de acceso se calcula a partir de los materiales clave.

En una realización, el contenido de este token de acceso puede comprender los datos criptográficos recibidos, el índice asociado a la clave de cifrado de solicitud $K_{enc}$ y el índice asociado a la clave de cifrado de respuesta $K_{res}$, la clave de autenticación $K_{auth}$, una vida útil, los derechos de la aplicación del consumidor (lista de parámetros de consultas autorizadas a la aplicación del consumidor) y el identificador del recurso relacionado representado como un Localizador Uniforme de Recursos (URL). Con estos datos, el dispositivo M2M o el servidor M2M puede recuperar las claves de sesión en el servidor de autorización M2M.

En otra realización, el contenido de este token de acceso puede comprender los datos criptográficos recibidos, el material de claves de sesión y la clave de autenticación. El material de las claves de sesión puede incluir las claves de sesión cifradas utilizando la clave del dispositivo M2M. La clave del dispositivo M2M se comparte entre el servidor de autorización M2M y el dispositivo M2M. En la realización ilustrada en la FIG. 2, el servidor M2M 12 que actúa como el dispositivo M2M comparte la clave del dispositivo M2M con el servidor de autorización M2M 16. En esta realización, el dispositivo M2M no necesita conectarse al servidor de autorización M2M para recuperar las claves de sesión; descifra las claves de sesión cifradas recibidas del servidor de autorización M2M.

En una realización, el contenido del token de acceso puede cifrarse con la clave compartida $K_s$ del servidor de autorización M2M 16 y el servidor M2M 12 y un algoritmo de encriptación que permite el descifrado seguro del token de acceso por el servidor M2M. Este algoritmo de encriptación es bien conocido por el experto en la materia y no necesita ser descrito más aún.

El servidor de autorización M2M puede proporcionar medios para que el servidor M2M verifique la autenticidad del token de acceso. Estos medios de autenticidad puede ser un simple mecanismo de firma - los algoritmos de firma son bien conocidos por la persona experta en la materia y no necesitan ser descritos más aún. Otro medio es agregar en el token de acceso unos datos de autenticación compartidos entre el servidor de autorización M2M y el servidor M2M. Estos datos de autenticación pueden ser unos datos secretos, una contraseña, un código de acceso, una frase de contraseña, cualquier código de identificación y/o similares. Otro medio es proporcionar un punto de acceso en el servidor de autorizaciones M2M para verificar el token de acceso.

El servidor de autorización M2M 16 elabora, en el paso 25, credenciales de valores. Estas credenciales de valores comprenden el token de acceso generado, las claves de sesión y la clave de autenticación $K_{auth}$.

En la etapa 26, el servidor de autorización M2M 16 devuelve las credenciales de valores a la aplicación del

consumidor 18 en respuesta a su solicitud en el paso 24. Las credenciales de valores se envian preferiblemente a través de un canal seguro a la aplicación del consumidor 18.

Tras la recepción, la aplicación del consumidor 18 calcula unos datos de autenticación. Estos datos de autenticación pueden cifrarse con la clave de autenticación $K_{auth}$. Los datos de autenticación comprenden los datos de sesión utilizados en el paso 23 para solicitar el token de acceso al servidor de autorización M2M y un valor incrementado de un contador de solicitudes del consumidor que se utilizará para realizar una gestión anti-repetición en el servidor M2M. La aplicación del consumidor 18 encripta los parámetros de consultas del token de acceso, seleccionado por el usuario 17, con la clave de encriptado de solicitud de sesión Key $K_{enc}$.

En el paso 27, la aplicación del consumidor 18 transmite al servidor M2M 12 el token de acceso, los datos de autenticación y la solicitud de acceso.

Tras la recepción, el servidor M2M 12, en el paso 28, recupera de su base de datos la clave compartida $K_s$ si el token de acceso está cifrado y lo descifra. Desde el token de acceso libre, el servidor M2M 12 puede verificar la validez del token de acceso (por ejemplo, verificando su vida útil). El servidor M2M 12 con la clave de autenticación $K_{auth}$ extraida del token de acceso puede descifrar los datos de autenticación. Si la verificación falla, el flujo del proceso se puede cerrar y el servidor M2M puede notificar a la aplicación del consumidor y/o al servidor de autorización M2M que los datos se han manipulado.

