(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 383 852**

(51) Int. CI.:
G07B 15/00 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09450207 .7**
(96) Fecha de presentación: **30.10.2009**
(97) Número de publicación de la solicitud: **2320386**
(97) Fecha de publicación de la solicitud: **11.05.2011**

(54) Título: **Procedimiento y dispositivos para generar datos de peaje anonimizados respecto a la ubicación**

(45) Fecha de publicación de la mención BOPI:
26.06.2012

(45) Fecha de la publicación del folleto de la patente:
26.06.2012

(73) Titular/es:
Kapsch TrafficCom AG
Am Europlatz 2
1120 Wien, AT

(72) Inventor/es:
Tijink, Jasja y
Kersten, Jan

(74) Agente/Representante:
Zea Checa, Bernabé

DESCRIPCIÓN

Procedimiento y dispositivos para generar datos de peaje anonimizados respecto a la ubicación

La presente invención se refiere a un procedimiento para generar datos de peaje anonimizados respecto a la ubicación a partir de las grabaciones de ubicación de un aparato de vehículo, que realiza las grabaciones de ubicación, con una identificación única en un sistema de peaje viario. La invención se refiere además a un servidor de cálculo de peaje y a un aparato de vehículo para la ejecución de este procedimiento.

Los aparatos de vehículo para sistemas de peaje viario se identifican también como "onboard units" u OBUs (unidades a bordo). En la actualidad existen dos realizaciones distintas de OBUs que pueden determinar y grabar automáticamente su posición, por ejemplo, mediante receptores de navegación por satélite: Los llamados OBUs "thick client" (cliente pesado) calculan datos de peaje anonimizados respecto a la ubicación sobre la base de mapas de peaje almacenados a partir de sus grabaciones de ubicación y los envían a una central del sistema de peaje viario, por ejemplo, a través de una red de telefonía móvil, lo que requiere una distribución costosa de los mapas de peaje a los OBUs y una alta capacidad de cálculo en los OBUs. A diferencia de esto, los llamados OBUs "thin client" (cliente liviano) no evalúan automáticamente sus grabaciones de ubicación, sino que las envían en estado "bruto" a la central que lleva a cabo el cotejo de mapas de peaje ("map matching") para generar datos de peaje a partir de esto. Por tanto, los OBUs "thin client" tienen una construcción esencialmente más simple y económica, pero son cuestionables desde el punto de vista de la protección de datos, porque la central del sistema de peaje viario conoce todas las grabaciones de ubicación ("perfil de movimiento") de un OBU, incluyendo su permanencia en lugares no sujetos a peaje.

Por consiguiente, el documento WO 2008/000227 ya propuso enviar las grabaciones de ubicación de un OBU "thin client" con una identificación de emisor anonimizada a un servidor de cálculo de peaje especial que ejecuta el "map matching" y reenvía al OBU los datos de peaje anonimizados respecto a la ubicación que el OBU transmite a continuación a la central. En este sistema resulta difícil controlar el cumplimiento de las obligaciones relativas a la protección de datos debido a la estructura arbitraria del servidor de cálculo de peaje. Además, esta solución genera un tráfico de datos adicional en el sistema de peaje viario.

Del documento WO 2009/001303 A1 es conocido que la central espere una confirmación de borrado del servidor de cálculo de peaje antes de asignar los datos de peaje anonimizados respecto a la ubicación, que se han recibido del servidor de cálculo de peaje, a una identidad de usuario recibida del OBU, lo que priva al OBU del derecho de disposición sobre la divulgación del OBU-ID (identificación de OBU) e implica el peligro de que la seguridad de los datos se vea comprometida.

La invención tiene el objetivo de eliminar las desventajas del estado de la técnica y crear especialmente un procedimiento para generar datos de peaje para OBUs "thin client", que garantice una protección de datos mejorada o una mayor confidencialidad para el usuario. Este objetivo se consigue mediante un procedimiento con las características de la reivindicación 1.

