(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 582 675**

(51) Int. CI.:

G07C 9/00 (2006.01)
B60R 25/24 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.01.2015 E 15700657 (8)**

(97) Fecha y número de publicación de la concesión europea: **08.06.2016 EP 2997550**

(54) Título: **Procedimiento de control de acceso**

(30) Prioridad:

22.05.2014 DE 102014107242

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.09.2016

(73) Titular/es:

HUF HÜLSBECK & FÜRST GMBH & CO. KG (100.0%)
Steeger Strasse 17
42551 Velbert, DE

(72) Inventor/es:

GENNERMANN, SVEN y
BAMBECK, DANIEL

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento de control de acceso

La invención concierne a un procedimiento para el control de acceso por individuos a unidades físicas. En particular, la invención concierne a un sistema y un procedimiento en los que pueden distribuirse y administrarse privilegios de acceso individuales en individuos.

La administración de derechos de acceso o derechos de uso puede encontrarse en muchos lugares en el ámbito de la técnica. Por ejemplo, hay unas complejas jerarquías y esquemas de derechos en la administración de privilegios de acceso en sistemas informáticos. Allí, se otorga el acceso a servicios o datos del sistema informático a un individuo que se identifica él mismo frente al sistema informático por medio de, por ejemplo, un indicativo secreto o datos biométricos. No obstante, si los derechos o privilegios asignados no son suficientes para realizar una acción requerida, ésta se impide por medio de medidas técnicas.

Además, son conocidos sistemas de cierre en los que para, el control de acceso, se identifica un medio de cierre para comprobar el acceso a una función, por ejemplo una entrada a una zona. En sistemas de este tipo se supone frecuentemente que el soporte del medio de cierre es también el autorizado para solicitar la correspondiente función. Conceptos correspondientes se encuentran también en el ámbito de los sistemas de cierre de vehículos, en particular en sistemas de entrada sin llave (Keyless-Entry) y arranque sin llave (Keyless-Go). Allí, un usuario lleva consigo una llave de vehículo designada como emisor de ID. Este emisor de ID contiene informaciones codificadas que legitiman la autorización del emisor de ID (no necesariamente del portador del emisor de ID) frente a un vehículo para ejercer funciones. Por tanto, si se proporciona el emisor de ID a un usuario adicional, éste está también en condiciones de recuperar y activar las funciones del vehículo con el emisor de ID.

En el ámbito de los sistemas de acceso para vehículos son conocidos numerosos sistemas de administración diferentes para permitir el acceso a vehículos. Por ejemplo, el documento US 2013/0259232 A1 describe un sistema para el acoplamiento o emparejamiento (pairing) de un teléfono móvil con un vehículo para poder activar funciones del vehículo con el teléfono móvil.

El documento DE 10 2011 078 018 A1 describe otro sistema para realizar funciones del vehículo, en donde una central telemática realiza una parte de la comunicación con el vehículo.

El documento US2012/0164989 concierne a otro procedimiento y sistema para una función de cierre inalámbrica de un vehículo.

El documento EP 1 910 134 B1 (WO2007/009453 A2) describe un sistema con una administración central que distribuye paquetes de datos como llaves a dispositivos móviles de acceso.

Sin embargo, los sistemas y procedimientos conocidos que hacen posible un acceso a dispositivos técnicos tienen desventajas. En algunos de los sistemas es posible generar o solicitar con dispositivos técnicos, como ordenadores portátiles, teléfonos inteligentes o similares, una autorización para acceder a dispositivos técnicos o para realizar funciones de tal modo que unos atacantes puedan obtener acceso no autorizado a dispositivos (por ejemplo, vehículos) o a sus funciones.

El problema de la invención es facilitar un procedimiento seguro y flexible para hacer posible una administración de privilegios ampliada para el acceso a unidades físicas.

Según la invención, se propone un procedimiento de acuerdo con las reivindicaciones 1-14.

Por tanto, según la invención, con respecto a la configuración de relaciones de comunicación y transportes de datos, se establece una relación cuadrangular en la que, por un lado, la plataforma de control puede ponerse en relación de comunicación tanto con el dispositivo móvil de entrada como también con la unidad de control de acceso de la unidad física controlada. Por su parte, el usuario interactúa con el dispositivo móvil de entrada. En su caso, interactúa también con la plataforma central por medio del uso de vías de comunicación separadas (por ejemplo, ordenador con conexión a internet). La identidad del usuario es un componente de código que hace posible la colaboración de los otros componentes, comprobándose la identidad en diferentes pasos. Estas comunicaciones de los diferentes componentes no se desarrollan necesariamente al mismo tiempo, pero es sustancial que se den recíprocamente las posibilidades de comunicación básicas de estos tres componentes uno con otro. Este concepto asegura una verificación de informaciones obtenidas a partir de una de las transmisiones con un lugar independiente. Como se describe más abajo, esta relación recíproca, en combinación con las peculiaridades del dispositivo móvil de entrada, asegura el acceso de forma especialmente segura y fiable.

Un usuario del procedimiento según la invención tiene acceso al dispositivo móvil de entrada, es decir, por ejemplo, a un teléfono inteligente con la aplicación instalada en él. Aun cuando este aparato pudiera ponerse en comunicación con la unidad de control de acceso del lado del vehículo, la unidad de control de acceso del lado del

vehículo no autorizaría sin más un acceso al vehículo, dado que dicho aparato carece de la legitimación necesaria. El vehículo acepta en efecto no sólo la identidad del dispositivo móvil de acceso como legitimación, sino sólo en combinación con la identidad verificada del usuario. Esta comprobación de identidad tiene éxito sólo cuando el dispositivo móvil de acceso contiene informaciones de la plataforma central que califican el dispositivo móvil de acceso y la persona identificada con éste como usuarios legítimos de la unidad física.

La invención incorpora la administración de los privilegios y las unidades físicas controladas en la plataforma central. Esta administración se substrae así a la manipulación por no autorizados, dado que solamente lugares de confianza pueden realizar modificaciones en la plataforma de control central. No es suficiente manipular los datos de un aparato móvil, dado que el dispositivo de control de acceso verifica los datos de autorización por medio de la conexión con la plataforma central.

La plataforma de control central puede contener informaciones sobre individuos humanos que se identifican frente a esta plataforma de control de manera fiable. No obstante, la plataforma de control central puede administrar también derechos asociados a indicativos anonimizados frente a unidades de control de acceso asociadas, de modo que en la plataforma de control central no haya vinculaciones con personas reales, sino solamente indicativos anonimizados.

Mientras que en sistemas de entrada o administraciones de acceso convencionales la identificación se realiza por medio de un utensilio correspondiente, una etiqueta, una clave, una tarjeta de clave o similares, los privilegios se adjudican y administran según la invención frente a personas o indicativos unívocos. Independientemente de qué medios utilice la persona para legitimarse frente a la plataforma de control central o al dispositivo de acceso, una concesión de privilegios no se vincula a tal medio (teléfono, clave, etc.), sino a la persona reconocida o a la identidad reconocida.

Es esencial para la invención que se almacenen en la plataforma de control central derechos asociados a la identidad de una persona o a un indicativo anonimizado. Estos derechos se refieren respectivamente a cantidades parciales de unidades de control de acceso que se administran por la plataforma central. Por ejemplo, frente a un indicativo pueden prefijarse derechos que son válidos para grupos o bien para todas las unidades de control de acceso asociadas. Otros derechos pueden asociarse a unidades de control de acceso individuales. En el ejemplo de un control de parque móvil esto significa que se asigna el derecho para abrir el vehículo a un miembro del personal de administración, por ejemplo para todos los vehículos del parque móvil, pero sólo se asigna para algunos vehículos el derecho a arrancar el vehículo.

De manera correspondiente, es necesario en primer lugar introducir en la plataforma de control central una inscripción con respecto a la identidad o indicativo anonimizado de un usuario admisible. Estas inscripciones pueden administrarse de manera tradicional con ayuda de un banco de datos que proporcione una interfaz para la consulta. Por medio de una interfaz con otros sistemas, por ejemplo sistemas de ofertantes de coches de alquiler, empresas de seguridad u ofertantes de coches compartidos, puede realizarse también la aceptación de indicativos. Mientras que los sistemas acoplados de los otros ofertantes conocen la identidad de sus clientes, estos transmiten a la plataforma central, por ejemplo, sólo un indicativo anonimizado y los derechos correspondientes. Los datos personales permanecen entonces en el contratista, pero la plataforma central administra los derechos con ayuda del indicativo.

