

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 441 815**

51 Int. Cl.:

G07B 15/06

(2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **06.08.2010 E 10450129 (1)**

97 Fecha y número de publicación de la concesión europea: **16.10.2013 EP 2423885**

54 Título: **Dispositivo y método para monitorizar el funcionamiento de un sistema de peaje viario**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
06.02.2014

73 Titular/es:

**KAPSCH TRAFFICCOM AG (100.0%)
Am Europlatz 2
1120 Wien, AT**

72 Inventor/es:

**TIJINK, JASJA;
NAGY, OLIVER y
KERSTEN, JAN**

74 Agente/Representante:

ZEA CHECA, Bernabé

ES 2 441 815 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Dispositivo y método para monitorizar el funcionamiento de un sistema de peaje viario

- 5 La presente invención se refiere a un dispositivo y un método para monitorizar el funcionamiento de un sistema de peaje viario que comprende al menos una unidad de a bordo que graba su posición en forma de datos de posición brutos y un ordenador proxy estacionario que recibe los datos de posición brutos de la unidad de a bordo y sobre esta base genera datos de peaje cotejados con mapas mediante el cotejo de mapas de peaje.
- 10 Los sistemas de peaje viario de este tipo son conocidos, por ejemplo, de los documentos EP2017790 o WO2009/001303 y se identifican también como sistemas “thin client” (cliente liviano). La unidad de a bordo, denominado también Onboard Unit u OBU (unidad de a bordo), puede tener un diseño económico con una pequeña capacidad de cálculo (“thin client”), porque el cotejo de mapas de peaje altamente computacional, es decir, el cotejo de los datos de posición con elementos geográficos relevantes para el cobro del peaje, por ejemplo, sobre un mapa de carretera digital preparado de manera correspondiente o adecuado, se ha trasladado a ordenadores proxy estacionarios eficientes del sistema de peaje viario. En este caso, los OBUs thin client determinan su posición, por ejemplo, con ayuda de la navegación por satélite o la radiolocalización en redes de radiobaliza o redes móviles de comunicaciones terrestres.
- 15
- 20 A pesar de que los sistemas de peaje thin client aportan ventajas considerables al usuario individual como resultado de los bajos costes de un OBU thin client, para el operador del sistema de peaje viario tienen la desventaja de no posibilitar una comprobación continua y segura del funcionamiento (“secure monitoring”). Así, por ejemplo, el operador de peaje no puede verificar la fiabilidad del cotejo de mapas de peaje en el ordenador proxy y, por tanto, a los suministradores de sistemas también les resulta difícil o imposible su comprobación.
- 25 Este tipo de monitorización del funcionamiento es posible, por el contrario, en los llamados sistemas de peaje “thick client” (cliente pesado). En estos sistemas de peaje se usan costosos OBUs thick client que disponen de sus propios mapas de peaje y de una alta capacidad de cálculo para ejecutar por sí mismos el cotejo de mapas de peaje y transmitir los datos de peaje cotejados con mapas a un sistema central. En relación con tales sistemas son conocidas distintas consideraciones de diseño que consisten en proveer a los datos de peaje, calculados por los OBUs thick client, de una firma emitida por el operador de peaje e instalada en el OBU a fin de garantizar la autenticidad de los datos respecto al sistema central del operador de peaje. Esta solución requiere el uso de OBUs con una alta capacidad de cálculo, que puedan ejecutar las funciones de autenticación exigidas por el operador de peaje, y no es adecuada para sistemas thin client convencionales.
- 30
- 35 La invención tiene el objetivo de crear una solución para la monitorización segura (secure monitoring) de sistemas de peaje viario thin client que combine las ventajas de seguridad del operador de sistemas thick client firmantes con las ventajas de costes de los sistemas thin client.
- 40 Este objetivo se consigue en un primer aspecto de la invención mediante un dispositivo con las características de la reivindicación 1.
- La invención crea así por primera vez una solución de certificación continua para datos de peaje generados por OBUs thin client. Un elemento de procesador, que está equipado con un elemento de datos y tiene un acceso protegido criptográficamente, representa para el operador de peaje un elemento confiable (“trusted element”) que se puede equipar con un elemento de datos de una autoridad expedidora confiable y proteger para su acceso exclusivo. Este tipo de elementos de procesador se puede fabricar de manera económica como módulos de un solo chip (single-chip) como los usados a gran escala en tarjetas SIM, tarjetas chip, etc. A diferencia del cotejo de mapas en el OBU, que es necesario en el caso de OBUs thick client, la comprobación de la plausibilidad, según la invención, de los datos de peaje cotejados con mapas respecto a los datos de posición o trayecto requiere sólo una pequeña capacidad de cálculo del elemento confiable (“trusted element”), como la que puede ser proporcionada sin problemas por elementos de procesador comerciales de tarjetas SIM o tarjetas chip.
- 45
- 50 Por el término “comparar de manera evaluativa” o “comprobar la plausibilidad” se entiende en la presente descripción una comprobación a grosso modo o una comparación aproximada de si los datos de peaje creados por el ordenador proxy pueden proceder de los datos de posición o de los datos de trayecto extraídos de los mismos, es decir, si son plausibles. Así, por ejemplo, se puede comprobar la plausibilidad de los datos de peaje de la zona al comprobarse si los datos de posición considerados se encuentran en la zona de los datos de peaje. Si los datos de peaje se basan en una distancia recorrida o en la duración del recorrido, la plausibilidad se puede comprobar, por ejemplo, con ayuda de una acumulación aproximada de las distancias situadas entre posiciones individuales de los datos de posición.
- 55
- 60