La invención se basa en un concepto, completamente nuevo y sorprendentemente simple, para la implementación de la protección de datos a nivel próximo a hardware ("privacy by design", privacidad en el diseño):

El OBU espera una confirmación explícita de borrado del servidor de cálculo de peaje y libera a continuación su identificación. De ese modo se obtiene la protección de datos condicionada por hardware ("privacy by design"). Un servidor de cálculo de peaje, especialmente adecuado para la invención, se caracteriza porque éste borra las grabaciones de ubicación después de procesarlas para obtener datos de peaje y envía al respecto una confirmación a un aparato de vehículo.

Un aparato de vehículo, especialmente adecuado para la invención, presenta medios de liberación que después de la recepción de una confirmación de borrado respecto a las grabaciones de ubicación enviadas transmiten su identificación de emisor con la identificación del aparato de vehículo.

La invención garantiza así de un modo simple y transparente para el usuario y el operador del sistema una confidencialidad, condicionada por hardware, de los datos sensibles de grabación de ubicación. Las grabaciones de ubicación se guardan en la central sólo el tiempo necesario para su procesamiento y a continuación se borran automáticamente. Esto permite disipar cualquier duda relacionada con un seguimiento o una elaboración central de un perfil de movimiento de los aparatos de vehículo. Además, la invención no provoca un tráfico de datos elevado en el sistema de peaje viario.

Si se desea, las grabaciones de ubicación en el servidor de cálculo de peaje se pueden codificar en cada realización antes del borrado con la clave pública de un sistema de archivo externo y enviar a éste. Un sistema de archivo de

este tipo deberá gozar como un tipo de fiduciario o notario de una gran confianza por parte de todos los participantes, es decir, tanto de los usuarios como del operador del sistema, y en caso de litigio podrá ser consultado por cualquiera de las partes.

El envío y la liberación desde el aparato de vehículo se lleva a cabo preferentemente mediante una red de telefonía, con especial preferencia una red de telefonía móvil. De este modo se pueden usar, por ejemplo, OBUs "thin client" convencionales que están equipados con un transceptor DSRC (comunicación dedicada de corto alcance) o de telefonía móvil.

Según otra realización preferida de la invención, las grabaciones de ubicación de un aparato de vehículo se envían en paquetes de datos provistos en cada caso de las mismas identificaciones de emisor, lo que simplifica la evaluación, ya que el aparato de vehículo, después de esperar el período de tiempo o recibir la confirmación de borrado, tiene que revelar su identificación sólo respecto a una única identificación de emisor.

Las grabaciones de ubicación de un aparato de vehículo se pueden enviar alternativamente en paquetes de datos provistos de identificaciones de emisor variables. Esto permite aumentar la confidencialidad en la interfaz de transmisión.

Con preferencia, los paquetes de datos provistos de identificaciones de emisor variables están provistos adicionalmente de identificaciones de paquete encadenadas que permiten su asignación entre sí. De este modo, el aparato de vehículo necesita liberar su identificación sólo respecto a la identificación de emisor del último paquete de datos.

La identificación, con la que se identifica un aparato de vehículo, puede ser tanto una identificación del propio aparato de vehículo como una identificación asignada al usuario del vehículo, por ejemplo, una identificación de una cuenta de usuario para cobrar las tasas de peaje en el sistema de peaje viario.

La identificación de emisor usada para enviar las grabaciones de ubicación al servidor de cálculo de peaje puede ser tanto un valor aleatorio como un código seleccionable libremente por el usuario, lo que aumenta aún más la transparencia para el usuario.

El procedimiento de la invención es adecuado para todos los tipos de aparatos de vehículo autolocalizadores, con independencia del modo en que determinan su ubicación, por ejemplo, mediante el reconocimiento de marcas terrestres o la identificación de balizas, por las que se guía el aparato de vehículo. Es especialmente ventajoso que el aparato de vehículo determine de forma conocida sus ubicaciones mediante navegación por satélite, pudiéndose usar para esto, por ejemplo, los OBUs "thin client" asistidos por GPS.

La invención se explica detalladamente a continuación por medio de ejemplos de realización que están representados en los dibujos adjuntos y cuyas figuras 1 y 2 muestran en un esquema de bloques dos realizaciones distintas de un sistema de peaje viario que funciona según el procedimiento de la invención y contiene componentes según la invención.

