(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 744 396**

(21) Número de solicitud: 201830840

(51) Int. CI.:

G06Q 30/06 (2012.01)
H04L 9/32 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

24.08.2018

(43) Fecha de publicación de la solicitud:

24.02.2020

(71) Solicitantes:

SEAT, S.A. (100.0%)
Autovía A-2, Km. 585
08760 MARTORELL (Barcelona) ES

(72) Inventor/es:

HERNÁNDEZ GÓMEZ, Ana Cristina y
CASTELLÀ ROCA, Jordi

(74) Agente/Representante:

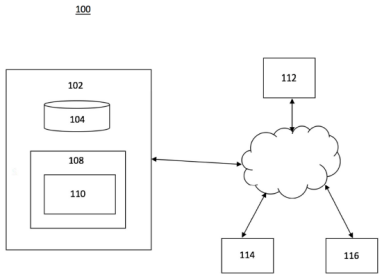
SALVÀ FERRER, Joan

(54) Título: **SISTEMA Y MÉTODOS PARA EL MANEJO DE CLAVES DE ACCESO Y DE TITULARIDAD PARA VEHÍCULOS, Y PARA FACILITAR EL USO COMPARTIDO DE VEHÍCULOS**

(57) Resumen:

Sistemas y métodos para el manejo de llaves digitales para vehículos motorizados, en particular para el manejo de acceso de tal manera que se facilita el acceso y uso compartido de vehículos. Los sistemas y métodos se basan en cadenas que registran las diferentes transacciones, en particular una cadena de acceso que registra cada instancia de concesión de acceso a un vehículo a un usuario identificado, y una cadena de titularidad la cual registra cada instancia de registro o cambio de titularidad. Dicho sistema comprende un servidor con un procesador programado mediante un programa informático que cuando es ejecutado provoca al servidor mediar diferentes tipos de transacciones relacionadas al manejo de llaves o claves, permisos de acceso, y titularidad de vehículos.

Fig. 1



ES 2 744 396 A1

DESCRIPCIÓN

SISTEMA Y MÉTODOS PARA EL MANEJO DE CLAVES DE ACCESO Y DE TITULARIDAD PARA VEHÍCULOS, Y PARA FACILITAR EL USO COMPARTIDO DE VEHÍCULOS

Sector de la técnica

La presente invención se refiere en general, en un primer aspecto, a un sistema y protocolos para facilitar el uso compartido de vehículos.

Un segundo aspecto de la invención se refiere a métodos de facilitación de uso compartido de vehículos.

La invención se aplica especialmente en plataformas para el uso compartido de vehículos.

Estado de la técnica anterior

El uso compartido de vehículos ha ido aumentado en popularidad, en parte por incentivos ambientales como por problemas de congestión de tráfico en los entornos urbanos. El uso compartido es mayormente conocido en el ámbito de vehículos para uso público, donde vehículos son proporcionados al público por empresas de alquiler de vehículos.

Además, existe el uso compartido convencional dentro de núcleos familiares o entre personas conocidas. Por tal razón existe interés en proveer alternativas prácticas y mas eficientes que el pase tradicional de llaves físicas.

Esto ha dado paso a la utilización de sistemas de acceso basados en llaves o claves digitales como una manera eficiente y práctica de facilitar el uso compartido de un vehículo.

Sin embargo, el manejo de llaves digitales conlleva riesgos de seguridad inherentes. Por tal manera, existe una necesidad de mecanismos seguros y robustos para generar, transmitir, y revocar llaves digitales.

Un ejemplo de acceso digital basado en llaves o claves criptográficas es conocido, en donde dueños de vehículos reciben acceso mediante una ficha de acceso generado por un servidor de claves. Este tipo de acceso se basa en llaves pre-compartidas entre el servidor y el vehículo. Por otra parte, los usuarios delegados deben proveer una ficha adicional, generada por el dueño. La seguridad de la ficha de delegación depende en la integridad de las llaves del dueño.

El control de accceso basado en fichas también también ha sido propuesto, dicho sistema implica la autenticación de *2-factores* donde los usuarios obtienen y manejan factores de

autenticación por separado, primero durante el registro del usuario y después durante la reserva del vehículo.

La soluciones conocidas utilizan y dependen de criptografía de claves simétricas como base de seguridad. Por tal razón, el uso de este tipo de técnicas en una plataforma para el uso compartido de vehículos puede exponer al sistema a fraude cuando un secreto compartido es obtenido irregularmente por una tercera parte.

Diferencia con la técnica anterior

Un sistema de manejo de claves es propuesto por Elkins, M., en "*A peer-to-peer approach to digital key sharing for vehicle access control*", el cual implica un esquema de car-sharing basado en *Public Key Infrastructure* (PKI) que no depende en secretos pre-compartidos. Sin embargo, este sufre de desventajas como la utilización de cadenas de datos largas o de códigos de barra impresos, los cuales ambos se prestan fácilmente para fraude en caso de manejo inapropiado.

Aparece por tanto necesario ofrecer una alternativa al estado de la técnica que proporcione un sistema que permita el manejo y cambio de titularidad, así como manejo de permisos de acceso a vehículos, y que no adolezca de los inconvenientes de los sistemas conocidos en el estado de la técnica.

Explicación de la invención

La presente invención propone remediar las vulnerabilidades del estado de la técnica mediante mejoras convenientes que ventajosamente evitan la dependencia de elementos para proporcionar a los usuarios con una prueba o evidencia de titularidad vulnerables a explotación mediante fraude.

Con tal fin, un aspecto de la presente invención se refiere a sistemas y métodos para el manejo de llaves de vehículos motorizados, el cual comprende un servidor con un procesador programado mediante un programa informático que cuando es ejecutado provoca al servidor mediar diferentes tipos de transacciones relacionadas al manejo de llaves, permisos de acceso, y titularidad de vehículos. Esto dentro del marco de una plataforma que además habilita el uso compartido de vehículos. En esta divulgación los términos llave y clave se usan indistintamente (para referirse a llaves digitales).

Uso compartido de vehículos

En un primer ejemplo de realización, la invención comprende un sistema que comprende un servidor con un procesador programado mediante un programa informático que cuando es ejecutado provoca al servidor mediar la concesión de permiso de acceso a un primer vehículo a un segundo usuario en respuesta a una solicitud de un primer usuario

La mediación del servidor comprende al menos los actos o etapas de recibir, de parte de un primer usuario, una cadena de permiso de acceso (p) a dicho primer vehículo, la cadena incluyendo una concatenación con al menos un registro conteniendo una autorización de acceso al primer vehículo a un segundo usuario generada por el primer usuario, después enviar dicha cadena de permiso de acceso (p) al segundo usuario, recibir, de parte del segundo usuario, la cadena de permiso de acceso (p, p+1) actualizada con una concatenación de un registro conteniendo una solicitud de firma de certificado, enviar dicha cadena de permiso de acceso (p, p+1) a una autoridad certificadora para la concesión de un certificado digital acreditando el acceso al primer vehículo al segundo usuario, recibir, de parte del segundo usuario, la cadena de permiso de acceso (p, p+1, p+2) concatenada con un registro conteniendo la aceptación de acceso del segundo usuario, firmada con el certificado digital de acceso, enviar dicha cadena de permiso de acceso (p, p+1, p+2) al primer usuario, recibir, de parte del primer usuario, la cadena de permiso de acceso (p, p+1, p+2, p+3) actualizada con una concatenación de un registro conteniendo confirmación del permiso de acceso, y enviar dicha cadena de permiso de acceso (p, p+1, p+2, p+3) al segundo usuario.

El primer usuario puede ser, por ejemplo, el titular de dicho primer vehículo un usuario que posee un certificado digital acreditándole titularidad de dicho primer vehículo.

Dicha concatenación puede comprender una computación de al menos una autorización, una firma digital del primer usuario que comprende un cifrado de la autorización, y un certificado digital acreditando el acceso al vehículo del primer usuario.