Si, por otro lado, la verificación es exitosa, el servidor M2M 12 puede verificar la integridad de los datos para comprobar que la aplicación del consumidor 18 sea válida. Para eso, en el paso 29, el servidor M2M calcula los datos criptográficos de los datos de sesión extraídos de los datos de autenticación descifrados. El servidor M2M 12 compara los datos criptográficos calculados con los datos criptográficos extraídos del token de acceso. Si la verificación falla, el flujo del proceso puede cerrarse, en el paso 30, y el servidor M2M puede notificar a la aplicación del consumidor y/o al servidor de autorización M2M que la aplicación del consumidor 18 no tiene autorización. Como solo la aplicación del consumidor conoce los datos de sesión asociados al token de acceso, el servidor M2M 12 puede autenticar la aplicación del consumidor. Por lo tanto, el servidor M2M puede establecer que la aplicación del consumidor 18 es una aplicación del consumidor autorizada para acceder a los servicios M2M. Si la verificación es exitosa, el servidor M2M 12 puede autenticarse al servidor de autorización M2M 16 y pasa el token de acceso para aplicar su validación del token de acceso (el usuario puede haber invalidado el token de acceso en el servidor de autorización M2M).

En la etapa 31, para autenticar el servidor M2M 12, el servidor M2M 12 es requerido para proporcionar a través de un canal (preferiblemente seguro), datos de autorización que sean conocidos por el único servidor M2M 12 y el servidor de autorización M2M 16. Los datos de autorización son cualquier código identificador/indicador adecuadamente configurado para permitir un acceso autenticado. Los datos de autorización pueden ser un Número de Identificación Personal (PIN), datos secretos, una contraseña, un código de acceso, una frase de contraseña, un certificado digital, cualquier código de identificación y/o similares.

A continuación, al recibir los datos de autorización, el servidor de autorización 12 analiza si los datos de autorización proporcionados son los datos esperados. Si la respuesta es no, es decir, cuando los datos proporcionados no se corresponden con los datos esperados almacenados en el servidor de autorización M2M 16, entonces el flujo del proceso puede cerrarse en el paso 33. Si la respuesta es si, es decir, cuando los datos proporcionados se corresponden con los datos esperados almacenados en el servidor de autorización M2M 16, entonces el servidor de autorización M2M 16 puede notificar, en el paso 34, al servidor M2M 12, que la autenticación es exitosa.

A continuación, en el paso 35, el servidor M2M 12 puede enviar una solicitud al servidor de autorización M2M para obtener las claves de sesión $K_{enc}$ y $K_{res}$. Esta solicitud comprende el índice de $K_{enc}$ y el índice de $K_{enc}$ del token de acceso descifrado. Tener dichos índices implica que el servidor 12 de M2M ha sido capaz de descifrar el token de acceso. Al recibirlo, el servidor de autorización M2M 12 extrae de su base de datos las claves de sesión asociadas a los índices relacionados recibidos. En resuesta, las claves de sesión extraídas se envían, en el paso 36, al servidor M2M 12. El servidor M2M 12 almacena en su base de datos las claves de sesión recibidas para asegurar las comunicaciones con la aplicación del consumidor 18. En otra realización, el servidor M2M 12 recupera las claves de sesión descifrando las claves de sesión cifradas usando la clave del dispositivo M2M.

El servidor M2M 12 descifra el contenido del token de acceso con la clave de cifrado de solicitud de sesión recibida $K_{enc}$. El servidor M2M 12 procesa el parámetro de solicitud descifrado. Como resultado del procesamiento, el servidor M2M 12 elabora una respuesta en consecuencia. En el paso 37, el servidor M2M 12 encripta la respuesta con la clave de cifrado de respuesta de sesión $K_{res}$. La respuesta cifrada se envía de vuelta a la aplicación del consumidor 18 a través del servidor M2M 12.

El flujo del proceso descrito en la FIG. 2 crea una seguridad de extremo a extremo entre la aplicación del consumidor 18 y el servidor M2M 12 que actúa como el dispositivo M2M. Las claves de sesión $K_{enc}$ y $K_{res}$ y la clave de autenticación $K_{auth}$ tal como se define en la presente invención proporcionan un canal seguro sobre el que la información puede transmitirse de manera segura a través de una aplicación del consumidor autorizada a través de

la red de acceso y el servidor M2M 12. Estas claves $K_{enc}$ y $K_{res}$ y $K_{auth}$ permiten establecer una sesión segura entre una aplicación del consumidor válida y el servidor M2M para habilitar el acceso a los recursos de los dispositivos M2M conectados al servidor M2M; el enlace entre el servidor M2M y el dispositivo M2M se encuentra fuera del alcance de esta realización cuando el servidor M2M se ve como un proveedor de recursos

La figura 3 muestra un diagrama de flujo que representa un conjunto de funciones 40 que pueden llevarse a cabo de acuerdo con otro ejemplo de realización en el que la seguridad de extremo a extremo se implementa entre la aplicación del consumidor y el dispositivo M2M. En esta realización, el servidor M2M solo juega el rol de Policy Enforcer y Data Access Enabler. En esta realización, las claves de sesión no están encriptadas por una clave de cifrado del dispositivo M2M; por lo tanto, el dispositivo M2M recuperará las claves del servidor de autorización M2M. El conjunto de funciones 40 se puede realizar para usar las credenciales de valores proporcionadas para acceder a los recursos de los dispositivos M2M. El conjunto de funciones 40 se muestra en los pasos 41 a 55. Una descripción de estos pasos sigue a continuación.

