(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 910 077**

(51) Int. CI.:

G06F 7/04 (2006.01)
G09C 5/00 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06Q 50/26 (2012.01)
H04W 12/06 (2011.01)
H04W 12/062 (2011.01)
H04W 12/084 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.12.2016 PCT/US2016/069207**

(87) Fecha y número de publicación internacional: **06.07.2017 WO17117390**

(96) Fecha de presentación y número de la solicitud europea: **29.12.2016 E 16882661 (8)**

(97) Fecha y número de publicación de la concesión europea: **02.02.2022 EP 3398050**

(54) Título: **Transmisión de identificación digital a bordo de vehículo**

(30) Prioridad:

29.12.2015 US 201562272434 P
28.12.2016 US 201615392261

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.05.2022

(73) Titular/es:

IDEMIA IDENTITY & SECURITY USA LLC (50.0%)
296 Concord Road, Suite 300
Billerica, MA 01821, US y
PODER, DANIEL (50.0%)

(72) Inventor/es:

PODER, DANIEL;
MIU, STEPHEN y
WU, YECHENG

(74) Agente/Representante:

CURELL SUÑOL, S.L.P.

DESCRIPCIÓN

Transmisión de identificación digital a bordo de vehículo

Campo

La presente memoria se refiere de manera general a identificaciones digitales.

Antecedentes

Con frecuencia se recupera información a partir de documentos físicos, tales como carnets de conducir, pólizas de seguro y permisos de circulación de vehículo, para verificar la identidad de un individuo que conduce un vehículo y recuperar información pertinente relacionada con el vehículo.

El documento US 9.083.581 describe un método que incluye mantener una lista de dispositivos autorizados; crear una asociación entre un dispositivo inalámbrico que está haciéndose funcionar por un usuario final y un elemento de unidad de a bordo (OBU), que está previsto en un vehículo; establecer una sesión a través de un puerto designado para ejecutar una aplicación en el elemento de OBU; y acceder a recursos asociados con el vehículo a través del elemento de OBU. En otros ejemplos, la autenticación del dispositivo inalámbrico puede realizarse mediante un punto de acceso de WiFi de privacidad equivalente al cableado (WEP) proporcionado por el elemento de OBU. La autenticación del dispositivo inalámbrico también puede realizarse mediante una etiqueta de identificación por radiofrecuencia (RFID). Los recursos pueden incluir cualquier número de elementos tales como altavoces, una pantalla, un micrófono, un receptor de sistema de posicionamiento global (GPS) o cualquier otro elemento adecuado que puede proporcionarse en el vehículo.

Sumario

La documentación relacionada con un vehículo, tal como una información de carnet de conducir, permiso de circulación de vehículo y póliza de seguro, se almacena habitualmente como documentos físicos dentro de un vehículo. Sin embargo, dado que tal documentación se actualiza periódicamente, con frecuencia un usuario necesita sustituir físicamente tal documentación dentro de un vehículo. Tales documentos también son con frecuencia difíciles de recuperar durante circunstancias de emergencia y/o son propensos a perderse a lo largo del tiempo. Por tanto, en determinadas circunstancias, con frecuencia los usuarios no pueden acceder de manera adecuada a información pertinente a tiempo.

Por consiguiente, un aspecto innovador descrito a lo largo de esta memoria incluye métodos que transmiten información de usuario de una identificación digital desde un dispositivo de usuario hasta un sistema a bordo de vehículo dentro de un vehículo. La información de usuario puede incluir información relacionada con una identificación de conductor digital, un permiso de circulación de vehículo y/o una póliza de seguro que están almacenados en el dispositivo de usuario. La información de usuario puede incluir adicionalmente información codificada relacionada con características de seguridad, instrucciones para acciones que deben realizarse en el sistema a bordo de vehículo y/o privilegios de usuario asociados con la utilización del vehículo. Con respecto a esto, la transmisión de la información de usuario a partir del dispositivo de usuario permite un acceso más conveniente a formatos digitales de información relacionada con el vehículo durante determinadas circunstancias en las que un usuario puede necesitar acceder a la información relacionada con el vehículo.

Las implementaciones pueden incluir una o más de las siguientes características. Por ejemplo, un método implementado por ordenador puede incluir: establecer una conexión entre un dispositivo de usuario y un sistema a bordo de vehículo; recibir, a partir del dispositivo de usuario, información de usuario incluida en una identificación digital en el dispositivo de usuario; recibir una selección de usuario para una parte de la información de usuario; y proporcionar, para emitirse en una pantalla asociada con el sistema a bordo de vehículo, la parte de la información de usuario incluida en la identificación digital en el dispositivo de usuario.

Los detalles de una o más implementaciones se exponen en los dibujos adjuntos y la siguiente descripción. Otras posibles características y ventajas resultarán evidentes a partir de la descripción, los dibujos y las reivindicaciones.

Otras implementaciones de estos aspectos incluyen sistemas, aparatos y programas informáticos correspondientes, configurados para realizar las acciones de los métodos, codificados en dispositivos de almacenamiento informáticos.

Breve descripción de los dibujos

La figura 1A es un diagrama que ilustra un ejemplo de un sistema a bordo de vehículo que conserva información de usuario a partir de un dispositivo de usuario del conductor del vehículo.

La figura 1B es un diagrama de bloques que ilustra un ejemplo de un sistema para transmitir información de

usuario que incluye un documento de identificación digital en un sistema a bordo de vehículo.

La figura 2 es un diagrama que ilustra ejemplos de identidades de usuario asociadas con información que se visualiza en un sistema a bordo de vehículo.

Las figuras 3A a 3E son unos diagramas de bloques que ilustran, cada uno, un ejemplo de un procedimiento para intercambio de información entre un dispositivo de usuario y en un sistema a bordo de vehículo.

En los dibujos, números de referencia similares representan partes correspondientes en su totalidad.

