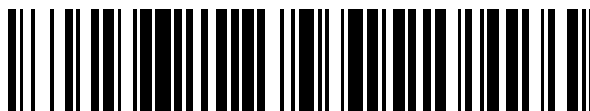


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 375 970**

51 Int. Cl.:

G06F 1/00 (2006.01)

G07F 7/10 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **05785661 .9**

96 Fecha de presentación: **21.09.2005**

97 Número de publicación de la solicitud: **1810112**

97 Fecha de publicación de la solicitud: **25.07.2007**

54 Título: **PROCEDIMIENTO E INSTALACIÓN PARA LA INICIALIZACIÓN ESPECÍFICA DE USUARIO DE DISPOSITIVOS DE IDENTIFICACIÓN IN SITU.**

30 Prioridad:
09.11.2004 AT 18652004

45 Fecha de publicación de la mención BOPI:
07.03.2012

45 Fecha de la publicación del folleto de la patente:
07.03.2012

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

72 Inventor/es:
EBERSTALLER, Bernd

74 Agente/Representante:
Zea Checa, Bernabé

ES 2 375 970 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

Procedimiento e instalación para la inicialización específica de usuario de dispositivos de identificación in situ.

[0001] La invención se refiere a un procedimiento según el preámbulo de la reivindicación 1 y a una instalación según el preámbulo de la reivindicación 20.

5 **[0002]** En los sistemas de identificación, de autorización, de permisos y de compensación que tienen una central y dispositivos de identificación móviles distribuidos, los dispositivos de identificación se fabrican habitualmente sin asociarse a un identificador de usuario, y hasta la salida no se inicializan con el identificador de usuario respectivo y se transfieren al usuario. A este respecto la inicialización tiene lugar o bien en estaciones de inicialización distribuidas o centrales.

10 **[0003]** Por el documento EP 0 730 253 A2 se conoce entregar de forma anónima portadores de claves dotados de identificadores de dispositivo y permitir acuses de recibo por escrito por el usuario a una central, que entonces gestiona las asignaciones de usuario/clave para peticiones de claves públicas/privadas.

[0004] La desventaja de las soluciones convencionales es que o bien son necesarias costosas etapas manuales, o bien en muchas ubicaciones de salida deben conseguirse estaciones de inicialización con un enlace de datos a la
15 unidad central, o que es necesaria una cara logística para la distribución de los dispositivos de identificación inicializados al usuario correcto.

[0005] El objetivo de la invención es poder realizar una personalización o inicialización específica de usuario segura de un dispositivo de identificación sin etapas manuales costosas, estaciones de inicialización distribuidas y sin el gasto logístico elevado de la distribución de dispositivos de identificación ya inicializados.

20 **[0006]** Este objetivo se consigue en un primer aspecto de la invención con un procedimiento del tipo mencionado al principio, que se caracteriza por los rasgos caracterizadores de la reivindicación 1, y en un segundo aspecto de la invención mediante una instalación del tipo mencionado al principio, que se caracteriza por los rasgos característicos de la reivindicación 20.

[0007] De esta manera puede entregarse un dispositivo de identificación con un identificador de dispositivo
25 aleatorio al usuario y personalizarse por éste *en situ* por medio del PIN de inicialización. Con ayuda del PIN de inicialización se verifica si la asignación del identificador de dispositivo propio del dispositivo de identificación coincide con la información transmitida en el PIN de inicialización sobre el identificador de dispositivo. En caso de concordancia, se calcula el identificador de usuario a partir del PIN de inicialización y el identificador de usuario se visualiza en el dispositivo de identificación. Con ello se concluye el proceso de inicialización del dispositivo de
30 identificación y se habilita por ejemplo un intercambio de datos entre el dispositivo de identificación y la unidad central. Mediante la transmisión del PIN de inicialización no es necesaria ninguna estación de inicialización costosa para la inicialización de los dispositivos de identificación.

[0008] En una forma de realización preferida del procedimiento según la invención, para restablecer el dispositivo de identificación al estado de entrega se genera un PIN de desinicialización, que se usa como el PIN de
35 inicialización. Tras la desinicialización, el dispositivo de identificación está listo de nuevo para una nueva inicialización.

[0009] En una realización adicional el identificador de dispositivo del dispositivo de identificación puede consistir en una parte pública y una parte privada (oculta). La parte pública del identificador de dispositivo se establece en la
40 fabricación y tanto va impresa en la carcasa de los dispositivos de identificación como almacenada en el dispositivo de identificación. La parte privada del identificador de dispositivo se establece también en la fabricación y se almacena en el dispositivo de identificación. La parte privada del identificador de dispositivo puede ser un número aleatorio o un número calculado según un algoritmo determinado. La parte pública y la parte privada del identificador de dispositivo se publican a la unidad de central antes de la entrega.