El registro de autorización de acceso puede comprender al menos una orden de autorización de acceso (F6); una identificación del primer vehículo como objeto del permiso de acceso, un certificado digital acreditando la identidad del segundo usuario, y un perfil del permiso de acceso.

Dicho perfil de acceso puede incluir al menos uno o más atributos definiendo respectivamente uno o más de: un tiempo de duración del permiso de acceso, una geocerca, una velocidad máxima, y una configuración del vehículo.

El servidor puede recibir dicha cadena de permiso de acceso de parte del primer usuario y del segundo usuario mediante dispositivos clientes.

Cambio de titularidad del vehículo

En un ejemplo de realización, el programa informático, cuando es ejecutado, además provoca al servidor de manejo de llaves mediar un cambio de titularidad a un primer vehículo, en respuesta a una solicitud por parte de un primer titular que posee un primer certificado digital acreditándole titularidad al primer vehículo.

Dicha mediación puede comprender los actos o etapas de: recibir, de parte del primer titular, una cadena de titularidad (z) que comprende al menos un registro correspondiente al registro de titularidad más reciente en una cadena de titularidad del primer vehículo, enviar dicha cadena de titularidad (z) al segundo titular, recibir, de parte del segundo titular, una cadena de titularidad actualizada con una concatenación de un registro conteniendo al menos un certificado digital firmado (z, z+1), verificar dicha cadena de titularidad actualizada (z, z+1),concatenar, en base al resultado positivo de la verificación, un registro (z+2) incluyendo una autorización firmada digitalmente a la cadena actualizada de titularidad, generando así una cadena de titularidad actualizada verificada (z, z+1, z+2), enviar dicha cadena de titularidad actualizada verificada (z, z+1, z+2) a una autoridad certificadora para la concesión al segundo titular de un segundo certificado digital acreditándole titularidad del primer vehículo, y para la revocación al primer titular del primer certificado digital acreditándole titularidad, recibir, de parte del segundo titular, un registro con una firma digital (z+3), verificar dicho registro (z+3), confirmar al segundo titular como titular del primer vehículo, firmar la confirmación digitalmente creando un registro (z+4), y enviar el registro (z+4) al primer titular y al segundo titular.

El servidor puede recibir dicha cadena de acceso de parte del primer titular y del segundo titular mediante dispositivos clientes.

Registro Inicial de Titularidad del Vehículo

La invención incluye además métodos para el registro del dueño inicial. Esta implica la creación de una cadena de titularidad del vehículo, la cual se mantiene actualiza. En un ejemplo de realización, el programa informático cuando es ejecutado además provoca al servidor mediar el registro de un usuario como titular de un vehículo en respuesta a una solicitud de un primer usuario, dicha mediación comprende generar una cadena de titularidad (t) que comprende al menos un registro de autorización de obtención de titularidad, el registro conteniendo al menos una firma digital confirmando autorización de obtención de titularidad, enviar dicha cadena de titularidad (t) al primer titular, recibir, de parte del primer titular, la

cadena de titularidad actualizada (t, t+1, t+2) con al menos una primera concatenación y una segunda concatenación, donde la primera concatenación (t+1) comprende una solicitud de certificado de acreditación de titularidad firmada digitalmente, y la segunda concatenación (t+2) comprende una confirmación de aceptación de titularidad firmada digitalmente, verificar cada concatenación de la cadena de titularidad actualizada (t, t+1, t+2), y enviar la cadena de titularidad actualizada (t, t+1, t+2, t+3) con una concatenación (t+3) que comprende la confirmación de aceptación firmada digitalmente al primer titular.

En algunos ejemplos de realización, los registros de titularidad (incluyendo el registro inicial) y los registro de cambio de titularidad se concatenan o registran en la misma cadena de titularidad. En estos casos, el sistema se basa en una sola cadena de titularidad que se actualiza según sea necesario.

El sistema según cualquiera de las realizaciones puede además comprender un medio de almacenamiento electrónico, para almacenar, por ejemplo, datos asociados a los usuarios, vehículos, y/o cadenas de transacciones.

El sistema puede ser proporcionado y/o manejado por, por ejemplo, un desarrollador (o ensamblador) de vehículos, o una empresa de alquiler de vehículo.

La Autoridad Certificadora puede ser parte del sistema o los servicios de Autoridad Certificadora pueden ser proporcionados al sistema por una entidad externa. Además, la Autoridad de Certficados puede comprender o estar compuestas por múltiples autoridades. En algunos ejemplos de realización, la Autoridad Certificadora está compuesta por tres autoridades distintas, específicamente, una Autoridad Certificadora de Usuarios, una Autoridad Certificadora de Vehículos, y una Autoridad Certificadora de Desarrollador de Vehículos.

En otro ejemplo de realización, la invención comprenden un procedimiento para facilitar a usuarios el acceso compartido a un vehículo, donde el procedimiento comprende las etapas de generar una cadena de acceso al vehículo, registrar secuencialmente, mediante concatenación de registros en dicha cadena de acceso al vehículo, las transacciones asociadas a autorización de acceso al vehículo, verificación de identidad de un usuario, y verificación de credenciales de un usuario, y cada instancia de concesión de acceso al vehículo por parte de un primer usuario a un segundo usuario.

En otro ejemplo de realización, la invención comprende un procedimiento para registrar cambios en titularidad de vehículos, donde el procedimiento comprende la generación de una cadena de titularidad del vehículo. Dicha generación de una cadena de titularidad comprende

al menos las etapas de iniciar una cadena con al menos un registro de una transacción asociada a la titularidad de un vehículo, registrar un cambio de titularidad mediante la concatenación de un nuevo registro, y repetir el paso de registrar un cambio para cada instancia de cambio de titularidad.

En otro aspecto, la invención comprende un programa informático para un procesador de lado cliente para manejar el acceso a un vehículo, que cuando es ejecutado provoca al procesador obtener un estatus de un certificado acreditando acceso a un vehículo, obtener una lista de revocación de certificados de acceso, detectar presencia del vehículo V dentro de un rango de comunicación, solicitar confirmación al usuario para establecer comunicación con dicho vehículo, establecer comunicación con el vehículo V, y enviar una cadena de acceso al vehículo en respuesta a una solicitud del vehículo V.

Breve descripción de los dibujos

Las anteriores y otras ventajas y características se comprenderán más plenamente a partir de la siguiente descripción detallada de unos ejemplos de realización con referencia a los dibujos adjuntos, que deben tomarse a título ilustrativo y no limitativo, en los que:

La Figura 1 es un diagrama esquemático ilustrando un ejemplo de realización de un sistema según un aspecto de la invención.

La Figura 2 ilustra un diagrama de flujo según un ejemplo de realización de un método según otro aspecto de la invención;

La Figura 3 ilustra un diagrama de flujo según un ejemplo de realización de un método según otro aspecto de la invención;

La Figura 4 ilustra un diagrama de flujo según un ejemplo de realización de un método según otro aspecto de la invención.

Descripción detallada de unos ejemplos de realización

En las figuras adjuntas se ilustra un ejemplo de realización del sistema y procedimiento según un primer aspecto de la invención, tal y como se aprecia en la Figura 1.

La Figura 1 ilustra un sistema 100 para proporcionar servicios de manejo de claves (alternativamente referidas en esta divulgación como llaves). Dichos servicios se basan en el uso de cadenas de bloques. En algunos ejemplos de realización, el sistema 100 puede incluir

uno o más servidores 102, que pueden estar configurados para comunicarse con la plataforma informática 112 y un vehículo 116. Esta configuración puede estar basada en una arquitectura cliente/servidor. Los usuarios, como, por ejemplo, un desarrollador de vehículos o dueños de vehículos, pueden acceder al sistema 100 a través de una o más plataformas informáticas 112. Las plataformas informáticas 112 pueden comprender plataformas dedicadas y distintas para cada tipo de usuario, por ejemplo, una primera plataforma puede comprender un “App” para un dispositivo inteligente (e.g., móvil), y una segunda plataforma puede estar basada en, e.g., la *Web* para un desarrollador de vehículos.

