(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 822 579**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04L 29/08 (2006.01)
H04W 12/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.06.2017 PCT/US2017/037342**

(87) Fecha y número de publicación internacional: **11.01.2018 WO18009313**

(96) Fecha de presentación y número de la solicitud europea: **13.06.2017 E 17734193 (0)**

(97) Fecha y número de publicación de la concesión europea: **22.07.2020 EP 3482579**

(54) Título: **Transferencia automática segura de datos con un vehículo de motor**

(30) Prioridad:

08.07.2016 US 201662360200 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.05.2021

(73) Titular/es:

AIRBIQUITY, INC. (100.0%)
1191 2nd Avenue, Suite 1900
Seattle, WA 98101, US

(72) Inventor/es:

MOINZADEH, KAMYAR;
LEUNG, KEEFE y
BELL, JACK, WILLIAM

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Transferencia automática segura de datos con un vehículo de motor

Campo técnico

Las realizaciones de la presente divulgación se refieren al campo de las comunicaciones seguras y, en particular, a los procedimientos y aparatos asociados con la transferencia automática segura de datos con un vehículo de motor.

Antecedentes

Un OEM (fabricante de equipo original) puede incrustar el software en un vehículo de motor en una fábrica; sin embargo, también existen esquemas para actualizar de forma segura el software del vehículo de motor después de que el vehículo de motor sale de fábrica. En un esquema conocido, los vehículos de motor pueden actualizarse en un punto de venta, como un concesionario.

En el escenario típico, el OEM puede proporcionar un dispositivo electrónico portátil que debe ser operado por el personal del punto de venta. El dispositivo electrónico puede acoplarse a Internet (por ejemplo, a través de un dispositivo de red de banda ancha del concesionario) y establecer una red de túnel segura a través de Internet entre el dispositivo electrónico y un servidor OEM. Los vehículos motorizados pueden ser conducidos por el personal a una distancia corta hasta un centro de servicio, donde el personal puede conectar el dispositivo electrónico portátil en cada vehículo motorizado y puede operar el dispositivo electrónico portátil y/o el vehículo motorizado para realizar la actualización del vehículo motorizado (se puede descargar una actualización desde el servidor OEM, a través de la red de túneles seguros, al dispositivo electrónico portátil y luego al vehículo de motor).

En algunos casos, puede ser conveniente actualizar de forma segura el software de los vehículos de motor en otros puntos a lo largo de una cadena de suministro, como en un punto intermedio en el campo y antes de llegar al punto de venta, por una variedad de razones. Sin embargo, en algunos tiempos y/o ubicaciones posibles a lo largo de la cadena de suministro, es posible que los vehículos motorizados no estén cerca de un centro de servicio y es posible que ni siquiera sean fácilmente accesibles incluso si estuvieran cerca de un centro de servicio (por ejemplo, los vehículos motorizados pueden estar asegurados a un aparato de transporte, dispuestos muy juntos, etc.) Puede que no sea posible y/o práctico realizar los esquemas conocidos para actualizar de forma segura el software del vehículo de motor en estos tiempos y/o ubicaciones.

Sumario de la invención

La invención reivindicada se refiere a un dispositivo como se define en la reivindicación independiente 1. Las diversas realizaciones se definen en las reivindicaciones dependientes.

Breve descripción de los dibujos

La Figura 1 ilustra un sistema para la transferencia automática segura de datos con un vehículo de motor, en algunas realizaciones.

La Figura 2 es un diagrama de flujo simplificado que ilustra algunas de las operaciones que puede realizar el dispositivo electrónico en el vehículo de la Figura 1, en algunas realizaciones.

La Figura 3 es un diagrama de flujo simplificado que ilustra algunas de las operaciones que se pueden realizar con otros dispositivos descritos con referencia a la Figura 1, en algunas realizaciones.

La Figura 4 es un diagrama de secuencia de mensajes que ilustra algunas de las operaciones que pueden realizarse en las realizaciones que utilizan más de un canal de comunicación.

Descripción detallada de las realizaciones preferentes

Por medio de antecedentes, los vehículos de motor típicamente tienen más de un modo de energía, como un primer modo de energía (por ejemplo, un modo de energía de marcha) en el que tanto el panel de instrumentos como los accesorios reciben energía (los accesorios pueden incluir, entre otros, componentes de entretenimiento), un segundo modo de energía (por ejemplo, un modo de energía para accesorios) en el que el panel de instrumentos no recibe energía pero los accesorios sí reciben energía, y uno o más terceros modos de energía más bajos en los que los accesorios no reciben energía pero otros sistemas pueden recibir energía y seguir funcionando.

Al menos uno de los uno o más terceros modos de energía inferior puede poner el vehículo de motor en un estado de energía desatendido. El estado de energía desatendido puede denominarse "apagado", pero en realidad algunos sistemas reciben energía y continúan funcionando en el estado de energía desatendido. Por ejemplo, algunos sistemas sin llave pueden continuar encendidos incluso después de que un operador haya "apagado y bloqueado el vehículo de motor para que estén listos cuando el operador regrese al vehículo".

Además, por medio de antecedentes, muchos dispositivos electrónicos modernos proporcionan una forma de conectarse a servidores externos como clientes y realizar operaciones especificadas por el servidor, como actualizar el software en el dispositivo. Garantizar la seguridad en este procedimiento es difícil en entornos no controlados porque los canales de comunicación disponibles a menudo se proporcionan como una conexión a Internet comercial o de consumidor típica, que podría comprometer la seguridad de diversas formas. En el caso del equipo en el vehículo, las consecuencias asociadas con la seguridad comprometida pueden ser significativas.

La Figura 1 ilustra un sistema 100 para la transferencia automática segura de datos con un vehículo de motor, en algunas realizaciones. El sistema 100 puede incluir un dispositivo en el vehículo 1 (por ejemplo, uno o más componentes del vehículo que pueden incluir un dispositivo informático y un sistema de comunicación inalámbrica) para establecer un canal de comunicación 15 con el dispositivo remoto 25, que puede ser un punto de acceso Wi-Fi seguro en algunos ejemplos. Un punto de acceso Wi-Fi seguro, a diferencia de un punto de acceso Wi-Fi abierto, puede requerir que un dispositivo proporcione un valor de autenticación, como una contraseña, antes de otorgar acceso al dispositivo a través del punto de acceso Wi-Fi (y muchos puntos de acceso Wi-Fi, ya sean seguros o abiertos, también pueden comunicarse mediante el uso de cifrado una vez que se otorga el acceso).

El dispositivo en el vehículo 1 puede incluir un procesador 12 configurado para realizar operaciones predefinidas en un vehículo de motor para realizar una transferencia de datos segura automática sin requerir intervención humana, y mientras el vehículo de motor está en un estado de energía desatendido. El canal de comunicación 15 puede usarse para descargar de forma segura cualquier tipo de datos desde el dispositivo remoto 25 al vehículo de motor (por ejemplo, una carga útil, como un software para ser instalado en el dispositivo en el vehículo 1 u otro dispositivo en el vehículo), o para cargar de forma segura una carga útil desde el vehículo de motor.

Por ejemplo, en algunas cadenas de suministro de vehículos de motor, puede haber un inventario de vehículos de motor en un puerto durante un tiempo durante y/o después de la descarga de un vehículo marino. Dicho inventario puede ser actualizado en el puerto por el procesador 12 de cada vehículo de motor que se comunica con el dispositivo remoto 25. Además, algunos o todos los procesadores 12 pueden cargar datos al dispositivo remoto 25. Los datos cargados pueden ser cualquier tipo de datos, como datos de sensores, códigos de diagnóstico (si los vehículos de motor tienen sensores en funcionamiento durante el transporte, se podría leer un registro generado por estos sensores para, por ejemplo, evaluar una condición de los vehículos de motor después de la marina transporte).

El procesador 12 puede identificar un tiempo para establecer el canal de comunicación 15 basándose en un evento de activación predefinido. La memoria 11 puede almacenar uno o más valores 14 para definir el evento de activación. Estos valores 14 pueden incorporarse en la memoria 11 en un tiempo de fabricación, en algunos ejemplos. El procesador 12 puede comenzar a monitorear en base al evento de activación predefinido, que puede incluir verificar uno o más recursos (no mostrados).