En una primera realización preferida de la invención, el primer elemento de procesador está dispuesto en el ordenador proxy del operador de peaje. De esta manera, el elemento de procesador puede estar directamente bajo el control del operador (o de un tercero de confianza) y puede presentar también un diseño en correspondencia específicamente con el operador.

5 Una realización alternativa preferida de la invención para un sistema de peaje viario, cuyo ordenador proxy reenvía los datos de peaje cotejados con mapas a la unidad de a bordo, se caracteriza porque el primer elemento de procesador está dispuesto en la unidad de a bordo. Esta solución tiene la ventaja de que el elemento de procesador puede cooperar con distintos ordenadores proxy de operadores de peaje diferentes. Además, los datos de peaje
10 suministrados por un OBU thin client están certificados así de la misma manera que los datos obtenibles de un OBU thick client certificado convencional.

15 Resulta particularmente favorable que el primer elemento de procesador esté insertado de manera sustituible en forma de módulo en la unidad de a bordo, por ejemplo, como una tarjeta SIM. Esto permite que el operador equipe los OBUs thin client, fabricados por terceros suministradores, con elementos de procesador de su confianza.

20 Como ya se explicó, el elemento de procesador puede cotejar los datos de posición brutos o los datos de trayecto extraídos de los mismos con los datos de peaje. Se usan preferentemente los datos de trayecto extraídos de los datos de posición, es decir, la unidad de a bordo está configurada para extraer datos de trayecto de los datos de posición brutos y enviarlos al primer elemento de procesador que compara de manera evaluativa los datos de peaje cotejados con mapas respecto a los datos de trayecto extraídos. Esto representa un incremento de la confidencialidad ("privacy"): El elemento de procesador, usado por el operador de peaje para la certificación, no conoce los datos de posición brutos del OBU ("position fix track"), sino sólo extractos o aspectos generales de los mismos, lo que protege el historial de movimiento del usuario contra un uso indebido de los datos.

25 Con este fin, los datos de trayecto extraídos son preferentemente las distancias recorridas o las duraciones del recorrido, acumuladas a partir de los datos de posición brutos, que no permiten deducir directamente los movimientos individuales del usuario con su unidad de a bordo.

30 Otra realización preferida de la invención presenta las características de la reivindicación 7 si se usan estos datos de trayecto.

35 Con preferencia, el segundo elemento de procesador está insertado también de manera sustituible en forma de módulo en la unidad de a bordo y con particular preferencia, el primer y el segundo elemento de procesador pueden ser incluso idénticos.

40 Otra realización de la invención particularmente ventajosa se caracteriza porque la unidad de a bordo está configurada para poner a disposición de una interfaz los datos de trayecto extraídos, que están firmados con el elemento de datos, a fin de que sean consultados por una infraestructura situada del lado de la carretera. De esta manera, el elemento de procesador o "trusted element" posibilita simultáneamente también un "secure freezing service" (servicio seguro de congelación) para los datos de posición generados continuamente en la unidad de a bordo o los datos de trayecto extraídos de los mismos. La infraestructura situada del lado de la carretera, como las balizas de peaje, los vehículos de control, etc., puede obtener así datos de control de confianza ("trusted") de los aparatos de vehículo que pasan.

45 En un segundo aspecto, la invención crea un método para monitorizar el funcionamiento de un sistema de peaje viario con las características de la reivindicación 11.

50 Si el ordenador proxy reenvía los datos de peaje cotejados con mapas a la unidad de a bordo, la llamada comparación evaluativa se lleva a cabo preferentemente en un elemento de procesador de la unidad de a bordo.