Alternativamente, se puede proporcionar una sola plataforma informática homogénea, capaz de servir a los diferentes tipos de usuario.

El servidor 102 puede estar configurado para ejecutar instrucciones legibles por máquina 110 (e.g., un programa informático). Las instrucciones legibles por máquina 110 incluyen al menos uno o más de los métodos descritos en esta divulgación.

En algunas implementaciones, la Autoridad Certificadora 114 puede ser una entidad separada del servidor. En otras implementaciones, parte o la totalidad de la funcionalidad de la Autoridad Certificadora 114 puede ser proporcionada por elementos incluidos en el mismo sistema 100.

El servidor 102 puede incluir uno o más procesadores 108 y un almacenamiento electrónico 104. El servidor 102 puede incluir líneas de comunicación o puertos para permitir el intercambio de información con una red y/u otras plataformas informáticas. El servidor 102 puede incluir una pluralidad de componentes de hardware, software y/o firmware que funcionan conjuntamente para proporcionar la funcionalidad del servidor 102. Por ejemplo, el servidor 102 puede ser implementado por una nube de plataformas informáticas que funcionan conjuntamente como el servidor 102.

El almacenamiento electrónico 104 puede comprender medios de almacenamiento no transitorios que almacenan electrónicamente información. Los medios de almacenamiento electrónico del almacenamiento electrónico 104 pueden incluir uno o ambos de almacenamiento en el sistema que se proporciona de forma integral o monolítica con el servidor 102 y/o almacenamiento extraíble que se puede conectar de forma extraíble a un servidor 102 a través de, por ejemplo, una unidad (e.g., una unidad de disco, etc.) o un puerto (e.g., un puerto USB, un puerto *firewire*, etc.). Alternativamente, el almacenamiento electrónico 104 puede incluir uno o más medios de almacenamiento ópticamente legibles (e.g., discos ópticos, etc.), medios de almacenamiento basados en carga eléctrica (e.g., un *RAM*, un *EEPROM*, etc.), medios de almacenamiento de estado sólido (e.g., una unidad de memoria *flash*, etc.) y/u otros medios de almacenamiento electrónicamente legibles. El

almacenamiento electrónico 104 puede incluir uno o más elementos de almacenamiento virtual (e.g., almacenamiento en la nube, una red privada virtual y/u otros elementos de almacenamiento virtual). El almacenamiento electrónico 104 puede almacenar, *inter alia*, información determinada por el procesador 108, algoritmos de *software*, información recibida del servidor 102, información recibida de la plataforma informática 104.

El procesador puede estar configurado para proporcionar procesamiento de información en el servidor 102. El procesador 108 puede incluir un procesador digital, un circuito digital diseñado para procesar información, una máquina de estado un procesador analógico un circuito analógico diseñado para procesar información, y/u otros mecanismos para procesar información electrónicamente. Aunque el procesador 108 se muestra en la Figura 1 como una entidad única, esto es solo para fines ilustrativos. En algunas realizaciones, el procesador 108 puede incluir múltiples unidades de procesamiento. El procesador 108 puede estar configurado para ejecutar las instrucciones legibles por máquina 110 y/u otros elementos de instrucciones legibles por máquina.

Las Figs. 2-4 ilustran varios métodos que se describen a continuación utilizando, en estos ejemplos, al servidor 102 como ejecutador de los métodos.

En el método ilustrado en la Figura 2, la mediación del servidor 102 media el uso compartido de vehículos. Dicha mediación inicia con el paso 202 que comprende recibir, de parte de un primer usuario, una cadena de permiso de acceso (p) a dicho primer vehículo, la cadena incluyendo una concatenación con al menos un registro conteniendo una autorización de acceso al primer vehículo a un segundo usuario generada por el primer usuario. Después en el paso 204 el servidor 102 envía dicha cadena de permiso de acceso (p) al segundo usuario. En el paso 206 el servidor 102, recibe, de parte del segundo usuario, la cadena de permiso de acceso (p, p+1) actualizada con una concatenación de un registro conteniendo una solicitud de firma de certificado. El servidor después envía en el paso 208 dicha cadena de permiso de acceso (p, p+1) a una autoridad certificadora para la concesión de un certificado digital acreditando el acceso al primer vehículo al segundo usuario. Después, en el paso 210 el servidor recibe, de parte del segundo usuario, la cadena de permiso de acceso (p, p+1, p+2) concatenada con un registro conteniendo la aceptación de acceso del segundo usuario, firmada con el certificado digital de acceso, y después en el paso 455 envía dicha cadena de permiso de acceso (p, p+1, p+2) al primer usuario. El servidor 102 después recibe, en el paso 212, de parte del primer usuario, la cadena de permiso de acceso (p, p+1, p+2, p+3) actualizada con una concatenación de un registro conteniendo confirmación del permiso de acceso, y finalmente el servidor 102 envía en el paso 214 dicha cadena de permiso de acceso (p, p+1, p+2, p+3) al segundo usuario.

En un método ilustrado en la Figura 3, el programa informático, cuando es ejecutado, además provoca al servidor de manejo de llaves 102 mediar un cambio de titularidad a un primer vehículo. Esta mediación puede ejercerse por el servidor 102 en respuesta a una solicitud por parte de un primer titular que posee un primer certificado digital acreditándole titularidad al primer vehículo.

Como parte de dicha mediación el servidor 102 recibe, en el paso 302, de parte del primer titular, una cadena de titularidad (z) que comprende al menos un registro correspondiente al registro de titularidad más reciente en una cadena de titularidad del primer vehículo. En el paso 304 el servidor 102 envía dicha cadena de titularidad (z) al segundo titular.

Después el servidor 102 recibe, en el paso 306, de parte del segundo titular, una cadena de titularidad actualizada con una concatenación de un registro conteniendo al menos un certificado digital firmado (z, z+1).

En el paso 308 el servidor 102 verifica dicha cadena de titularidad actualizada (z, z+1), y concatena, en base al resultado positivo de la verificación, un registro (z+2) incluyendo una autorización firmada digitalmente a la cadena actualizada de titularidad, generando así una cadena de titularidad actualizada verificada (z, z+1, z+2).

En el paso 310 el servidor 102 envía dicha cadena de titularidad actualizada verificada (z, z+1, z+2) a una autoridad certificadora para la concesión al segundo titular de un segundo certificado digital acreditándole titularidad del primer vehículo, y para la revocación al primer titular del primer certificado digital acreditándole titularidad. El servidor 102 después recibe en el paso 312, de parte del segundo titular, un registro con una firma digital (z+3), y en el paso 314 verifica dicho registro (z+3). El servidor después confirma en el paso 316 al segundo titular como titular del primer vehículo, y en el paso 318 firma la confirmación digitalmente creando un registro (z+4). Finalmente, en el paso 320 el servidor 102 envía el registro (z+4) al primer titular y al segundo titular.

En el método ilustrado en la Figura 4 el servidor 102 media para efectuar el registro inicial de titularidad de un vehículo. Como parte de dicha mediación el servidor 102 genera en el paso 402 una cadena de titularidad (t) que comprende al menos un registro de autorización de obtención de titularidad, el registro conteniendo al menos una firma digital confirmando autorización de obtención de titularidad. El servidor 102 después envía en el paso 404 dicha cadena de titularidad (t) al primer titular. El servidor después recibe, en el paso 406, de parte del primer titular, la cadena de titularidad actualizada (t, t+1, t+2) con al menos una primera concatenación y una segunda concatenación, donde la primera concatenación (t+1) comprende una solicitud de certificado de acreditación de titularidad firmada digitalmente, y la

segunda concatenación (t+2) comprende una confirmación de aceptación de titularidad firmada digitalmente. En el paso 408 el servidor 102 verifica cada concatenación de la cadena de titularidad actualizada (t, t+1, t+2), y finalmente en el paso 410 el servidor 102 envía la cadena de titularidad actualizada (t, t+1, t+2, t+3) con una concatenación (t+3) que comprende la confirmación de aceptación firmada digitalmente al primer titular.