El uno o más recursos pueden incluir recursos locales, por ejemplo, en el vehículo y/o remotos. Un ejemplo de recurso remoto es una geovalla. En algunos ejemplos, el evento de activación predefinido puede incluir una proximidad predeterminada a la geovalla. El procesador 12 puede obtener datos indicativos de la geovalla en base a una señal recibida. El procesador 12 puede comparar los datos con los valores 14, y reconocer una ocurrencia del evento predefinido (por ejemplo, puede detectar que el vehículo de motor está en la proximidad predeterminada de la geovalla para establecer el canal de comunicación 15).

Un ejemplo de un recurso local, por ejemplo, un recurso en el vehículo, es un reloj 5 del vehículo de motor. En algunos ejemplos, el evento de activación predefinido puede incluir un tiempo predeterminado. El procesador 12 puede obtener datos generados por el reloj 5 y comparar estos datos con los valores 14. El procesador 12 puede reconocer una ocurrencia del evento predefinido (por ejemplo, puede detectar que un tiempo actual es igual al tiempo predeterminado para establecer el canal de comunicación 15).

Además del uso de una red Wi-Fi segura en algunos ejemplos, el uso del evento de activación predeterminado puede proporcionar seguridad. Por ejemplo, el canal de comunicación 15 puede establecerse en una geografía física del puerto, que puede tener seguridad física como vallas y guardias. Además, un tiempo predeterminado para establecer el canal de comunicación puede proporcionar seguridad porque el tiempo puede ser indicativo de la ubicación física del vehículo de motor (el tiempo puede indicar una ubicación del vehículo de motor a lo largo de una cadena de suministro).

El canal de comunicación 15 puede establecerse en un transceptor Wi-Fi de la interfaz inalámbrica 7, que puede ofrecer un cifrado fuerte para proteger contra ataques de intermediarios. En otros ejemplos, el canal de comunicación 15 puede establecerse en cualquier porción de la interfaz inalámbrica 7, que incluye una característica de seguridad, como un cifrado fuerte. Puede ser posible usar un receptor y/o transmisor dedicado para la transferencia automática de datos segura, que puede ser diferente de los receptores y/o transmisores que usará un consumidor.

Como se indicó anteriormente, en algunos ejemplos, el dispositivo remoto 25 puede requerir que los dispositivos se autentiquen antes del comienzo de una transferencia de datos. El dispositivo remoto 25 puede ser un punto de acceso Wi-Fi seguro, en algunos ejemplos.

Además de un requisito de autenticación, el dispositivo remoto 25 puede (en algunos ejemplos) incluir también un almacén de datos 21 para almacenar datos que se descargarán a los vehículos de motor (por ejemplo, una actualización de un vehículo de motor) y un dispositivo 22 como un servidor integrado o una interfaz para conectarse directamente a un servidor separado para proporcionar la actualización del vehículo directamente a cada vehículo de motor. En estos ejemplos, a diferencia de los dispositivos electrónicos portátiles que pueden operarse en centros de servicio, el dispositivo remoto 25 puede no requerir acceso a Internet de banda ancha para acceder a un servidor remoto a través de Internet. En estos ejemplos, el dispositivo 22 puede descargar la actualización del vehículo de motor directamente al dispositivo 1 del vehículo a través del canal de comunicación 15. Es posible que el dispositivo remoto 25 no requiera ningún componente para conectarse a Internet y, de hecho, estos componentes pueden omitirse del dispositivo remoto 25 por un número de razones tales como ahorro de costes y/o consideraciones de seguridad. En otros ejemplos, el dispositivo remoto 25 puede no incluir el dispositivo 22 y/o el almacén de datos 21, y en estos ejemplos el dispositivo remoto 25 puede establecer una red de túnel segura a través de Internet a un servidor OEM en cualquier tiempo (como antes al establecimiento del canal de comunicación 15).

El dispositivo remoto 25 puede ser un dispositivo móvil en algunos ejemplos, por ejemplo, no solo portátil sino que también puede estar configurado para funcionar mientras se transporta. Se puede disponer un inventario de vehículos de motor muy cerca uno del otro o de otros objetos, como en una zona de descarga de un puerto o en un aparato de envío. En algunos ejemplos, especialmente en función del alcance del transceptor/receptor/transmisor particular de la interfaz inalámbrica 7, puede ser conveniente transportar el dispositivo remoto móvil 25 alrededor de un perímetro de un inventario de vehículos de motor desatendidos y/o entre el motor vehículos. En algunos ejemplos, un dispositivo remoto móvil 25 puede ser llevado por una persona o en un vehículo de servicio (que puede ser controlado por una persona o moverse (por ejemplo, conducir, volar, etc.) de forma autónoma en una realización más mecanizada, para moverse a lo largo del perímetro u otra trayectoria).

Algunos ejemplos pueden usar un canal de comunicación diferente adicional (no mostrado). En estos ejemplos, un evento de activación predeterminado puede estar asociado con el vehículo de motor que se comunica a través de un canal de comunicación diferente sobre un receptor o transceptor de la interfaz inalámbrica 7, que no necesita ser el mismo receptor o transceptor usado para el canal de comunicación 15. El uso de un canal de comunicación como parte de un evento de activación puede proporcionar seguridad en algunos ejemplos (aunque esto no es obligatorio). Por ejemplo, el procesador 12 puede no tener alguna información requerida para establecer el canal de comunicación 15 hasta que se establezca y/o descifre un canal de comunicación diferente (por ejemplo, el dispositivo remoto 25 puede ser *reconocible* mediante el uso de únicamente la información a recuperar de los diferentes canales de comunicación). Una realización que usa este canal de comunicación diferente se describirá más adelante con mayor detalle con respecto a la Figura 4. En otros ejemplos, esta información puede ser identificada por el procesador 12 sin establecer un canal de comunicación diferente (por ejemplo, el procesador 12 puede acceder a información almacenada en una memoria del vehículo de motor).

La Figura 2 es un diagrama de flujo simplificado que ilustra algunas de las operaciones 200 que pueden ser realizadas por el dispositivo en el vehículo 1 de la Figura 1, en algunas realizaciones. En el bloque 201, el dispositivo en el vehículo 1 puede monitorear una fuente de primeros datos, por ejemplo, monitorear información de generación de vehículos de motor y/o información generada de forma remota desde el vehículo de motor. En el bloque 202, el dispositivo en el vehículo 1 puede verificar los primeros datos en base a uno o más valores para especificar un evento de activación predefinido para el acoplamiento a un dispositivo remoto. Una porción de uno o más valores puede estar incrustados en la fabricación del vehículo y/o una porción de uno o más valores puede ser proporcionada dinámicamente por una llamada (como una llamada celular entrante que incluye información cifrada recuperable para obtener la porción de uno o más valores). En el diamante 203, el dispositivo en el vehículo 1 puede determinar si ocurrió el evento de activación predefinido. Si el evento de activación predefinido no ocurrió, el procedimiento puede regresar al bloque 201 hasta, digamos, un próximo alcance (regular o de cualquier otra manera) para realizar el diamante 203.

En el bloque 204, el dispositivo en el vehículo 1 puede identificar los segundos datos adecuados para comunicarse con el dispositivo remoto. Los segundos datos pueden estar ubicados en una memoria del dispositivo en el vehículo 1 o en una memoria accesible al dispositivo en el vehículo 1 antes de que ocurra el evento de activación. En otros ejemplos, los segundos datos pueden recibirse como parte del evento desencadenado y/o pueden volverse accesibles como parte del evento de activación. Los segundos datos pueden incluir información sobre una característica del dispositivo remoto, por ejemplo, información para autenticar el dispositivo en el vehículo 1 en el dispositivo remoto, una dirección u otra información para descubrir el dispositivo remoto, etc.

En el bloque 205, el dispositivo en el vehículo 1 puede establecer un canal de comunicación con el dispositivo remoto mediante el uso de la segunda información. En el bloque 206, el dispositivo en el vehículo 1 puede descargar y/o cargar los terceros datos a través del canal de comunicación. Los terceros datos pueden incluir una actualización del vehículo de motor y/o información a cargar desde el vehículo de motor.