55 Según otra característica de la invención, los datos de trayecto se extraen de los datos de posición brutos en la unidad de a bordo y los datos de peaje cotejados con mapas se comparan de manera evaluativa con los datos de trayecto extraídos en el elemento de procesador.

A este respecto, los datos de trayecto extraídos son preferentemente distancias recorridas o duraciones del recorrido que se acumulan a partir de los datos de posición.

60 Resulta particularmente favorable que el método presente las características de la reivindicación 15.

Con preferencia, los datos de trayecto extraídos, que están firmados con el elemento de datos, se ponen a disposición en la unidad de a bordo a fin de que sean consultados por una infraestructura situada del lado de la carretera.

En relación con otras características y ventajas del método según la invención se remite a las explicaciones anteriores sobre el dispositivo según la invención.

5 La invención se explica detalladamente a continuación por medio de ejemplos de realización representados en los dibujos adjuntos. En los dibujos muestran:

Fig. 1 un esquema de bloques de un primer dispositivo de la invención, en el que están representados simultáneamente los flujos de datos del método según la invención; y

10 Fig. 2 un esquema de bloques de una segunda realización del dispositivo de la invención que muestra simultáneamente los flujos de datos de una segunda realización del método según la invención.

15 La figura 1 muestra un dispositivo y un método para monitorizar con seguridad el funcionamiento ("secure monitoring") en el marco de un sistema de peaje viario 1 representado esquemáticamente. El sistema de peaje viario 1 comprende una pluralidad de aparatos de vehículo u OBU 2 (se muestra sólo un OBU de manera representativa) en forma de "thin clients" que de un modo conocido determinan continuamente su propia posición geográfica, por ejemplo, con ayuda de la navegación por satélite o la radiolocalización en una red de radiobalizas, estaciones móviles de comunicaciones, etc. Las posiciones ("position fixes"), determinadas por un OBU 2, se graban como datos de posición "brutos" ("position fix tracks") 3 en una memoria del OBU. Los datos de posición 3 se pueden complementar o mejorar mediante la combinación de los datos de sensor de los distintos sensores del vehículo, en el que está montado el OBU 2, por ejemplo, los datos de medición del tacómetro, de la brújula o de la aceleración, como es conocido por el técnico.

25 Los OBU 2 pueden estar conectados mediante una interfaz de radio 4, por ejemplo, según el estándar DSRC (Dedicated Short Range Communication, comunicación dedicada de corto alcance), a una infraestructura 5 situada del lado de la carretera (Roadside Equipment, RSE), por ejemplo, radiobalizas DSRC, puntos de acceso WLAN (Wireless Local Area Network, red de área local inalámbrica), estaciones de base WAVE (Wireless Access in a Vehicle Environment, conexión inalámbrica en entorno vehicular), etc., por la que pasan durante su recorrido y a la que pueden enviar una copia de los datos de posición 3 con fines de control.

30 Los OBU 2 están conectados también mediante la misma interfaz de radio 4 o mediante otra interfaz de radio 6, por ejemplo, una conexión de datos en una red móvil de comunicaciones, con (al menos) un ordenador proxy 7 del sistema de peaje viario 1, al que transmiten sus datos de posición 3 de manera continua o por lotes, por ejemplo, periódicamente o en caso necesario. El ordenador proxy 7 dispone de una alta capacidad de cálculo, por ejemplo, en forma de "server farm" (granja de servidores), y de una gran cantidad de mapas terrestres o mapas de peaje para ejecutar un cotejo de mapas ("map matching") entre los datos de posición brutos 3, por una parte, y las posiciones geográficas predefinidas, como el trazado de carreteras, los puntos de cobro de peaje virtuales, etc. Este cotejo de mapas de peajes mejora la exactitud de la determinación de posición del OBU 2, porque las determinaciones de posiciones dispersas o diferentes (position fixes) se pueden asignar respectivamente a posiciones correctas en una red de carreteras. Así, por ejemplo, la exactitud de los datos de posición brutos 3 respecto a la distancia recorrida ("driven distance") durante la determinación convencional por GPS podría ser aproximadamente de $\pm 5\%$, mientras que después de ejecutarse el cotejo de mapas en el ordenador proxy 7 podría presentar una exactitud de $\pm 1\%$.

45 Los datos de posición mejorados, que se cotejaron de esta manera con mapas, se usan en el ordenador proxy 7 como base para los datos de peaje 8 cotejados con mapas. Por lo general, estos datos de peaje no permiten sacar conclusiones individuales sobre las posiciones individuales de los datos de posición 3, ya que en función del principio o de la realización del sistema de peaje representan una evaluación resumida o abstracta y "anonimizada respecto a la ubicación" de estas posiciones individuales, por ejemplo, en forma de los tramos transitados de una red de carreteras o de la distancia recorrida ("driven distance") o de la duración del recorrido. Estos últimos se pueden usar, por ejemplo, para aplicar el cobro de tasas en función de la vía a carreteras de peaje ("pay as you drive") o aplicar el cobro de tasas en función del tiempo a aparcamientos sujetos a tasas, etc. Los datos de peaje 8 cotejados con mapas se pueden proveer opcionalmente de tales informaciones de tasas de peaje en el ordenador proxy 7.