El número de elementos, registros y/o concatenaciones en las cadenas de titularidad y en las cadenas de permiso de acceso según la invención puede diferir del número de elementos identificados en las cadenas de titularidad y las cadenas de permiso de acceso en los ejemplos de realización descritos.

En algunos ejemplos de realización, la cadena de titularidad se utiliza para ambos, el registro inicial de titularidad del vehículo, y para el registro de cambios de titularidad del vehículo.

Ejemplo de realización detallada del sistema y métodos

Arquitectura del Sistema

Un sistema según un aspecto de la invención puede comprender las siguientes entidades:

- Servidor de manejo de llaves/claves (SMC) es un servidor or conjunto de servidores que actúan como punto central de la arquitectura del sistema y asisten en parte la interacción entre las entidades. El sistema, por ejemplo, pueder asistir de las siguientes maneras:
    - Proporciona soporte en procedimientos asociados al usuario(s) (registro de usuario, registro de titular de vehículo, traslado de titularidad).
    - Valida y asiste solicitudes de usuarios como la generación de llaves/claves digitales para otros usuarios.

- El desarrollador de vehículos M maneja o controla el SMC. Cada instancia (i.e. centro productivo) de M se indica mediante m_i y posee un par de claves $\{Pk_{m_i}, Sk_{m_i}\}$ y un certificado $Cert_{m_i}$ emitido por CM.
- El vehículo c_i está equipado con un módulo de control qu maneja el acceso. Este posee una interfaz de comunicación de largo alcance (e.g., LTE) para interacción con el SMC al igual que interfaces de comunicacion de corto-alcance (e.g., BLE, NFC, WiFi) para comunicación con dispositivos inteligentes.

Cada vehículo c_i posee un Número de Identificación de Vehículo (NIV) único, un par de claves $\{Pk_{c_i}, Sk_{c_i}\}$ y un certificado $Cert_{c_i}$ emitido por CC.

- El usuario u_i se registra en la plataforma para usar el sistema de uso compartido de vehículos. Cada usuario u_i posee credenciales únicos, incluyendo un par de claves $\{Pk_{u_i}, Sk_{u_i}\}$ y un certificado $Cert_{u_i}$ emitido por CU. Además, se proporcionan credenciales de acceso cuando el usuario es registrado como el titular (dueño) del vehículo o cuando obtiene permiso de acceso a un vehículo de parte de otro titular. Los credenciales de acceso incluyen un par de claves $\{Pk_{a_i}, Sk_{a_i}\}$ y un certificado $Cert_{a_i}$ emitido por CU y asociado a un vehículo c_i. El certificado $Cert_{a_i}$ contiene extensions que permiten al sistema identificar al usuario u_i como titular o como un usuario autorizado al que se le permite acceso al vehículo.

- La aplicación o "App" es un programa informático para ser ejecutado en dispositivos inteligentes (e.g., un móvil). Esta permite a los usuarios interactuar con las entidades que componen sistema.

- Tres Autoridades de Certificados llamadas CU, CC y CM. Las tareas de manejo de certificado se distribuyen en tres Autoridades de Certificados (AC) diferentes, para así disminuir la complejidad de las funciones de manejo de certificados y garantizar la escalabilidad del sistema.
    - La Autoridad Certificadora de Usuarios - CU atesta la identidad de usuarios y sus permisos de acceso.
    - La Autoridad Certificadora de Vehículos - CC emite los certificados para cada vehículo.
    - La Autoridad Certificadora de Desarrollador de vehículos - CM emite y maneja los certificados del centro de manufactura de vehículos.

Cada CA es capaz de emitir un respuesta de estatus de certificado ε_{a_x}, la cual es proporcionado después de establecer una conexión segura, según la especficación *OCSP Online Certificate Status Protocol* (OCSP por sus siglas en Inglés) *Stapling*.

La profundidad del árbol se indica mediante l, mientras que el ancho del árbol a nivel de hoja se indica mediante s. La CA raíz se mantiene *off-line*, mientras solo los nodos hoja son

conectados a la red. Así, si un nodo hoja es comprometido en terminos de seguridad, los nodos restantes no se afectan.

I. Especificación de protocolo

A continuación se describen un conjunto de protocolos para el manejo de claves/llaves en una plataforma de uso compartido de vehículos.

Primeramente, se prepara al vehículo con un registro que declara al desarrollador como el titular actual del vehículo. Cuando el vehículo es vendido (del desarrollador al primer dueño), o del primer dueño al segundo dueño y así sucesivamente), el titular digital del vehículo cambia y esta información se actualiza en el vehículo.

Las transacciones mencionadas son registradas en la cadena de titularidad $\{\delta_0', \dots, \delta_n'\}$, un conjunto de registros enlazados que contiene información sobre el titular actual del vehículo.

Cuando el titular (dueño) quiere compartir su vehículo con otro usuario, se crea una cadena de acceso $\{\rho_0', \dots, \rho_n'\}$. Esta permite la validación de una autorización a usuario respecto a un vehículo y las condiciones que limitan el permiso. Ambas cadenas contienen registros autenticos que proporcionan integridad al sistema y que enlazan o asocian las transacciones del sistema a una entidad en particular.

Para identificar las operaciones ejecutadas por una entidad en cada una de las cadenas, un conjunto de banderas se definen en la Tabla 1. La Tabla 2 comprende símbolos utilizados en la descripción del sistema. OTP en la Tabla 2 se refiere a *One-Time Password*.

Tabla 1 – Banderas del Sistema

Bandera	**Descripción**
F_0	Proporcionar datos iniciales.
F_1	Comenzar traslado de titular.
F_2	Aceptar titularidad del vehículo.
F_3	Terminar traslado de titular.
F_4	Autorizar Nuevo titular.
F_5	Actualizar titular en el vehículo.
F_6	Comenzar autorización de acceso.
F_7	Aceptar autorización de acceso.
F_8	Terminar autorización de acceso.

Tabla 2 – Símbolos de Sistema

Símbolo	Descripción
I	Datos personal del usuario.

β	OTP ficha de identificación.
α	Código de validación.
η_i	Número telefónico del usuario u_i.
$\{Pk_{x_i}, Sk_{x_i}\}$	Par asimétrico de claves de x_i
CSR_{x_i}	Solicitud de Firma de Certificado de x_i
ε_{x_i}	Estatus de Certificado de $Cert_{x_i}$
$CRL_{CA_{l,s}}$	Lista de Revocación de Certificado de $CA_{l,s}$

A. Preparación del Sistema

Para ejecutar operaciones criptográficas, el vehículo debe ser provisto de datos y material criptográfico específico. Se assume que este procedimiento es ejecutado en un ambiente seguro como una fábrica, durante ensamblaje del vehículo.

El desarrollador proporciona a cada vehículo c_i con (i) par asimétrico de claves $\{Pk_{c_i}, Sk_{c_i}\}$, (ii) certificado de vehículo $Cert_{c_i}$, (iii) un repositorio con las Autoridades de Certificados disponibles $CU_{l,s}$, $CM_{l,s}$, $CC_{l,s}$ y (iv) la transacción inicial de titularidad $\delta_0' = \{\gamma, \delta_0, Cert_{m_i}\}$. Donde $\delta_0 = Sk_{m_i}(\gamma)$, y $\gamma = \{F_0, t, Cert_{m_i}\}$. Este registro indica al desarrollador del vehículo como el titular actual del vehículo.

B. Registro de Usuario

Los usuarios deben registrarse en la aplicación y obtener credenciales personales para autenticar después respecto al servidor.

- El usuario u_i ejecuta los siguientes pasos:

    1. Introduce información personal $I = \{Nombre, Apellido, Dirección, \eta_i, ID\}$ el la App.
    2. Genera $\{Pk_{u_i}, Sk_{u_i}\}$ y CSR_{u_i}.
    3. Establece un canal seguro de comunicación con $CU_{l,s}$ y envía $\{I, CSR_{u_i}\}$.