Según la figura 1, un OBU 1 se mueve a bordo de un vehículo en el marco de un sistema de peaje viario con una central 2. La central 2 cobra el uso local del OBU 1 que está sujeto a peaje, por ejemplo, la circulación por una carretera de peaje, la entrada en una zona de pago, la permanencia en un aparcamiento sujeto al pago de tasas, etc., mediante cuentas de usuario correspondientes, y específicamente sobre la base de datos de peaje T que se generan por el uso local del OBU 1, como es conocido en la técnica.

El OBU 1 es del tipo "thin client" autolocalizador y determina de forma continua, por ejemplo, periódica, su ubicación, por ejemplo, con ayuda de un receptor de navegación por satélite, y graba las ubicaciones determinadas de este modo ("position fixes", posición establecida) p_1, p_2, p_3, ... (en general p_i) en una memoria interna de grabación de ubicación.

Cada OBU 1 está provisto de una identificación única OID en el sistema de peaje viario, por ejemplo, una identificación única del propio OBU 1 y/o de su usuario o de una cuenta de este último. Sobre la base de la identificación OID de un OBU 1 y sus grabaciones de ubicación p_i se podría deducir el perfil de movimiento de un OBU 1, lo que se impide de la forma que aparece a continuación.

Las grabaciones de ubicación p_i del OBU 1 se dividen, incluso aunque esto no sea obligatorio, en paquetes de datos individuales 3 para una manipulación más fácil. Los paquetes de datos 3 se pueden proveer de una identificación de paquete P_i (véase la figura 2), por ejemplo, una enumeración continua, y de un header (cabecera) (no mostrado) que contiene, por ejemplo, metadatos, como la cantidad de grabaciones de ubicación p_i contenidas en el paquete de datos, un valor hash de éstas, etc.

En un primer paso 4, las grabaciones de ubicación p_i o los paquetes de datos 3 se envían del OBU 1 a un servidor de cálculo de peaje 5, por ejemplo, mediante una red de telefonía móvil, a saber, con una identificación de emisor RID distinta a la identificación OID, pero en cierto modo "anónima". La identificación de emisor RID es, por ejemplo, un código seleccionado libremente por el usuario o un valor generado de forma aleatoria por el OBU 1. Como identificación de emisor RID se podría usar alternativamente una identificación temporal de red de telefonía móvil o una dirección temporal de internet del OBU 1, aunque con un carácter anónimo correspondientemente reducido.

El servidor de cálculo de peaje 5 contiene un dispositivo de "map matching" 6 que asigna las grabaciones de ubicación recibidas p_i a lugares, regiones o tramos, sujetos a peaje, a partir de una base de datos de mapas de peaje 6' y determina las tasas de peaje correspondientes a partir de la base de datos de mapas de peaje 6'. Sobre la base de las tasas de peaje de las grabaciones de ubicación p_i recibidas respecto a una identificación de emisor RID, el dispositivo de "map matching" 6 calcula los datos de peaje T "anonimizados así respecto a la ubicación" que ya no permiten sacar conclusiones de las grabaciones de ubicación individuales p_i. Los datos de peaje T son, por ejemplo, una única suma de tasas para todas las grabaciones de ubicación p_i de todos los paquetes de datos 3 de una identificación de emisor RID.

Delante del dispositivo de "map matching" 6 del servidor de cálculo de peaje 5 está conectado un buffer 7 en forma de una memoria circular, a la que llegan sucesivamente todas las grabaciones de ubicación p_i o paquetes de datos 3 enviados por OBUs 1 para ser procesados por el dispositivo 6. Por tanto, debido a la carga de trabajo promedio del dispositivo 6 se puede fijar un período de tiempo en el que las grabaciones de ubicación p_i, que han llegado en un momento determinado al buffer 7, se han transformado en datos de peaje anonimizados respecto a la ubicación T y se han borrado automáticamente por la llegada de nuevas grabaciones de ubicación. Esto último ocurre, por ejemplo, si el buffer 7 está realizado, según muestra la figura 1, como memoria circular que se sobrescribe continuamente de manera automática y cíclica con los nuevos datos que llegan. Si a modo de excepción se supera este período de tiempo en caso de un aprovechamiento extraordinariamente bajo del buffer 7, mediante un borrado adicional periódico, por ejemplo, diario, de entradas en el buffer 7, más antiguas que el período de tiempo mencionado, se puede garantizar que ya no haya ninguna grabación de ubicación p_i en el servidor de cálculo de peaje 5 después del período de tiempo predefinido que se ha mencionado.