Descripción detallada

La memoria describe métodos y sistemas para que un dispositivo de usuario interaccione con un vehículo de modo que pueda determinarse un estado del usuario o un estado del vehículo de una manera eficiente y razonable. En un caso, puede transmitirse información de usuario desde un dispositivo de usuario de un usuario hasta un sistema a bordo de un vehículo que está conduciéndose por el usuario. La información de usuario puede incluir información relacionada con una identificación digital, un permiso de circulación de vehículo y/o una póliza de seguro que están almacenados en el dispositivo de usuario. La información de usuario puede estar en forma de un documento de identificación digital. La información de usuario puede incluir adicionalmente información codificada relacionada con características de seguridad, instrucciones para acciones que deben realizarse en el sistema a bordo de vehículo y/o privilegios de usuario asociados con la utilización del vehículo. Con respecto a esto, la transmisión de la información de usuario a partir del dispositivo de usuario permite un acceso más conveniente a información de usuario o de vehículo relevante durante determinadas situaciones tales como un control de tráfico. En otro ejemplo, la transmisión puede permitir que el sistema a bordo en el vehículo visualice o comunique información incluyendo un carnet de conducir digital a un agente de la autoridad durante una operación de parada y registro. La información también puede comunicarse a un dispositivo informático que porta el agente de la autoridad. Esta comunicación de datos puede tener lugar, aunque el vehículo esté en funcionamiento en una autopista. La información puede incluir adicionalmente, por ejemplo, información de póliza de seguro portada por el usuario.

En otro caso, se establece una conexión entre un dispositivo de usuario y un sistema a bordo de un vehículo para que el dispositivo de usuario reciba información a partir del sistema a bordo de vehículo. En este caso, la información de vehículo puede incluir información de titularidad de vehículo, información de permiso de circulación de vehículo o identificación de vehículo (VIN). En particular, la información de VIN puede estar respaldada por una clave pública del fabricante. La información de titularidad y permiso de circulación puede incluir la historia completa de permiso de circulación y titularidad, con cada cambio o actualización encadenado a la última transacción y respaldado, por ejemplo, por una marca de agua digital del departamento de vehículos motorizados (DMV) que autoriza la actualización/cambio de registro. Dicha información de vehículo puede incluir adicionalmente información de mantenimiento que se encadena de una manera similar, por ejemplo, mediante una clave pública del distribuidor o mecánico o una marca de agua digital del comerciante. La información de vehículo puede permitir una visibilidad instantánea del estado y la historia del vehículo.

En aún otro caso, una vez establecida una conexión entre un dispositivo de usuario y un sistema a bordo de un vehículo, puede transmitirse información de usuario desde el dispositivo de usuario hasta el sistema a bordo de vehículo. La información de usuario puede estar en forma de un carnet de conducir digital. En este caso, el sistema a bordo de vehículo puede comparar la información de usuario a partir del carnet de conducir digital con una base de datos de conductores autorizados o usuarios abonados para determinar si el usuario es un conductor autorizado del vehículo. Si el usuario es realmente un conductor autorizado, el vehículo se desbloqueará para que el usuario tome el control. En algunos casos, este desbloqueo puede liberar todos los bloqueos mecánicos y electrónicos del volante, los frenos, la palanca de cambios y el panel frontal. El desbloqueo puede realizarse en respuesta a una validación satisfactoria del carnet de conducir digital del usuario, así como a una coincidencia del nombre del usuario en la base de datos de conductores permitidos. En algunos casos, la información de usuario puede compararse con una lista de pasajeros actualmente abonados al servicio. En otros casos, la información de vehículo puede obtenerse en el dispositivo móvil del usuario de modo que se realiza una decisión en cuanto a si el vehículo es un vehículo legítimo que ha solicitado el usuario (o abonado para el servicio). En tales casos, el vehículo puede incluir un vehículo autónomo. De hecho, implementaciones dadas a conocer en la presente memoria permiten la navegación autónoma y facilitan compartir información de telemetría y posición de vehículo, así como información de certificación/aprobación para control técnico del vehículo.

La figura 1A es un diagrama que ilustra un ejemplo de un sistema 100 a bordo de un vehículo. El sistema 100 puede visualizar información de usuario a partir, por ejemplo, de un documento de identificación digital. En resumen, el sistema 110 puede incluir un dispositivo de visualización 112 que proporciona una interfaz 114 para un usuario y un sistema de audio 116 que proporciona reproducción de audio. En este caso, el usuario se refiere generalmente al operador del vehículo. Puede visualizarse información de usuario en la interfaz 114 basándose en intercambio de transmisiones de datos con un dispositivo de usuario 120. El dispositivo de usuario 120 puede presentar una identificación 122 digital que incluye información de usuario que puede visualizarse en la pantalla 112. El dispositivo de usuario puede incluir un dispositivo informático móvil que puede portar el usuario. Los

ejemplos incluyen un dispositivo de teléfono inteligente, un dispositivo de tipo tableta o un dispositivo ponible.

La información de usuario visualizada en la interfaz 114 puede incluir información de carnet de conducir 114a, un permiso 114b de circulación de vehículo, información del seguro 114c, ajustes 114d de seguridad y/o información de cuenta de usuario 114e. La información de carnet de conducir 114a puede ser información asociada con un carnet de conducir digital almacenado en el dispositivo de usuario. El carnet de conducir digital puede incluir generalmente todas las características y aspectos de un carnet de conducir físico. La información de usuario puede transmitirse desde el dispositivo de usuario 120 hasta el sistema a bordo de vehículo 110 mediante un protocolo de comunicación inalámbrica o cableada tal como Bluetooth, Wi-Fi o bus serie universal (USB). Cuando el carnet de conducir digital incluye características ocultas, la información de usuario transmitida puede no revelar información oculta incorporada de otro modo en el documento de identificación digital.

En el ejemplo representado en la figura 1A, el sistema a bordo de vehículo 110 intercambia transmisiones de datos con el dispositivo de usuario 120 que incluyen el permiso 114b de circulación de vehículo. Después de intercambiar las transmisiones de datos, el permiso 114b de circulación de vehículo está disponible para su visualización en la interfaz 114. El permiso 114b de circulación de vehículo es aplicable a la certificación para vehículo autónomo. El sistema a bordo de vehículo es un dispositivo informático que incluye al menos un procesador y una pantalla (para interacciones con el usuario). El sistema a bordo de vehículo puede estar incorporado en, o en comunicación con, por ejemplo, un sistema de posicionamiento global (GPS), un sistema de navegación y seguridad para automóviles On-Star®. Tal como se ilustra, el contenido electrónico almacenado en el dispositivo de usuario 120 se transmite al sistema a bordo de vehículo 112, de tal manera que el contenido electrónico está accesible en lugar de documentación en papel.