Al recibir una entrada de un usuario para solicitar un acceso a recursos de los dispositivos M2M 10, el dispositivo de usuario 14 inicia la ejecución de la aplicación del consumidor 18, en el paso 41. Cuando se inicia la aplicación del consumidor, en el paso 42, se realizan los pasos 22 a 27 de la FIG. 2. En la etapa 43, la aplicación del consumidor 18 transmite al servidor M2M 12 el token de acceso, los datos de autenticación y la solicitud de acceso elaborados en los pasos 22 a 27 de la FIG. 2. Tras la recepción, el servidor M2M puede verificar, en el paso 44, la validez del token de acceso (por ejemplo, verificando su vida útil, su autenticidad...).

El servidor M2M 12 puede descifrar el identificador único de datos de sesión encriptados y el contador de solicitudes con la clave de sesión $K_{auth}$ recuperada del token de acceso. El servidor M2M 12 puede verificar la integridad de los datos para comprobar que la aplicación del consumidor es una aplicación del consumidor válida. Para eso, el servidor M2M calcula unos datos criptográficos de los datos de la sesión descifrada. El servidor M2M 12 compara los datos criptográficos calculados con los datos criptográficos del token de acceso descifrado.

En una realización, durante las verificaciones del paso 44, el servidor M2M 12 puede comprobar si el contador de solicitudes recibidas es mayor que el contador de solicitudes guardado previamente. Si la respuesta es afirmativa, el servidor M2M 12 guarda el contador de solicitudes entrante y elimina el anterior guardado. Con esta realización, el servidor M2M 12 puede implementar una anti-repetición.

Si una de las verificaciones falla, el flujo del proceso puede cerrarse, en el paso 45, y el servidor M2M 12 puede notificar a la aplicación del consumidor y/o al servidor de autorización M2M que los datos están manipulados. Si, por otro lado, la verificación es exitosa, el servidor M2M 12 puede transmitir, en el paso 46, al dispositivo M2M 10 el parámetro de solicitud cifrado de la solicitud de acceso.

Con el flujo de procesos propuesto por la presente invención, el servidor M2M no necesita tener conocimiento de las aplicaciones del consumidor autorizadas; delega esta gestión en el servidor de autorización.

En una realización, para recuperar las claves de sesión $K_{enc}$ y $K_{res}$ del servidor de autorización M2M, el dispositivo M2M 10 se autentica al servidor de autorización M2M 16. Para eso, en el paso 48; el dispositivo M2M 10 está involucrado para proporcionar a través de un canal (preferiblemente seguro), un dato de autorización que es conocido por el único dispositivo M2M 10 y el servidor de autorización M2M 16. Este dato de autorización es cualquier código identificador/indicador adecuadamente configurado para permitir un acceso autenticado. Dicho dato de autorización puede ser un Número de Identificación Personal (o PIN), un dato secreto, una contraseña, un código de acceso, una frase de contraseña, un certificado digital, cualquier código de identificación y/o similares.

Luego, al recibir los datos de autorización, el servidor de autorización 16 analiza, en el paso 48, si los datos de autorización son los datos esperados. Si la respuesta es no, es decir, cuando los datos proporcionados no se corresponden con los datos esperados almacenados en el servidor de autorización M2M 16, entonces el flujo del proceso puede cerrarse en el paso 49. Si la respuesta es sí, es decir, cuando los datos proporcionados se corresponden con los datos esperados almacenados en el servidor de autorización M2M 16, entonces el servidor de autorización M2M 16 puede notificar, en el paso 50, al dispositivo M2M 10 que la autenticación es exitosa.

Seguidamente, en el paso 51, el dispositivo M2M 10 envía una solicitud al servidor de autorización M2M para obtener las claves de sesión $K_{enc}$ y $K_{res}$. Esta solicitud comprende los índices de las claves de sesión extraídas del token de acceso descifrado y enviadas en el enlace del servidor M2M/dispositivo M2M. Una vez recibido, el servidor de autorización M2M 16 extrae de su base de datos las claves de sesión asociadas a los índices recibidos. Las claves de sesión extraídas se envían en respuesta, en el paso 52, al dispositivo M2M 10.

En la etapa 53, el dispositivo M2M descifra el parámetro de solicitud con la clave de cifrado de solicitud de sesión recibida $K_{enc}$. El parámetro de solicitud descifrado es procesado por el dispositivo M2M 10. Como resultado del proceso, el dispositivo M2M 10 elabora una respuesta en consecuencia. En el paso 54, el dispositivo M2M 10 encripta la respuesta con la clave de cifrado de respuesta de sesión $K_{res}$. La respuesta cifrada se envía de vuelta a la aplicación del consumidor 18 a través del servidor M2M 12.