[0010] En una configuración adicional de la invención está previsto que, por motivos de seguridad, en la
45 generación del PIN de inicialización o PIN de desinicialización se emplee un procedimiento de codificación, y en el dispositivo de identificación se decodifique de manera correspondiente el PIN de inicialización o PIN de desinicialización.

[0011] El PIN de inicialización o PIN de desinicialización puede comunicarse al usuario e introducirse por éste
50 manualmente por medio de un teclado al dispositivo de identificación; alternativamente puede transmitirse desde la unidad central, por ejemplo a través de una interfaz de radio al dispositivo de identificación.

[0012] Una realización adicional de la invención es que el procedimiento según la invención se utiliza en registro automático de los trayectos o rutas de vehículos, para calcular a partir de ahí tarifas de peaje y generar datos telemáticos de tráfico para el análisis de los flujos de tráfico. A este respecto se asigna a cada vehículo un dispositivo para vehículos (unidad de a bordo, OBU), que dispone de un identificador de dispositivo y un identificador de usuario asociado, por ejemplo la matrícula. Estos dispositivos para vehículos se distribuyen en puntos de venta distribuidos por ejemplo gasolineras, aduanas, puertos etc., y se comunican al usuario el PIN de inicialización según el procedimiento según la invención. Tras la entrada del PIN de inicialización en el dispositivo de identificación éste está listo para registrar las trayectorias así como los datos telemáticos de tráfico y transmitirlos a la unidad central. El PIN de inicialización puede enviarse también desde la unidad central al dispositivo de identificación y la inicialización tiene lugar o bien de manera completamente automática o bien semiautomática. En el caso de la inicialización automática se muestra visualmente al usuario, que la inicialización ha tenido lugar. En el caso de la inicialización semiautomática se visualiza el identificador de usuario, y deben confirmarse por el usuario la inicialización y el identificador de usuario.

[0013] Según una variante adicional de la invención tras la inicialización puede desactivarse el dispositivo de identificación y activarse de nuevo, por ejemplo cuando el vehículo sujeto a peaje abandona la región sujeta a peaje. Tras la desactivación se mantienen todos los datos de la inicialización en el dispositivo de identificación, pero se interrumpe el registro del trayecto y de los datos telemáticos de tráfico. La activación y desactivación puede tener lugar tal como en el caso de la inicialización manualmente, semiautomáticamente o automáticamente por medio de un PIN de activación o PIN de desactivación.

[0014] Una característica adicional de la invención consiste en que en el PIN de inicialización también están contenidos datos y autorizaciones funcionales específicos de usuario, tales como por ejemplo clase de contaminantes del vehículo, número del eje o peso máximo autorizado. Las autorizaciones y datos específicos de usuario pueden modificarse en el dispositivo de identificación también por medio de un PIN de autorización.

[0015] El dispositivo de identificación envía datos a la unidad central tras la inicialización y la recepción de los datos se confirma con un PIN de confirmación.

[0016] La generación de los PIN de activación, PIN de desactivación, PIN de autorización o PIN de confirmación tiene lugar según el procedimiento según la invención tal como en el caso de la inicialización.

[0017] En una configuración adicional de la invención la comunicación por radio por partes entre el dispositivo de identificación móvil y una estación de radio estacionaria puede ser radiocanal de microondas; *Dedicated Short Range Communication* (DSRC) (comunicación de corto alcance dedicada); un radiocanal o un canal de radiotelefonía móvil, por ejemplo GSM, UMTS o un enlace de datos inalámbrico, por ejemplo WLAN, WiMAX.

[0018] La descripción de un ejemplo de realización del procedimiento y de la instalación de la invención tiene lugar por medio de las siguientes figuras:

figura 1: representación esquemática del sistema

figura 2: desarrollo esquemático de la inicialización

figura 3: diagrama de flujo de la generación de PIN

figura 4: desarrollo esquemático de la activación

[0019] En la figura 1 se muestra la representación esquemática del sistema. Este ejemplo de realización se ocupa en detalle de un sistema de peaje de carreteras. En cambio, la invención no está limitada a estos sistemas, sino que puede utilizarse para todos los sistemas de comunicación en los que se inicializan dispositivos distribuidos desde una unidad central o bien automáticamente o bien manualmente asignando un identificador de usuario unívoco (por ejemplo en este ejemplo de realización la matrícula) a un identificador de dispositivo (por ejemplo número de serie) de un dispositivo de identificación distribuido.