55 El ordenador proxy 7 reenvía los datos de peaje 8 cotejados con mapas y anonimizados respecto a la ubicación al OBU 2 en la realización de la figura 1, véase flecha 8'. Como es conocido por el técnico, esto permite garantizar el anonimato ("privacy") de los datos de posición sensibles 3 y, por tanto, el recorrido del vehículo, si el OBU 2 se identifica con un identificador temporal anónimo respecto al ordenador proxy 7 para el cotejo de datos de peaje.

60 Los dispositivos y métodos siguientes se usan para permitir la verificación del funcionamiento de esta operación por parte de un operador de peaje que necesita los datos de peaje 8 a fin de aplicar el cobro de tasas y para poder garantizarle al mismo la funcionalidad del sistema.

El OBU 2 realiza, independientemente del ordenador proxy 7, sin el cotejo de mapas de peaje y sólo con medios de cálculo simples, a saber, con preferencia mediante un elemento de procesador 13 descrito en detalle más adelante,

una evaluación aproximada de los datos de peaje que se identifica a continuación como datos de trayecto 9 extraídos de los datos de posición 3. Los datos de trayecto 9 se usan para poder comprobar la plausibilidad de los datos de peaje 8 generados por el ordenador proxy 7. Por consiguiente, los datos de trayecto se pueden comparar con los datos de peaje 8, aunque de manera mucho menos exacta, porque se basan en los datos de posición brutos 3 no mejorados. Si los datos de peaje 8 representan, por ejemplo, la distancia recorrida (“driven distance”) o la duración del recorrido, entonces los datos de trayecto 9, extraídos de los datos de posición 3 por el OBU 2, representan asimismo una distancia recorrida o duración del recorrido calculada a partir de los mismos. En el ejemplo, mencionado antes, de los datos de posición 3 determinados por GPS y los datos de peaje 8 cotejados con mapas de peaje, la exactitud de los datos de trayecto 9 es, por ejemplo, de $\pm 5\%$ y la exactitud de los datos de peaje 8 es, por ejemplo, de $\pm 1\%$.

Por tanto, los datos de peaje 8 no se pueden comparar directamente con los datos de trayecto 9 debido a estas diferencias de exactitud, pero sí se puede comprobar su plausibilidad respecto a los mismos, es decir, se puede comprobar si los datos de peaje 8 son plausibles sobre la base de los datos de trayecto 9.

A tal efecto, en el OBU 2 está previsto un elemento de procesador 10 protegido de manera especial que puede ser insertado, por ejemplo, por el propio operador de peaje en el OBU 2, por ejemplo, en forma de una tarjeta SIM o chip. El acceso al elemento de procesador 10 está protegido criptográficamente a nivel de hardware, de modo que, por ejemplo, sólo el operador de peaje tiene acceso a los datos y programas contenidos aquí. El elemento de procesador 10 representa así un elemento confiable (“trusted element”) para el operador de peaje y cumple de manera similar los altos requisitos de seguridad, como los que deben cumplir, por ejemplo, los procesadores de un solo chip (single chip) integrados en tarjetas SIM, tarjetas de crédito, tarjetas bancarias, etc.

El elemento de procesador 10 con acceso protegido criptográficamente está provisto además de manera conocida de una firma criptográfica 10', por ejemplo, un certificado criptográfico, es decir, un elemento de datos criptográfico 10' que el elemento de procesador 10 puede añadir a todas sus salidas de datos para poder demostrar su autenticidad respecto a la autoridad expedidora de la firma o del certificado, por ejemplo, el operador de peaje.

En el elemento de procesador 10 se ejecuta la comparación de plausibilidad descrita de los datos de peaje 8 con los datos de trayecto 9. Esta comparación de la plausibilidad no requiere una alta capacidad de cálculo, como ocurre en el caso del cotejo de mapas de peaje en el ordenador proxy 7, porque aquí es necesario ejecutar únicamente, por ejemplo, un cálculo evaluativo aproximado entre una distancia recorrida que aparece indicada de manera exacta en los datos de peaje 8 y de manera inexacta en los datos de trayecto 9. Por tanto, la comprobación de la plausibilidad en el elemento de procesador 10 se puede ejecutar con la capacidad de cálculo disponible en un procesador simple de un solo chip y de elemento confiable.