La Figura 3 es un diagrama de flujo simplificado que ilustra algunas de las operaciones 300 que pueden realizarse con otros dispositivos descritos con referencia a la Figura 1, en algunas realizaciones. En el bloque 301, el dispositivo remoto 25 puede autenticar un dispositivo electrónico instalado en un vehículo de motor en respuesta a la ocurrencia de un evento de activación predefinido. En el bloque 302, el dispositivo remoto 25 puede establecer un canal de comunicación con el dispositivo electrónico en respuesta a la ocurrencia del evento de activación. En el bloque 303, el dispositivo remoto 25 puede transmitir y/o recibir datos por el canal de comunicación.

La Figura 4 es un diagrama de secuencia de mensajes que ilustra algunas de las operaciones que pueden realizarse en las realizaciones que utilizan más de un canal de comunicación. El dispositivo en el vehículo 402 puede realizar cualquiera de las operaciones realizadas por el dispositivo en el vehículo 1 (Figura 1), y el dispositivo remoto 404 puede realizar cualquiera de las operaciones realizadas por el dispositivo remoto 25 (Figura 1).

El segundo canal de comunicación 403 puede ser similar al canal de comunicación 15 (Figura 1). El primer canal de comunicación 401 puede establecerse a través de Internet mediante el uso de una porción diferente de una interfaz inalámbrica del vehículo de motor (por ejemplo, un transceptor diferente, un receptor diferente, un transmisor diferente, etc.), y puede extenderse a un servidor como un Servidor OEM. El receptor/transceptor sobre el cual se establece el primer canal de comunicación 401 no necesita tener el mismo ancho de banda y/o incluir la misma seguridad que el receptor/transceptor sobre el cual se establece el segundo canal de comunicación 403. En un ejemplo, el receptor/transceptor sobre el cual se establece el primer canal de comunicación 401 es un transceptor celular que puede tener un ancho de banda menor que un transceptor/receptor/transmisor diferente sobre el cual se establece el segundo canal de comunicación 403 (por ejemplo, una conexión Wi-Fi transceptor), y en algunos ejemplos la conexión se puede realizar mediante el uso de una unidad de control de transmisión de vehículos de motor (TCU) a través de la conexión celular y a través de Internet. En otras realizaciones, el primer canal de comunicación 401 puede ser un dispositivo NFC (comunicaciones de campo cercano), un transceptor inalámbrico de corto alcance tal como un transceptor Bluetooth, un punto de acceso Wi-Fi (por ejemplo, diferente al punto de acceso Wi-Fi seguro, como un punto de acceso Wi-Fi abierto).

El servidor (de nuevo no mostrado, puede ser el servidor OEM u otro servidor diferente a cualquier servidor correspondiente al dispositivo remoto 404) puede establecer el primer canal de comunicación 401 con el dispositivo en el vehículo 402 con el fin de activar una transferencia automática segura de datos con el dispositivo remoto 404. Como ya se mencionó, el primer canal 401 no necesita incluir la misma seguridad que el segundo canal de comunicación 403 (el primer canal de comunicación 401 puede no ser seguro, en algunos ejemplos).

El servidor puede enviar el mensaje 411 al dispositivo en el vehículo 402 a través del primer canal de comunicación 401. El mensaje 411 puede enviarse mediante SMS (servicio de mensajes cortos) o mediante el uso de una conexión a Internet usando un protocolo de red seguro como SSL (capa de conexión segura). El mensaje 411 se puede cifrar mediante el uso de un algoritmo público/privado (la clave pública puede residir en el vehículo de motor).

El mensaje 411 puede incluir una lista de canales de comunicación seguros conocidos. El mensaje 411 puede incluir información de conexión, tal como uno o más SSID (identificadores de conjunto de servicios), contraseñas para cada SSID, información de tipo de seguridad para cada SSID, o similares, o combinaciones de los mismos (para cada uno de los canales de comunicación seguros enumerados). El mensaje 411 puede incluir uno o más valores para especificar un evento de activación predefinido, por ejemplo, información sobre un tiempo seleccionado, información sobre un recurso remoto tal como una geovalla, o similares, o combinaciones de los mismos.

El mensaje 411 puede enviarse como una simple serie de bytes mediante el uso de API de comunicación de bajo nivel (interfaces de programación de aplicaciones) del remitente. El mensaje 411 puede enviarse mediante un punto de acceso Wi-Fi, tal como un punto de acceso Wi-Fi abierto.

En la operación 412, el dispositivo en el vehículo 402 puede descubrir (por ejemplo, buscar un canal de comunicación seguro en la lista) y conectarse al segundo canal de comunicación 403 en base a la lista. La operación 412 puede realizarse inmediatamente después del mensaje de identificación 411, o la información del evento de activación puede especificar condiciones de activación asociadas con un tiempo diferente para realizar el descubrimiento. En algún ejemplo, el dispositivo en el vehículo 402 puede configurarse para intentar conectarse a un punto de acceso Wi-Fi oculto mediante el uso de SSID en la lista (por ejemplo, en lugar de escanear o si el escaneo falla). En la operación 413, el dispositivo en el vehículo 402 puede establecer una conexión con el dispositivo remoto 404 a través del segundo canal de comunicación conectado 403. El dispositivo en el vehículo 402 puede enviar una solicitud de autenticación 414 (que puede basarse en un valor de autenticación recuperado del primer canal de comunicación 401) al dispositivo remoto 404. El dispositivo remoto 404 puede devolver una respuesta de autenticación 415, por ejemplo autenticando el dispositivo en el vehículo 402 al dispositivo remoto 404. Este protocolo de enlace de autenticación puede proporcionar otra capa de seguridad.

El dispositivo en el vehículo 402 puede enviar una solicitud de manifiesto de operación 416 para identificar si se debe realizar alguna operación (por ejemplo, para identificar si se debe realizar una actualización, cambiar una configuración, etc.). Esto puede identificar uno o más de: actualización del sistema operativo, actualización de la aplicación del usuario, actualización del mapa, actualización de las preferencias o similares, o combinaciones de los mismos. El dispositivo remoto 404 (por ejemplo, un servidor del mismo) puede enviar un manifiesto de operación

417, que puede hacer que el dispositivo en el vehículo 402 realice operaciones 418 en base a selecciones identificadas en el manifiesto 417. El dispositivo en el vehículo 402 puede transmitir un mensaje 419 que incluye los resultados de la operación, y el dispositivo remoto 404 (por ejemplo, un servidor del mismo) puede enviar un reconocimiento 420. El dispositivo en el vehículo 402 puede realizar una desconexión 421 en respuesta a recibir el reconocimiento 420 y/o alcanzar un tiempo de espera.

En algunos ejemplos, los principios descritos anteriormente se pueden aplicar cuando el propietario de un vehículo lleva su vehículo a un concesionario para un mantenimiento programado. El propietario del vehículo puede esperar en una sala de espera y el vehículo motorizado puede, sin supervisión en el estacionamiento, realizar cualquiera de las operaciones descritas en la presente memoria para realizar una transferencia automática segura de datos (el vehículo motorizado puede conectarse a un punto de acceso Wi-Fi oculto en el concesionario en algunos ejemplos). No es necesario traer el vehículo de motor al centro de servicio ni ser atendido en el estacionamiento. En algunos ejemplos, el vehículo de motor y/o el servidor OEM pueden enviar un mensaje al dispositivo portátil personal del propietario del vehículo y/o al dispositivo informático del personal del concesionario cuando esté completo.

En algunos ejemplos, los principios descritos anteriormente pueden aplicarse a una flota de vehículos de motor en servicio o un vehículo de motor de alquiler devuelto. Un conductor de flota o cliente puede devolver un vehículo de motor a un estacionamiento para dejarlo hasta el próximo día laboral o devolver el alquiler. En el estacionamiento, el vehículo de motor puede realizar cualquiera de las operaciones descritas en la presente memoria para realizar una transferencia automática segura de datos para actualizar el vehículo de motor y/o extraer datos del vehículo de motor (por ejemplo, datos de sensores recopilados para el día).

En algunos ejemplos, los principios descritos anteriormente se pueden aplicar a la transferencia automática segura de datos para cualquier dispositivo portátil que requiera una actualización segura o que almacene datos de alto valor de privacidad, incluidos, entre otros, dispositivos médicos destinados a hospitales o instalaciones de atención, dispositivos industriales, dispositivos de Internet de Cosas (IoT), productos domésticos de IoT como seguridad del hogar, automatización del hogar, aeronaves y equipos de aviación relacionados, dispositivos de monitoreo remoto o similares, o combinaciones de los mismos.