[0020] La instalación según la figura 1 consiste en una unidad central 1 para recopilar datos de los dispositivos de identificación 4 y para el procesamiento previo y transferencia a un centro de compensación no mostrado. La unidad central está conectada a través de una red de información pública 2 con estaciones de radio 3 estacionarias dispuestas en la región. Las estaciones de radio 3 pueden ser balizas para la comunicación por microondas o DSRC con los dispositivos de identificación 4, estaciones base de una red de radiotelefonía móvil o nodos de acceso de una conexión a Internet WLAN o WiMAX. También es posible una combinación de estas tecnologías para la transmisión de datos bidireccional entre dispositivos de identificación 4 y estaciones de radio estacionarias 3.

[0021] Los dispositivos de identificación se entregan a almacenes de distribución. Cuando sea necesario, un usuario (por ejemplo un transportista) concluye un contrato (figura 2) con un operador de la unidad central (por ejemplo un operador de peaje de carreteras), y se asocia al mismo un dispositivo de identificación 4 con un único

identificador de dispositivo 103. Al mismo tiempo se transmiten ésta y el identificador de usuario 104 (por ejemplo la matrícula del vehículo) a través de una vía de comunicación no representada en la figura 1 de la unidad central 1. La unidad central 1 genera a partir del identificador de dispositivo 103 y del identificador de usuario 104 un PIN de inicialización 102, en el que están contenidos los dos identificadores y opcionalmente autorizaciones adicionales.

5 Tales autorizaciones pueden ser en este ejemplo de aplicación, además de otros, la clase ambiental del vehículo o también el número de sus ejes.

[0022] El PIN de inicialización se transmite al usuario, por ejemplo a través de una red de comunicación o mediante una llamada telefónica, y se introduce por ésta en el dispositivo de identificación 4. Alternativamente puede enviarse el PIN de inicialización directamente desde la unidad central 1 al dispositivo de identificación.

10 **[0023]** Con la coincidencia del identificador de dispositivo propio del dispositivo de identificación con el identificador de dispositivo transmitido en el PIN de inicialización se inicializa o personaliza el dispositivo de identificación de manera específica de usuario y con ello se activa para el funcionamiento previsto. Durante el funcionamiento el dispositivo de identificación recopila datos, por ejemplo trayectos, y transmite los mismos a través de la interfaz de radio 5, una estación de radio estacionaria 3 y la red de información 2 a la unidad central para su
15 evaluación adicional.

[0024] La figura 3, por medio del ejemplo de aplicación del peaje de carreteras, se ocupa de la generación del PIN de inicialización 401. La OBU-ID 402 corresponde al identificador de dispositivo del dispositivo de identificación y en la realización no representada adicionalmente en la figura 3 el identificador de dispositivo 103 puede consistir en una parte pública y una parte privada. La parte pública del identificador de dispositivo se determina en la fabricación del
20 dispositivo de identificación y por ejemplo tanto va impreso en la carcasa del dispositivo de identificación como almacenado en el dispositivo de identificación. La parte privada del identificador de dispositivo 402 se determina asimismo en la fabricación y se almacena en el dispositivo de identificación. La parte privada del identificador de dispositivo puede ser un número aleatorio o un número calculado según un algoritmo determinado. La parte pública y la parte privada del identificador de dispositivo se publican en la unidad central 1 antes de la entrega del dispositivo
25 de identificación. En este ejemplo de realización, en el caso de un cierre del contrato, es decir la asignación de un usuario con su identificador de usuario para un dispositivo de identificación con un identificador de dispositivo, sólo se transmite la parte pública del identificador de dispositivo a la unidad central 1 y ésta complementa la parte privada del identificador de dispositivo para calcular el PIN de inicialización.

[0025] En una variante adicional el identificador de dispositivo puede comprimirse para simplificar las etapas
30 adicionales (403).

[0026] En la generación del PIN de inicialización se relacionan entre sí la matrícula 404, que en este caso corresponde al identificador de usuario, y la OBU-ID 403 (405) y se codifican por medio de un procedimiento de codificación 406. Para la inicialización del dispositivo de identificación se transmite el PIN de inicialización al usuario (en este caso: transportista) para la entrada en el dispositivo de identificación 407.