- La Autoridad Certificadora $CU_{l,s}$ ejecuta los siguientes pasos:
    1. Verifica CSR_{u_i}.

2. Genera un código α válido durante cierto interval de tiempo y un ficha β.
3. Envía β via la App y α a u_i utilizando un segundo canal de comunicación (e.g. SMS usando η_i, correo postal usando la dirección, etc.).

- El usuario u_i establece un canal seguro de comunicación con $CU_{l,s}$ después de recibir α y antes de la expiración de dicho intervalo de tiempo, y envía α y β.
- La Autoridad Certificadora $CU_{l,s}$ verifica α y β; si ambos son válidos emite $Cert_{u_i}$ y lo envía a u_i.
- El usuario u_i recibe y verifica $Cert_{u_i}$, almacena apropiadamente $\{Pk_{u_i}, Sk_{u_i}\}$ y $Cert_{u_i}$.

C. Registro de Titular

Cuando el vehículo c_i es comprado, el titular u_i debe obtener los credenciales digitales que confieren permisos totales sobre el vehículo de parte del desarrollador de vehículos m_i. Esto requiere que el titular esté registrado en la plataforma (Ver sección IV-B)

- El desarrollador de vehículos m_i ejecuta los siguientes pasos:
  1. Obtiene I y $Cert_{u_i}$ mediante η_i.
  2. Crea una authorización ψ_i para obtener un nuevo par de claves para u_i, donde $\psi_i = \{F_1, c_i, Cert_{u_i}, P_i\}$. El perfil P_i contiene un conjunto de atributos asignados al dueño del vehículo u_i .
  3. Envía δ_1' a u_i mediante el SMC, donde $\delta_1' = \{\psi_i, \delta_1, Cert_{m_i}\}$ y $\delta_1 = Sk_{m_i}(\psi_i)$.
- El usuario u_i ejecuta los siguientes pasos después de haber recibido δ_1':
  1. Verifica que δ_1' es válido.
  2. Genera un nuevo par de claves $\{Pk_{a_i}, Sk_{a_i}\}$ y computa CSR_{a_i}.
  3. Computa $\delta_2' = \{CSR_{a_i}, \delta_2, Cert_{u_i}\}$, donde $\delta_2 = Sk_{u_i}(\delta_1', CSR_{a_i})$; envía δ_2' y δ_1'.
- La Autoridad Certificadora $CU_{l,s}$ ejecuta los siguientes pasos:
  1. Verifica δ_2' usando $Cert_{u_i}$, δ_1' usando $Cert_{m_i}$ y CSR_{a_i}.
  2. Verifica que el certificado $Cert_{u_i}$ incluído en δ_1' es el mismo que ha sido usado para firmar δ_2.
  3. Si las verificaciones anteriores has sido exitosas, entonces $CU_{l,s}$ emite un nuevo certficado $Cert_{a_i}$ con las extensiones $Owner$ y c_i, y lo envía a u_i.
- El usuario u_i ejecuta los siguientes pasos:
  1. Verifica la firma y extensions de $Cert_{a_i}$ (incluyendo c_i y $Owner$) usando δ_1'.
  2. Computa δ_3' y lo envía a m_i, donde $\delta_3' = \{F_2, \delta_3, Cert_{a_i}\}$, y $\delta_3 = Sk_{a_i}(\delta_2', F_2)$.
- El desarrollador de vehículos m_i ejecuta los siguientes pasos:

1. Verifica $Cert_{a_i}$ y las extensiones $Owner$ y c_i usando δ_1'. Además, verifica la cadena $\{\delta_1', \delta_2', \delta_3'\}$ y la bandera F_2.
2. Computa δ_4' y lo envía a u_i , donde $\delta_4' = \{F_3, \delta_4, Cert_{m_i}\}$, y $delta_4 = Sk_{m_i}(\delta_3', F_3)$.

- El usuario u_i verifica y almacena la cadena $\{\delta_1', \delta_2', \delta_3', \delta_4'\}$

D. Cambio de titular de vehículo

Cuando el usuario actual u_i vende el vehículo c_i a u_j el Nuevo propietario de be obtener credenciales digitales que conceden permisos totales sobre el vehículo. Este procedimiento requiere que u_j esté registrado y que el propietario actual u_i autorice la emission de credenciales para el nuevo propeitario.

- El dueño u_i ejecuta los siguientes pasos:
  1. Obtiene el número telefónico η_j.
  2. Obtiene $Cert_{u_j}$ usando η_j y crea la autorización de traslado ψ_j, donde $\psi_j = \{F_1, c_i, Cert_{u_j}, P_j\}$.
  3. Envía δ_z' a u_j mediandte SMC, donde $\delta_z' = \{\psi_j, \delta_z, Cert_{a_i}\}$ y $\delta_z = Sk_{a_i}(\delta_{z-1}', \psi_j)$. El registro δ_{z-1}' corresponde al ultimo elemento de la cadena de titularidad. Al usar $Cert_{a_i}$, es possible asociar al usuario u_i con el vehículo c_i.
- El usuario u_j ejecuta los siguientes pasos después de haber recibido δ_z':
  1. Verifica que la firma digital δ_z es válida.
  2. Verifica que el perfil P_j contiene las propiedades, permisos y funcionalidad vehicular del titular u_i.
  3. Genera $\{Pk_{a_j}, Sk_{a_j}\}$ y CSR_{a_j}.
  4. Computa $\delta_{z+1}' = \{CSR_{a_j}, \delta_{z+1}, Cert_{u_j}\}$, donde $\delta_{z+1} = Sk_{u_j}(\delta_z', CSR_{a_j})$.
  5. Envía δ_{z+1}' y δ_z' a m_i.
- El desarrollador de vehículos m_i ejecuta los siguientes pasos:
  1. Verifica δ_z' usando $Cert_{a_i}$ y δ_{z+1}' usando $Cert_{u_j}$.
  2. Verifica que u_i es el titular de c_i mediante $Cert_{a_i}$; veifica que P_j sea válido según P_i. El perfil del nuevo titular debe contener los mismos atributos que el perfil anterior.
  3. Crea una nueva autorización de certificado $\psi_j' = \{F_4\}$.

4. Envía $\{\delta'_z, \delta'_{z+1}, \delta'_{z+2}\}$ a $CU_{l,s}$ y u_j , donde $\delta'_{z+2} = \{\psi'_j, \delta_{z+2}, Cert_{m_i}\}$ y $\delta_{z+2} = Sk_{m_i}(\delta'_{z+1}, \psi'_j)$.

- La Autoridad Certificadora $CU_{l,s}$ ejecuta los siguientes pasos:
  1. Verifica δ'_{z+1} usando $Cert_{u_j}$, δ'_{z+2} usando $Cert_{m_i}$ y CSR_{a_j}.
  2. Verifica que $Cert_{u_j}$ (incluyendo en δ'_z) fue utilizado para firmar δ'_{z+1}.
  3. Revoca $Cert_{a_i}$, emite $Cert_{a_j}$ con las extensiones $Owner$ y c_i, y lo envía a u_j.
- El usuario u_j ejecuta los siguientes pasos:
  1. Verifica la firma digital y extensions del certificado $Cert_{a_j}$, incluyendo c_i and $Owner$, usando δ'_z.
  2. Computa δ'_{z+3} y lo envía a m_i, donde $\delta'_{z+3} = \{F_2, \delta_{z+3}, Cert_{a_j}\}$, y $\delta_{z+3} = Sk_{a_j}(\delta'_{z+2}, F_2)$.
- El desarrollador de vehículos m_i ejecuta los siguientes pasos:
  1. Verifica la cadena $\{\delta'_z, \delta'_{z+1}, \delta'_{z+2}, \delta'_{z+3}\}$, $Cert_{a_j}$, sus extensiones $Owner$, c_i y la bandera F_2 usando δ'_z.
  2. Computa δ'_{z+4}, dondee $\delta'_{z+4} = \{F_3, \delta_{z+4}, Cert_{m_i}\}$ y $\delta_{z+4} = Sk_{m_i}(\delta'_{z+3}, F_3)$.
  3. Envía δ'_{z+4} a u_i y u_j.
- Los usuarios u_j y u_i verificans y almacenan la cadena $\{\delta'_z, \delta'_{z+1}, \delta'_{z+2}, \delta'_{z+3}\}$.