En otra realización, el servidor M2M envía al dispositivo M2M al mismo tiempo los derechos de la aplicación del consumidor extraídos del token de acceso descifrado. Antes de procesar el parámetro de solicitud descifrado en el paso 53 de la FIG. 3, el dispositivo M2M verifica si el parámetro de solicitud descifrado es coherente con los derechos de acceso. Por ejemplo, una solicitud de parámetro filtrado por selección de fecha es compatible con un derecho GET, un parámetro que solicita un conjunto de valores es compatible con un derecho SET pero no con un derecho GET. La comprobación de compatibilidad depende de la especificación del dispositivo y eso se encuentra fuera del alcance de esta invención. Si la respuesta es sí, el parámetro de solicitud descifrado se procesa en el paso 53. Si la respuesta es no, el flujo del proceso se puede cerrar y el dispositivo M2M 10 puede notificar al servidor M2M y/o a la aplicación del consumidor que el acceso solicitado no está autorizado.

El flujo del proceso descrito en la FIG. 3 crea una seguridad de extremo a extremo entre la aplicación del consumidor 18 y el dispositivo M2M 10. Las claves de sesión $K_{enc}$ y $K_{res}$ tal como se definen por la presente invención proporcionan un canal seguro sobre el que la información se puede transmitir de forma segura a través de la aplicación del consumidor 18 y sobre el servidor M2M 12 al dispositivo M2M 10. El flujo del proceso tal como se ha descrito permite, por un lado, autenticar la aplicación del consumidor al servidor M2M 12 y, por otro lado, autenticar el dispositivo M2M al servidor de autorización 16.

En una realización de la presente invención, el dispositivo M2M puede encriptar continuamente datos usando la clave de cifrado de respuesta $K_{res}$ para enviarlos al servidor M2M para su almacenamiento. El dispositivo M2M proporciona los datos cifrados al servidor M2M que se ejecuta como un habilitador (encriptado) de acceso a datos. El usuario, a través de la aplicación del consumidor, puede enviar la solicitud de acceso directamente al servidor M2M. En respuesta, el servidor M2M puede transmitir los datos cifrados a la aplicación del consumidor sin tener que acceder al dispositivo M2M. La aplicación de consumidor con la clave de cifrado de respuesta almacenada en el paso 26 de la FIG. 2, puede descifrar la respuesta.

La clave de cifrado de respuesta de sesión $K_{res}$ tal como se define en la presente invención proporciona un canal seguro unidireccional sobre el cual la información puede transmitirse de manera segura a través de la aplicación del consumidor 18 sobre la red de acceso y/o Internet al dispositivo M2M a través del servidor M2M. La clave de cifrado de respuesta de sesión $K_{res}$, como la definida por la presente invención, proporciona un canal multidireccional desde el dispositivo a una o más aplicaciones del consumidor. La clave de sesión $K_{auth}$ permite autenticar la aplicación del consumidor, al servidor M2M para acceder a los recursos de los dispositivos M2M.

En una realización, si la aplicación del consumidor determina que se ha alcanzado la vida útil de los datos de sesión, la aplicación del consumidor 18 puede generar una nueva sesión de datos y el flujo de proceso (que puede implicar una nueva autenticación del usuario), descrita en las FIG. 2 y FIG., 3 se realizan nuevamente o para renovar la clave de cifrado de solicitud de sesión $K_{enc}$ y la clave de cifrado de respuesta $K_{res}$, y/o la clave de autenticación $K_{auth}$ y el token de acceso, o mantener las claves generadas previamente. Esta elección puede depender del nivel de seguridad a alcanzar.

En otra realización, si se alcanza la vida útil del token de acceso, la aplicación del consumidor 18 puede generar nuevos datos de sesión y solicitar la renovación del token de acceso al Servidor de Autorización con los derechos asociados al anterior token de acceso. El flujo de proceso descrito en la FIG. 2 y FIG. 3 se realiza nuevamente para compartir las claves generadas en el nuevo token de acceso con la aplicación del consumidor, el servidor M2M y el dispositivo M2M. En el nuevo token de acceso, la clave de cifrado de solicitud de sesión $K_{enc}$, la clave de cifrado de respuesta $K_{res}$ y/o la clave de autenticación $K_{auth}$ se renuevan o se mantienen las claves generadas previamente. Esta elección puede depender del nivel de seguridad a alcanzar. El token de acceso anterior se envía en el paso 24.