El dispositivo móvil de acceso puede establecer una comunicación de datos con la plataforma de control central. La plataforma de control central facilita al dispositivo móvil de acceso informaciones que hacen posible una legitimación frente a la unidad de control de acceso de una unidad física. Esta puede ser, por ejemplo, un certificado que se expida por la plataforma de control central.

El dispositivo móvil de acceso sirve además para asegurar la identidad del portador frente a una unidad de control de acceso. El dispositivo móvil de acceso está equipado para esto de tal manera que sea posible una identificación fiable del usuario. Esta identificación de un usuario puede realizarse, por ejemplo, por medio de un indicativo sólo conocido para él o por medio de la consulta de datos biométricos, como, por ejemplo, un reconocimiento facial, un análisis de voz o una huella digital. Sólo cuando tiene éxito esta identificación frente al dispositivo móvil de acceso, puede accederse a las informaciones contenidas en el dispositivo móvil de acceso. La naturaleza de la identificación necesaria puede depender de la relevancia de seguridad del derecho solicitado. Si un usuario desea, por ejemplo, la consulta de datos de vehículo (kilometraje, llenado del depósito, etc.) en la proximidad inmediata del vehículo, puede ser suficiente con introducir un PIN en el aparato móvil o un gesto de barrido en un panel de mando del aparato. Para el arranque del vehículo es necesario, por ejemplo, una detección facial. La forma específica de comprobación de identidad que es necesaria para un privilegio específico puede estar archivada en la plataforma central.

Si la identificación frente al dispositivo móvil de acceso es un éxito, se establece una conexión con la unidad física a controlar, más exactamente con la unidad de control de acceso de la unidad física, y las informaciones de entrada, que se han transmitido al menos parcialmente desde la plataforma de control central hasta el dispositivo móvil de acceso, se utiliza para acceder a las funciones de la unidad física.

En este caso, entra en acción la conexión según la invención de la unidad de control de acceso del lado de la unidad física con la plataforma de control central. Por medio de esta conexión es posible que la unidad de control de acceso del lado de la unidad física verifique si las informaciones de acceso transmitidas por el dispositivo de acceso móvil son realmente datos de acceso legítimos para las funciones solicitadas. Los sistemas convencionales no disponen de una conexión de este tipo y, por consiguiente, se deben fiar solamente de la comprobación de los datos por el dispositivo móvil de acceso.

La plataforma de control central conoce tanto las unidades intervinientes en el procedimiento de legitimación como también los privilegios asociados de una persona identificada por medio de estas unidades. La plataforma de control central conoce, por un lado, la identidad o indicativo de un usuario y, por otro lado, la identidad del dispositivo móvil de acceso y la identidad de la unidad de control de acceso en la unidad física. Todos estos dispositivos se identifican con ayuda de características unívocas. Sólo la plataforma de control central dispone de todos los conocimientos para hacer posible un acceso con administración central.

En una configuración sencilla de la invención se establece en la plataforma central un indicativo que caracteriza a un usuario. Para el indicativo se depositan y vinculan datos de un dispositivo móvil de acceso. Por ejemplo, esto puede comprender una IMEI de un aparato móvil. Se almacena además un conjunto de derechos de acceso para el indicativo en la plataforma central. Esta primera identificación se realiza, por ejemplo, intercalando un lugar de confianza, por ejemplo una autoridad o un proveedor de servicios de confianza.

Antes de la primera utilización se envía desde la plataforma central un mensaje al aparato móvil registrado que debe servir como dispositivo móvil de acceso. Se invita al usuario del aparato a que se someta a un primer registro. El usuario proporciona entonces al aparato móvil una serie de informaciones que se aprovechan más tarde para la comprobación de la identidad. Por ejemplo, se almacena un PIN o un gesto de barrido y se registran datos comparativos biométricos (escaneo facial, muestra de voz, huella digital, etc.). Si se realiza esto, pueden recuperarse ya datos de la plataforma central y éstos pueden almacenarse en el dispositivo móvil de acceso. Estos datos pueden contener, por ejemplo, datos de identificación, así como datos que documentan la autenticidad de los datos. Por ejemplo, los datos pueden estar firmados con un certificado de la plataforma central o bien pueden estar codificados. A continuación, el sistema está preparado para su utilización.

Si un usuario quisiera ahora acceder a un dispositivo físico, por ejemplo un vehículo, entonces tiene que encontrarse en la proximidad de la unidad física con la unidad de control de acceso asociada. En primer lugar, debe identificarse entonces frente al dispositivo móvil de acceso. Sólo si esto tiene éxito, el dispositivo móvil de acceso accede generalmente a los datos almacenados en el dispositivo móvil de acceso y transmite los datos relativos a un derecho requerido a la unidad de control de acceso que administra los derechos en una unidad física. Esta transmisión se realiza por medio de una conexión inalámbrica, por ejemplo por Bluetooth o WLAN o NFC. En el lado de la unidad de control de acceso se comprueba si los datos son auténticos. Esto se explica con más detalle a continuación. La unidad de control de acceso accede en este caso a datos que ha obtenido directamente de la plataforma central a través de la conexión de comunicación (directamente en el transcurso de la comprobación de derechos actual o en diferido, ya en un momento anterior).

Por medio de la comunicación recíproca de los componentes anteriormente explicada pueden establecerse limitaciones de acceso extremadamente seguras. Los sistemas convencionales dependían de realizar la comprobación de la autenticidad con ayuda de datos almacenados de manera permanente en la unidad de control de acceso. Se depositaban allí de manera permanente, por ejemplo, certificados de lugares de confianza. La posibilidad según la invención de actualizar los datos hasta una comprobación en directo protege los accesos dado que esta vía de comunicación es independiente de la vía entre el dispositivo móvil de acceso y la plataforma central y también es independiente de datos del dispositivo móvil de acceso que eventualmente se hayan manipulado.

Preferiblemente, el dispositivo móvil de acceso transmite una clave o certificado para el acceso a una determinada unidad de control de acceso asociada de una unidad física. Por ejemplo, una parte de una clave asimétrica se transmite desde la plataforma central a la unidad de control de acceso asociada de la unidad física para verificar el certificado. En este caso, pueden utilizarse procedimientos de codificación asimétricos convencionales, por ejemplo según el concepto de la clave pública y la clave privada.

La ventaja de esta clase de control de acceso está en que, particularmente para la organización y establecimiento de los derechos de acceso, debe existir ciertamente una conexión de todos los participantes en la comunicación con la plataforma de control central, pero son posibles también de forma transitoria en un momento posterior un control de acceso y una función de acceso sin la cooperación de la plataforma de control central. Por ejemplo, la plataforma de control central del dispositivo móvil de acceso y de la unidad de control de acceso en la unidad física puede transmitir informaciones que estén provistas de un certificado de la plataforma de control central. Tanto en el dispositivo de acceso móvil como también en la unidad física y la unidad de control de acceso puede preverse que se confíe, en cualquier caso temporalmente, en una cierta clase de certificados, por ejemplo los certificados expedidos por la plataforma de control central, aun cuando no sea posible transitoriamente tener acceso directo a la plataforma de control central. Para ello, los certificados pueden estar provistos de datos de vencimiento tras cuya

expiración los certificados ya no se aceptan para la legitimación mutua.

Por tanto, para una identidad de usuario o indicativo puede haber numerosos esquemas diferentes con respecto a privilegios para el acceso a diferentes unidades físicas. Pueden prefijarse para una misma identidad diferentes privilegios para diferentes vehículos, por ejemplo en caso de una aplicación de la invención a un control del acceso a un vehículo, si bien la misma identidad personal del usuario es el elemento vinculante. En la plataforma de control puede tener lugar también, en el sentido de una administración de privilegios, una concesión o restricción de derechos global, por ejemplo una restricción con respecto a la clase de utilización o al alcance de la utilización para un determinado vehículo (por ejemplo, la velocidad más alta permitida independientemente del vehículo utilizado).