Ejemplos

El ejemplo 1 es un dispositivo electrónico en el vehículo para operar en un vehículo de motor en un estado de energía desatendido, el dispositivo electrónico en el vehículo que comprende: una interfaz inalámbrica para comunicarse con un recurso de red seguro remoto; y una memoria para almacenar uno o más valores para especificar un evento de activación predefinido para acoplar el vehículo de motor en el estado de energía desatendido al recurso de red seguro remoto; un procesador configurado para: identificar un recurso a monitorear; reconocer una ocurrencia de un evento de activación predefinido verificando los primeros datos obtenidos en respuesta a monitorear el recurso identificado contra uno o más valores; en respuesta a un reconocimiento de la ocurrencia de un evento de activación predefinido, identificar los segundos datos adecuados para acoplar el dispositivo electrónico en el vehículo al recurso de red seguro remoto; establecer un canal de comunicación al recurso de red segura remota a través de la interfaz inalámbrica mediante el uso de los segundos datos; y descargar los terceros datos a través del canal de comunicación al vehículo de motor en el estado de energía desatendido o cargar los terceros datos a través del canal de comunicación desde el vehículo de motor en el estado de energía desatendido.

El ejemplo 2 incluye el tema del ejemplo 1 o cualquier otro ejemplo en la presente memoria, en el que los primeros datos comprenden el contenido de una señal recibida a través de un canal de comunicación establecido independientemente del recurso de red segura remota.

El ejemplo 3 incluye el tema de cualquiera de los ejemplos 1-2 o cualquier otro ejemplo en la presente memoria, en el que uno de los canales de comunicación se establece mediante el uso de un primer receptor de la interfaz inalámbrica o un transmisor que corresponde al primer receptor y el otro de los canales de comunicación se establece mediante el uso de un segundo receptor diferente de la interfaz inalámbrica.

El ejemplo 4 incluye el tema de cualquiera de los ejemplos 1-3 o cualquier otro ejemplo en la presente memoria, en el que el primer receptor incluye un receptor de un transceptor Wi-Fi y el segundo receptor incluye un receptor de al menos uno de un transceptor celular o un Transceptor inalámbrico de corto alcance.

El ejemplo 5 incluye el tema de cualquiera de los ejemplos 1-4 o cualquier otro ejemplo, en el que los primeros datos comprenden información de conexión para establecer una conexión sobre la que se extiende el canal de comunicación.

El ejemplo 6 incluye el tema de cualquiera de los ejemplos 1-5 o cualquier otro ejemplo en la presente memoria, en el que la información de conexión comprende un identificador de conjunto de servicios (SSID) y un valor de tipo de seguridad.

El ejemplo 7 incluye el tema de cualquiera de los ejemplos 1-6 o cualquier otro ejemplo en la presente memoria, en el que la información de conexión comprende una contraseña.

El ejemplo 8 incluye el tema de cualquiera de los ejemplos 1-7 o cualquier otro ejemplo en la presente memoria, en el que los primeros datos comprenden información indicativa de que el vehículo de motor se ha movido dentro de una proximidad predefinida de una referencia.

El ejemplo 9 incluye el tema de cualquiera de los ejemplos 1-8 o cualquier otro ejemplo en la presente memoria, en el que la referencia comprende una geovalla.

El ejemplo 10 incluye el tema de cualquiera de los ejemplos 1-9 o cualquier otro ejemplo en la presente memoria, en el que el evento de activación predeterminado comprende un tiempo programado.

El ejemplo 11 incluye el tema de cualquiera de los ejemplos 1-10 o cualquier otro ejemplo en la presente memoria, en el que los segundos datos comprenden datos de conexión residentes en una memoria electrónica del vehículo de motor antes de que ocurra el evento predefinido.

El ejemplo 12 incluye el tema de cualquiera de los ejemplos 1-11 o cualquier otro ejemplo en la presente memoria, en el que los terceros datos comprenden una actualización para descargarse en el vehículo de motor.

El ejemplo 13 incluye el tema de cualquiera de los ejemplos 1-12 o cualquier otro ejemplo en la presente memoria, en el que el recurso de red segura comprende un punto de acceso Wi-Fi seguro.

El ejemplo 14 incluye el tema de cualquiera de los ejemplos 1-13 o cualquier otro ejemplo en la presente memoria, en el que el recurso identificado comprende un recurso en el vehículo.

El ejemplo 15 incluye el tema de cualquiera de los ejemplos 1-14 o cualquier otro ejemplo en la presente memoria, en el que el recurso identificado es un dispositivo correspondiente a una geovalla u otro dispositivo remoto separado del vehículo de motor.

El ejemplo 16 es un procedimiento, que comprende: establecer un primer canal de comunicación con un vehículo de motor en un estado de energía desatendido; transmitir, a través del primer canal de comunicación, datos que representan un valor de autenticación adecuado para establecer un segundo canal de comunicación que acopla el vehículo de motor y un punto de acceso inalámbrico remoto del vehículo de motor; en el que el segundo canal de comunicación es diferente al primer canal de comunicación; establecer, mediante el uso del punto de acceso inalámbrico, el segundo canal de comunicación con el dispositivo electrónico en respuesta a la transmisión sobre el primer canal de comunicación; y transmitir o recibir una carga útil a través del segundo canal de comunicación.

El ejemplo 17 incluye el tema del ejemplo 16 o cualquier otro ejemplo en la presente memoria, en el que el segundo canal de comunicación incluye una capa de seguridad que no está presente en el primer canal de comunicación.

El ejemplo 18 incluye el tema de cualquiera de los ejemplos 16-17 o cualquier otro ejemplo en la presente memoria, en el que los datos que representan el valor de autenticación comprenden datos cifrados.

El ejemplo 19 incluye el tema de cualquiera de los ejemplos 16-18 o cualquier otro ejemplo en la presente memoria, en el que el punto de acceso inalámbrico comprende un punto de acceso oculto identificado por la información representada por los datos, y en el que establecer el segundo canal de comunicación comprende conectarse al punto de acceso oculto sensible a al menos un intento de escaneo fallido.

El ejemplo 20 incluye el tema de cualquiera de los ejemplos 16-19 o cualquier otro ejemplo en la presente memoria, en el que el punto de acceso inalámbrico comprende un primer punto de acceso seguro para operar en base a una característica de seguridad, y en el que el primer canal de comunicación se establece mediante el uso de un segundo punto de acceso diferente que no opera en base a dicha característica de seguridad.

El ejemplo 21 es un dispositivo electrónico que comprende: una primera interfaz de entrada/salida; una segunda interfaz de entrada/salida que es diferente a la primera interfaz de entrada/salida; y circuitos para identificar un canal seguro correspondiente a un recurso de red seguro remoto, los circuitos configurados para: determinar si utilizar la primera interfaz de entrada/salida para obtener información que se puede usar para autenticar el dispositivo electrónico con el recurso de red seguro; en respuesta a una verificación para usar la primera interfaz de entrada/salida para obtener información que se puede usar para autenticar el dispositivo electrónico con el recurso de red seguro, obtener los primeros datos cifrados a través de la primera interfaz de entrada/salida y recuperar, a partir de los primeros datos cifrados, dicha información; y establecer una conexión con el recurso de red seguro a través de la segunda interfaz de entrada/salida mediante el uso de dicha información; y descargar o cargar los segundos datos que sean diferentes a los primeros datos cifrados a través de la conexión.

El ejemplo 22 puede incluir el tema del ejemplo 21 o cualquier otro ejemplo en la presente memoria, en el que los segundos datos comprenden al menos uno de software de vehículo de motor, información de diagnóstico recopilada por un vehículo de motor en el que está instalado el dispositivo electrónico, o datos privados asociados con un operador del vehículo de motor (por ejemplo, información de ubicación, preferencias del usuario o similares).

El ejemplo 23 puede incluir el tema de cualquiera de los ejemplos 21-22 o cualquier otro ejemplo en la presente memoria, en el que los segundos datos están cifrados y cifrados de forma diferente a los primeros datos cifrados.