En otra realización, el token de acceso libre comprende la clave de cifrado de solicitud de sesión $K_{enc}$ y la clave de cifrado de respuesta $K_{res}$ cifradas con una clave compartida entre el servidor de autorización M2M y el dispositivo M2M. En este caso, el dispositivo M2M no necesita conectar con el servidor de autorización M2M para recuperar las claves de sesión; recupera las claves descifrando las claves de sesión cifradas enviadas por el servidor M2M al dispositivo M2M (preferiblemente por enlace seguro).

En otra realización, el testigo de acceso no está cifrado y el enlace entre la aplicación del consumidor 18 y el servidor M2M 12 es seguro a nivel de transporte, por ejemplo utilizando el enlace de protocolo SSL/TLS.

La invención es simple y fácil de implementar y muchas realizaciones no requieren el uso de un enorme mecanismo de criptografía y, por lo tanto, permite soluciones de bajo coste. En particular, no es necesario que el servidor M2M 12 que se ejecuta como Policy Enabler y el dispositivo M2M dependan del certificado del servidor, lo que simplifica la implementación de dicho sistema seguro IoT. No es necesaria una autenticación mutua entre la aplicación del consumidor 18 y el dispositivo de M2M 10 para garantizar la confidencialidad de los recursos y la integridad/origen de la solicitud de acceso. La invención permite la implementación de la seguridad de extremo a extremo autorizada entre la aplicación del consumidor y el dispositivo M2M 10 a través de un canal potencialmente inseguro. De todos modos, algunas realizaciones particulares, principalmente la realización en la que el token de acceso no está encriptado, el enlace entre la aplicación del consumidor (consumidor) y el servidor M2M debe asegurarse a nivel de transporte para asegurar la confidencialidad de los datos confidenciales suministrados por el token de acceso.

REIVINDICACIONES

1. Un método para asegurar comunicaciones Máquina a Máquina entre una aplicación del consumidor M2M y un proveedor de recursos M2M en el que cuando se inicia una solicitud de acceso:

- envío una solicitud de credenciales de valores desde la aplicación del consumidor a un servidor de autorización M2M,
- recepción, por la aplicación del consumidor, desde el servidor de autorización M2M de las credenciales de valores generadas, que comprenden un token de acceso, claves de encriptación de sesión y una clave de autenticación,
- transmisión, desde la aplicación del consumidor M2M, del token de acceso y un mensaje de autenticación al proveedor de recursos M2M para autenticar la aplicación del consumidor,
- transmisión de la solicitud de acceso desde la aplicación del consumidor al proveedor de recursos M2M, comprendiendo dicha solicitud de acceso un parámetro de solicitud encriptado con las claves de sesión para acceder o controlar los recursos,
- autenticación, por el proveedor de recursos, de la aplicación del consumidor como autorizada del mensaje de autenticación y el contenido del token de acceso,
- recuperación, por el proveedor de recursos, de las claves de sesión del contenido del token de acceso,
- descifrado, por el proveedor de recursos, del parámetro de solicitud cifrado con las claves de sesión,
- envío, desde el proveedor de recursos, de la respuesta cifrada del parámetro de solicitud a la aplicación del consumidor.

2. El método según la reivindicación anterior, en el que el proveedor de recursos es un dispositivo M2M o un servidor M2M.

3. El método según cualquiera de las reivindicaciones anteriores, en el que la generación del token de acceso comprende los siguientes pasos:

- generación de datos de sesión por la aplicación del consumidor, dichos datos de sesión identifican de forma univoca la transacción en curso entre la aplicación del consumidor y el proveedor de recursos,
- cálculo de los datos criptográficos a partir de los datos de sesión generados,
- adición de los datos criptográficos a la solicitud de credenciales de valores,
- el token de acceso generado por el servidor de autorización M2M comprende los datos criptográficos de la solicitud de credenciales de valores, información para recuperar las claves de sesión y una clave de autenticación generada.

4. El método según la reivindicación anterior, en el que el token de acceso se cifra con una clave compartida entre el servidor de autorización M2M y el proveedor de recursos.

5. El método según la reivindicación 3, en el que la información para recuperar las claves de sesión comprende o un índice asociado a las claves de sesión en una base de datos del servidor de autorización M2M, o claves de sesión cifradas con una clave compartida entre el servidor de autorización M2M y el proveedor de recursos.

6. El método según cualquiera de las reivindicaciones anteriores, en el que la autenticación de la aplicación del consumidor por parte del proveedor de recursos comprende los siguientes pasos:

- encriptar los datos de sesión con la clave de autenticación, por la aplicación del consumidor,
- enviar el token de acceso y los datos de sesión encriptados desde la aplicación del consumidor al servidor M2M,
- Desde la clave de autenticación del token de acceso, descifrado de los datos de sesión cifrados,
- desde los datos de sesión descifrados, calcular los datos criptográficos,
- Si la comparación de los datos criptográficos calculados con los datos criptográficos del token de acceso es exitosa, la aplicación del consumidor es autenticada.