En caso de una comprobación de plausibilidad satisfactoria de los datos de peaje 8, el elemento de procesador 10 provee a estos datos de su firma 10' y les da salida como datos de peaje firmados 11, véase camino 11'. Los datos de peaje firmados 11 pueden ser reenviados por el elemento de procesador 10 del OBU 2, por ejemplo, nuevamente a través de la interfaz de radio 6, al ordenador proxy 7 y desde aquí pueden ser transmitidos a un ordenador central 12 del sistema de peaje viario 1, véase camino 11'. Alternativamente, estos pueden ser transmitidos también de manera directa por el OBU 2 al ordenador central 12, a saber, tanto “online”, por ejemplo, mediante la interfaz de radio 4 ó 6, como también “offline” mediante un soporte de datos.

El elemento de procesador 10 comprueba la plausibilidad y firma o certifica así en cada caso individual o continuamente por secciones los datos de peaje 8 que entran en un flujo constante.

En una realización alternativa simplificada, el OBU 2 podría prescindir de extraer los datos de trayecto 9 de los datos de posición 3 y los datos de posición 3 se podrían enviar directamente al elemento de procesador 10. En este caso, el elemento de procesador 10 comprueba la plausibilidad de los datos de peaje 8 directamente respecto a los datos de posición 3, teniendo que ejecutar el elemento de procesador 10 una cantidad creciente de pasos de cálculo o una comprobación de plausibilidad altamente simplificada. Así, por ejemplo, éste comprueba únicamente si posiciones individuales procedentes de los datos de posición 3 están comprendidas en un peaje por zonas indicado en los datos de peaje 8, etc.

En una realización preferida se prevé en el OBU 2 un segundo elemento de procesador (“trusted element”) 13 con acceso protegido criptográficamente para extraer los datos de trayecto 9 de los datos de posición 3. El elemento de procesador 13 está provisto de una firma propia 13', con la que provee (firma) los datos de trayecto 9 que ha generado.

Los datos de trayecto 9, firmados por el elemento de procesador 13, pueden ser puestos a disposición además en el OBU 2 para que sean consultados por la infraestructura 5 a través de la interfaz 4. El elemento de procesador (“trusted element”) 13 posibilita un “secure freezing service” para los datos de posición 3 o los datos de trayecto 9

ES 2 441 815 T3

extraídos de los mismos. La firma o la certificación de los datos de trayecto 9 garantiza respecto a la infraestructura 5 que los datos de trayecto 9 consultados a través de la interfaz 4 sean generados y firmados por un elemento de cálculo correspondientemente confiable, a saber, un elemento de procesador (“trusted element”) 13.

- 5 El primer y el segundo elemento de procesador 10, 13 de la figura 1 pueden ser también el mismo elemento de procesador físico. Esto no es posible en la realización de la figura 2 que se describe a continuación. Los números de referencia iguales de la figura 2 identifican los mismos elementos que en la figura 1 y sólo se analizan las diferencias en relación con la figura 1.
- 10 En la realización de la figura 2, el ordenador proxy 7 ya no reenvía los datos de peaje 8 cotejados con mapas al OBU 2. Por tanto, el primer elemento de procesador 10 está dispuesto en el ordenador proxy 7 o conectado al mismo, y el OBU 2 envía también, de manera adicional a los datos de posición 3, los datos de trayecto extraídos 9 al ordenador proxy 7, véase flecha 9'. Opcionalmente, los datos de trayecto 9 pueden haber sido generados de nuevo por el segundo elemento de procesador 13 dispuesto en el OBU 2 a partir de los datos de posición brutos 3 y pueden estar firmados con la firma 13', de modo que el ordenador proxy 7 o el primer elemento de procesador 10 puede estar seguro de que los datos de trayecto 9 se extrajeron correctamente en el OBU 2. En este caso también, los datos de trayecto firmados 9 pueden ser puestos a disposición nuevamente por el OBU 2 a través de la interfaz 4 para consultas de control.
- 15
- 20 El primer elemento de procesador 10 en el ordenador proxy 7 vuelve a comprobar la plausibilidad de los datos de peaje 8, cotejados con mapas en el ordenador proxy 7, respecto a los datos de trayecto 9 (firmados opcionalmente) y sin son plausibles, los provee de su firma 10' para dar salida a los datos de peaje firmados 11 (flecha 11").