35 **[0027]** Según el mismo procedimiento en el caso de una resolución del contrato se genera un PIN de desinicialización, desarrollándose la etapa para la transmisión del identificador de dispositivo 103 del dispositivo de identificación, dado que ya se conoce la asignación de la unidad central. La desinicialización reinicializa en el dispositivo de identificación todos los datos específicos de contrato o de usuario, de modo que el dispositivo de identificación está preparado para una nueva inicialización.

40 **[0028]** Para determinados casos es necesario que se desactive el dispositivo de identificación, por ejemplo cuando el vehículo sale del campo sujeto a peaje y debe volver a activarse posteriormente al regresar (véase la figura 4). Para este fin tiene lugar una petición 501 a la unidad central 1, o bien automáticamente a través de la interfaz de radio 5 y la red de información 2 en el caso de la salida del campo sujeto a peaje o según una petición manual, por ejemplo una llamada telefónica con el centro de llamadas de la unidad central 1. En cada caso se genera por la
45 unidad central un PIN de desactivación 502 a partir del identificador de dispositivo y del identificador de usuario, empleándose el mismo procedimiento que en el caso de la generación del PIN de inicialización. O bien el PIN de desactivación 502 se envía automáticamente a través de la red de información 2 y la interfaz de radio 3 al dispositivo de identificación 4 y tiene lugar la desactivación automática del dispositivo de identificación 4, o bien en el caso de la petición manual se comunica al usuario el PIN de desactivación 502 y éste lo introduce en el dispositivo de
50 identificación 4, para realizar la desactivación del dispositivo de identificación 4.

[0029] Una nueva activación del dispositivo de identificación 4 tiene lugar según el mismo procedimiento que la desactivación según la figura 4 por medio de un PIN de activación.

[0030] La variación de autorizaciones del dispositivo de identificación tiene lugar asimismo según el procedimiento de desactivación del dispositivo de identificación según la figura 4 por medio de un PIN de autorización.

[0031] Los datos telemáticos de tráfico se envían a través de la interfaz de radio 3 y la red de información 2 a la unidad central 1 y desde la unidad central 1 tiene lugar una confirmación automática por medio de un PIN de confirmación. Si ésta no llegara, entonces para el usuario es posible reclamar manualmente el PIN de confirmación según el procedimiento según la figura 4 y tras su obtención realizar manualmente la confirmación mediante la entrada del PIN de confirmación manualmente.

[0032] Naturalmente, la invención no está limitada al campo de utilización discutido a modo de ejemplo de los sistemas de peaje de carreteras, sino que puede aplicarse en un estado no personalizado en cualquier tipo de dispositivos de identificación, que debe entregarse con el fin de una fabricación a gran escala más sencilla, almacenamiento y distribución segura durante la manipulación e inicializarse o personalizarse de manera específica de usuario *in situ* de manera sencilla, segura y transparente, para obtener validez para fines de identificación o autorización. Ejemplos de tales aplicaciones adicionales son la personalización de licencias electrónicas de vehículos o de usuario o de tarjetas inteligentes o tarjetas RFID para fines de identificación y de licencia.