La invención se explica con más detalle ahora con ayuda de ejemplos de realización que se muestran en las figuras adjuntas.

La figura 1 muestra un esquema de un desarrollo de la comunicación según un primer ejemplo de realización de la invención.

La figura 2 muestra un esquema de una organización y administración de la plataforma central de acuerdo con un segundo ejemplo de realización de la invención.

La figura 3a muestra un primer esquema de un acceso a un vehículo de acuerdo con el segundo ejemplo de realización de la invención.

La figura 3b muestra un segundo esquema de un acceso a un vehículo de acuerdo con el segundo ejemplo de realización de la invención.

En la figura 1 están representadas simbólicamente las diferentes estaciones y unidades funcionales separadas. El trascurso temporal del flujo de mensajes y el intercambio de información están representados por las flechas entre estas unidades. Las unidades físicas controladas son en este ejemplo vehículos en los que una unidad de control de acceso está acoplada con el sistema de control central del vehículo, que controla los derechos para las funciones del vehículo y puede liberar o bloquear funciones.

Antes de que el procedimiento pueda transcurrir en la forma mostrada, puede realizarse un proceso de aprendizaje. Esto significa que pueden facilitarse a la plataforma de control central informaciones relativas a las identidades de los usuarios y los privilegios, así como a los vehículos controlados. Esto puede suceder, por ejemplo cuando una persona se identifica con medios de identificación adecuados (por ejemplo, pase o cédula personal) frente a un lugar de confianza. Este lugar de confianza puede ser el concesionario del vehículo que efectúa una comprobación personal de la identidad y asocia una entrada de identidad correspondiente con una autorización para el acceso a un determinado vehículo.

Estos datos se introducen por el concesionario durante la compra o el mantenimiento del vehículo en un banco de datos que es accesible a la plataforma de control central. Es esencial que las identidades y los privilegios asociados a las identidades se administren en la plataforma de control central y puedan realizarse modificaciones sólo a través de la plataforma de control central. El uso del sistema central puede tener lugar de manera convencional, por ejemplo por medio de una administración de un banco de datos a través de una máscara de entrada que se representa en un navegador de internet. La administración propiamente dicha detrás del extremo frontal puede ser cualquier clase de banco de datos con protección apropiada.

Por tanto, según la invención, la administración de privilegios tiene lugar en un lugar central, a saber, la plataforma de control central. Además, se pueden dar a conocer a la plataforma de control central las unidades físicas de acceso controlado, en este caso los vehículos. Para ello se almacena una identificación unívoca del vehículo en la plataforma de control central. En una administración de flotas o en un concepto de coches compartidos pueden almacenarse en la plataforma de control central todos los vehículos como unidades físicas. A los vehículos están asociadas unívocamente unas respectivas unidades de control de acceso que pueden conectarse con la plataforma de control central.

Finalmente, es todavía esencial que la plataforma de control se dé a conocer también frente a cada aparato móvil de acceso. El aparato móvil de acceso puede asociarse en este caso a un usuario o un indicativo en la plataforma de control central, es decir, puede vincularse con éste. Esto trascurre, por ejemplo, de modo que una persona identificada frente a un lugar de confianza registra el aparato de acceso, en este caso un teléfono inteligente. Por ejemplo, se indica el número de llamada del teléfono inteligente. Puede enviarse entonces un mensaje a este número de llamada desde el lugar de confianza, en cuyo caso el contenido del mensaje tiene entonces que indicarse de nuevo al lugar de confianza por la persona identificada. Por tanto, se cierra un anillo y se verifica que, en efecto, la identificación indicada del aparato móvil de acceso pertenece realmente a la persona identificada.

Además, se describe ahora el procedimiento según la invención en su aplicación, haciéndose referencia a la figura

1.

Al comienzo del procedimiento, un usuario, a través de una actividad de usuario, solicita por el teléfono inteligente obtener acceso a un vehículo, en cuya proximidad se encuentra el usuario con el aparato móvil (por ejemplo, teléfono inteligente o tableta). La entrada de usuario, por ejemplo una recuperación de aplicación en el aparato móvil, está indicada con la flecha de comunicación 1. El dispositivo móvil de acceso verifica ahora la identidad del usuario, para lo cual se realiza en este ejemplo un reconocimiento facial (flecha 2). El usuario tiene su cara en la cámara integrada en el teléfono inteligente y un software que se encuentra en el aparato coteja la cara con los datos biométricos almacenados y autentificados.

Si fracasa esta autentificación frente al aparato móvil, se suspende el procedimiento en este punto y se frustra un intento de acceso al vehículo.

La verificación de la identidad puede realizarse con ayuda de datos almacenados de forma codificada en el aparato móvil, es decir, los datos biométricos almacenados en el aparato móvil pueden presentarse en forma codificada.

Si la identidad frente al aparato móvil se verifica de manera exitosa con el intercambio de comunicación 2, entonces el dispositivo móvil de acceso establece contacto con el vehículo, lo que puede ocurrir por medio de una interfaz NFC estándar o una conexión Bluetooth. La unidad móvil de acceso establece una conexión con la unidad de control de acceso del vehículo en la flecha de comunicación 3. La unidad móvil de acceso solicita en este mensaje, por ejemplo, la activación de una función de vehículo, por ejemplo una apertura de puerta.

A continuación, el aparato móvil notifica a la unidad de control de acceso del vehículo la identidad verificada del usuario. Según este ejemplo, esto sucede con ayuda de certificados que son expedidos por la plataforma de control central y están almacenados en el teléfono inteligente. En particular, pueden utilizarse para ello procedimientos de certificación convencionales con claves públicas y privadas. Por tanto, en el aparato móvil se presenta, por ejemplo, una información de identidad que está firmada con la clave privada de la plataforma de control central. En la unidad de control de acceso en el vehículo se tiene que, de manera semejante a un navegador de internet, las claves de certificado matrices se presentan en la configuración de las claves públicas de la plataforma de control central. Sólo si las informaciones de identidad transmitidas son informaciones certificadas correctamente, puede descodificarse para el vehículo la información sobre la identidad y ésta puede reconocerse como correcta.

Con estas informaciones de identidad la unidad de control de acceso del vehículo se dirige a la plataforma de control en la flecha 4 y consulta sobre los derechos de acceso que se presentan para esta identidad. La unidad de control de acceso dispone para ello de un módulo GSM para la comunicación con la plataforma central por medio de una red de telefonía móvil. La plataforma de control accede en las flechas 5 y 6 tanto a una administración de identidad acoplada con la plataforma de control como también a una administración de privilegios. Estas administraciones no tienen que estar localizadas en el mismo lugar que la plataforma de control central. Por ejemplo, en un concepto de coches compartidos puede estar presente una administración de identidad central que, abarcando varias firmas, sea atendida por varios ofertantes de coches compartidos. Los privilegios que están asociados a estas identidades, es decir, la cuestión de si una persona puede acceder a un vehículo determinado en una flota de vehículos compartidos, pueden almacenarse en las respectivas firmas. Por tanto, si hay diferentes firmas de coches compartidos, la plataforma de control central puede acceder a una administración de identidad central según la unidad de vehículo consultante y a un conjunto de privilegios especial de un determinado ofertante de coches compartidos al que pertenece el vehículo identificado. En la comunicación entre el vehículo y la plataforma de control central puede utilizarse también una comunicación basada en certificados para asegurar la autenticidad de las partes comunicantes.

Por tanto, en la plataforma de control central se determina qué privilegios tiene la persona identificada con respecto al vehículo. Por ejemplo, los privilegios pueden estar configurados de modo que la persona tenga derechos de acceso completos al vehículo para abrir las puertas y arrancar el motor. Alternativamente, puede ocurrir que la persona identificada sea un miembro del taller de un ofertante de coches compartido que tenga básicamente el derecho de abrir todos los vehículos, pero no pueda realizar viajes con velocidades superiores a 20 km/h.