REIVINDICACIONES

1. Dispositivo para monitorizar el funcionamiento de un sistema de peaje viario (1), que comprende al menos una unidad de a bordo (2) que graba su posición en forma de datos de posición brutos (3) y un ordenador proxy estacionario (7) que recibe los datos de posición brutos (3) de la unidad de a bordo (2) y sobre esta base genera datos de peaje (8) que están cotejados con mapas mediante la comparación con elementos geográficos relevantes para el cobro de peaje sobre un mapa de carreteras digital y que representan una evaluación resumida y anonimizada respecto a la ubicación de los datos de posición brutos (3), **caracterizado por** al menos un primer elemento de procesador (10) que tiene acceso protegido criptográficamente y está equipado con un elemento de datos criptográfico (10') y que recibe, por una parte, de la unidad de a bordo (2) los datos de posición brutos (3) o los datos de trayecto (9) extraídos de los mismos que son una estimación de los datos de peaje basada en los datos de posición brutos (3) y que recibe, por la otra parte, del ordenador proxy (7) los datos de peaje (8) cotejados con mapas y está configurado para comparar de manera evaluativa los datos de peaje (8) comparados con mapas respecto a los datos de posición brutos o los datos de trayecto (3, 9) extraídos de los mismos y para entregarlos firmados con su elemento de datos (10') en caso de una comparación evaluativa satisfactoria.
2. Dispositivo según la reivindicación 1, **caracterizado porque** el primer elemento de procesador (10) está dispuesto en el ordenador proxy (7).
3. Dispositivo según la reivindicación 1 para un sistema de peaje viario (1), cuyo ordenador proxy (7) reenvía los datos de peaje (8) cotejados con mapas a la unidad de a bordo (2), **caracterizado porque** el primer elemento de procesador (10) está dispuesto en la unidad de a bordo (2).
4. Dispositivo según la reivindicación 3, **caracterizado porque** el primer elemento de procesador (10) está insertado de manera sustituible en forma de módulo en la unidad de a bordo (2).
5. Dispositivo según una de las reivindicaciones 1 a 4, **caracterizado porque** la unidad de a bordo (2) está configurada para extraer los datos de trayecto (9) de los datos de posición brutos (3) y enviarlos al primer elemento de procesador (10) que compara de manera evaluativa los datos de peaje (8) cotejados con mapas respecto a los datos de trayecto extraídos (9).
6. Dispositivo según la reivindicación 5, **caracterizado porque** los datos de trayecto extraídos (9) son distancias recorridas o duraciones de recorrido acumuladas a partir de los datos de posición brutos (3).
7. Dispositivo según la reivindicación 5 ó 6, **caracterizado por** al menos un segundo elemento de procesador (13) que tiene acceso protegido criptográficamente y está equipado con un elemento de datos criptográfico (13'), así como dispuesto en la unidad de a bordo (2) y configurado para generar los datos de trayecto extraídos (9) a partir de los datos de posición brutos (3) y firmarlos con su elemento de datos (13').
8. Dispositivo según la reivindicación 7, **caracterizado porque** el segundo elemento de procesador está insertado de manera sustituible en forma de módulo en la unidad de a bordo.
9. Dispositivo según las reivindicaciones 3 y 7, **caracterizado porque** el primer y el segundo elemento de procesador (10, 13) son idénticos.
10. Dispositivo según una de las reivindicaciones 7 a 9, **caracterizado porque** la unidad de a bordo (12) está configurada para poner a disposición los datos de trayecto extraídos (9), que están firmados con el elemento de datos (13'), en una interfaz (4) para ser consultados por una infraestructura (5) situada del lado de la carretera.
11. Método para monitorizar el funcionamiento de un sistema de peaje viario (1), que comprende al menos una unidad de a bordo (2) que graba su posición en forma de datos de posición brutos (3) y un ordenador proxy estacionario (7) que recibe los datos de posición brutos (3) de la unidad de a bordo (2) y sobre esta base genera datos de peaje (8) que están cotejados con mapas mediante la comparación con elementos geográficos relevantes para el cobro de peaje sobre un mapa de carreteras digital y que representan una evaluación resumida y anonimizada respecto a la ubicación de los datos de posición brutos (3), **caracterizado porque** en un elemento de procesador (10), que tiene acceso protegido criptográficamente y está equipado con un elemento de datos criptográfico (10'), se comparan de manera estimada los datos de peaje (8), cotejados con mapas, del ordenador proxy (7) respecto a los datos de posición brutos (3) de la unidad de a bordo (2) o los datos de trayecto (9) extraídos de los mismos que son una estimación de los datos de peaje (8) basada en los datos de posición brutos (3) y se entregan firmados con el elemento de datos (10') en caso de una comparación evaluativa satisfactoria.