Un usuario puede utilizar la interfaz 114 en diversas circunstancias. En un ejemplo, el usuario puede utilizar la interfaz 114 para recuperar información pertinente durante servicios de emergencia. Por ejemplo, durante una llamada de servicio con un servicio de ayuda en carretera de emergencia, el usuario puede transmitir la información de usuario visualizada en la interfaz 114 a un receptor de emergencia designado con el fin de proporcionar información relacionada con el vehículo (por ejemplo, el permiso 114b de circulación de vehículo y la información del seguro 114c). En un caso de este tipo, la interfaz 114 puede incluir una opción para transmitir la información de usuario visualizada como paquete de datos al receptor de emergencia designado. En este caso, la transmisión puede ser automática de modo que se dispensa información a un dispositivo del personal ambulatorio a medida que llegan.

En otro ejemplo, un usuario puede utilizar la interfaz 114 para transmitir información solicitada, por ejemplo, durante una operación de parada y registro, por un agente de la autoridad. Por ejemplo, al recibir una solicitud de una información de vehículo y carnet de conducir, en vez de proporcionar al agente de la autoridad documentación en papel, el usuario puede utilizar, en vez de eso, la interfaz 114 para recuperar información actualizada asociada con la identificación 122 digital. En tal caso, dado que el dispositivo de usuario 120 actualiza periódicamente la información de usuario accediendo al sistema de registro del usuario en un servidor de extremo posterior, la información visualizada en la interfaz 114 puede reflejar información más exacta en comparación con la documentación en papel. Dado que la información de usuario se ha obtenido previamente por el sistema a bordo de vehículo, reproducir la misma información en una pantalla del sistema a bordo de vehículo proporciona un intercambio de información fluido sin recurrir a copias físicas que pueden perderse fácilmente debido a la falta de utilización. En determinados casos, el intercambio de información se realiza entre el sistema a bordo de vehículo y un dispositivo de usuario del agente de la autoridad. El intercambio de información de esta manera puede proporcionar al agente de la autoridad la ventaja adicional de visualizar información actual del conductor en una pantalla del dispositivo de usuario del agente de la autoridad para evitar que el agente de la autoridad entre en el vehículo. Además, la información del conductor está actualizada; y características de seguridad, tales como marcas de agua digitales, que acompañan a la información transmitida certifican la validez de la información.

En determinados casos, dicho intercambio / transmisión de información puede producirse mientras el vehículo no se ha detenido, por ejemplo, cuando el vehículo está desplazándose en una autopista. Para ilustración, la información que codifica el carnet de conducir digital del usuario puede transmitirse desde el sistema a bordo de vehículo hasta un dispositivo del agente de policía. El agente de policía puede estar patrullando en la autopista y se le puede pedir que busque más detalles sobre vehículos circundantes, por ejemplo, durante una alerta Amber. El agente de policía también puede inspeccionar dicha información a partir de una pantalla del sistema a bordo de vehículo después de un control de tráfico regular (por ejemplo, parada y registro). En estos casos que implican vehículos en movimiento/no detenidos, puede intercambiarse información entre vehículos autónomos. Como ejemplo ilustrativo, la presencia de un vehículo y su información de permiso de circulación/carnet de conducir puede emitirse por radiodifusión de manera proactiva a su entorno y recibirse por un vehículo vecino. De esta manera, un vehículo puede detectar a sus vecinos. De hecho, esta información puede complementar información a partir de otros sensores tales como cámaras y sensores de movimiento. En caso de accidentes que implican dos o más vehículos, puede intercambiarse información del seguro de una manera similar.

En otro ejemplo, un usuario puede utilizar la interfaz 114 para establecer una identidad o privilegio para utilizar un vehículo durante un control de tráfico si no es el propietario del vehículo o el usuario asociado con el permiso 114b

de circulación de vehículo. Por ejemplo, tal como se describe más particularmente con respecto a la figura 2, un conocido del propietario del vehículo puede estar asociado con la cuenta del propietario del vehículo. La asociación puede crearse estableciendo un perfil de usuario limitado asociado con el dispositivo de usuario del conocido. En tal caso, después de detenerse por un agente de la autoridad y solicitársele el permiso 114b de circulación de vehículo, el conocido puede navegar por las cuentas de usuario 114e para visualizar el perfil de usuario que indica que el propietario del vehículo ha consentido la utilización del vehículo por parte del conocido. Con respecto a esto, puede utilizarse la interfaz 114 para establecer una identidad de usuario asociada con un vehículo que puede no reflejarse necesariamente dentro de los documentos de registro referentes a la propiedad o permiso de circulación del vehículo.

En algunas implementaciones, la información de usuario transmitida a partir del dispositivo de usuario 120 puede utilizarse para autenticar a un usuario antes de proporcionar acceso para conducir. En dichos ejemplos, la información de usuario puede incluir ajustes 114d de seguridad que especifican datos de credenciales de usuario asociados con la identificación 122 digital en el dispositivo de usuario. Por ejemplo, el sistema a bordo de vehículo 110 puede estar configurado para proporcionar acceso a identificaciones digitales que se especifican por el propietario del vehículo. Con respecto a esto, el sistema a bordo de vehículo 110 puede utilizarse como característica de seguridad para protegerse contra robo de vehículo en casos en los que el propietario del vehículo u otro usuario ha perdido las llaves del vehículo o se le han robado las llaves.