Esta información se transmite de nuevo en 7 por la plataforma de control central a la unidad de control de acceso del vehículo, la cual emite ajustes o señales correspondientes hacia el sistema de control del vehículo. Por consiguiente, el sistema de control realiza entonces, por ejemplo un bloqueo de las puertas y se conecta la autorización para realizar otras funciones del vehículo.

Por tanto, se garantiza en resumen que se efectúe una comprobación de identidad para que pueda utilizarse generalmente el dispositivo móvil de acceso. En segundo lugar, el dispositivo móvil de acceso está equipado con una identificación certificada por la plataforma de control central, lo que garantiza una seguridad frente a todas las unidades físicas controladas con ella.

El certificado en el teléfono inteligente, en otra configuración de este ejemplo de realización, puede estar provisto de un trascurso temporal de corta duración, de modo que el dispositivo móvil de acceso tiene que recuperar

regularmente de la plataforma de control central un nuevo certificado a través de una conexión de datos. La solución basada en certificados descrita de esta manera, vinculada con la comprobación de identidad en el aparato móvil, tiene otras ventajas. El procedimiento fundamental según la invención utiliza una conexión de datos entre el vehículo (unidad de control de acceso) y la plataforma de control central para la verificación de los derechos. Sin embargo, esta conexión no siempre está garantizada, por ejemplo en viajes en la zona con mala calidad de la red de datos o en garajes profundos. No obstante, el procedimiento permite en este caso realizar un control de acceso con ayuda del certificado. Por un lado, el usuario tiene que identificarse frente al aparato móvil, lo que es posible con ayuda de los datos almacenados en el aparato móvil. Si se efectúa esta verificación con éxito, se presentan en el aparato móvil datos de certificación válidos procedentes de la plataforma de control central, cuya validez no ha concluido todavía. Solamente con esta información es posible que se otorguen en el lado del vehículo ciertos privilegios para acceder al vehículo, aun cuando no pueda establecerse ninguna comunicación directa con la plataforma de control central. En el lado del vehículo, allí en la unidad de control de acceso, se presentan, debido a conexiones anteriores con la plataforma central, las informaciones de certificación almacenadas de la plataforma de control central y puede verificarse que, en el caso de un control de identidad realizado con éxito, está presente un certificado válido del dispositivo móvil de acceso. Este certificado puede ser ya suficiente, por ejemplo, para que un usuario pueda acceder al vehículo y, por ejemplo a una velocidad máxima, por ejemplo de 50 km/h, pueda recorrer un trayecto limitado, por ejemplo de un máximo de 2 km, dentro del cual se tiene que establecer una comunicación de la unidad de control de acceso con la plataforma de control central. Tan pronto como se ha establecido la conexión, se efectúan la comprobación completa y la concesión de privilegios completa.

Este concepto de la confianza provisional en base a una certificación es posible debido a que, por un lado, se ha efectuado una identificación del usuario frente al aparato móvil y se ha comunicado también esta identidad al vehículo y, por otro lado, se puede acreditar un ajuste de confianza provisional basado en certificados frente al vehículo. Este procedimiento no sería posible si, como ocurre en procedimientos convencionales, faltara la constatación indubitable de la identidad. Sin embargo, dado que esta identidad es condición previa para acceder generalmente en el aparato móvil al certificado presente allí en forma codificada, el vehículo puede tolerar un otorgamiento de confianza provisional y una concesión de privilegios también provisional. De esta manera, el procedimiento según la invención es superior a procedimientos convencionales que presuponen una conexión forzosa en todo momento con una plataforma de acceso central o bien se fían de un aparato móvil de acceso, por ejemplo una llave o un teléfono inteligente con una aplicación correspondiente, sin que sea necesaria una verificación de la identidad del usuario.

En un aparato móvil pueden estar almacenados para este fin numerosos certificados diferentes, por ejemplo para empresas diferentes de coches compartidos. Además, la concesión de privilegios puede efectuarse también de muy diferentes maneras. Se puede realizar, por ejemplo para obtener una identidad, un ajuste priorizado de privilegios que, por ejemplo, permita en principio solamente la conducción con velocidad reducida, independientemente de la unidad propiamente dicha del vehículo. Por ejemplo, para obtener una identidad de un conductor de cierta edad se puede fijar que éste deberá conducir en principio solamente con una velocidad máxima de, por ejemplo, 120 km/h. Este privilegio de rango superior se comunica al vehículo con independencia de la unidad consultante de coches compartidos o de flotas, de modo que, por ejemplo, un mismo vehículo sea hecho funcionar en modos de vehículo diferentes, según la identidad de la persona accedente. Esta configuración es posible solamente debido a que está presente una plataforma de control central que tiene informaciones de identidad que a su vez pueden estar vinculadas con diferentes ajustes de privilegios, incluso en lugares diferentes. Una misma identidad puede legitimarse por medio de diferentes aparatos móviles en diferentes unidades físicas. Esto es posible solamente debido a que se verifica la identidad de la persona en el aparato móvil y no se reconoce en sí el dispositivo móvil de acceso (el teléfono inteligente) como medio de acceso legítimo. Por consiguiente, el procedimiento es netamente superior a un procedimiento de esta clase para la utilización de simples llaves de encendido, ya que allí no tiene lugar una comprobación de la identidad en combinación con el aparato móvil y, además, en caso de pérdida o de robo, se puede bloquear a distancia un dispositivo móvil de acceso de una manera sencilla para impedir el acceso a un vehículo.

Todas las comunicaciones realizadas en el procedimiento según la invención pueden efectuarse con protecciones convencionales, por ejemplo mediante el establecimiento de conexiones TLS en el caso de comunicaciones basadas en internet.

Una vez que se ha descrito con referencia a la figura 1 un desarrollo de principio y general del procedimiento, se describe ahora otro ejemplo de realización haciendo referencia a las demás figuras.

La figura 2 muestra de manera esquemática la secuencia de accesos a la plataforma central y el establecimiento y la manipulación de datos y vinculaciones allí almacenados. La plataforma central está construida según este ejemplo en una arquitectura convencional MVC (Model-View-Controller). Un usuario puede acceder a la plataforma central a través de una interfaz de web utilizando para ello un navegador correspondiente en su aparato local. La interfaz de web de la plataforma central se proporciona a través de un servidor de web convencional. El plano de datos y las aplicaciones externas están separados del plano del servidor de web. En el plano de datos están almacenados los

datos, por ejemplo en un servidor de banco de datos convencional (servidor SQL).

Teniendo en cuenta la vida útil de un vehículo, que se supone también en este caso como una unidad física, se representa de izquierda a derecha en la figura 2 la secuencia de accesos a lo largo del tiempo de vida del mismo. Durante la fabricación el fabricante tiene primeramente el control físico sobre el vehículo. El fabricante tiene también en este momento acceso a la plataforma central para realizar las primeras entradas referentes al vehículo. Realiza entradas para el vehículo y su dispositivo de control de acceso (SID – Smart Identity Device) y vincula el dispositivo de control de acceso con el vehículo. Gracias a esta vinculación en el lado del fabricante se establece una vinculación unívoca y permanente entre el sistema de vehículo y el SID. Por consiguiente, el sistema de vehículo acepta las órdenes de control del SID vinculado. Después de la terminación del vehículo y de esta vinculación se transporta el vehículo hasta el concesionario, como se muestra en la figura 2.

Tan pronto como se ha suministrado o entregado el vehículo a un usuario, el concesionario establece este usuario como identidad en la plataforma central a través de la interfaz de web y transmite el vehículo al usuario en la plataforma central. Por tanto, el concesionario establece la vinculación entre el vehículo y su SID asociado y un reconocimiento de usuario creado por él.