REIVINDICACIONES

1. Procedimiento para la inicialización específica de usuario de dispositivos de identificación (4) in situ, especialmente unidades de a bordo en sistemas de peaje de carreteras, partiendo de una unidad central (1), teniendo cada dispositivo de identificación (4) en el estado de entrega un identificador de dispositivo unívoco (103),
5 al que está asociado un identificador de usuario unívoco (104) en la unidad de central (1), **caracterizado por que** en la unidad central (1), a partir del identificador de dispositivo (103) y del identificador de usuario (104), se genera un PIN de inicialización (102) y se transmite al dispositivo de identificación (4), y a partir del PIN de inicialización el dispositivo de identificación (4), usando su identificador de dispositivo (103), calcula el identificador de usuario (104) para la inicialización específica de usuario.
- 10 2. Procedimiento según la reivindicación 1, **caracterizado por que** el dispositivo de identificación (4) visualiza el identificador de usuario calculado (104) y/o la envía bajo petición.
3. Procedimiento según la reivindicación 1 ó 2, **caracterizado por que** el identificador de dispositivo (103) del dispositivo de identificación consiste en una parte pública y en una parte privada.
4. Procedimiento según la reivindicación 3, **caracterizado por que** la parte privada del identificador de dispositivo se
15 forma por un número aleatorio o por un algoritmo.
5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado por que** la unidad central genera también un PIN de desinicialización para restablecer la inicialización del dispositivo de identificación (4).
6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado por que** para la inicialización válida del dispositivo de identificación (4) el identificador de dispositivo transmitido con el PIN de inicialización (102) se
20 compara con el identificador de dispositivo (103) del dispositivo de identificación (4).
7. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado por que** el PIN de inicialización (102) comprende también datos y autorizaciones funcionales del dispositivo de identificación (4).
8. Procedimiento según una de las reivindicaciones 1 a 7, **caracterizado por que** para generar el PIN de inicialización y cualquier posible PIN de desinicialización se emplea un procedimiento de codificación (406) y el PIN
25 de inicialización (102) y cualquier posible PIN de desinicialización se decodifican en el dispositivo de identificación (4).
9. Procedimiento según una de las reivindicaciones 1 a 8 junto con la reivindicación 5, **caracterizado por que** tras la inicialización el dispositivo de identificación (4) debe desinicializarse antes de una nueva inicialización.
10. Procedimiento según una de las reivindicaciones 1 a 9, **caracterizado por que** el PIN de inicialización (102) o
30 cualquier posible PIN de desinicialización se introducen manualmente en el dispositivo de identificación (4) o se transmiten a través de una interfaz de radio (5).
11. Procedimiento según una de las reivindicaciones 1 a 10, **caracterizado por que** el dispositivo de identificación (4) es un dispositivo para vehículos de un sistema telemático de tráfico.
12. Procedimiento según la reivindicación 11, **caracterizado por que** el dispositivo para vehículos es una unidad de
35 a bordo y el sistema telemático de tráfico es un sistema de peaje de carreteras.
13. Procedimiento según una de las reivindicaciones 1 a 12, **caracterizado por que** la comunicación por radio (5) entre dispositivo de identificación (4) y unidad central (1) es al menos en parte un radioenlace de microondas.
14. Procedimiento según una de las reivindicaciones 1 a 12, **caracterizado por que** la comunicación por radio (5) entre dispositivo de identificación (4) y unidad central (1) es al menos en parte un radioenlace de DSRC.
- 40 15. Procedimiento según una de las reivindicaciones 1 a 12, **caracterizado por que** la comunicación por radio (5) entre dispositivo de identificación (4) y unidad central (1) es al menos en parte un sistema de radiotelefonía móvil, por ejemplo GSM, UMTS.