En otros casos, dichas características de seguridad se utilizan para desbloquear el vehículo de modo que el usuario puede pasar a ser el conductor. En particular, el sistema a bordo de vehículo puede verificar las características de seguridad a partir del carnet de conducir digital para determinar si el documento digital es legítimo. Una copia legítima es una copia válida que presenta las características de seguridad requeridas, pero sin signos de haber sido manipulada. Si se determina que el documento de identidad digital es legítimo y válido, el sistema a bordo de vehículo puede verificar adicionalmente la información de identidad a partir del documento de identidad digital con una base de datos de terceros. En algunos casos, la base de datos de terceros es una base de datos remota que aloja datos de identidad que se han examinado por una autoridad, tal como el departamento de vehículos motorizados (DMV) o el departamento de estado. Si la información de identidad se valida adicionalmente de acuerdo con entradas aprobadas ya presentes en la base de datos de terceros, el vehículo puede desbloquearse para que el usuario ocupe el asiento del conductor. En este caso, el usuario puede obtener acceso completo para utilizar el vehículo, incluyendo el sistema de motor, el sistema de arranque y el sistema de freno. En particular, este mecanismo de desbloqueo puede combinarse con una verificación biométrica, por ejemplo, utilizando una huella dactilar o un retrato facial. Este aspecto biométrico, en combinación con el aspecto de validación del carnet de conducir digital, puede formar un procedimiento de “dos factores”. En primer lugar, a la persona que intenta acceder se le puede validar su documento de identificación digital, tal como un carnet de conducir digital, por el sistema a bordo de vehículo, tal como se comentó anteriormente. En segundo lugar, la persona puede demostrar que es la persona identificada presentando un elemento biométrico al sistema a bordo del vehículo. Por ejemplo, el usuario puede presentar una huella dactilar en la palanca de cambios o en el volante. El usuario también puede mirar al espejo retrovisor para que se tome su elemento biométrico facial. El elemento biométrico adquirido en el sitio puede compararse con la información biométrica en el documento de identificación digital, que se ha examinado por una fuente de autoridad, tal como el DMV.

La figura 1B es un diagrama de bloques que ilustra un ejemplo de un sistema 100 para transmitir información de usuario desde el dispositivo de usuario 120 hasta el sistema a bordo de vehículo 110. En resumen, el sistema 100 puede incluir el sistema a bordo de vehículo 110, el dispositivo de usuario 120, un servidor de autoridad emisora 130 y un servidor de identificación digital 140. Los componentes del sistema 100 pueden intercambiar comunicaciones a través de una red 105. La información del usuario puede residir en el dispositivo de usuario 120. La información también puede residir en la nube y estar lista para recuperarse a demanda. Una vez comunicada al sistema a bordo de vehículo 110, la información de usuario puede residir en el sistema a bordo de vehículo 110.

La red 105 puede incluir uno o más de entre Internet, una red de área amplia (WAN), una red de área local (LAN), redes telefónicas cableadas o inalámbricas, analógicas o digitales (por ejemplo, una red telefónica pública conmutada (PTSN), red digital de servicios integrados (ISDN), una red celular y línea de abonado digital (DSL)), radio, televisión, cable, satélite o cualquier otro mecanismo de suministro o tunelación para transportar datos.

La red 105 puede incluir múltiples redes o subredes, cada una de las cuales puede incluir, por ejemplo, una ruta de datos cableada o inalámbrica. La red 105 puede incluir una red conmutada por circuito, una red de datos conmutada por paquetes o cualquier otra red que puede transportar comunicaciones electrónicas (por ejemplo, comunicaciones de datos o voz). Por ejemplo, la red 105 puede incluir redes basadas en el protocolo de Internet (IP), modo de transferencia asíncrono (ATM), PSTN, redes conmutadas por paquetes basadas en IP, X.25 o retransmisión de tramas, u otras tecnologías comparables y puede soportar voz utilizando, por ejemplo, VoIP, u otros protocolos comparables utilizados para comunicaciones de voz. La red 105 puede incluir una o más redes que incluyen canales de datos inalámbricos y canales de voz inalámbricos. La red 105 puede ser una red inalámbrica, una red de banda ancha o una combinación de redes que incluyen una red inalámbrica y una red de banda ancha. La red 105 también puede abarcar tecnologías de comunicación de campo cercano, tales como NFC (comunicación de campo cercano), Bluetooth®, comunicaciones de audio a alta frecuencia y comunicaciones de

infrarrojos.

El sistema a bordo de vehículo 110 puede ser un grupo de componentes de hardware y software que están instalados en un vehículo y configurados para funcionar basándose en la recepción de entrada de usuario. Por ejemplo, el sistema a bordo de vehículo 110 puede incluir un dispositivo de visualización 112, una interfaz 114, un sistema de audio 116 y un módulo de comunicación 118. El dispositivo de visualización 112 puede ser un sistema de navegación para automóviles que se utiliza normalmente para proporcionar datos de posición durante una operación de determinación de ruta.

El dispositivo de visualización 112 puede incluir características adicionales tales como recibir y transmitir llamadas telefónicas a través del dispositivo de usuario 120 o proporcionar señales para hacer funcionar los otros componentes de hardware o software del sistema a bordo de vehículo 110. La interfaz 114 puede ser una interfaz de usuario que se genera en el dispositivo de visualización 112. La interfaz 114 puede aceptar entrada de usuario (por ejemplo, pantalla táctil) que proporciona señales relacionadas con el funcionamiento y control de los componentes de hardware o software del sistema a bordo de vehículo 110. Por ejemplo, la interfaz 114 puede incluir elementos de interfaz que corresponden a operaciones particulares que van a realizarse por los componentes del sistema a bordo de vehículo 110.

En algunas implementaciones, el sistema a bordo de vehículo 110 puede funcionar en un sistema operativo móvil que proporciona la capacidad de descargar e instalar aplicaciones para móviles. En dichas implementaciones, la interfaz 114 puede visualizarse dentro de una aplicación para móviles que está configurada para intercambiar comunicaciones con una aplicación para móviles en el dispositivo de usuario 110. Por ejemplo, las aplicaciones para móviles en el sistema a bordo de vehículo 110 y el dispositivo de usuario 120 pueden ser aplicaciones de identificación digital que están configuradas para recuperar información de identificación digital a partir de un sistema de usuario de registro en la base 142 de datos de identificación digital.