E. Actualizar titular en el vehículo

Cuando hay un nuevo titular, la cadena de titularidad en el vehículo debe ser actualizada. Esto ocurre después de ejecutar los pasos en la Sección IV-C o Sección IV-D.
En general, si el vehículo está en-linea, la comunicación se establece directamente entre el SMC y el vehículo c_i. De otra manera, el usuario u_j releva los mensajes a c_i.

- Cuando hay una conexión entre el vehículo y la nube SMC, m_i ejecuta los siguientes pasos (cuando el vehículo está *off-line*, los pasos son ejecutados por u_j):
  1. Establece una conexión segura con el vehículo c_i y envía la cadena $\{\delta'_z, \dots, \delta'_{z+k}\}$.
- El vehículo c_i ejecuta los siguientes pasos:
  1. Verifica δ'_z usando δ'_{z-1}. Notar que el vehículo posee una cadena de titularidad terminando en δ'_{z-1}, lo cual corresponde al último elemento de la cadena de titularidad.

2. Verifica el resto de la cadena $\{\delta'_z, \dots, \delta'_{z+k}\}$ y el estatus de los certificados.
3. Si las verificaciones previas están correctas, la titularidad de c_i es actualizada a u_j y la nueva cadena $\{\delta'_z, \dots, \delta'_{z+k}\}$ es almacenada en el vehículo.
4. Computa δ'_{z+k+1} y la envía a u_j y m_i, donde $\delta'_{z+k+1} = \{F_5, \delta_{z+k+1}, Cert_{c_i}\}$ y $\delta_{z+k+1} = Sk_{c_i}(\delta'_{z+k}, F_5)$. Si no hay conexión con la nube, δ'_{z+k+1} es enviada a u_j y reenviada a m_i.

- El nuevo titular u_j recibe δ'_{z+k+1} y verifica la cadena recibida. Finalmente, m_i verifica la información y actualize la cadena.

F. Uso compartido de vehículos con condiciones de servicio

El titular u_j autoriza a compartir el vehículo bajo ciertos terminus o condiciones de servicio al usuario u_x. Para obtener los credenciales de acceso, el usuario u_x debe tener los credenciales personales obtenidos de la manera descrita en la Section IV-B.

- Cuando el titular u_j pretende compartir el vehículo c_i con el usuario u_x, ejecuta los siguientes pasos:
  1. Obtiene el número telefónico η_x y con esto $Cert_{u_x}$.
  2. Crea una autorización χ para compartir c_i con u_x, donde $\chi = \{F_6, c_i, Cert_{u_x}, P_x\}$. u_j define en el perfil P_x un conjunto de atributos, incluyendo la duración temporal del permiso, lo cual definirá el tiempo de validez del certificado de acceso. Además, P_x puede comprender (i) limitaciones en las acciones permitidas, como: cerrar con llave, abrir o encender el vehículo; (ii) activación o desactivación de la navegación/sistema de asistencia de conducir; or (iii) limitaciones respecto al área de viaje, o la velocidad máxima.
  3. Envía ρ'_0 a u_x mediante SMC,donde $\rho'_{\{0\}} = \{\chi, \rho_0, Cert_{a_j}\}$ y $\rho_0 = Sk_{a_j}(\chi)$.
- El usuario u_x ejecuta los siguientes pasos después de recibir ρ'_0:
  1. Verifica que la firma digital ρ_0 sea válida, y valida que P_x corresponda con el acuerdo entre u_j y u_x.
  2. Genera $\{Pk_{a_x}, Sk_{a_x}\}$ yCSR_{a_x}.
  3. Computa ρ'_1 y lo envía junto con ρ'_0 a $CU_{l,s}$, donde $rho'_1 = \{CSR_{a_x}, \rho_1, Cert_{u_x}\}$, y $\rho_1 = Sk_{u_x}(\rho'_0, CSR_{a_x})$.
- La Autoridad Certificadora $CU_{l,s}$ ejecuta los siguientes pasos:

1. Verifica ρ_1', ρ_0', el estatus de $Cert_{a_j}$ y valida que el titular actual de c_i, indicado por $Cert_{a_i}$ es u_j.
2. Verifica CSR_{a_x} y valida que $Cert_{u_x}$ (incluído en ρ_0') fue usado para firmar ρ_1.
3. Emite $Cert_{a_x}$, con extensiones $Access$, c_i y lo envía a u_x.

- El usuario u_x ejecuta los siguientes pasos:
  1. Verifica $Cert_{a_x}$ y sus extensiones c_i y $Access$, usando ρ_0'.
  2. Computa ρ_2' y lo envía a u_j, donde $\rho_2' = \{F_7, \rho_2, Cert_{a_x}\}$, y $\rho_2 = Sk_{a_x}(\rho_1', F_7)$.
- El titular u_j ejecuta los siguientes pasos:
  1. Verifica $Cert_{a_x}$ y sus extnsiones c_i y $Access$, usando ρ_0'.
  2. Verifies the chain $\{\rho_0', \rho_1', \rho_2'\}$ and the flag F_7.
  3. Almacena $Cert_{a_x}$, computa ρ_3' y lo envía a u_x, donde $\rho_3' = \{F_8, \rho_3, Cert_{a_i}\}$, y $\rho_3 = Sk_{a_j}(\rho_2', F_8)$.
- El usuario u_x verifica y almacena la cadena $\{\rho_0', \rho_1', \rho_2', \rho_3'\}$.

G. Uso del vehículo según las condiciones de servicio

Para usar el vehículo c_i según las condiciones de servicio, el usuario u_x debe tener $Cert_{a_x}$ asociado al vehículo y autorizado por el usuario titular u_j. Además, la respuesta de estatus de certificado ε_{a_x} se utiliza para verificar que el certificado no haya sido revocado cuando el usuario intenta acceder al vehículo.

El usuario u_x debe ser capaz de validar la identidad de c_i contenida en $Cert_{c_i}$ mediante obtención de $CRL_{CC_{l,s}}$ y verificar que $Cert_{c_i}$ no haya sido revocado.

- De manera ininterrumpida (preferiblemente), la App ejecutada en el telefóno móvil de (u otro dispositivo inteligente) u_x ejecuta los siguientes pasos de manera frecuente:
  1. Obtiene la respuesta de estatus de certificado ε_{a_x} correspondiendo a $Cert_{a_x}$.
  2. Obtiene la $CRL_{CC_{l,s}}$ requeridad para verificar el $Cert_{c_i}$ de c_i emitido por $CC_{l,s}$.

Solamente cuando u_x está cercano o próximo a c_i, la aplicación de móvil despierta y permite al usuario interactuar con el vehículo. El rango mínimo de próximidad depende en la tecnología de comunicación usada entre u_x y c_i.

Cálculos de distancia pueden ser ejecutados, por ejemplo, mediante medición de tiempo-retorno o mediante protocolos de delimitación de distancia. Cuando ya el usuario esté dentro del rango de comunicación, la aplicación solicita establecer una conexión segura con c_i. Esta acción require que u_x introduzca un PIN (por sus siglas en Inglés, *Personal Identifcation Number*), huella(s) digital(es), patron, etc. Una conexión segura con el vehículo c_i es establecida después de la confirmación.