16. Procedimiento según una de las reivindicaciones 1 a 12, **caracterizado por que** la comunicación por radio (5) entre dispositivo de identificación (4) y unidad central (1) es al menos en parte un enlace de datos inalámbrico, por
45 ejemplo WLAN, WiMAX.

17. Procedimiento según una de las reivindicaciones 1 a 16, **caracterizado por que** la unidad central (1) genera bajo petición para el dispositivo de identificación inicializado (4) también un PIN de activación o de desactivación (502).
18. Procedimiento según una de las reivindicaciones 1 a 17, **caracterizado por que** la unidad central genera bajo petición para el dispositivo de identificación inicializado (4) un PIN de autorización para modificar las autorizaciones y los datos del dispositivo de identificación (4).
19. Procedimiento según una de las reivindicaciones 1 a 18, **caracterizado por que** se devuelve un PIN de confirmación para los datos transmitidos desde el dispositivo de identificación (4) a la unidad central (1).
20. Instalación para la inicialización específica de usuario de dispositivos de identificación (4) in situ, especialmente unidades de a bordo en sistemas de peaje de carreteras, con al menos un dispositivo de identificación (4), que comprende un identificador de dispositivo unívoco (103) en el estado de entrega, una memoria para registrar un identificador de usuario (104) en el estado inicializado, y un visualizador y/o dispositivo transmisor para este último,
- caracterizada por que** la instalación presenta una unidad central (1) con una unidad para la generación del PIN de inicialización (102) a partir de en cada caso una pareja de un identificador de dispositivo (103) y un identificador de usuario asociado (104) y para la transmisión del PIN de inicialización generado (102) a un dispositivo de identificación (4), calculando y almacenando el dispositivo de identificación (4) el identificador de usuario (104) a partir del PIN de inicialización transmitido (102) por medio de su identificador de dispositivo (103) y bajo petición lo visualiza y/o envía.
21. Instalación según la reivindicación 20, **caracterizada por que** el dispositivo de identificación (4) presenta un dispositivo de entrada para la entrada del PIN de inicialización (102) y preferentemente otros PIN de desinicialización, PIN de activación (502), PIN de desactivación (502), PIN de autorización y/o PIN de confirmación.
22. Instalación según una de las reivindicaciones 20 ó 21, **caracterizada por que** la unidad central (1) presenta una unidad de codificación (406) para la codificación del PIN de inicialización y preferentemente otros PIN de desinicialización, PIN de activación, PIN de desactivación, PIN de autorización y/o PIN de confirmación y el dispositivo de identificación (4) un dispositivo de decodificación para la correspondiente decodificación.
23. Instalación según una de las reivindicaciones 20 a 22, **caracterizada por que** el dispositivo de identificación (4) es un dispositivo para vehículos de un sistema telemático de tráfico.
24. Instalación según la reivindicación 23, **caracterizada por que** el sistema telemático de tráfico es un sistema de peaje de carreteras.
25. Instalación según una de las reivindicaciones 20 a 24, **caracterizada por que** la comunicación por radio (5) entre dispositivo de identificación (4) y unidad central (1) es al menos en parte un radioenlace de microondas.
26. Instalación según una de las reivindicaciones 20 a 24, **caracterizada por que** la comunicación por radio (5) entre dispositivo de identificación (4) y unidad central (1) es al menos en parte un radioenlace de DSRC.
27. Instalación según una de las reivindicaciones 20 a 24, **caracterizada por que** la comunicación por radio (5) entre dispositivo de identificación (4) y unidad central (1) es al menos en parte un sistema de radiotelefonía móvil, por ejemplo GSM, UMTS.
28. Instalación según una de las reivindicaciones 20 a 24, **caracterizada por que** la comunicación por radio (5) entre dispositivo de identificación (4) y unidad central (1) es al menos en parte un enlace de datos inalámbrico, por ejemplo WLAN, WiMAX.