12. Método según la reivindicación 11 para un sistema de peaje viario (1), cuyo ordenador proxy (7) reenvía los datos de peaje (8) cotejados con mapas a la unidad de a bordo(2), **caracterizado porque** la comparación evaluativa mencionada se lleva a cabo en un elemento de procesador (10) de la unidad de a bordo (2).
- 5 13. Método según la reivindicación 11 ó 12, **caracterizado porque** los datos de trayecto (9) se extraen de los datos de posición brutos (3) en la unidad de a bordo(2) y los datos de peaje (8) cotejados con mapas se comparan de manera evaluativa respecto a los datos de trayecto (9) extraídos en el elemento de procesador (10).
- 10 14. Método según la reivindicación (13), **caracterizado porque** los datos de trayecto extraídos (9) son distancias recorridas o duraciones de recorrido que se acumulan a partir de los datos de posición (3).
- 15 15. Método según una de las reivindicaciones 11 a 14, **caracterizado porque** en el mismo elemento de procesador o en otro elemento de procesador (10, 13) que tiene acceso protegido criptográficamente y está equipado con un elemento de datos criptográfico (10', 13'), los datos de trayecto extraídos (9) se generan a partir de los datos de posición brutos (3) y se firman con el elemento de datos (10', 13').
- 20 16. Método según la reivindicación 15, **caracterizado porque** los datos de trayecto extraídos (9), que están firmados con el elemento de datos (10', 13'), se ponen a disposición en la unidad de a bordo (2) para ser consultados por una infraestructura (5) situada del lado de la carretera.