El ejemplo 24 puede incluir el tema de cualquiera de los ejemplos 21-23 o cualquier otro ejemplo en la presente memoria, en el que obtener los primeros datos cifrados comprende además establecer una conexión celular de paquetes de datos (por ejemplo, una conexión celular de paquetes de datos iniciada localmente) y descargar los primeros datos cifrados a través de la conexión celular de paquetes de datos.

El ejemplo 25 puede incluir el tema de cualquiera de los ejemplos 21-24 o cualquier otro ejemplo en la presente memoria, en el que la conexión con los recursos de red segura se establece mediante el uso de una conexión WI-FI.

El ejemplo 26 puede incluir el tema de cualquiera de los ejemplos 21-25 o cualquier otro ejemplo en la presente memoria, en el que los primeros datos cifrados se obtienen de un dispositivo de red de acceso público (por ejemplo, un dispositivo con acceso a Internet), y en el que los segundos datos se obtienen de un dispositivo de red privada diferente (por ejemplo, no accesible a Internet).

El ejemplo 27 puede incluir el tema de cualquiera de los ejemplos 21-26 o cualquier otro ejemplo en la presente memoria, en el que dicha conexión es más segura que una conexión a través de la cual se obtienen los primeros datos cifrados.

El ejemplo 28 puede incluir el tema de cualquiera de los ejemplos 21-27 o cualquier otro ejemplo en la presente memoria, en el que dicha segunda interfaz de entrada/salida tiene un ancho de banda mayor que la primera interfaz de entrada/salida.

El ejemplo 29 puede incluir el tema de cualquiera de los ejemplos 21-28 o cualquier otro ejemplo en la presente memoria, en el que el circuito se configura para recuperar dicha información mediante el uso de una primera clave pública de un par de claves pública/privada, la clave pública almacenada en el dispositivo electrónico, en el que dicha información incluye una segunda clave diferente que se puede usar para conectarse al recurso de red seguro.

El ejemplo 30 puede incluir el tema de cualquiera de los ejemplos 21-29 o cualquier otro ejemplo en la presente memoria, en el que dicha información comprende un identificador de conjunto de servicios (SSID) y una contraseña para un punto de acceso SSID (por ejemplo, un punto de acceso SSID oculto).

El ejemplo 31 puede incluir el tema de cualquiera de los ejemplos 21-30 o cualquier otro ejemplo en la presente memoria, en el que el dispositivo electrónico descubre al menos uno de los SSID o contraseña en respuesta a dicha recuperación de la información (por ejemplo, el descubrimiento de al menos uno de el SSID o la contraseña son previamente desconocidos para el dispositivo electrónico antes del tiempo de descifrado de los primeros datos cifrados).

El ejemplo 32 puede incluir el tema de cualquiera de los ejemplos 21-31 o cualquier otro ejemplo en la presente memoria, en el que el dispositivo electrónico descubre al menos una porción de dicha información en respuesta a dicha recuperación de la información (por ejemplo, la porción descubierta de dicha información es previamente desconocido para el dispositivo electrónico antes de un tiempo de descifrado de los primeros datos cifrados).

El ejemplo 33 puede incluir el tema de cualquiera de los ejemplos 21-32 o cualquier otro ejemplo en la presente memoria, en el que el circuito comprende un dispositivo informático de un vehículo de motor.

El ejemplo 34 puede incluir el tema de cualquiera de los ejemplos 21-33 o cualquier otro ejemplo en la presente memoria, en el que el circuito está configurado además para: monitorear una señal inalámbrica que corresponda a al menos uno de un transmisor externo al vehículo de motor o un sensor externo al vehículo de motor e incluye datos predeterminados o datos correspondientes a un evento predeterminado; en el que la determinación se realiza en respuesta a la detección de dicha señal inalámbrica.

El ejemplo 35 puede incluir el tema de cualquiera de los ejemplos 21-34 o cualquier otro ejemplo en la presente memoria, en el que el dispositivo electrónico está instalado en un equipo portátil (por ejemplo, un vehículo de motor) y la señal inalámbrica está asociada con una geovalla o dispositivo para detectar el equipo portátil cerca de una ubicación geográfica predeterminada.

El ejemplo 36 puede incluir el tema de cualquiera de los ejemplos 21-35 o cualquier otro ejemplo en la presente memoria, en el que el circuito está configurado además para: en respuesta a una verificación de no usar la primera interfaz de entrada/salida para obtener información que se puede usar para autenticar la electrónica dispositivo con el recurso de red seguro, identificando dicha información desde un dispositivo de memoria de un vehículo de motor.

El ejemplo 37 puede incluir el tema de cualquiera de los ejemplos 21-36 o cualquier otro ejemplo en la presente memoria, en el que dicha información comprende una lista de canales de comunicación seguros conocidos.

El ejemplo 38 puede incluir el tema de cualquiera de los ejemplos 21-37 o cualquier otro ejemplo en la presente memoria, en el que la información se identifica de la memoria protegida.

El ejemplo 39 puede incluir el tema de cualquiera de los ejemplos 21-38 o cualquier otro ejemplo en la presente memoria, en el que se confirma que el circuito obtiene un horario de un dispositivo remoto, y la verificación es en respuesta a un reloj y/o contador que alcanza un valor correspondiente al horario.

El ejemplo 40 puede incluir el tema de cualquiera de los ejemplos 21-39 o cualquier otro ejemplo en la presente memoria, en el que la señal inalámbrica se recibe a través de al menos una de la primera interfaz de entrada/salida, la segunda interfaz de entrada/salida o una tercera interfaces entrada/salida diferentes del dispositivo electrónico.

El ejemplo 41 puede incluir el tema de cualquiera de los ejemplos 21-40 o cualquier otro ejemplo en la presente memoria, en el que la primera información cifrada se obtiene de una puerta de enlace de red pública (por ejemplo, reenviada por la puerta de enlace de red pública), y en el que se obtienen los segundos datos independientemente de las puertas de enlace de la red (por ejemplo, directamente desde un punto de acceso que no funciona como una puerta de enlace de red pública).

El ejemplo 42 puede incluir el tema de cualquiera de los ejemplos 21-41 o cualquier otro ejemplo en la presente memoria, en el que la conexión se establece (por ejemplo, directamente a) un punto de acceso inalámbrico portátil.

El ejemplo 43 puede incluir el tema de cualquiera de los ejemplos 21-42 o cualquier otro ejemplo en la presente memoria, en el que la primera interfaz de entrada/salida comprende al menos uno de un transceptor celular, un transceptor inalámbrico de corto alcance (por ejemplo, un transceptor Bluetooth), o transceptor de Comunicación de campo cercano (NFC).

El ejemplo 44 puede incluir el tema de cualquiera de los ejemplos 21-43 o cualquier otro ejemplo en la presente memoria, en el que cada una de las primeras y segundas entradas/interfaces comprende una interfaz inalámbrica distinta.

El ejemplo 45 puede incluir el tema de cualquiera de los ejemplos 21-44 o cualquier otro ejemplo en la presente memoria, en el que establecer la conexión comprende además la tunelización al recurso de red segura en base a dicha información.

El ejemplo 46 puede incluir el tema de cualquiera de los ejemplos 21-45 o cualquier otro ejemplo en la presente memoria, en el que el circuito funciona en un vehículo desatendido.

El ejemplo 47 puede incluir el tema de cualquiera de los ejemplos 21-46 o cualquier otro ejemplo en la presente memoria, en el que los segundos datos comprenden un software de vehículo de motor (por ejemplo, una actualización de software de vehículo de motor y/o microprograma de vehículo de motor).

El ejemplo 48 es un vehículo de motor, que comprende: circuitos para identificar un canal seguro correspondiente a un primer recurso de red, los circuitos configurados para: determinar si comunicarse a través de un canal no seguro para obtener información de un segundo recurso de red diferente, la información que se puede usar para autenticar un componente del vehículo de motor con el recurso de red seguro; en respuesta a una comprobación para comunicarse a través del canal no seguro, obtener los primeros datos cifrados del segundo recurso de red y recuperar, a partir de los datos cifrados, dicha información; y establecer una conexión a través del canal seguro al primer recurso de red mediante el uso de dicha información; y descargar o cargar los segundos datos que sean diferentes a los primeros datos cifrados a través de la conexión.

El ejemplo 49 puede incluir el tema del ejemplo 48, en el que el segundo recurso de red comprende un servidor remoto.