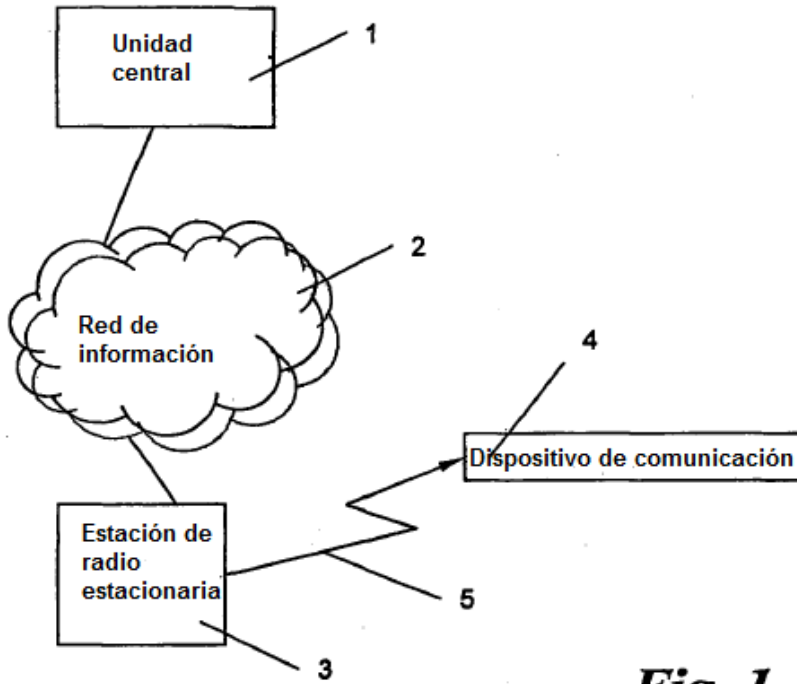


Fig. 1

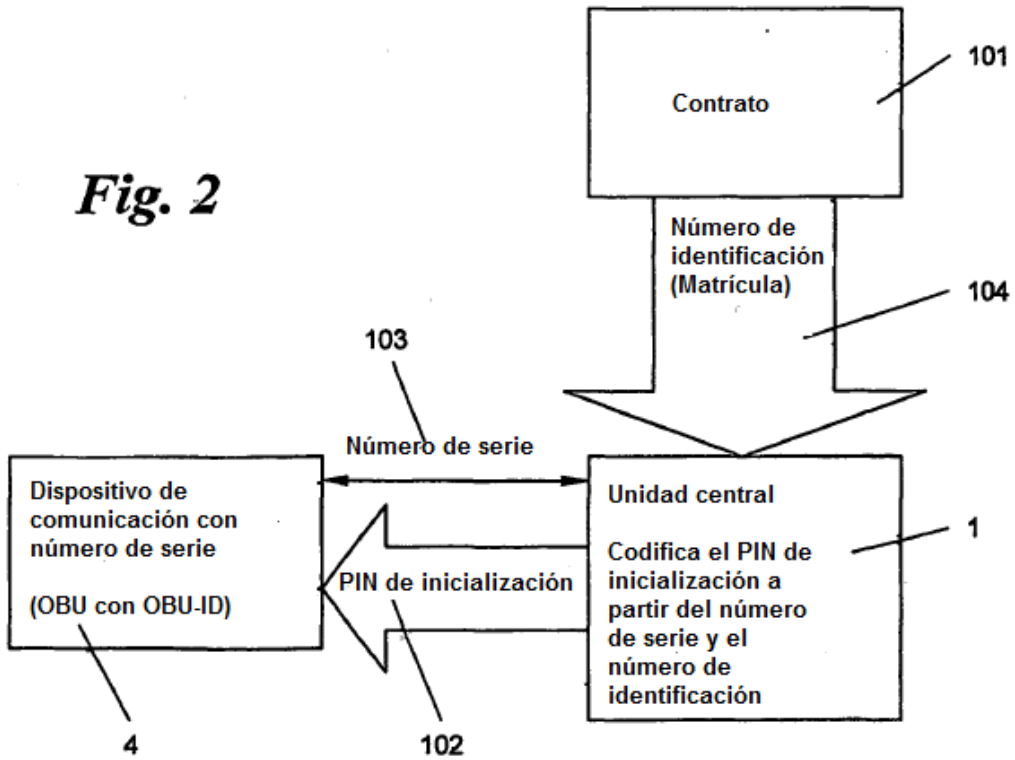


Fig. 2