A continuación, se entrega físicamente el vehículo al nuevo propietario. El propietario establecido por el usuario dispone de los derechos de inscribir además en la plataforma central, para los vehículos y SIDs vinculados a él, otros usuarios como usuarios del vehículo. El propietario del vehículo puede adjudicar deliberadamente derechos a estos otros usuarios, por ejemplo el propietario mismo o los miembros de su familia (pero también clientes de alquiler en el caso de una administración de coches de alquiler) a través de la interfaz de web de la plataforma central. Además, el propietario del vehículo puede decidir qué usuario puede acceder a qué derechos con qué clase de medidas de autentificación y si los derechos están sometidos a una limitación temporal, es decir que resultan inválidos en un momento determinado o después de un periodo de tiempo prefijado. Se trata en este caso de determinar la manera en que un usuario puede acceder al vehículo con un aparato móvil de entrada, en este caso un teléfono inteligente. El propietario del vehículo puede fijar para ello que sea necesaria únicamente la introducción de un PIN para algunas clases de acceso y derechos, mientras que para otros derechos (por ejemplo, el arranque del vehículo) es necesario el reconocimiento de datos biométricos (por ejemplo, reconocimiento facial o reconocimiento de huella digital).

El vehículo puede ser entregado después al respectivo usuario por el propietario del vehículo, lo que se representa como columna derecha en la figura 2. Este usuario del vehículo puede consultar, por ejemplo a través de su teléfono inteligente, después de una identificación con éxito en la plataforma central, qué derechos tiene él con respecto a un vehículo determinado, pero no puede modificar estos derechos.

Se puede reconocer que en los diferentes planos están previstos diferentes derechos de acceso y de variación de los datos en la plataforma central. Mientras que el fabricante puede asignar tanto el vehículo como el SID correspondiente y puede vincular estos, un concesionario ya no puede ejercer influencia alguna sobre los datos del vehículo y del SID. Por el contario, el concesionario puede asignar un propietario a cada vehículo y vincular este propietario con los datos ya existentes del vehículo y del SID. El propietario puede a su vez controlar, establecer y variar los derechos en el vehículo y asignar otros usuarios del vehículo. Finalmente, el usuario puede comprobar solamente sus derechos propios en la plataforma central.

Cada uno de los procesos de asociación puede estar protegido por diferentes conceptos de seguridad. En este ejemplo de realización, al asociar un vehículo a un propietario del mismo por el concesionario, se inicia, por ejemplo, el proceso siguiente:

Si el concesionario ingresa en la plataforma central la orden de que se debe ligar un vehículo a una identidad recién establecida, se almacena entonces primeramente en el banco de datos la vinculación que vincula el propietario con el vehículo y el SID asociado al vehículo. A continuación, se utiliza un número de teléfono móvil archivado para el propietario del vehículo a fin de enviar un mensaje (por ejemplo un SMS) de la plataforma central a este número de teléfono móvil. Por medio de este mensaje se informa al propietario del vehículo de que le ha sido asociado un nuevo vehículo en la plataforma central. Además, se envía un mensaje (por ejemplo nuevamente un SMS) al SID vinculado del vehículo asociado. En este mensaje se invita (activa) al SID para que plantee una consulta a la plataforma central a fin de recuperar de la plataforma central una actualización de derechos de acceso. Esta clase de mensajes de activación se emplea también cuando se modifiquen adjudicaciones de derechos con relación al respectivo SID del vehículo. Esta activación es más segura que el envío directo de ajustes de privilegios, ya que una manipulación de una consulta activada de la plataforma central es más improbable que si el SID aceptara directamente datos transmitidos.

En el ejemplo de realización el SID es inducido por el mensaje recibido a establecer una conexión de datos con la plataforma central a través de un módulo GSM. A continuación, se descargan datos actualizados en el SID, incluyendo los datos referentes al usuario recién inscrito. El SID en el lado del vehículo codifica y almacena los derechos de acceso del usuario en el dispositivo. La conexión se asegura mediante la comprobación de certificados,

pudiendo estar archivados ya en el SID de parte del fabricante certificados matrices de la plataforma central.

De manera análoga, la adjudicación de derechos por el usuario para su vehículo puede desarrollarse en un momento posterior. Tan pronto como el usuario varía en la plataforma central adjudicaciones de derechos para sus vehículos, la plataforma central envía al SID correspondiente del vehículo un mensaje que activa una actualización de la adjudicación de derechos en el SID del vehículo.

En este caso, es posible también en el plano del usuario vincular derechos de acceso con consignas de tiempo o duraciones de validez, es decir, adjudicar temporalmente derechos a otros usuarios del vehículo. La adjudicación de los derechos para el propietario del vehículo se efectúa en principio de manera permanente, si bien el propietario puede transmitir también los derechos al usuario de una manera temporalmente limitada o bien para intervalos de tiempo. Tales limitaciones temporales se comunican después por la plataforma central al SID del vehículo y se almacenan también allí en forma codificada. Por ejemplo, puede estar previsto que el SID no admita un nuevo arranque del vehículo después de vencidos los derechos de uso o limite fuertemente la velocidad máxima.

Aparte de esta adjudicación fundamental de derechos dentro de la plataforma central y de la transmisión de derechos de la plataforma central al SID de un vehículo, es relevante también la interacción entre el usuario y su aparato móvil, especialmente un teléfono inteligente.

En el teléfono inteligente se ejecuta una aplicación que puede desarrollar una comunicación tanto con la plataforma central como con el SID del vehículo. A este fin, se transfiere, por ejemplo, una aplicación por el concesionario al aparato del propietario del vehículo o bien se pueden descargar aplicaciones de las plataformas y tiendas virtuales pertinentes para diferentes sistemas operativos.

En la primera utilización de la aplicación en un aparato móvil se invita al usuario a introducir un nombre de usuario y una contraseña. Se utilizan estos datos para calcular un valor hash que se transmite a la plataforma central. La comunicación con la plataforma central puede efectuarse entonces a través de un modo de transmisión usual, por ejemplo a través de un protocolo http (codificado). La plataforma central comprueba si el usuario existe en su banco de datos, y calcula también un valor hash con ayuda de los datos referentes al nombre del usuario y la contraseña almacenados en la plataforma central. Siempre que este cotejo de nombre de usuario y valor hash arroje una autentificación positiva, se transmiten a la aplicación por la plataforma central los SIDs y vehículos asociados al usuario. Estos datos se almacenan codificados por la aplicación en el teléfono inteligente para el reconocimiento del usuario.

Una vez que se ha comprobado ahora que el usuario es en principio auténtico, se le invita, para asegurar los derechos de acceso, a que aprenda diferentes métodos de autentificación en el teléfono inteligente. En particular, se le invita a entregar un PIN unívoco, ejecutar un gesto de muestra sobre la pantalla del teléfono inteligente y realizar un reconocimiento facial o un reconocimiento de huella digital.

Estos diferentes métodos de autentificación representan diferentes etapas seguras para el acceso a funciones diferentes del vehículo. En la plataforma central se prefija cuál de las autentificaciones o bien qué vinculación de estas autentificaciones es suficiente para el acceso a una función del vehículo.

A continuación, es posible para el usuario de la aplicación en el teléfono inteligente activar por primera vez para una operación de acceso uno de los vehículos que fue notificado por la plataforma central a la aplicación como vehículo asociado. Si el usuario selecciona un vehículo para activarlo, la aplicación envía una consulta de activación a la plataforma central y la plataforma central establece un código aleatorio que es válido para un periodo de tiempo limitado. Este código de activación aleatorio se envía al teléfono móvil del usuario por medio de un mensaje separado. El usuario tiene que introducir el código de activación del mensaje separado en la aplicación y la aplicación devuelve este código de activación a la plataforma central. De esta manera, se asegura que el usuario reciba realmente el mensaje por la vía que está almacenada en la plataforma central.

La plataforma central valida el código de activación y envía una confirmación correspondiente a la aplicación en el teléfono inteligente. La aplicación en el teléfono inteligente establece entonces un par de claves, constituidas por una clave privada y una clave pública, y establece una CSR (Certificate Signing Request) que se envía a la plataforma central. La plataforma central recibe esta CSR y genera un certificado X509 para el usuario y la combinación de SID y vehículo asociada al mismo. Esto significa que para cada usuario y cada combinación de vehículo/SID se establece un certificado que contiene tanto la ID del usuario como el indicativo del SID en el certificado. Estos datos del certificado se devuelven a la aplicación en el teléfono inteligente, juntamente con la dirección Bluetooth del SID del vehículo en cuestión.