El ejemplo 50 puede incluir el tema de cualquiera de los ejemplos 48-49 o cualquier otro ejemplo en la presente memoria, el circuito configurado para realizar la verificación a un tiempo programado o monitorear una señal inalámbrica que corresponda a al menos uno de un transmisor externo al vehículo motor o un sensor externo al vehículo de motor e incluye datos predeterminados o datos correspondientes a un evento predeterminado; en el que la determinación se realiza en respuesta al tiempo programado o la detección de dicha señal inalámbrica.

El ejemplo 51 puede incluir el tema de cualquiera de los ejemplos 48-50 o cualquier otro ejemplo en la presente memoria, en el que la señal inalámbrica está asociada con una geovalla o dispositivo para detectar el vehículo de motor cerca de una ubicación geográfica predeterminada.

El ejemplo 52 puede incluir el tema de cualquiera de los ejemplos 48-51 o cualquier otro ejemplo en la presente memoria, en el que el circuito está configurado además para: en respuesta a una verificación para no usar el canal no seguro para obtener dicha información, identificando dicha información de un dispositivo de memoria acoplado al vehículo de motor o un dispositivo de memoria del vehículo de motor.

El ejemplo 53 puede incluir el tema de cualquiera de los ejemplos 48-52 o cualquier otro ejemplo en la presente memoria, en el que dicha información comprende una lista de uno o más canales de comunicación seguros.

El ejemplo 54 puede incluir el tema de cualquiera de los ejemplos 48-53 o cualquier otro ejemplo en la presente memoria, en el que el circuito se configura para descubrir una lista de uno o más canales de comunicación seguros que responden al descifrado de dichos primeros datos cifrados.

El ejemplo 55 puede incluir un procedimiento para identificar un canal seguro correspondiente a un primer recurso de red, comprendiendo el procedimiento: determinar si comunicarse a través de un canal no seguro para obtener

información de un segundo recurso de red diferente, la información que se puede usar para autenticar un componente del vehículo de motor con el recurso de red seguro; en respuesta a una verificación para comunicarse por el canal no seguro, obtener los primeros datos cifrados del segundo recurso de red y recuperar, a partir de los datos cifrados, dicha información; y establecer una conexión a través del canal seguro al primer recurso de red mediante el uso de dicha información; y descargar o cargar los segundos datos que son diferentes a los primeros datos cifrados a través de la conexión.

La mayor parte del equipo discutido anteriormente comprende hardware y software asociado. Por ejemplo, es probable que el dispositivo remoto y/o en el vehículo típico incluya uno o más procesadores y software ejecutable en esos procesadores para llevar a cabo las operaciones descritas. Usamos el término software en la presente memoria en su sentido comúnmente entendido para referirnos a programas o rutinas (subrutinas, objetos, complementos, etc.), así como también a datos, que se puede usar por una máquina o procesador. Como es bien sabido, los programas de ordenador generalmente comprenden instrucciones que se almacenan en medios de almacenamiento legibles por máquina o legibles por ordenador. Algunas realizaciones de la presente invención pueden incluir programas ejecutables o instrucciones que se almacenan en medios de almacenamiento legibles por máquina o por ordenador, como una memoria digital. No implicamos que se requiera un "ordenador" en el sentido convencional en ninguna realización particular. Por ejemplo, pueden usarse varios procesadores, integrados o de cualquier otra manera, en equipos tales como los componentes descritos en la presente memoria.

La memoria para almacenar software nuevamente es bien conocida. En algunas realizaciones, la memoria asociada con un procesador dado puede almacenarse en el mismo dispositivo físico que el procesador (memoria "incorporada"); por ejemplo, memoria RAM o FLASH dispuesta dentro de un microprocesador de circuito integrado o similar. En otros ejemplos, la memoria comprende un dispositivo independiente, como una unidad de disco externa, una serie de almacenamiento o un llavero FLASH portátil. En tales casos, la memoria se "asocia" con el procesador digital cuando los dos están acoplados operativamente entre sí, o en comunicación entre sí, por ejemplo mediante un puerto de E/S, conexión de red, etc., de manera que el procesador pueda leer un archivo almacenado en la memoria. La memoria asociada puede ser de "solo lectura" por diseño (ROM) o en virtud de la configuración de permisos, o no. Otros ejemplos incluyen, entre otros, WORM, EPROM, EEPROM, FLASH, etc. Estas tecnologías a menudo se implementan en dispositivos semiconductores de estado sólido. Otras memorias pueden comprender partes móviles, como una unidad de disco giratoria convencional. Todas estas memorias son "legibles por máquina" o "legibles por ordenador" y pueden usarse para almacenar instrucciones ejecutables para implementar las funciones descritas en la presente memoria.

Un "producto de software" se refiere a un dispositivo de memoria en el que una serie de instrucciones ejecutables se almacenan en un formato legible por máquina para que una máquina o procesador adecuado, con acceso apropiado al producto de software, pueda ejecutar las instrucciones para llevar a cabo un procedimiento implementado por las instrucciones. En ocasiones, los productos de software se usan para distribuir software. Cualquier tipo de memoria legible por máquina, incluidas, entre otras, las resumidas anteriormente, puede usarse para fabricar un producto de software. Dicho esto, también se sabe que el software se puede distribuir mediante transmisión electrónica ("descarga"), en cuyo caso típicamente habrá un producto de software correspondiente en el extremo de transmisión de la transmisión, o en el extremo receptor, o ambos.

Habiendo descrito e ilustrado los principios de la invención en una realización preferente de la misma, debería ser evidente que la invención puede modificarse en disposición y detalle sin apartarse de tales principios. El ámbito de la protección está definido por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un dispositivo electrónico en un vehículo (1) para operar en un vehículo de motor en un estado de energía desatendido, comprendiendo el dispositivo electrónico en el vehículo:

una interfaz inalámbrica (7) para comunicarse de forma segura con un recurso de red remoto (25); y
una memoria (11) para almacenar uno o más valores para especificar un evento de activación predefinido (14) para acoplar el vehículo de motor en el estado de energía desatendido al recurso de red remoto;
un procesador (12) configurado para:

identificar un recurso a monitorear;
reconocer una ocurrencia del evento de activación predefinido verificando los primeros datos obtenidos en respuesta a la monitorización del recurso identificado contra el uno o más valores;
en respuesta a un reconocimiento de la ocurrencia de un evento de activación predefinido, identificar los segundos datos adecuados para acoplar el dispositivo electrónico en el vehículo al recurso de red remoto;
establecer un canal de comunicación (15) al recurso de red remoto a través de la interfaz inalámbrica mediante el uso de los segundos datos; y
descargar los terceros datos a través del canal de comunicación al vehículo de motor en el estado de energía desatendido o cargar los terceros datos a través del canal de comunicación desde el vehículo de motor en el estado de energía desatendido.

2. El dispositivo electrónico en un vehículo según la reivindicación 1, en el que los primeros datos comprenden el contenido de una señal recibida a través de un canal de comunicación establecido independientemente del recurso de red remoto, o
la información indicativa de que el vehículo de motor se ha movido dentro de una proximidad predefinida de una referencia, por ejemplo, una referencia que comprende una geovalla.

3. El dispositivo electrónico en un vehículo según la reivindicación 2, en el que uno de los canales de comunicación se establece mediante el uso de un primer receptor de la interfaz inalámbrica o un transmisor que corresponde al primer receptor y el otro de los canales de comunicación se establece mediante el uso de un segundo receptor diferente de la interfaz inalámbrica.

4. El dispositivo electrónico en un vehículo según la reivindicación 3, en el que el primer receptor incluye un receptor de un transceptor Wi-Fi y el segundo receptor incluye un receptor de al menos uno de entre un transceptor celular o un transceptor inalámbrico de corto alcance.

5. El dispositivo electrónico en un vehículo según la reivindicación 3, en el que los primeros datos comprenden información de conexión para establecer una conexión sobre la cual se extiende el canal de comunicación, en el que opcionalmente la información de conexión comprende un identificador de conjunto de servicios (SSID) y un valor de tipo de seguridad o una contraseña.

6. El dispositivo electrónico en un vehículo según la reivindicación 1, en el que el evento de activación predeterminado comprende un tiempo programado.

7. El dispositivo electrónico en un vehículo según la reivindicación 1, en el que los segundos datos comprenden datos de conexión residentes en una memoria electrónica del vehículo de motor antes de que ocurra el evento predefinido.