7. Método según cualquiera de las reivindicaciones anteriores, en el que la autenticidad del token de acceso es verificada por el proveedor de recursos, o a partir de una firma calculada por el servidor de autorización M2M o de datos de autenticación añadidos por el servidor de autorización M2M al token de acceso.

8. El método según cualquiera de las reivindicaciones anteriores, en el que los datos de autenticación comprenden un valor incrementado de un contador que se usa para realizar una gestión anti-repetición, el proveedor de recursos M2M verifica si el valor del contador recibido en los datos de autenticación es mayor que un valor de contador previo guardado, si esta verificación es exitosa, el proveedor de recursos M2M guarda el valor del contador entrante y elimina el anteriormente guardado.

9. El método según cualquiera de las reivindicaciones anteriores, en el que:

- cuando la autenticación de la aplicación del consumidor es exitosa, el proveedor de recursos M2M se autentica al servidor de autorización M2M.
- Si la autenticación es exitosa, recupera las claves de sesión.

10. El método según cualquiera de las reivindicaciones anteriores, en el que la solicitud de acceso comprende también los datos de sesión encriptados con la clave de autenticación de sesión y el token de acceso.

11. El método según cualquiera de las reivindicaciones anteriores, en el que un dispositivo M2M encripta datos de forma continua con las claves de sesión para enviarlos al proveedor de recursos M2M para su almacenamiento.

12. El método según cualquiera de las reivindicaciones anteriores, en el que el token de acceso comprende el identificador único de recurso (URL) y la lista de parámetros de consultas autorizadas por la aplicación del consumidor, si el parámetro de solicitud cifrado está en la lista de acceso autorizado, el parámetro de consulta cifrado es procesado por el proveedor de recursos.

13. El método según cualquiera de las reivindicaciones anteriores, en el que durante la autenticación de la aplicación del consumidor por parte del servidor M2M, se verifica el tiempo de vida útil del token de acceso.

14. El método según la reivindicación anterior, en el que cuando se alcanza la vida útil del token de acceso

- se generan, respectivamente, unos nuevos datos de sesión y/o un nuevo token de acceso.
- las claves de sesión y/o la clave de autenticación, se renuevan o mantienen.

15. Un sistema de comunicaciones M2M, que comprende una aplicación del consumidor, estando dicha aplicación del consumidor configurada para comunicarse con un proveedor de recursos M2M a través de una red de acceso, donde los mensajes de solicitud de acceso que transitan entre la aplicación del consumidor y el dispositivo M2M durante esta comunicación están asegurados por un servidor de autorización M2M de acuerdo con cualquiera de las reivindicaciones anteriores.

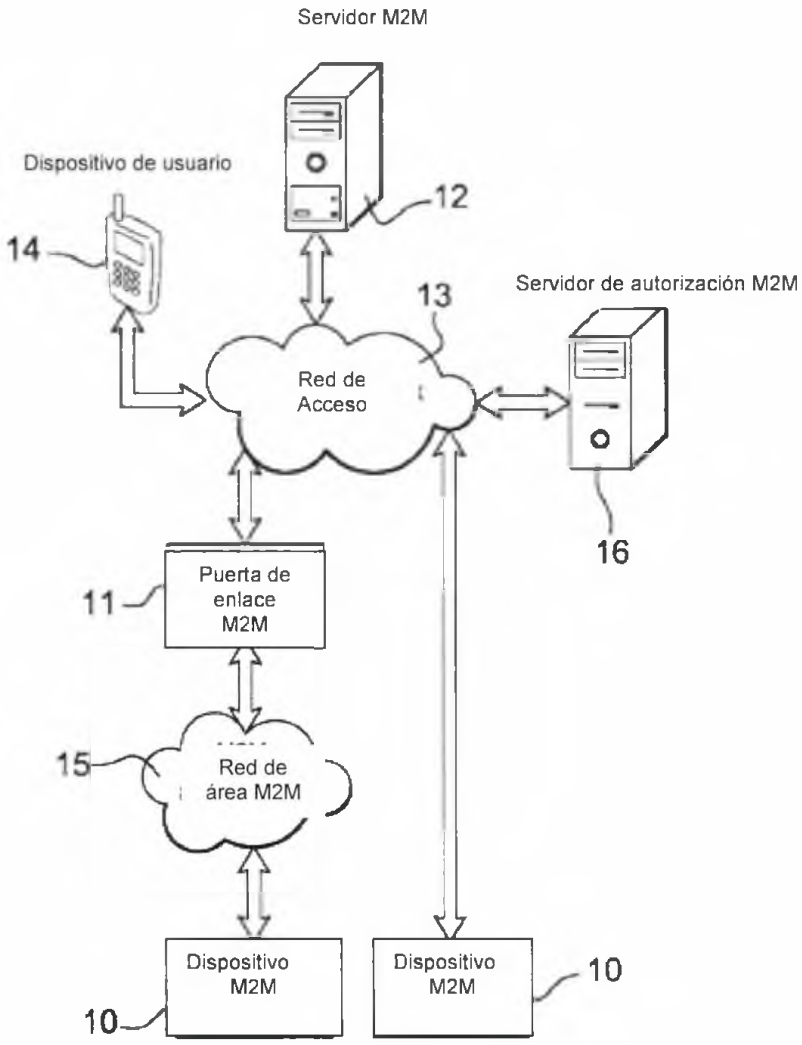
Servidor M2M
Dispositivo de usuario
12
14
13
Servidor de autorización M2M
Red de
Acceso
16
11
Puerta de
enlace
M2M
15
Red de
área M2M
Dispositivo
M2M
10
Dispositivo
M2M
10