En algunas implementaciones, uno o más de los componentes de hardware y software del sistema a bordo de vehículo 110 pueden fabricarse o bien por un fabricante de vehículo o bien por un fabricante de terceros. Por ejemplo, uno o más de los componentes de hardware y software pueden ser mejoras de mercado secundario para el vehículo que se instalan después de haberse fabricado el vehículo por el fabricante de equipos originales (OEM). Por ejemplo, el dispositivo de visualización 112 puede ser un sistema de navegación para automóviles de terceros que se instala como complemento al vehículo

El dispositivo de usuario 120 puede ser un dispositivo informático electrónico portátil que visualiza la identificación 122 digital asociada con un usuario. Por ejemplo, el dispositivo de usuario 120 puede ser, por ejemplo, un teléfono inteligente, un ordenador de tipo tableta, un ordenador portátil, un dispositivo de asistente digital personal, una tableta electrónica, un reloj inteligente, un vidrio inteligente o cualquier dispositivo electrónico con una pantalla que está conectado a una red. Además, el dispositivo de usuario 120 puede incluir una identificación 122 digital, una interfaz de usuario 124 y un módulo de comunicación 126.

La identificación 122 digital puede ser una versión electrónica de una información de usuario que normalmente se proporciona en documentación en papel. Por ejemplo, la identificación 122 digital puede incluir un carnet de conducir digital emitido a un conductor registrado por un departamento de estado de vehículos motorizados. Además, la identificación 122 digital puede incluir otros tipos de información auxiliar asociada referente a un vehículo. Por ejemplo, la identificación 122 digital puede incluir información de póliza de seguro de vehículo del usuario, información de permiso de circulación de vehículo y/u otra información de usuario asociada con la utilización del vehículo. La identificación 122 digital también puede incluir datos de credenciales de usuario que se utilizan como características de seguridad para restringir el acceso al vehículo a usuarios autorizados. Por ejemplo, la identificación 122 digital puede especificar información de cuenta de usuario que permite que un usuario asociado con la identificación 122 digital se autentique en el sistema a bordo de vehículo 110 para recibir acceso a un vehículo del sistema a bordo de vehículo 110. En algunos casos, la información específica de vehículo sigue al vehículo y reside en el sistema a bordo de vehículo 110. En estos casos, la información específica de vehículo no sigue a la propiedad o el control, a medida que el propietario o conductor cambia.

El dispositivo de usuario 120 puede intercambiar comunicaciones con el servidor de identificación digital 140 para recibir y transmitir información de usuario relacionada con la identificación 122 digital, datos de usuario que están incluidos en la identificación digital, datos de credenciales utilizados a partir de la identificación 122 digital y/o ajustes de configuración que ajustan la visualización de la identificación 122 digital en el dispositivo de usuario 120 y/o el sistema a bordo de vehículo 110. Por ejemplo, durante un procedimiento de verificación, cuando puede habilitarse la identificación 122 digital en el dispositivo de usuario 120, puede transmitirse un paquete de datos que incluye datos de credenciales al servidor de identificación digital 140 para determinar si la identificación 122 digital todavía es válida o incluye información precisa y, en respuesta a determinar que la identificación 122 digital todavía es válida, los datos devueltos incluyen datos de credenciales que pueden transmitirse entonces al sistema a bordo de vehículo 110. En este ejemplo, si el servidor de identificación digital 140 determina que los datos de credenciales son válidos, entonces puede determinarse que la identificación digital es válida y proporcionarse para su visualización en la interfaz 114 del sistema a bordo de vehículo 110. Alternativamente, si el servidor de identificación

digital 140 determina que los datos de credenciales no son válidos, entonces puede determinarse que la identificación 122 digital es inválida y puede restringirse el acceso al vehículo.

En algunas implementaciones, el dispositivo de usuario 120 puede incluir una aplicación para móviles que intercambia comunicaciones con el servidor de identificación digital 140 como servidor de aplicación y el sistema a bordo de vehículo 110 como cliente. Por ejemplo, la aplicación para móviles puede estar asociada con una cuenta de usuario que está almacenada en la base 142 de datos de identificación digital. Además, la aplicación para móviles puede intercambiar de manera periódica información relacionada con el estado de seguridad asignado por el servidor de identificación digital 140 para determinar si la identificación 122 digital es válida. En algunos casos, la aplicación para móviles puede incluir adicional o alternativamente diversas visualizaciones de la aplicación para móviles de tal manera que la aplicación para móviles puede utilizarse como forma de identificación en sustitución de una tarjeta de identificación física o visualizarse en la interfaz 114.

El servidor de autoridad emisora 130 puede ser un servidor remoto que se gestiona por la autoridad emisora (por ejemplo, un departamento de estado de vehículos motorizados) y se utiliza para controlar el acceso a información de usuario protegida que se incluye en tarjetas de identificación físicas emitidas por la autoridad emisora. Por ejemplo, el servidor de autoridad emisora 130 puede proporcionar acceso a información demográfica de usuarios, información histórica asociada con usuarios (por ejemplo, tarjetas de identificación anteriores emitidas, número de renovaciones, etc.) y/u otros tipos de información de usuario que utilizan procedimientos de autorización que requieren la validación de credenciales de acceso. Por ejemplo, tras recibir una petición de la información de usuario protegida por parte del servidor de identificación digital 140, el servidor de autoridad emisora 130 puede requerir un intercambio de las credenciales de acceso para validar una petición autorizada.

El servidor de identificación digital 140 puede consultar al servidor de autoridad emisora 130 con respecto a información de usuario protegida durante una operación de identificación digital. Por ejemplo, durante un procedimiento de inscripción, después de que un usuario haya elegido inscribirse en un programa de identificación digital, el servidor de identificación digital 140 puede consultar al servidor de autoridad emisora 130 utilizando un número de identificación de usuario para extraer información de usuario protegida que va a incluirse en una identificación 122 digital generada. En otro ejemplo, durante una operación de verificación, el servidor de identificación digital 140 puede acceder al servidor de autoridad emisora 130 para determinar si una identificación 122 digital para un usuario incluye información de usuario falsa indicativa de una identificación 122 digital fraudulenta.