Los datos son recibidos por la aplicación y almacenados en forma codificada. La aplicación dispone entonces de la dirección Bluetooth del SID asociado, lo que permite un emparejamiento de la aplicación en el teléfono inteligente y el SID asociado a través de Bluetooth.

Lo que antecede sobre este ejemplo de realización describe todas las actuaciones de preparación que deben

realizarse solamente una vez o al modificar los derechos de acceso. Asimismo, estos procesos pueden realizarse parcialmente si el propietario o el usuario del vehículo quisiera utilizar un nuevo teléfono móvil para acceder a un vehículo existente.

En la práctica, el acceso cotidiano con el sistema inicialmente inscrito a un vehículo es con mucho el caso más frecuente. A este fin, se establece una conexión inalámbrica de corte alcance entre la aplicación en el aparato móvil y el SID en un vehículo. Este proceso de emparejamiento trascurre de la manera conocida, y eventualmente es necesaria al principio una confirmación del acoplamiento de ambos aparatos, lo que depende de la clase del sistema operativo utilizado y de los ajustes en un teléfono inteligente. Sin embargo, el teléfono inteligente ha obtenido ya los datos de dirección del SID para la conexión Bluetooth cuando se activan un vehículo y su SID asociado, de modo que se puede suprimir también una confirmación de esta clase.

Cuando se ha realizado con éxito un emparejamiento de este tipo, el usuario, manteniendo abierta la aplicación, puede acceder a funciones del vehículo, por ejemplo a través de una interfaz gráfica que se visualiza sobre la pantalla de un teléfono inteligente sensible al tacto.

Las funciones del vehículo pueden afectar, por ejemplo, a cerraduras de puertas, al arranque del motor, al arranque de una calefacción o una calefacción de estacionamiento, a la apertura de ventanillas, a la apertura del portón trasero o a la conexión de dispositivos de iluminación.

La figura 3a muestra a título de ejemplo un desarrollo de acceso cuando un usuario quisiera acceder con su teléfono inteligente a una función del vehículo. Este diagrama debe leerse de arriba abajo.

El usuario abre en su teléfono móvil la aplicación para acceder a su vehículo y selecciona el comando para desbloquear las puertas. La aplicación en el teléfono inteligente comprueba con ayuda de los datos almacenados qué autentificación por el usuario es necesaria para esta función y solicita esta autentificación al usuario siempre que la autorización en esta etapa no se hubiera realizado todavía al poner en marcha la aplicación.

La aplicación determina seguidamente que no está acoplada con el SID del vehículo activado y establece primeramente una conexión Bluetooth con el SID del vehículo. A través de la conexión Bluetooth se establece una conexión de datos segura, es decir, a través de un plano de protocolo por encima del Bluetooth. La aplicación retransmite entonces al SID el comando para abrir las puertas. Sin embargo, en este ejemplo no se conoce todavía el usuario por parte del SID (el SID no está aún activado para este usuario). Por consiguiente, el SID responde al teléfono móvil indicando que el usuario no es conocido. La aplicación invita seguidamente al SID a activar el usuario, tras lo cual el SID plantea una consulta de activación en la plataforma central a través del módulo GSM. La plataforma central confirma al SID que el usuario está legitimado para el vehículo y ha activado el SID y envía informaciones de entrada correspondientes.

Seguidamente, el SID confirma al teléfono móvil la activación del usuario. La aplicación en el teléfono inteligente repite luego la solicitud de apertura de las puertas, lo que es confirmado por el SID, y, por último, se desbloquean las puertas para el usuario.

El escenario descrito es el escenario del peor caso en el que el desarrollo puede comprender todos los pasos mostrados. Sin embargo, es usual que, al aproximarse el usuario al vehículo, se establezca ya una conexión Bluetooth y el usuario sea ya también conocido en el SID. Se desarrolla entonces el procedimiento con claramente menos pasos y con extraordinaria rapidez. Este desarrollo de la manera usual se muestra en la figura 3b.

El modo de proceder según la invención hace posible una administración extraordinariamente segura y una gestión flexible de derechos de usuario, por ejemplo en parques móviles, pero también cuando se utilizan otras unidades físicas, por ejemplo máquinas o similares. Gracias a los canales de comunicación separados entre el SID en cada unidad física y la plataforma central, por un lado, y entre la plataforma central y un dispositivo móvil (teléfono inteligente), por otro lado, se aumenta la seguridad. Como quiera que, además, un usuario es invitado todavía a autentificarse en un aparato móvil de acceso para poder acceder generalmente a los datos archivados en el aparato móvil en forma codificada, se añade una etapa de seguridad adicional.

La memoria codificada en el aparato móvil de acceso (especialmente un teléfono inteligente) contiene, por ejemplo, las informaciones sobre vehículos activados, las informaciones sobre los SIDs acoplados con los vehículos, especialmente sus direcciones Bluetooth y sus códigos de conexión, los certificados de cliente y las claves para la comunicación y la lista de los métodos de autentificación en presencia de solicitudes de comandos, así como las informaciones de usuario, especialmente nombres de usuarios y contraseñas.

En la memoria de los SIDs para cada vehículo se almacenan, por ejemplo, de manera codificada, la clave privada del SID, un certificado del SID y un certificado y/o una clave pública de la plataforma central.

El almacenamiento de estos datos en los dispositivos hace posible una clase flexible de control de acceso. En particular, las informaciones de certificados almacenadas en el SID de un vehículo se pueden utilizar para establecer

una relación de confianza temporal entre el vehículo y un usuario accedente con un teléfono inteligente. La aplicación del usuario recibe de la plataforma central, como se ha descrito anteriormente, informaciones de acceso para un SID. En este caso, la información se codifica con una clave privada de la plataforma central. El SID en el lado del vehículo contiene informaciones sobre los certificados matrices de la plataforma central. Incluso en el caso en el que el SID no tiene acceso a la plataforma central, se puede otorgar en cualquier circunstancia con esta construcción un acceso temporal de un usuario a un vehículo. En efecto, si el SID puede verificar positivamente con ayuda de las informaciones almacenadas referentes a certificados matrices que las informaciones enviadas por el teléfono inteligente al SID a través de la aplicación fueron realmente firmadas por la plataforma central, se puede establecer entonces una relación de confianza temporal. Esto es relevante especialmente cuando se quiera proporcionar acceso, por ejemplo, a un nuevo usuario en un coche de alquiler, pero el coche de alquiler está estacionado, por ejemplo, en una zona con mala conexión de telefonía móvil. Si el cotejo del certificado en el SID del vehículo tiene éxito, se puede otorgar entonces acceso del usuario al vehículo y el vehículo consultará sobre los derechos de usuario completos tan pronto como exista una conexión a la red.

REIVINDICACIONES

1. Procedimiento de control del acceso a dispositivos físicos,

en el que cada dispositivo físico está equipado con una unidad de control de acceso que puede bloquear y liberar el acceso a funciones de la unidad física,

en el que está formada una plataforma de control central,

en el que entre la plataforma de control central y las unidades de control de acceso pueden establecerse conexiones de comunicación inalámbricas,

en el que están presentes dispositivos de acceso móviles que pueden ser llevados consigo por un usuario y pueden producir conexiones de comunicación inalámbricas con las unidades de control de acceso y la plataforma de control central,

de tal manera que, en presencia de un acceso de un usuario utilizando el dispositivo de entrada móvil a un dispositivo físico, se realiza una comprobación de la identidad del usuario, identificándose el usuario frente al dispositivo de entrada móvil,

en el que, tras la comprobación exitosa de la identidad, se establece una conexión de comunicación inalámbrica entre el dispositivo de entrada móvil y la unidad de control de acceso del dispositivo físico,

en el que se transmite por el dispositivo móvil de entrada al menos la identidad del usuario y datos de entrada unívocos a la unidad de control de acceso,

caracterizado por que

la unidad de control de acceso, con ayuda de informaciones recibidas y con ayuda de informaciones adicionales que la unidad de control de acceso recibe de la plataforma de control central, determina y proporciona al usuario derechos de acceso al dispositivo físico,

en cuyo caso la unidad de control de acceso, tras la obtención de las informaciones del dispositivo de acceso móvil, envía a la plataforma de control central las informaciones sobre la identidad del usuario y un distintivo unívoco de la propia unidad de control de acceso a través de una conexión de comunicación inalámbrica, seguidamente la plataforma de control central determina los derechos de acceso del usuario identificado a la unidad física asociada a la unidad de control de acceso y la plataforma de control central transmite las autorizaciones de acceso a la unidad de control de acceso a través de la conexión de comunicación inalámbrica y la unidad de control de acceso otorga los derechos de acceso con ayuda de estas informaciones.