Fig. 1

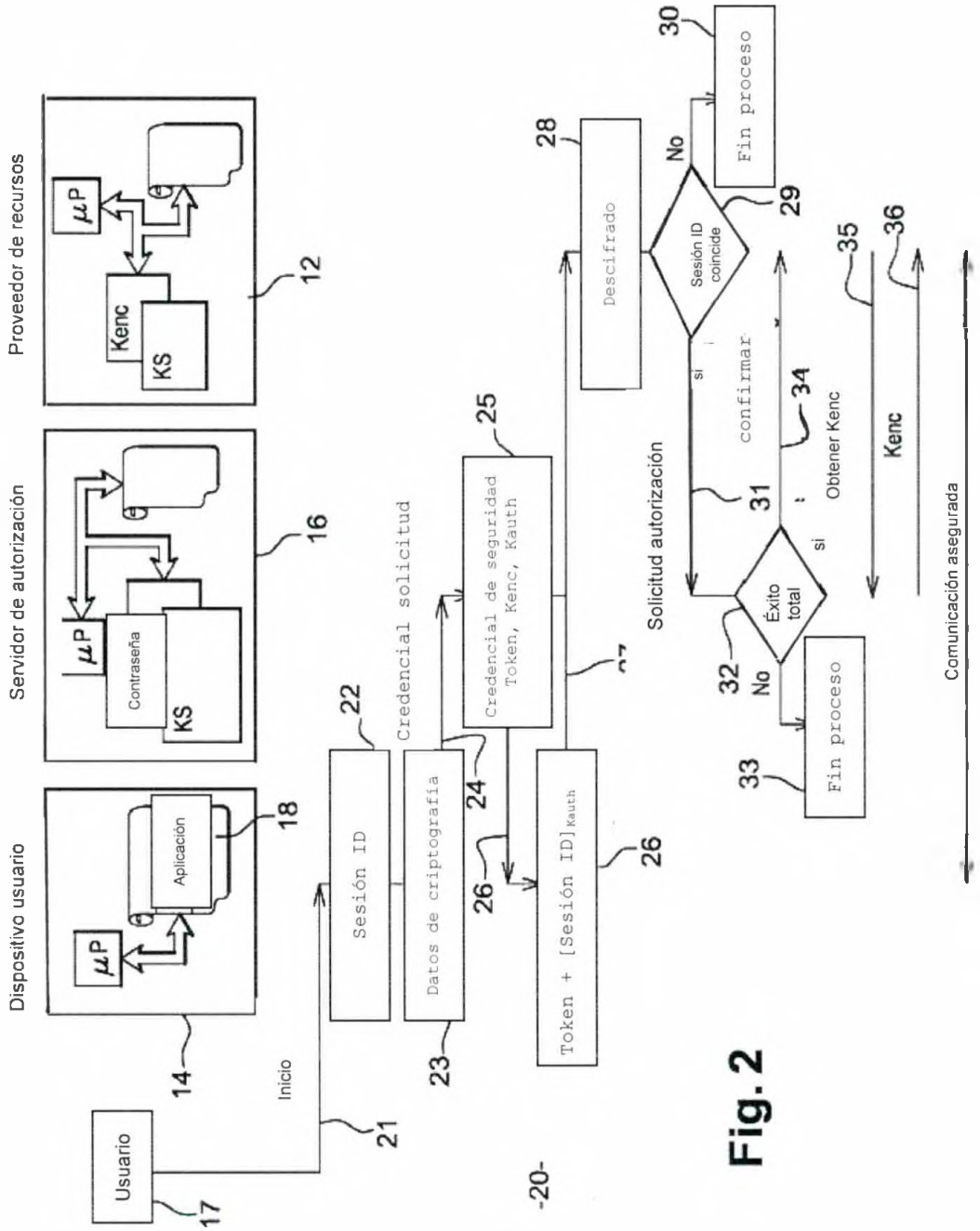
Dispositivo usuario
Servidor de autorización
Proveedor de recursos
Usuario
Inicio
Aplicación
Contraseña
KS
Kenc
Sesión ID
Datos de criptografía
Credencial solicitud
Credencial de seguridad
Token, Kenc, Kauth
Token + [Sesión ID]Kauth
Descifrado
Sesión ID coincide
No
Fin proceso
Solicitud autorización
confirmar
Éxito total
Obtener Kenc
Kenc
Comunicación asegurada
14
16
12
17
18
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
-20-