En algunas implementaciones, el servidor de autoridad emisora 130 puede estar configurado con protocolos de seguridad adicionales en comparación con el servidor de identificación digital 140 para proteger información de usuario confidencial asociada con el usuario. Por ejemplo, en algunos casos, el servidor de autoridad emisora 130 puede estar asociado con una agencia del gobierno federal que gestiona programas nacionales que requieren acceso especializado (por ejemplo, una autorización gubernamental). En dichos casos, el servidor de identificación digital 140 puede estar configurado para acceder a la información de usuario protegida almacenada dentro del servidor de autoridad emisora 130 según un acuerdo de seguridad especial que garantiza que el intercambio de la información de usuario protegida se controla y regula según estatutos de privacidad federales. Por ejemplo, el servidor de autoridad emisora 130 puede rastrear información relacionada con cada intercambio con el servidor de identificación digital 140 de tal manera que, en el caso de que el servidor de identificación digital 140 determine que una identificación 122 digital particular es inválida, puede recibirse una notificación por el servidor de autoridad emisora 130 para tomar medidas de seguridad adicionales para proteger más información de usuario confidencial que puede estar asociada con, pero no incluida en, la identificación 122 digital. Con respecto a esto, el intercambio de comunicación entre el servidor de identificación digital 140 y el servidor de autoridad emisora 130 puede utilizarse para garantizar la protección de información de usuario más allá de la información de usuario incluida en la identificación 122 digital.

En algunas implementaciones, el sistema puede incluir una o más autoridades emisoras adicionales tales como una compañía de seguros que proporciona seguro de vehículo a un usuario. En tales implementaciones, el servidor de autoridad emisora 130 puede almacenar información relacionada con el seguro (por ejemplo, información de póliza, indemnizaciones de seguro anteriormente presentadas, detalles de cobertura, etc.) asociada con un vehículo. Con respecto a esto, el dispositivo de usuario 120 puede consultar al servidor de autoridad emisora asociado con la compañía de seguros para recuperar información del seguro, que entonces puede incluirse dentro de la identificación 122 digital.

El servidor de identificación digital 140 puede ser un servidor remoto que se monitoriza y se gestiona por una organización o institución que está autorizada por una autoridad emisora de identificación para proporcionar la identificación 122 digital a un usuario. En algunos casos, la organización o institución que gestiona el servidor de identificación digital 140 puede ser una organización que está designada por la autoridad emisora de identificación (por ejemplo, departamento de estado de vehículos motorizados) para acceder a información de identificación para una pluralidad de usuarios a los que se les ha emitido una tarjeta de identificación física. En otros casos, la organización o institución que gestiona el servidor de identificación digital 140 puede ser la autoridad emisora de identificación (por ejemplo, una institución gubernamental) que emite a una pluralidad de usuarios una tarjeta de

identificación física.

El servidor de identificación digital 140 puede coordinar y administrar los procedimientos de extremo posterior que están implicados en proporcionar una identificación digital a la pluralidad de usuarios a los que se les ha emitido una identificación física a partir de la autoridad emisora de identificación. Por ejemplo, el servidor de identificación digital 140 puede iniciar procedimientos para inscribir a usuarios con la identificación 122 digital, y gestionar protocolos de seguridad para detectar una posible utilización fraudulenta o violaciones de privacidad asociadas con las identificaciones digitales. En algunos casos, los procedimientos relacionados con la identificación 122 digital, tal como se describió anteriormente, pueden coordinarse con el servidor de autoridad emisora 130, para garantizar que información de usuario protegida que incluye información personalmente identificable no se expone al proporcionar la identificación 122 digital.

Tal como se describe, la información de usuario protegida puede referirse a información de usuario dentro de la identificación 122 digital que puede incluir información personalmente identificable asociada con el usuario tal como, por ejemplo, números de seguridad social, lugar de residencia y/u otra información demográfica que está asociada con otros tipos de información que el usuario considera privada. Además, la información de usuario protegida puede incluir historias médicas del usuario que están protegidas según la ley de transferencia y responsabilidad de seguros médicos de 1996 (HIPAA). El acceso a la información de usuario protegida dentro de la identificación 122 digital puede restringirse por el servidor de identificación digital 140 mediante la utilización de procedimientos de autorización particulares (por ejemplo, requerir códigos de acceso de usuario) para acceder a la información protegida en el dispositivo de usuario 120.

El servidor de identificación digital 140 puede intercambiar comunicaciones con la base 142 de datos de identificación digital, que incluye información de usuario para usuarios inscritos y/u otros detalles de configuración relacionados con el programa de identificación digital. Por ejemplo, la base 142 de datos de identificación digital puede incluir una entrada de usuario asociada con un usuario que incluye información de cuenta asociada con usuarios inscritos y cualquier tipo de información de usuario que puede proporcionarse por el usuario durante un procedimiento de inscripción de identificación digital.

En algunas implementaciones, la base 142 de datos de identificación digital puede incluir entradas de usuario tanto para usuarios que están inscritos en el programa de identificación digital como para usuarios potenciales que el servidor de identificación digital 140 ha identificado como usuarios que es probable que se inscriban en el programa de identificación digital. Por ejemplo, la base 142 de datos de identificación digital puede incluir un campo que indica si una entrada de usuario está asociada con un usuario inscrito o un usuario potencial. En tales implementaciones, el servidor de identificación digital 140 puede acceder a la base 142 de datos de identificación digital para recuperar información de usuario para la identificación 122 digital asociada con un usuario inscrito e información de usuario para un usuario candidato con el fin de enviar un correo electrónico de inscripción que proporciona un código de inscripción para el usuario candidato.

En algunas implementaciones, la entrada de usuario para usuarios inscritos puede crearse automáticamente por el servidor de identificación digital 140 dentro de la base 142 de datos de identificación digital. En tales implementaciones, el usuario puede presentar un formulario de inscripción en línea que incluye un conjunto de campos de usuario para proporcionar información de usuario. En respuesta, el servidor de identificación digital 140 puede iniciar un procedimiento implementado por ordenador que genera automáticamente una entrada de usuario para el usuario en la base 142 de datos de identificación digital e inserta los valores presentados para el conjunto de campos de usuario como información de usuario que se incluye en la entrada de usuario.

En algunas implementaciones, el servidor de identificación digital 140 puede intercambiar adicionalmente comunicaciones con un servidor de imágenes, que almacena fotografías asociadas con una tarjeta de identificación de usuario. En algunas implementaciones, el servidor de imágenes puede gestionarse por una entidad u organización independiente que gestiona el servidor de identificación digital 140. Por ejemplo, en tales implementaciones, el servidor de imágenes puede gestionarse por la autoridad emisora de identificación. En otras implementaciones, el servidor de imágenes puede gestionarse por la autoridad emisora autorizada que también gestiona el servidor de identificación digital 140. En dichas implementaciones, el servidor de imágenes puede ser un subcomponente del servidor de identificación digital 140.