2. Procedimiento según la reivindicación 1, en el que la unidad de control de acceso transmite también a la plataforma de control central informaciones sobre el distintivo unívoco del dispositivo móvil de entrada.

3. Procedimiento según la reivindicación 1, en el que la unidad de control de acceso obtiene y almacena además a intervalos temporales, independientemente de los accesos del usuario, informaciones procedentes de la plataforma de control central, y en el que la unidad de control de acceso, con ayuda de estas informaciones almacenadas y las informaciones obtenidas del dispositivo móvil de entrada durante el intento de acceso, determina y otorga los derechos de acceso.

4. Procedimiento según una de las reivindicaciones anteriores, en el que la identificación del usuario frente al dispositivo móvil de entrada se realiza con ayuda de datos biométricos, en particular realizando un reconocimiento facial y/o realizando un reconocimiento de voz y/o un reconocimiento de huella digital.

5. Procedimiento según una de las reivindicaciones anteriores, en el que el dispositivo móvil de entrada está implementado en un aparato de comunicación móvil, en particular un teléfono inteligente, en el que se ejecuta una aplicación que realiza la comprobación de la identidad y la comunicación entre el aparato de comunicación móvil y la unidad de control de acceso.

6. Procedimiento según una de las reivindicaciones anteriores, en el que entre el dispositivo móvil de entrada y la plataforma de control central se establece una conexión de comunicación y en el que se transmiten informaciones de certificado por la plataforma de control central al dispositivo de entrada móvil, estando las informaciones de certificación asociadas a respectivas identidades de usuario.

7. Procedimiento según la reivindicación 6, en el que entre una unidad de control de acceso y la plataforma de control central se establece una conexión de comunicación y en el que la plataforma de control central transmite a la unidad de control de acceso informaciones de certificado para su almacenamiento, las cuales permiten la comprobación de la autenticidad e integridad de las informaciones que se transmiten de un dispositivo móvil de

entrada a la unidad de control de acceso.

8. Procedimiento según la reivindicación 7, en el que la plataforma de control central transmite al dispositivo móvil de entrada una confirmación de la identidad, estando al menos una parte de la confirmación cifrada con una clave privada de la plataforma de control central, y en el que la unidad de control de acceso obtiene de la plataforma de control central una clave pública con cuya ayuda pueden verificarse las informaciones de identidad obtenidas de los dispositivos móviles de entrada.

9. Procedimiento según una de las reivindicaciones 6 a 8, en el que las informaciones de certificado transmitidas por la plataforma de control central al dispositivo móvil de entrada están provistas de una información de desarrollo temporal que indica el tiempo de validez de la certificación.

10. Procedimiento según una de las reivindicaciones anteriores, en el que la unidad de control de acceso, cuando no puede establecerse ninguna comunicación de datos con la plataforma de control central, verifica con las informaciones almacenadas la validez de un certificado a partir de la transmisión por el dispositivo móvil de entrada y, en caso de un certificado válido, otorga un sentido prefijado de derechos de acceso al usuario identificado.

11. Procedimiento según la reivindicación 10, en el que el sentido de derechos de acceso permite una utilización limitada de la unidad física, incluyendo en particular una limitación temporal o funcional.

12. Procedimiento según una de las reivindicaciones anteriores, en el que se utilizan vehículos en calidad de dispositivos físicos.

13. Procedimiento según una de las reivindicaciones anteriores, en el que, para cada combinación de usuario y unidad física, se elabora un certificado unívoco que se almacena en el dispositivo móvil de entrada.

14. Procedimiento según una de las reivindicaciones anteriores, en el que la plataforma de control central para cada unidad física almacena una dirección unívoca de la unidad de control de acceso asociada para el establecimiento de una conexión inalámbrica de corto alcance, en particular una conexión Bluetooth, y transmite esta dirección al dispositivo móvil de entrada.

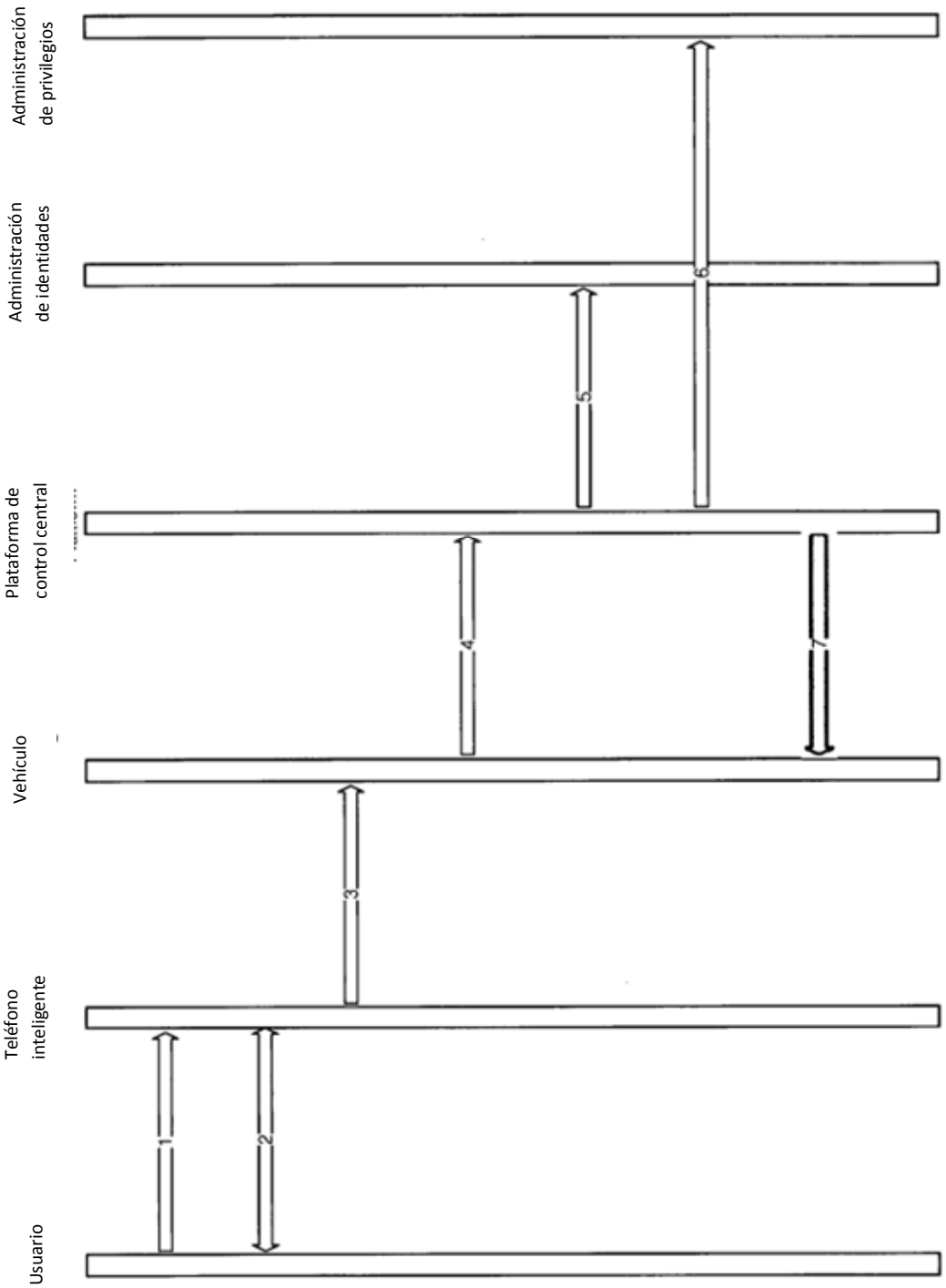

Administración de privilegios
Administración de identidades
Plataforma de control central
Vehículo
Teléfono inteligente
Usuario
1
2
3
4
5
6
7