Fig. 2

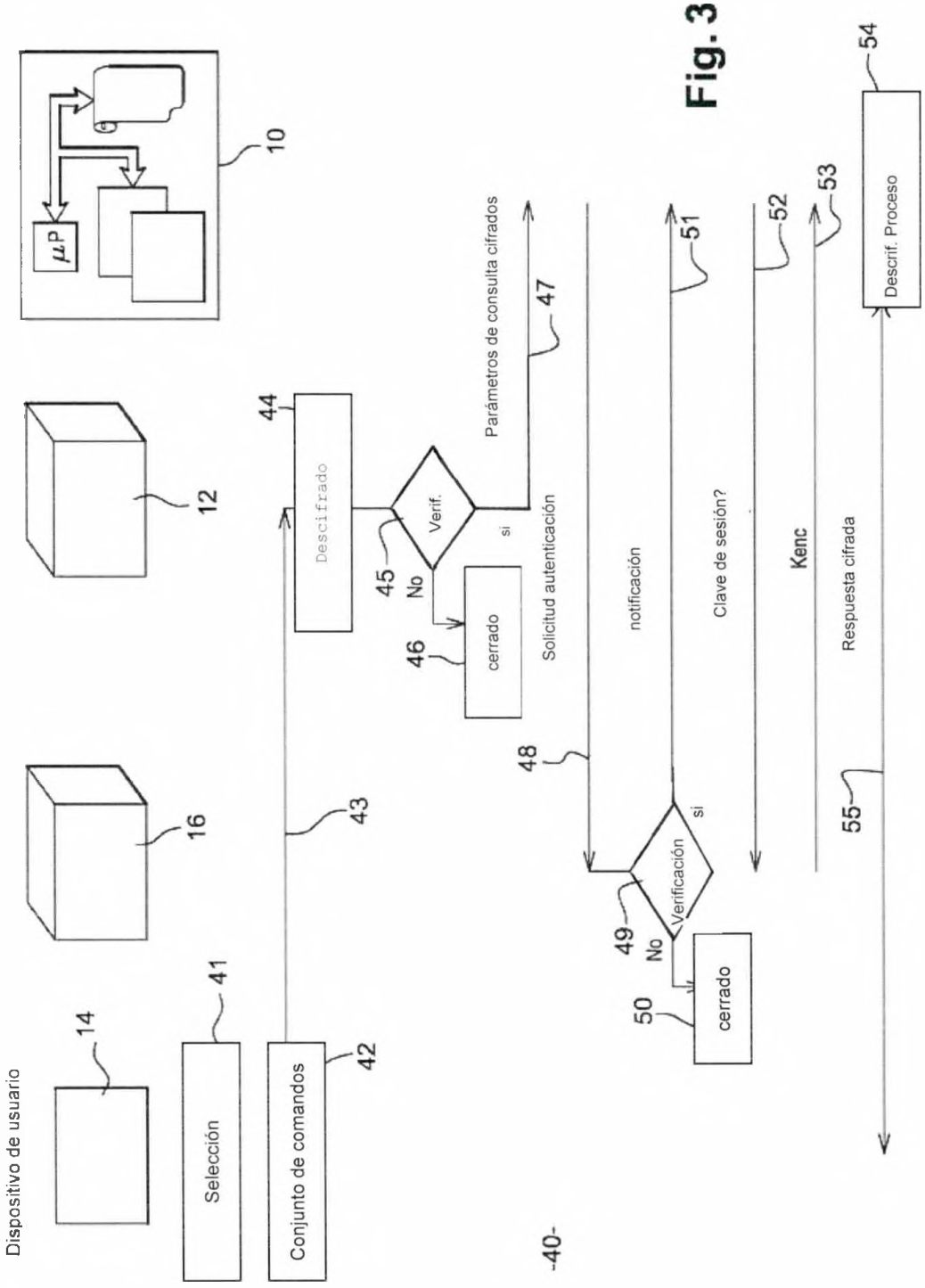
Dispositivo de usuario
14
Selección
41
Conjunto de comandos
42
43
16
12
10
μP
44
Descifrado
45
Verif.
No
si
46
cerrado
Parámetros de consulta cifrados
47
Solicitud autenticación
48
notificación
49
Verificación
No
si
50
cerrado
51
Clave de sesión?
52
Kenc
53
Respuesta cifrada
54
Descrif. Proceso
55
-40-

Fig. 3