Si alguna vez hubiera que borrar grabaciones de ubicación p_i sin procesar en caso de una carga extraordinariamente alta de la memoria circular 7 o del dispositivo de "map matching" 6, el OBU 1 puede volver a transmitir estas grabaciones de ubicación p_i, ya sea de forma automática o a solicitud del servidor de cálculo de peaje 5 o a solicitud de la central 2.

Si se desea, el servidor de cálculo de peaje 5 puede archivar antes del borrado las grabaciones de ubicación p_i codificadas de manera fiable para ser usadas como prueba, por ejemplo, al codificarlas con la clave pública de un sistema de archivo 9 y enviarlas a éste (paso 10). Ni el usuario ni el operador del sistema de peaje viario puede conocer la clave privada del archivo 8 que se necesita para descodificar las grabaciones de ubicación p_i. Sólo tendrá conocimiento de ésta el operador del sistema de archivo 9 que actúa casi como notario o fiduciario para ambas partes.

En el paso 8, el servidor de cálculo de peaje 5 envía a continuación los datos de peaje calculados T con la identificación de emisor RID a la central 2.

Por la otra parte, el OBU 1 espera el período de tiempo mencionado (paso 11) y libera o revela a continuación su "identidad", es decir, su identificación OID (paso 12). La liberación se lleva a cabo en la figura 1 al enviar el OBU 1 la identificación de emisor RID, que ha usado, con su identificación OID a la central 2. La central 2 puede asignar así los datos de peaje T, recibidos del servidor de cálculo 5 con la identificación de emisor RID, a la identificación OID obtenida del OBU 1 respecto a esta identificación de emisor RID (paso 13) con el fin de generar datos de peaje anonimizados respecto a la ubicación T que están asignados al OBU 1.

La figura 2 muestra distintas variantes de componentes del procedimiento de la figura 1. En este caso, la asignación de los datos de peaje respecto a la identificación OID no se lleva a cabo en la central 2, sino directamente en el servidor de cálculo de peaje 5 al liberar el OBU 1 su identificación OID en el paso 12 para el servidor de cálculo de peaje 5 y al enviar este último el resultado de la asignación 13 a la central 2 (paso 14).

La figura 2 muestra además que el OBU 1, en vez de esperar un período de tiempo 11, espera en este caso la llegada de una confirmación explícita 15 del servidor de cálculo de peaje 5 sobre el borrado realizado de las grabaciones de ubicación p_i. Después de llegar la confirmación de borrado 15, el OBU 1 revela su identificación OID en el paso 12.

La figura 2 muestra también la variante de que los paquetes de datos individuales 3 se pueden proveer de identificaciones de emisor variables RID_i con el fin de dificultar el seguimiento en la interfaz 4. En el paso 12, el OBU

1 puede identificar asimismo varias identificaciones de emisor RID_i, usadas por éste en último lugar, con su identificación OID.

Si los paquetes de datos individuales 3 están encadenados entre sí, por ejemplo, mediante referencias mutuas correspondientes en sus identificaciones de paquete P_i, es suficiente que el OBU 1 identifique en el paso 12 sólo la última identificación de emisor RID_i de una secuencia encadenada de paquetes de datos con su identificación OID, porque el servidor de cálculo de peaje 5 puede contener la identificación de emisor precedente RID_i como resultado de los encadenamientos de paquetes.

De manera alternativa, el servidor de cálculo de peaje 5 podría acumular también los datos de peaje T_i que se acumulan continuamente en forma de identificaciones de emisor encadenadas RID_i, por ejemplo, en una suma de tasas, y suprimir a este respecto siempre sólo la última identificación de emisor RID_i. También en este caso es suficiente que el OBU 1 identifique en el paso 12 sólo su última identificación de emisor RID_i con su identificación OID.

Por último, la figura 2 muestra también el uso de una memoria pila como buffer 7. La memoria pila 7 se borra, por ejemplo, periódicamente o sus entradas más antiguas se eliminan después de un período de tiempo predefinido, si no han sido procesadas de forma oportuna, y/o el OBU 1 espera en este caso siempre una confirmación de borrado 16.