8. El dispositivo electrónico en un vehículo según la reivindicación 1, en el que los terceros datos comprenden una actualización para ser descargada en el vehículo de motor.

9. El dispositivo electrónico en un vehículo según la reivindicación 1, en el que el recurso de red comprende un punto de acceso Wi-Fi seguro.

10. El dispositivo electrónico en un vehículo según la reivindicación 1, en el que el recurso identificado comprende un recurso en el vehículo, o es un dispositivo correspondiente a una geovalla u otro dispositivo remoto separado del vehículo de motor.

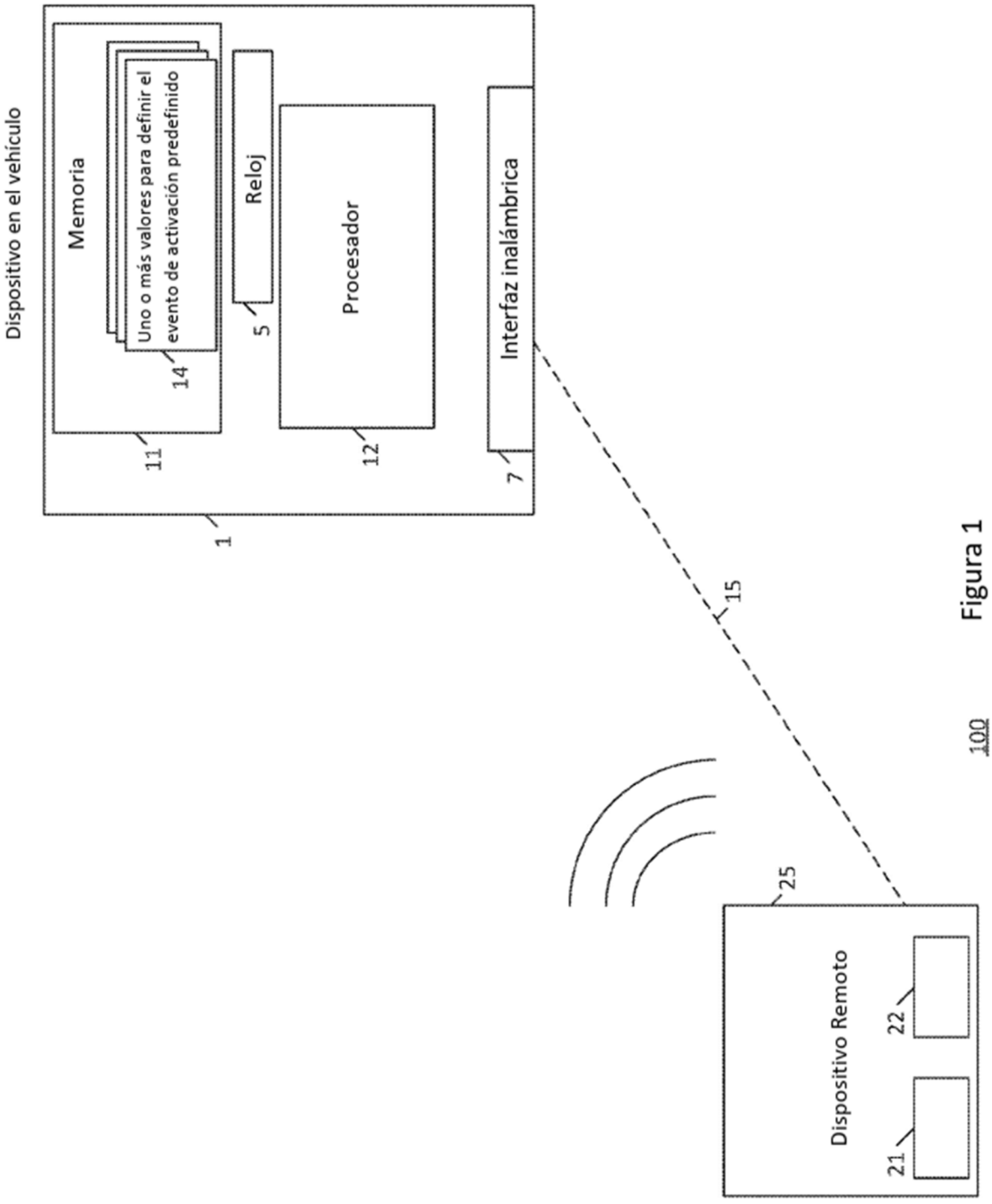

Dispositivo en el vehículo
Memoria
Uno o más valores para definir el evento de activación predefinido
Reloj
Procesador
Interfaz inalámbrica
1
11
14
5
12
7
15
25
Dispositivo Remoto
21
22
100

Figura 1

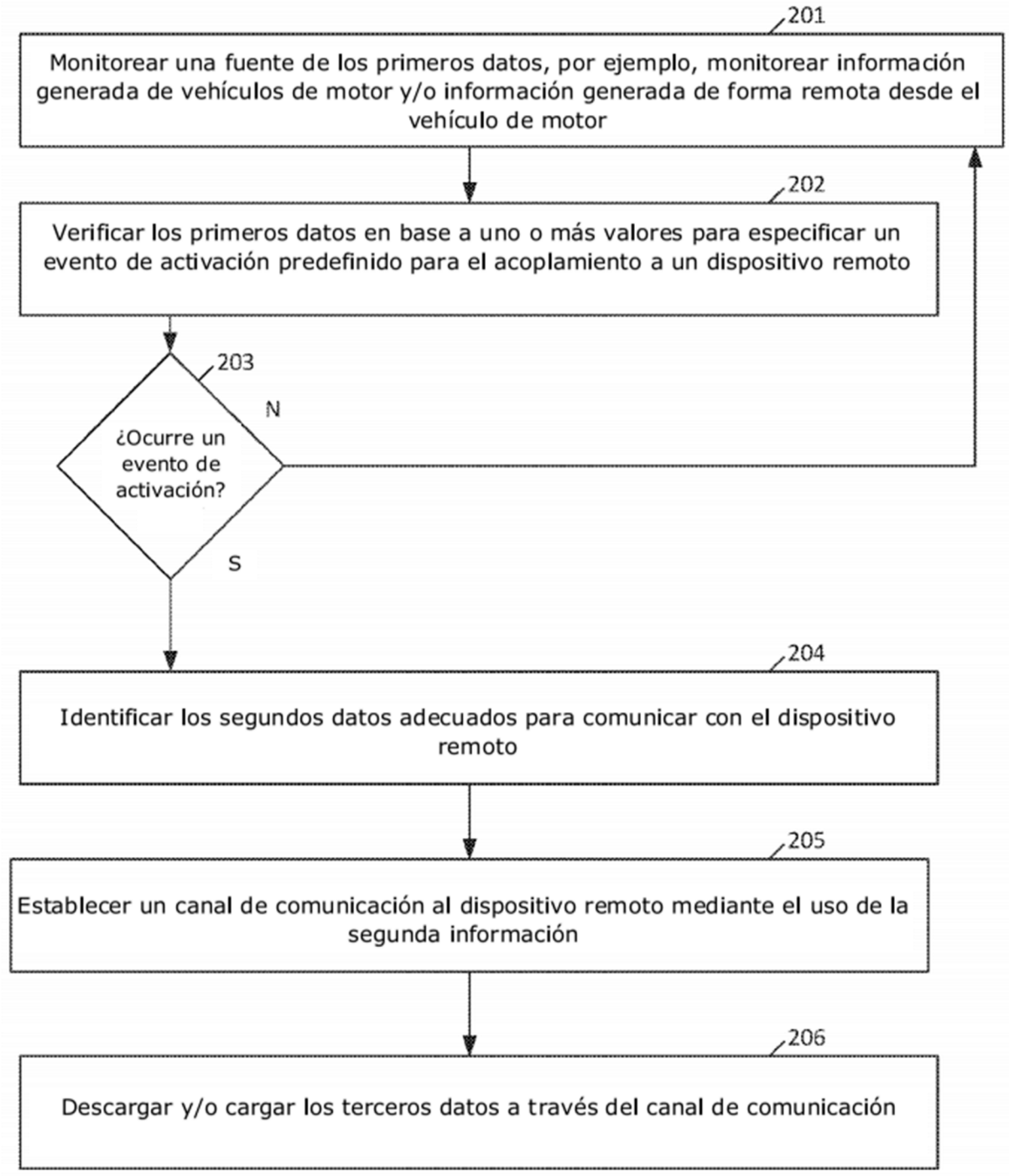
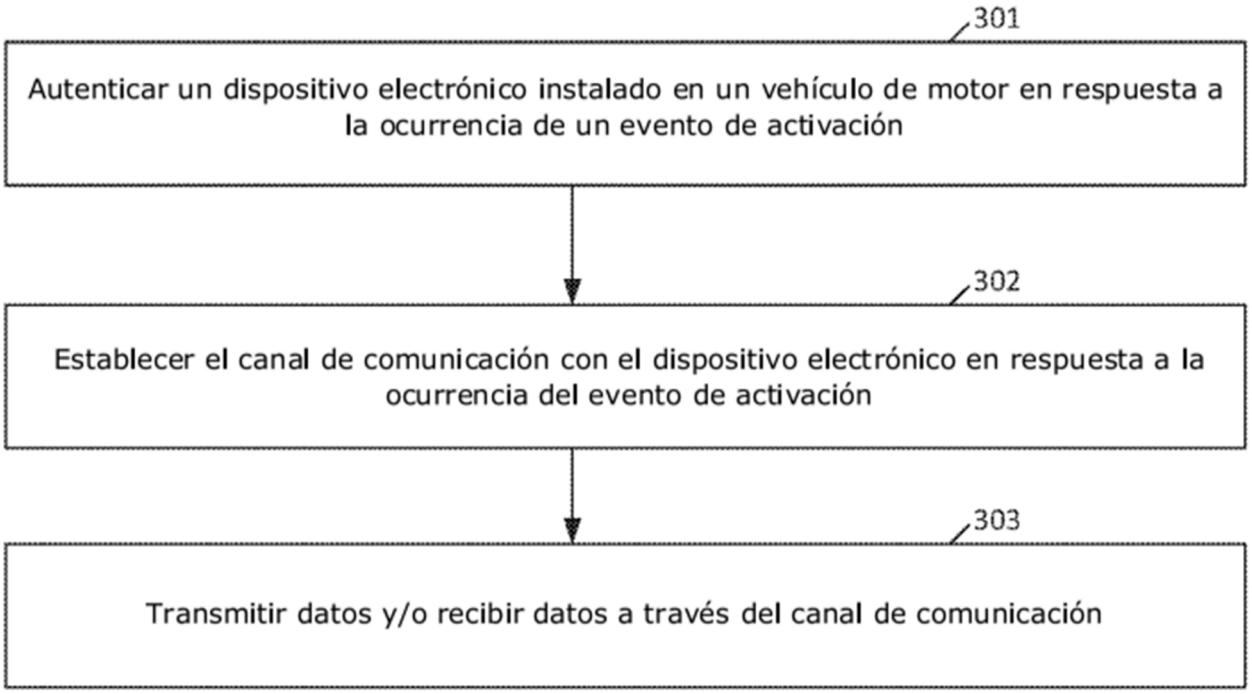