- Después de haberse establecido la comunicación segura y c_i haber recibido ε_{a_x} de u_x, c_i ejecuta los siguientes pasos:
    1. Verifica que el certificado $Cert_{a_x}$ no haya expirado y no haya sido revocado.
    2. Verifica si el certificado tiene la extensión $Owner$ o $Access$.
    3. Si el certificado tiene la extensión $Access$:
        a. Comprueba si existe una cadea $\{\rho'_0, \rho'_1, \rho'_2, \rho'_3\}$ dond ρ'_2 contiene $Cert_{a_x}$.
        b. Si la verificación anterior falla, envía una solicitud para obtener la cadena $\{\rho'_0, \rho'_1, \rho'_2, \rho'_3\}$.
        c. Verifica y almacena la cadena.
        d. Verifica que $Cert_{a_x}$ tenga la extensión c_i.
    4. Si el certificado tiene la extensión $Owner$:
        a. Verifica que $Cert_{a_x}$ tenga la extensión c_i.
    5. Si la verificaciones anteriores son exitosas, proporciona acceso y prepara las funciones del vehículo según P_x incluído en ρ'_0.

Un experto en la materia podría introducir cambios y modificaciones en los ejemplos de realización descritos sin salirse del alcance de la invención según está definido en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Sistema para el manejo de llaves de vehículos motorizados, el sistema comprende:

-un servidor que comprende un procesador programado con un programa informático que cuando es ejecutado provoca al servidor mediar la concesión de permiso de acceso a un primer vehículo a un segundo usuario en respuesta a una solicitud de un primer usuario, dicha mediación comprende:

-recibir, de parte de un primer usuario, una cadena de permiso de acceso (p) a dicho primer vehículo, la cadena incluyendo una concatenación con al menos un registro conteniendo una autorización de acceso al primer vehículo a un segundo usuario generada por el primer usuario;

-enviar dicha cadena de permiso de acceso (p) al segundo usuario;

-recibir, de parte del segundo usuario, la cadena de permiso de acceso (p, p+1) actualizada con una concatenación de un registro conteniendo una solicitud de firma de certificado;

-enviar dicha cadena de permiso de acceso (p, p+1) a una autoridad certificadora para la concesión de un certificado digital acreditando el acceso al primer vehículo al segundo usuario;

-recibir, de parte del segundo usuario, la cadena de permiso de acceso (p, p+1, p+2) concatenada con un registro conteniendo la aceptación de acceso del segundo usuario, firmada con el certificado digital de acceso;

-enviar dicha cadena de permiso de acceso (p, p+1, p+2) al primer usuario;

-recibir, de parte del primer usuario, la cadena de permiso de acceso (p, p+1, p+2, p+3) actualizada con una concatenación de un registro conteniendo confirmación del permiso de acceso; y

-enviar dicha cadena de permiso de acceso (p, p+1, p+2, p+3) al segundo usuario.

2. Sistema según la reivindicación 1, donde el primer usuario es el titular de dicho primer vehículo y/o posee un certificado digital acreditándole titularidad de dicho primer vehículo.

3. Sistema según la reivindicación 1 o 2, donde dicha concatenación comprende una computación de al menos:

-una autorización,

-una firma digital del primer usuario que comprende una encriptación de la autorización, y

-un certificado digital acreditando el acceso al vehículo del primer usuario.

4. Sistema según una o más de las reivindicaciones anteriores, donde el registro de autorización de acceso comprende:

(i) orden de autorización de acceso (F6);

(ii) identificación del primer vehículo como objeto del permiso de acceso;

(iii) certificado digital acreditando la identidad del segundo usuario; y

(iv) un perfil del permiso de acceso.

5. Sistema según la reivindicación 3, donde el perfil de acceso incluye al menos uno o más atributos definiendo respectivamente uno o más de: un tiempo de duración del permiso de acceso, una geocerca, una velocidad máxima, y una configuración del vehículo.

6. Sistema según uno o más de las reivindicaciones anteriores, donde el servidor recibe dicha cadena de permiso de acceso de parte del primer usuario y del segundo usuario mediante dispositivos clientes.

7. Sistema según una o más de las reivindicaciones anteriores, en el que el programa informático cuando es ejecutado además provoca al servidor mediar el registro de un usuario como titular de un vehículo en respuesta a una solicitud de un primer usuario, dicha mediación comprende:

-generar una cadena de titularidad (t) que comprende al menos un registro de autorización de obtención de titularidad, el registro conteniendo al menos una firma digital confirmando autorización de obtención de titularidad;

-enviar dicha cadena de titularidad (t) al primer titular;

-recibir, de parte del primer titular, la cadena de titularidad actualizada (t, t+1, t+2) con al menos una primera concatenación y una segunda concatenación, donde

la primera concatenación (t+1) comprende una solicitud de certificado de acreditación de titularidad firmada digitalmente, y

la segunda concatenación (t+2) comprende una confirmación de aceptación de titularidad firmada digitalmente;

-verificar cada concatenación de la cadena de titularidad actualizada (t, t+1, t+2),

y

-enviar la cadena de titularidad actualizada (t, t+1, t+2, t+3) con una concatenación (t+3) que comprende la confirmación de aceptación firmada digitalmente al primer titular.

8. Sistema según una o más de las reivindicaciones anteriores, en el que el programa informático, cuando es ejecutado, además provoca al servidor de manejo de llaves mediar un cambio de titularidad a un primer vehículo, en respuesta a una solicitud por parte de un primer titular que posee un primer certificado digital acreditándole titularidad al primer vehículo, dicha mediación comprende:

-recibir, de parte del primer titular, una cadena de titularidad (z) del primer vehículo que comprende al menos un registro correspondiente al registro de titularidad más reciente;

-enviar dicha cadena de titularidad (z) al segundo titular;

-recibir, de parte del segundo titular, una cadena de titularidad actualizada con una concatenación de un registro conteniendo al menos un certificado digital firmado (z, z+1);

-verificar dicha cadena de titularidad actualizada (z, z+1),

-concatenar, en base al resultado positivo de la verificación, un registro (z+2) incluyendo una autorización firmada digitalmente a la cadena actualizada de titularidad, generando así una cadena de titularidad actualizada verificada (z, z+1, z+2);

-enviar dicha cadena de titularidad actualizada verificada (z, z+1, z+2) a una autoridad certificadora para la concesión al segundo titular de un segundo certificado digital acreditándole titularidad del primer vehículo, y para la revocación al primer titular del primer certificado digital acreditándole titularidad;

-recibir, de parte del segundo titular, un registro con una firma digital (z+3), verificar dicho registro (z+3), confirmar al segundo titular como titular del primer vehículo, firmar la confirmación digitalmente creando un registro (z+4), y enviar el registro (z+4) al primer titular y al segundo titular.

9. Sistema según la reivindicación 8, donde la cadena de titularidad (z) corresponde a la cadena de titularidad (t, t+1, t+2, t+3), de tal manera que un registro de titularidad y un registro de cambio de titularidad se concatenan en la misma cadena de titularidad.

10. Sistema según una o más de las reivindicaciones anteriores, donde el servidor recibe dicha cadena de acceso de parte del primer titular y del segundo titular mediante dispositivos clientes.

11. Sistema según una o más de las reivindicaciones anteriores, donde el sistema además comprende un medio de almacenamiento electrónico.

12. Procedimiento para facilitar a usuarios el acceso compartido a un vehículo, el procedimiento comprende:

-generar una cadena de acceso al vehículo;

-registrar secuencialmente, mediante concatenación de registros en dicha cadena de acceso al vehículo, las transacciones asociadas a autorización de acceso al vehículo, verificación de identidad de un usuario, y verificación de credenciales de un usuario, y cada instancia de concesión de acceso al vehículo por parte de un primer usuario a un segundo usuario.

13. Procedimiento para registrar cambios en titularidad de vehículos, el procedimiento comprende:

-la generación de una cadena de titularidad del vehículo, lo cual comprende las etapas de:

- iniciar una cadena con al menos un registro de una transacción asociada a la titularidad de un vehículo;

-registrar un cambio de titularidad mediante la concatenación de un nuevo registro; y

-repetir el paso de registrar un cambio para cada instancia de cambio de titularidad.