La invención no está limitada a las realizaciones representadas, sino que comprende todas las variantes y modificaciones que entran en el marco de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para generar datos de peaje anonimizados respecto a la ubicación (T) a partir de las grabaciones de ubicación (p_i) de un aparato de vehículo (1), que realiza las grabaciones de ubicación, con una identificación única (OID) en un sistema de peaje viario, con los siguientes pasos:
enviar (4) las grabaciones de ubicación (p_i) con al menos una identificación de emisor (RID), distinta a la identificación (OID) del aparato de vehículo (1), a un servidor de cálculo de peaje (5),
calcular (6) datos de peaje anonimizados respecto a la ubicación (T) a partir de las grabaciones de ubicación (p_i) y borrar a continuación las grabaciones de ubicación (p_i) en el servidor de cálculo de peaje (5),
esperar en el aparato de vehículo (1) la llegada de una confirmación explícita (15) del servidor de cálculo de peaje (5) sobre el borrado realizado de las grabaciones de ubicación (p_i), y a continuación
liberar (12) la identificación (OID), perteneciente a la identificación de emisor (RID), mediante su transmisión del aparato de vehículo (1) al servidor de cálculo de peaje (5) que asigna los datos de peaje anonimizados respecto a la ubicación (T) a la identificación (OID) y los envía a una central (2) del sistema de peaje.

2. Procedimiento según la reivindicación 1, **caracterizado porque** las grabaciones de ubicación (p_i) en el servidor de cálculo de peaje (5) se codifican antes del borrado con la clave pública de un sistema de archivo externo (9) y se envían a éste.

3. Procedimiento según la reivindicación 1 ó 2, **caracterizado porque** el envío (4) y la liberación (12) desde el aparato de vehículo (1) se lleva a cabo mediante una red de telefonía, preferentemente una red de telefonía móvil.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado porque** las grabaciones de ubicación (p_i) de un aparato de vehículo (1) se envían en paquetes de datos (3) provistos en cada caso de las mismas identificaciones de emisor (RID).

5. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado porque** las grabaciones de ubicación (p_i) de un aparato de vehículo se envían en paquetes de datos (3) provistos de identificaciones de emisor variables (RID_i).

6. Procedimiento según la reivindicación 5, **caracterizado porque** los paquetes de datos (3) están provistos de identificaciones de paquete encadenadas (P_i) que permiten su asignación entre sí, liberándose (12) la identificación (OID) sólo respecto a la identificación de emisor (RID_i) del último paquete de datos (3).

7. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado porque** la identificación mencionada (OID) es una identificación de aparato de vehículo o de cuenta de usuario.

8. Procedimiento según una de las reivindicaciones 1 a 7, **caracterizado porque** la identificación de emisor (RID) es un valor aleatorio o un código seleccionable por el usuario.

9. Servidor de cálculo de peaje (5) para la ejecución del procedimiento según una de las reivindicaciones 1 a 8, configurado para la recepción de grabaciones de ubicación (p_i) y el cálculo de datos de peaje anonimizados respecto a la ubicación (T), **caracterizado porque** borra las grabaciones de ubicación (p_i) después de procesarlas para obtener datos de peaje (T) y envía al respecto una confirmación (15) a un aparato de vehículo (1).

10. Aparato de vehículo (1), que realiza grabaciones de ubicación, con una identificación (OID), para la ejecución del procedimiento según una de las reivindicaciones 1 a 8, configurado para el envío (4) de sus grabaciones de ubicación (p_i) con al menos una identificación de emisor (RID) distinta a la identificación (OID), **caracterizado por** medios de liberación que después de la recepción de una confirmación de borrado (15) respecto a las grabaciones de ubicación enviadas (p_i) transmiten su identificación de emisor (RID) con su identificación (OID).