La figura 2 es un diagrama que ilustra ejemplos de cuentas de usuario asociadas con información que se visualiza en un sistema a bordo de vehículo. Tal como se representa, el sistema a bordo de vehículo 110 puede recibir transmisiones a partir de dispositivos de usuario asociados con los usuarios 202a, 202b y 202c y visualizar información de usuario respectiva asociada con cada uno de los usuarios 210a, 210b y 210c.

Los usuarios 202a, 202b y 202c pueden ser diferentes usuarios que utilizan un único vehículo (por ejemplo, individuos de una familia que utilizan un coche familiar, diferentes clases de empleados que utilizan un vehículo de empresa, grupo de amigos que comparten un coche, etc.). Los usuarios 202a, 202b y 202c pueden estar asociados con cuentas de usuario 204a, 204b y 204c, respectivamente, que se almacenan en el servidor de identificación digital 140. Mediante sensores de asiento, puede recopilarse información biométrica a partir del conductor y, por

tanto, puede identificarse al conductor real. Haciendo brevemente referencia a la figura 1, en algunos casos, la interfaz 114 puede proporcionar directivas al usuario para que seleccione, por ejemplo, una opción de menú que representa a una persona particular como conductor para asumir responsabilidades del vehículo.

En el ejemplo representado en la figura 2, el usuario 202a es un propietario de vehículo, el titular del seguro principal y el individuo al que el permiso de circulación de vehículo indica que está registrado el vehículo. En este ejemplo, el sistema a bordo de vehículo 110 visualiza el estado del usuario e indica que el usuario dispone de todos los privilegios para utilizar el vehículo. El usuario 202b es un usuario autorizado que no es el propietario de vehículo sino un conocido del propietario de vehículo, que la información de póliza de seguro indica que es un dependiente del usuario 202a. Además, el permiso de circulación de vehículo para el vehículo indica que el usuario 202b no está registrado en el vehículo. Por consiguiente, el usuario 202b puede disponer de un subconjunto de los privilegios del usuario 202a en cuanto a que algunos aspectos de control sobre el vehículo pueden estar limitados basándose en el estado del usuario 202b (por ejemplo, actualizar información de servicio de vehículo). El usuario 202c es un usuario registrado que tampoco es el propietario de vehículo y además dispone de un carnet de conducir provisional, que la información de póliza de seguro indica que también es un dependiente del usuario 202a. Por ejemplo, el usuario 202c puede ser un adolescente que no tiene edad legal para obtener un carnet de conducir completo. Por consiguiente, el usuario 202c puede disponer de restricciones adicionales con respecto a los privilegios en comparación con el usuario 202b dado su estado de carnet de conducir provisional y tipo de usuario (por ejemplo, restricciones de límite de velocidad, regiones previamente seleccionadas para conducir, etc.).

En algunas implementaciones, el conjunto de privilegios de usuario puede utilizarse para proporcionar diferentes tipos de acceso a vehículo a usuarios basándose en su tipo de usuario, estado legal de un carnet de conducir y/o título en el permiso de circulación de vehículo. Con respecto a esto, puede utilizarse información de usuario transmitida a partir de la identificación 122 digital para clasificar inicialmente a los usuarios y proporcionar el nivel apropiado de acceso a vehículo basándose en la clasificación. Por ejemplo, tal como se describió anteriormente, un propietario de vehículo puede utilizar el sistema a bordo de vehículo 110 para especificar un conjunto de opciones de seguridad parentales que impiden que un usuario restringido utilice un vehículo de una manera peligrosa (por ejemplo, exceso de velocidad por encima de un límite de velocidad de umbral preestablecido, accediendo al vehículo durante determinados periodos de tiempo o utilizando el vehículo más allá de una distancia de umbral establecida). En algunos casos, sólo usuarios cualificados pueden manipular ciertos tipos de vehículos. Como ilustración, autobuses escolares, vehículos de construcción o furgonetas pueden requerir permisos separados. Por tanto, el acceso a esos tipos de vehículos puede restringirse a un subconjunto de conductores que se han cualificado o formado para conducir vehículos especializados. En otros casos, sólo conductores por encima de una edad legal y sin deficiencias físicas (tales como ceguera legal) pueden utilizar vehículos. En todavía otros casos, conducir en determinadas áreas geográficas puede restringirse a conductores cualificados por cuestiones de eficiencia o seguridad. Dichas situaciones pueden incluir conducir vehículos en un aeropuerto, una base militar o una zona protegida.

La figura 3A es un diagrama de bloques que ilustra un ejemplo de un procedimiento 300A para transmitir información de usuario para su visualización en un sistema a bordo de vehículo. En resumen, el procedimiento 300A puede incluir establecer una conexión entre un dispositivo de usuario y un sistema a bordo de vehículo (310), recibir información de usuario a partir del dispositivo de usuario (320), recibir una selección de usuario para una parte de la información de usuario (330) y proporcionar la parte de la información de usuario para su emisión en una pantalla del sistema a bordo de vehículo (340).

En más detalle, el procedimiento 300A puede incluir establecer una conexión entre un dispositivo de usuario y un sistema a bordo de vehículo (310). Por ejemplo, el dispositivo de usuario 120 puede establecer una conexión con el sistema a bordo de vehículo 110. La conexión puede ser una o más de una conexión de Bluetooth, una conexión de Wi-Fi, una conexión de infrarrojos, una conexión celular y/o cualquier otro protocolo de comunicación inalámbrica adecuado. En algunos casos, la conexión puede establecerse mediante conexiones cableadas, tales como conexiones de USB (bus serie universal) o firewire (IEEE 1394). La conexión puede establecerse únicamente cuando el sistema a bordo de vehículo 110 puede verificar que el dispositivo de usuario es un dispositivo de confianza. Esta verificación puede realizarse interrogando el sistema a bordo de vehículo 110 al dispositivo de usuario para obtener información que indica que se ha examinado el dispositivo de usuario (o la aplicación en el dispositivo de usuario). La información puede cargarse previamente en el dispositivo de usuario mediante el procedimiento de aprobación anterior. En algunos casos, la información puede incorporarse en el firmware del dispositivo de usuario. En otros casos, la información puede descargarse a partir de la parte de aprobación de confianza. Dado que el procedimiento de conexión está centrado en el usuario, el sistema a bordo de vehículo 110 también puede interrogar al usuario, a través del dispositivo de usuario, con respecto a información tal como contraseña, código de acceso o respuestas a preguntas de seguridad para permitir transmitir información de usuario desde el dispositivo de usuario hasta el sistema a bordo de vehículo 110.