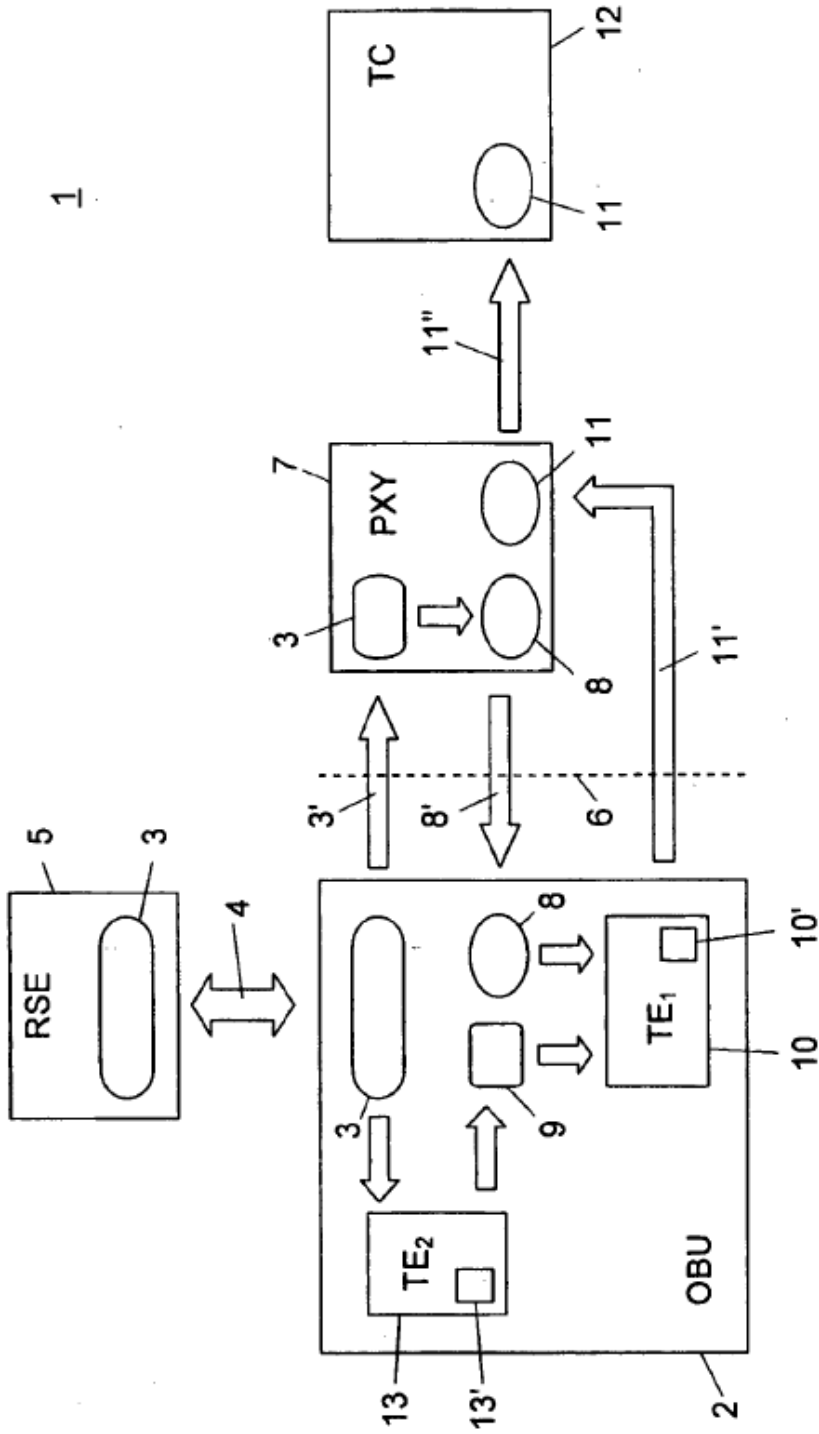


Fig. 1

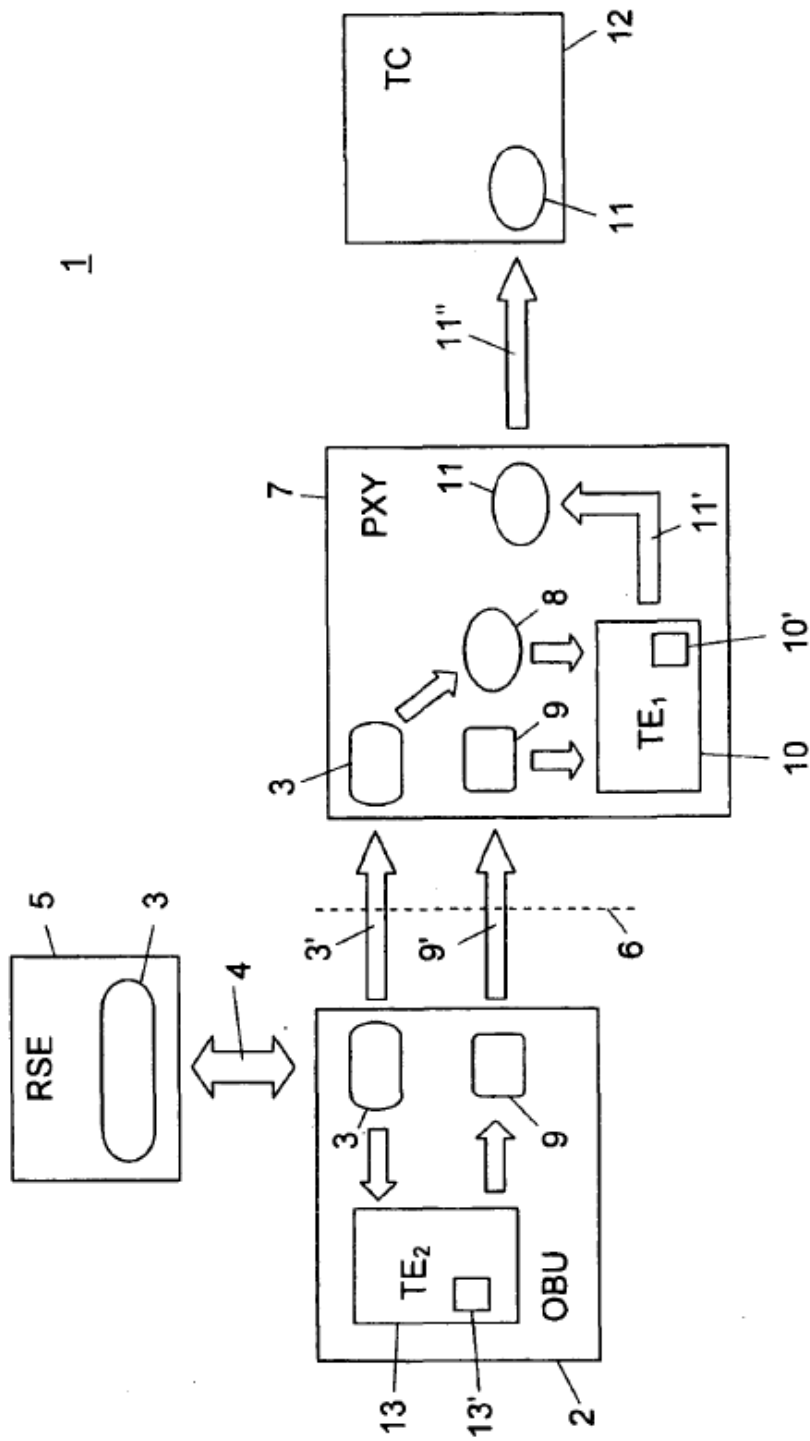


Fig. 2

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

5 *Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.*

Documentos de patente citados en la descripción

• EP2017790A [0002]

• WO2009001303 [0002]