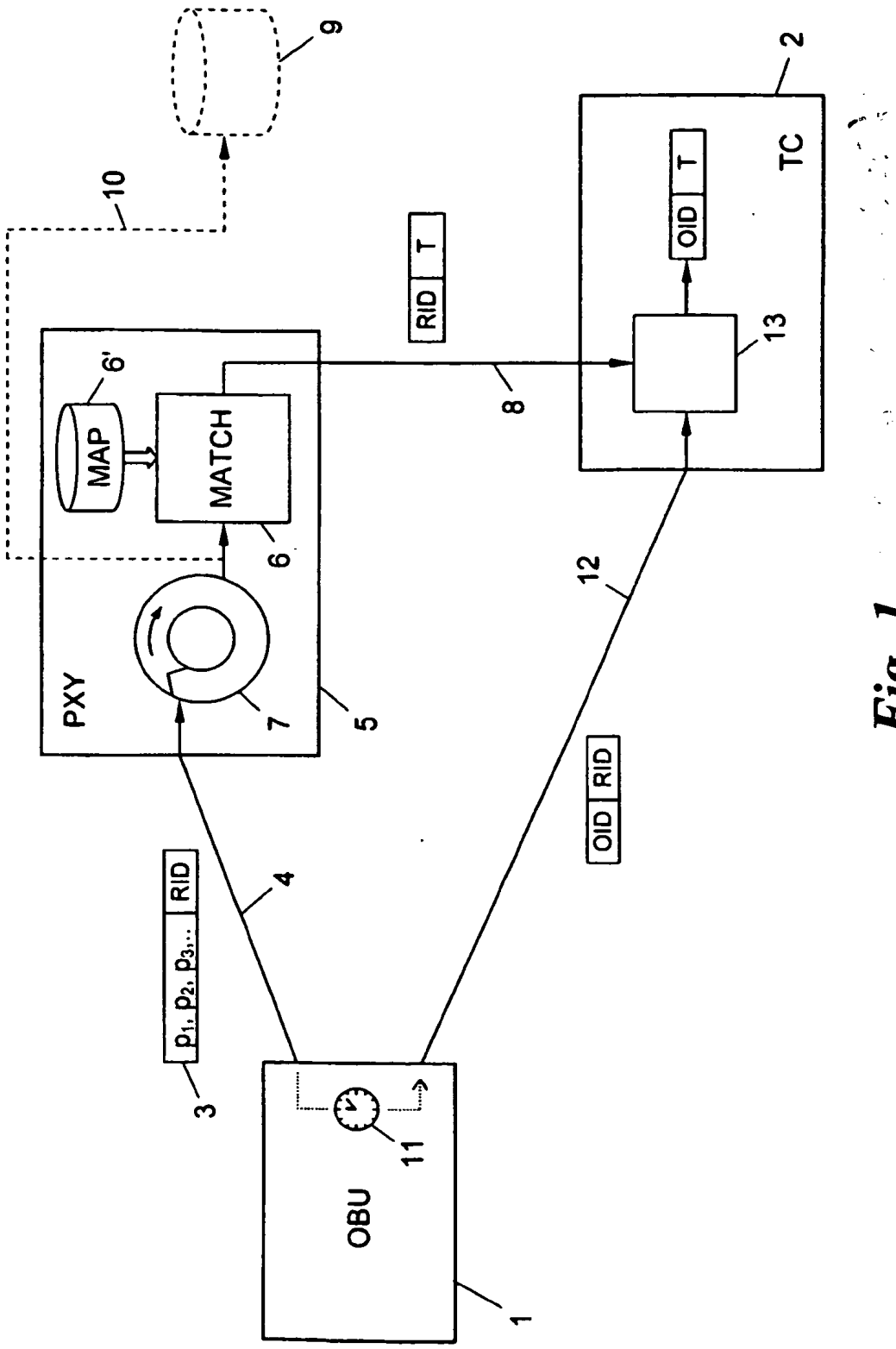
9
10
2
TC
OID
T
RID
T
13
8
6'
MAP
MATCH
6
PXY
7
5
12
OID
RID
4
RID
$p_1, p_2, p_3, ..$
3
OBU
11
1