201
Monitorear una fuente de los primeros datos, por ejemplo, monitorear información generada de vehículos de motor y/o información generada de forma remota desde el vehículo de motor
202
Verificar los primeros datos en base a uno o más valores para especificar un evento de activación predefinido para el acoplamiento a un dispositivo remoto
203
¿Ocurre un evento de activación?
N
S
204
Identificar los segundos datos adecuados para comunicar con el dispositivo remoto
205
Establecer un canal de comunicación al dispositivo remoto mediante el uso de la segunda información
206
Descargar y/o cargar los terceros datos a través del canal de comunicación
200

Figura 2


301
Autenticar un dispositivo electrónico instalado en un vehículo de motor en respuesta a la ocurrencia de un evento de activación
302
Establecer el canal de comunicación con el dispositivo electrónico en respuesta a la ocurrencia del evento de activación
303
Transmitir datos y/o recibir datos a través del canal de comunicación

300

Figura 3

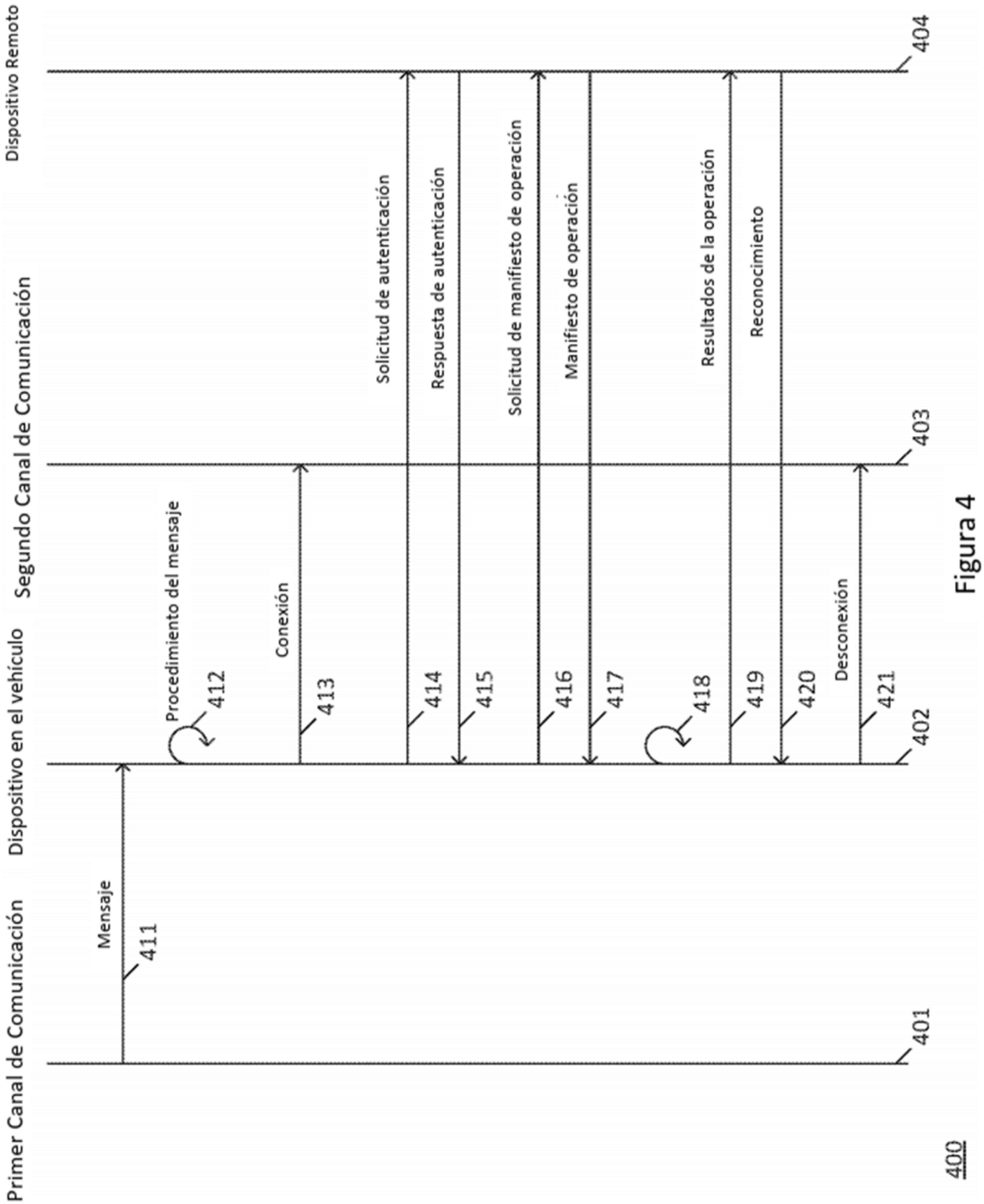

Primer Canal de Comunicación
Dispositivo en el vehículo
Segundo Canal de Comunicación
Dispositivo Remoto
401
402
403
404
Mensaje
411
Procedimiento del mensaje
412
Conexión
413
Solicitud de autenticación
414
Respuesta de autenticación
415
Solicitud de manifiesto de operación
416
Manifiesto de operación
417
Resultados de la operación
418
Reconocimiento
419
420
Desconexión
421
400

Figura 4