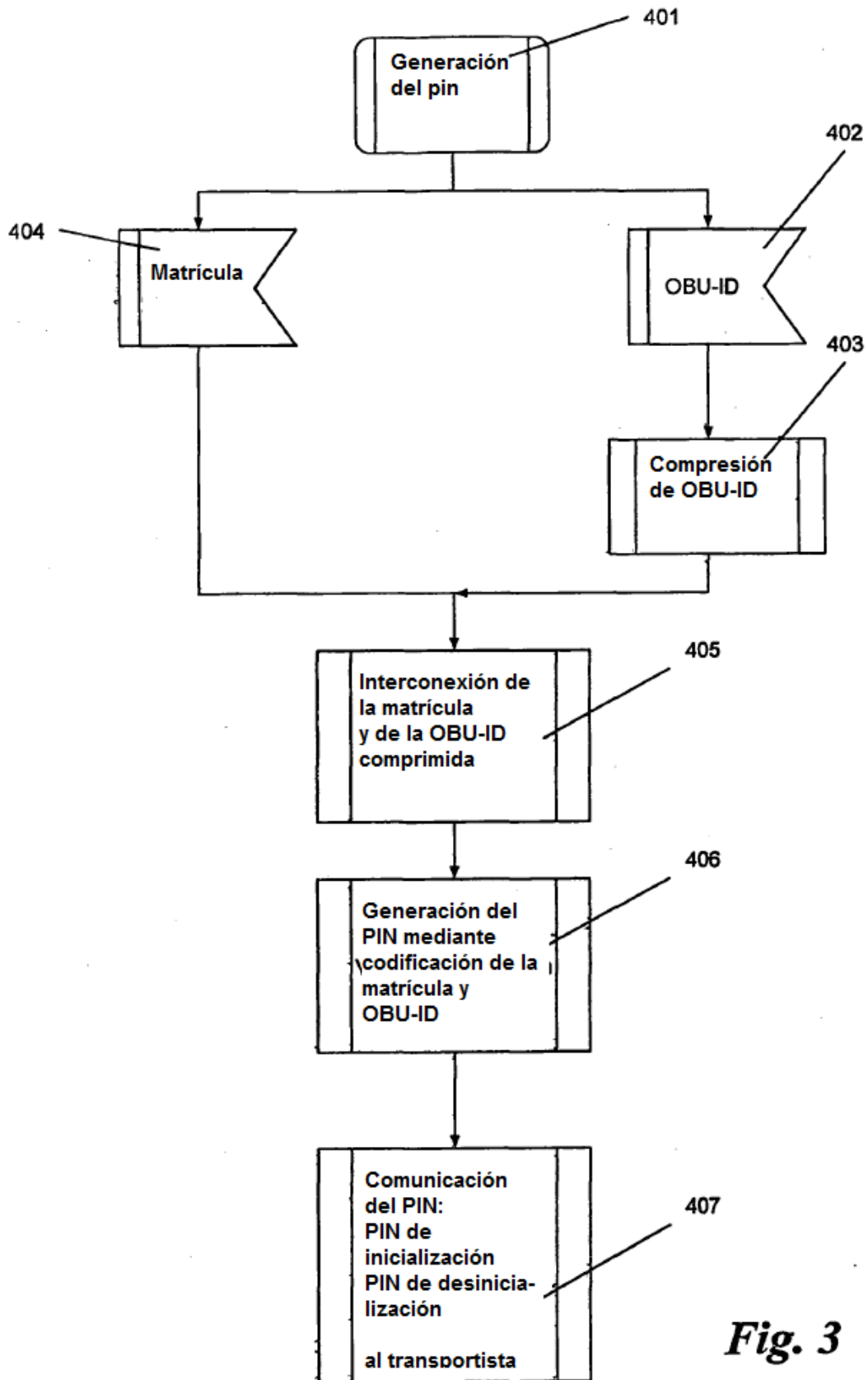


Fig. 3

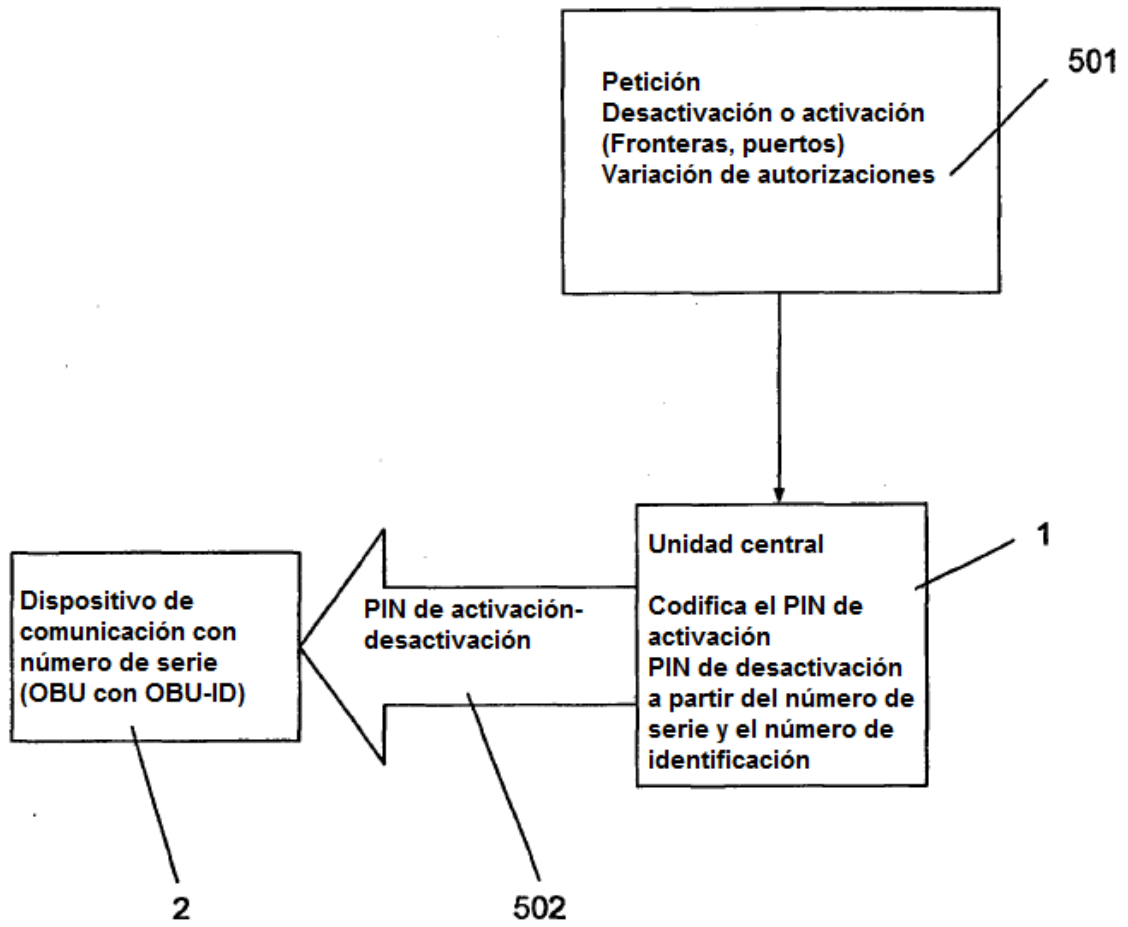


Fig. 4