Fig. 1

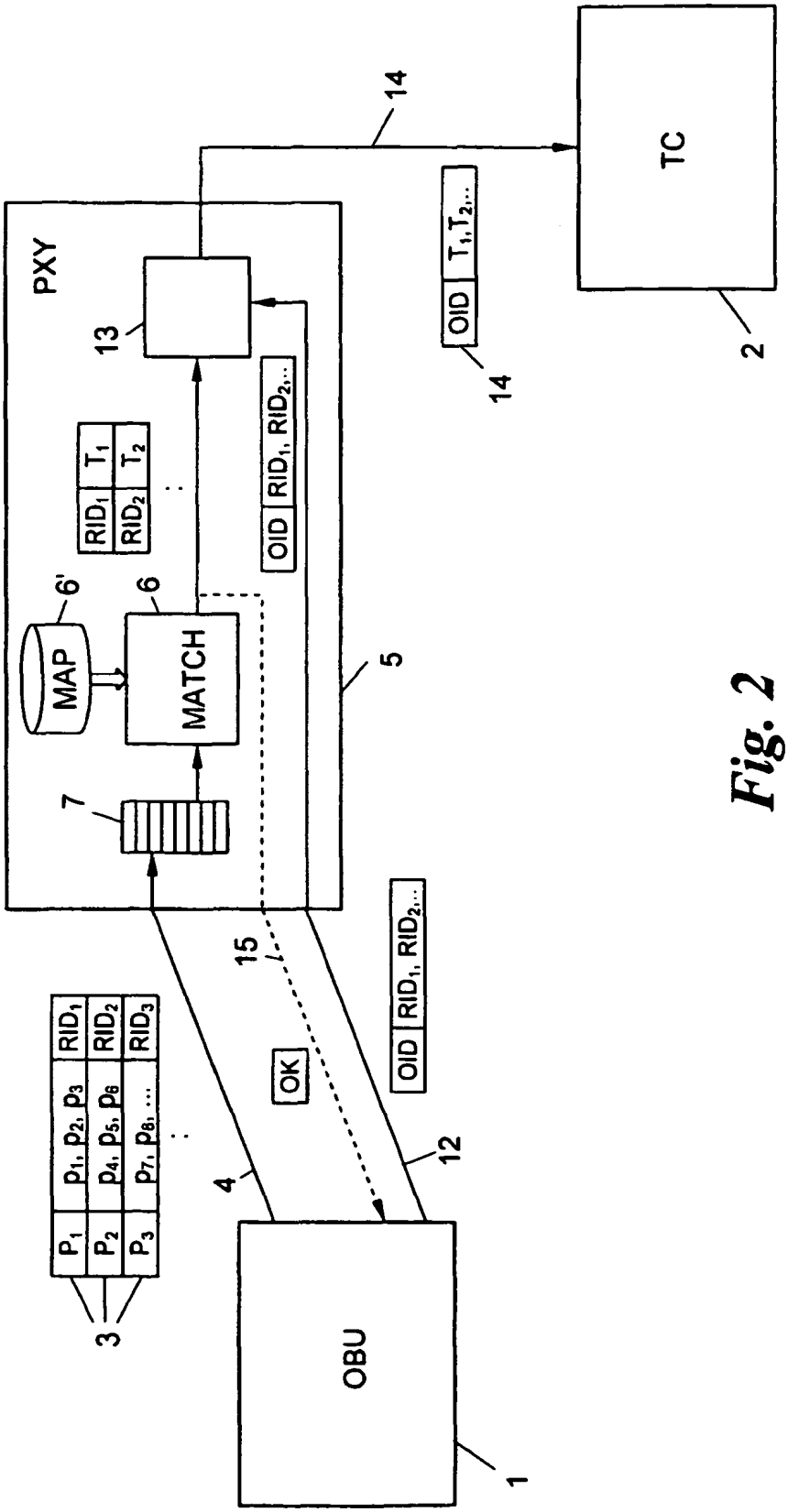
TC
14
OID
T1, T2,...
14
2
PXY
13
RID1
T1
RID2
T2
OID
RID1, RID2,...
6'
6
MAP
MATCH
5
7
15
OK
OID
RID1, RID2,...
12
4
P1
P2
P3
P1, P2, P3
P4, P5, P6
P7, P8, ...
RID1
RID2
RID3
3
OBU
1

Fig. 2

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

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

- WO 2008000227 A **[0003]**
- WO 2009001303 A1 **[0004]**