14. Programa informático para un procesador de lado cliente para manejar el acceso a un vehículo, que cuando es ejecutado provoca al procesador:

-obtener un estatus de un certificado acreditando acceso a un vehículo V;

-obtener una lista de revocación de certificados de acceso;

-detectar presencia del vehículo V dentro de un rango de comunicación;

-solicitar confirmación al usuario para establecer comunicación con dicho vehículo;

-establecer comunicación con el vehículo V;

-enviar una cadena de acceso al vehículo en respuesta a una solicitud del vehículo V.

Fig. 1

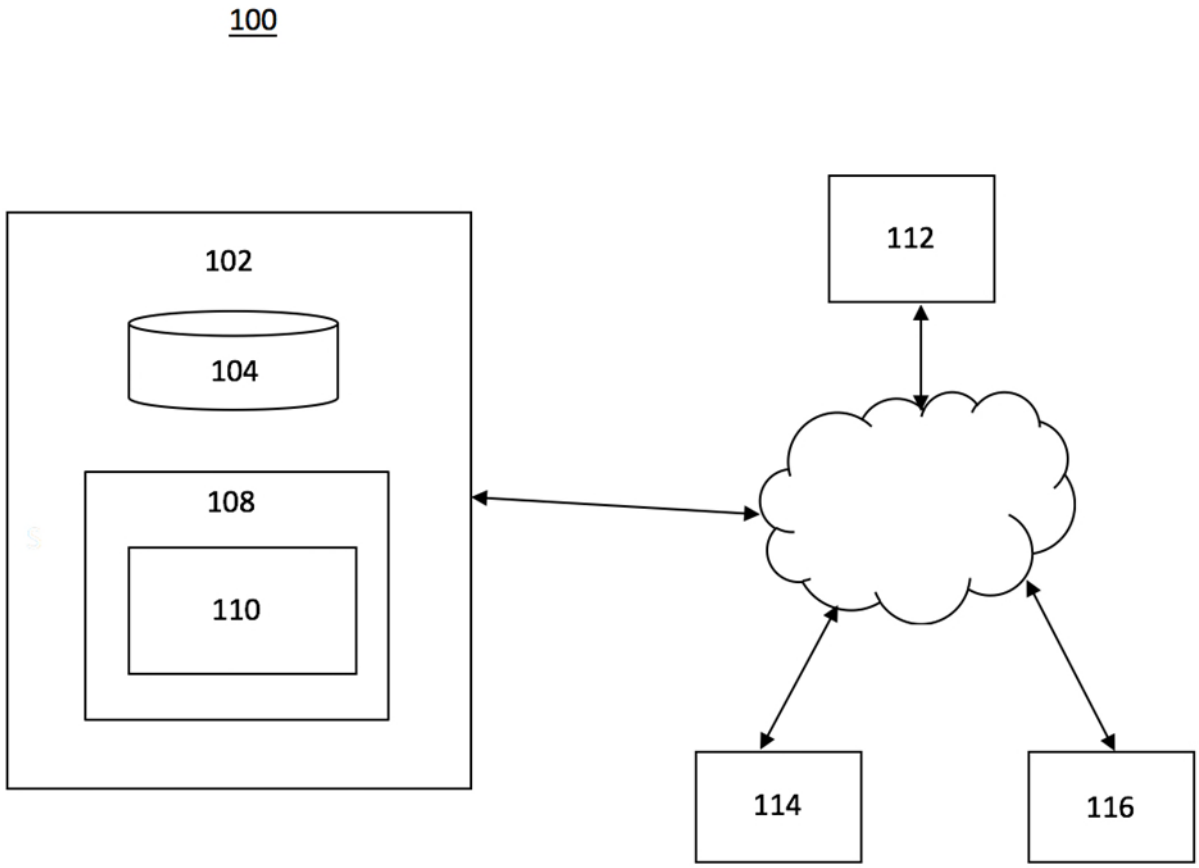


Fig. 2

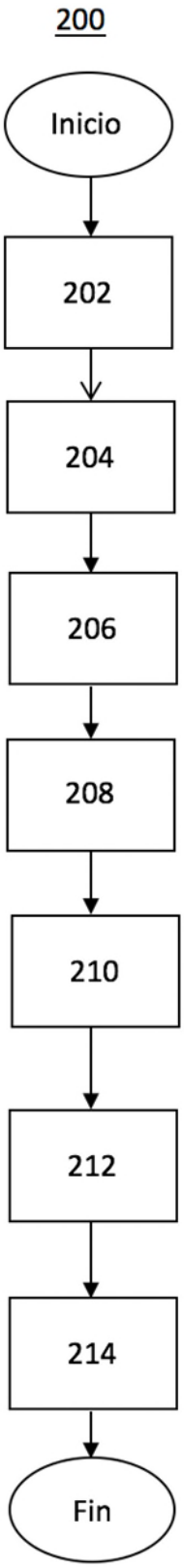


Fig. 3

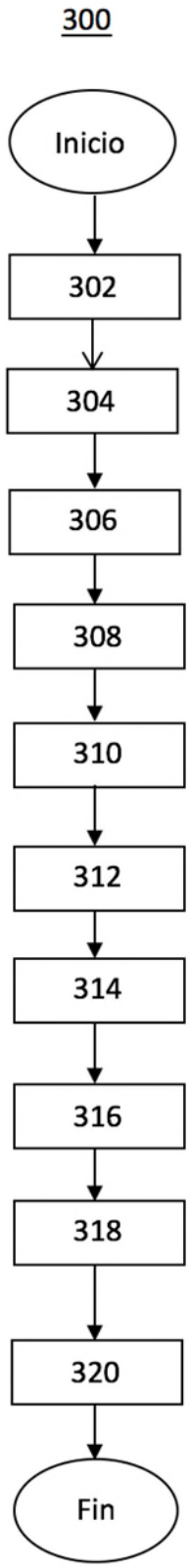
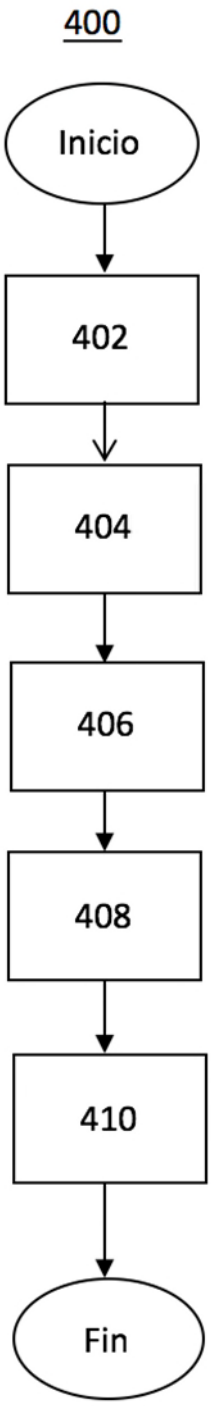


Fig. 4



OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201830840

(22) Fecha de presentación de la solicitud: 24.08.2018

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G06Q30/06*** (2012.01)
H04L9/32 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	US 2008282090 A1 (LEYBOVICH JONATHAN) 13/11/2008, párr. [0001], [0005 - 0008], [0016 - 0048]; fig. 1 - 5.	1-13
X	HABLANDO DE MANZANAS. ¿Cómo funciona el servicio Car2Go?. YouTube, 09/10/2016 [en línea][recuperado el 02/09/2019]. Recuperado de Internet <URL: https://www.youtube.com/watch?v=oucT7xz2EDY>. min. 0:29-1:25	14
A	Communication protocol. Wikipedia, 25/01/2018 [en línea][recuperado el 02/09/2019]. Recuperado de Internet <URL: http://web.archive.org/web/20180125141543/https://en.wikipedia.org/wiki/Communication_protocol#Basic_requirements>. apart. 2	1-13

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado
☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
02.09.2019	A. Oropesa García	1/2

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06Q, H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, internet