Fig. 1

Fig. 2

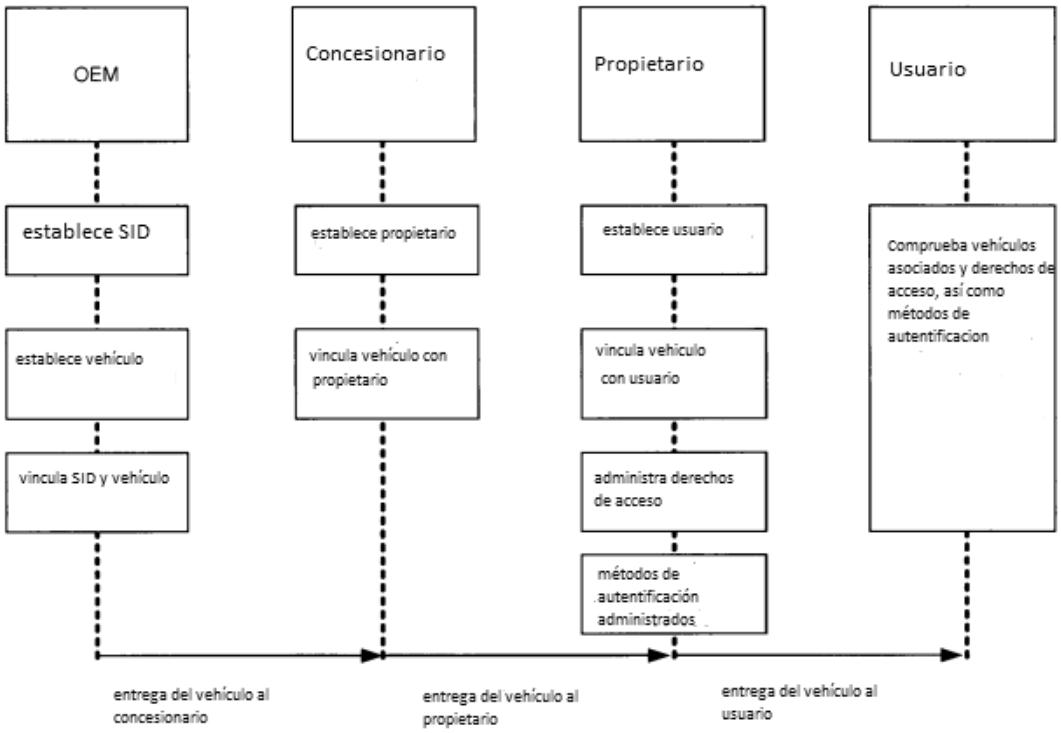

OEM
Concesionario
Propietario
Usuario
establece SID
establece vehículo
vincula SID y vehículo
establece propietario
vincula vehículo con propietario
establece usuario
vincula vehículo con usuario
administra derechos de acceso
métodos de autentificación administrados
Comprueba vehículos asociados y derechos de acceso, así como métodos de autentificacion
entrega del vehículo al concesionario
entrega del vehículo al propietario
entrega del vehículo al usuario

Fig. 3a

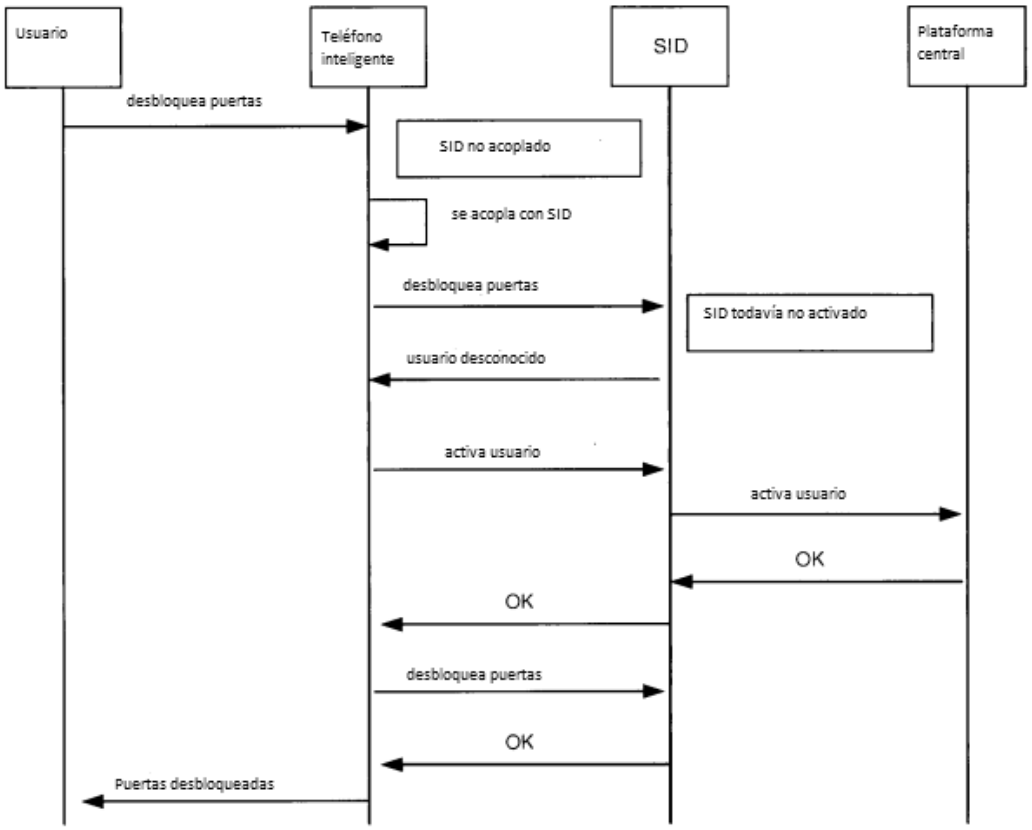
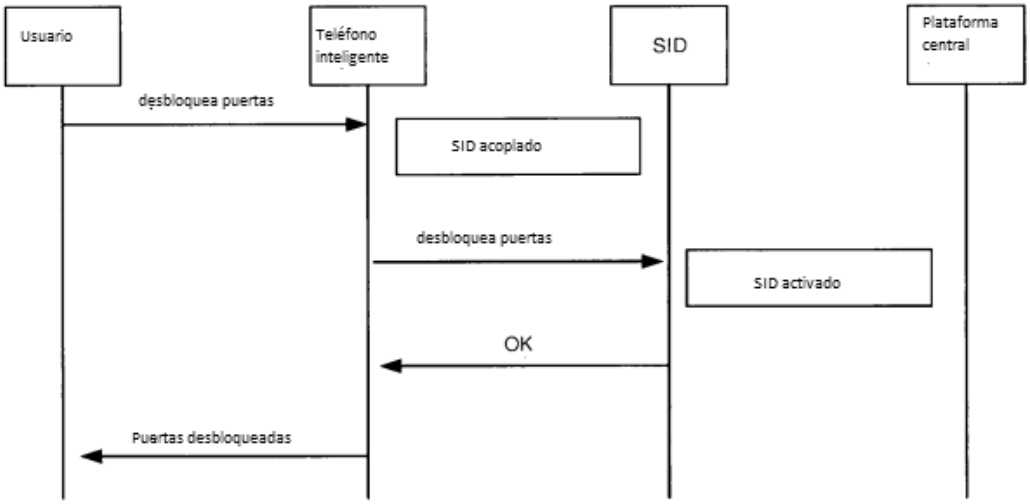

Usuario
Teléfono inteligente
SID
Plataforma central
desbloquea puertas
SID no acoplado
se acopla con SID
desbloquea puertas
SID todavía no activado
usuario desconocido
activa usuario
activa usuario
OK
OK
desbloquea puertas
OK
Puertas desbloqueadas

Fig. 3b


Usuario
Teléfono inteligente
SID
Plataforma central
desbloquea puertas
SID acoplado
desbloquea puertas
SID activado
OK
Puertas desbloqueadas