En algunos casos, la conexión puede establecerse cuando no ha habido casos anteriores de enchufarse el dispositivo de usuario en el sistema a bordo de vehículo 110. En estos casos, después de establecer la conexión entre el dispositivo de usuario 120 y el sistema a bordo de vehículo 110, puede realizarse una operación de sincronización de datos de tal manera que se transmiten actualizaciones de la identificación 122 digital desde la

última sesión de conexión al sistema a bordo de vehículo 110.

El procedimiento 300A puede incluir recibir información de usuario a partir del dispositivo de usuario (312). Por ejemplo, el sistema a bordo de vehículo 120 puede recibir información de usuario incluida en la identificación 122 digital en el dispositivo de usuario 120 a través de la conexión establecida. Por ejemplo, tal como se describe con respecto a la figura 1A, la información de usuario puede incluir información de carnet de conducir, información de permiso de circulación de vehículo, información de cobertura de seguro, ajuste de seguridad y/o ajustes de cuenta de usuario. En particular, la información de usuario puede incluir un carnet de conducir digital del usuario. Puede transmitirse una copia de atributos verificados a partir de una credencial autenticada al sistema a bordo de vehículo 110. Esta copia puede estar dedicada para una aplicación de software de reproducción en el sistema a bordo de vehículo 110. Esta copia puede no retransmitirse a partir del sistema a bordo de vehículo 110. En algunos casos, la copia puede caducar y agotarse un temporizador, de modo que la copia se establece para desaparecer después de un periodo de tiempo.

El procedimiento 300A puede incluir recibir, en el sistema a bordo de vehículo, una selección de usuario para una parte de la información de usuario (314). En algunos casos, el usuario puede seleccionar una parte de la información de usuario para ver en una pantalla del sistema a bordo de vehículo 110 a partir del dispositivo de usuario 120. En una ilustración, el dispositivo de usuario 122 puede procesar inicialmente una selección de usuario en un interfaz de usuario del dispositivo de usuario 122 y, en respuesta, proporcionar una indicación de la selección de usuario y una instrucción para visualizar la selección de usuario al sistema a bordo de vehículo 110. En otro caso, el usuario puede seleccionar la parte de la información de usuario en la interfaz 114 del sistema a bordo de vehículo 110. Por ejemplo, el usuario puede navegar a un elemento de interfaz que corresponde a la parte de la información de usuario tal como se representa en la figura 1A.

El procedimiento 300A puede incluir proporcionar la parte de la información de usuario para su emisión en una pantalla del sistema a bordo de vehículo (316). Por ejemplo, en respuesta a recibir la selección de usuario de la parte de la información de usuario, el sistema a bordo de vehículo 110 puede proporcionar la parte de la información de usuario para su emisión en una pantalla. Tal como se representa en el ejemplo en la figura 1A, la parte de la información de usuario puede visualizarse en la interfaz 112. Por ejemplo, durante una operación de parada y registro, el carnet de conducir digital del conductor puede visualizarse para un agente de la autoridad que realiza la inspección. Este ejemplo también es aplicable para un conductor de un coche de alquiler.

La figura 3A es un diagrama de bloques que ilustra un ejemplo de un procedimiento 300A para transmitir información de usuario para su visualización en un sistema a bordo de vehículo. En resumen, el procedimiento 300A puede incluir establecer una conexión entre un dispositivo de usuario y un sistema a bordo de vehículo (310), recibir información de usuario a partir del dispositivo de usuario (320), recibir una selección de usuario para una parte de la información de usuario (330) y proporcionar la parte de la información de usuario para su emisión en una pantalla del sistema a bordo de vehículo (340).

En más detalle, el procedimiento 300A puede incluir establecer una conexión entre un dispositivo de usuario y un sistema a bordo de vehículo (310). Por ejemplo, el dispositivo de usuario 120 puede establecer una conexión con el sistema a bordo de vehículo 110. La conexión puede ser una o más de una conexión de Bluetooth, una conexión de Wi-Fi, una conexión de infrarrojos, una conexión celular y/o cualquier otro protocolo de comunicación inalámbrica adecuado. En algunos casos, la conexión puede establecerse mediante conexiones cableadas, tales como USB (bus serie universal), firewire (IEEE 1394), OBD (sistemas de diagnóstico a bordo) o variaciones. La conexión puede establecerse únicamente cuando el sistema a bordo de vehículo 110 puede verificar el dispositivo de usuario como dispositivo de confianza. Esta verificación puede realizarse interrogando el sistema a bordo de vehículo 110 al dispositivo de usuario para obtener información que indica que se ha examinado el dispositivo de usuario (o la aplicación en el dispositivo de usuario). La información puede cargarse previamente en el dispositivo de usuario mediante el procedimiento de aprobación anterior. En algunos casos, la información puede incorporarse en el firmware del dispositivo de usuario. En otros casos, la información puede descargarse a partir de la parte de aprobación de confianza. Dado que el procedimiento de conexión está centrado en el usuario, el sistema a bordo de vehículo 110 también puede interrogar al usuario, a través del dispositivo de usuario, con respecto a información tal como contraseña, código de acceso o respuestas a preguntas de seguridad para permitir transmitir información de usuario desde el dispositivo de usuario hasta el sistema a bordo de vehículo 110.

En algunos casos, la conexión puede establecerse cuando ha habido casos anteriores de enchufar el dispositivo de usuario en el sistema a bordo de vehículo 110. En estos casos, tras establecer la conexión entre el dispositivo de usuario 120 y el sistema a bordo de vehículo 110, puede realizarse una operación de sincronización de datos de tal manera que se transmiten actualizaciones de la identificación 122 digital desde la última sesión de conexión al sistema a bordo de vehículo 110.

En algunos casos, información residente en el sistema a bordo de vehículo 110 puede transmitirse a un dispositivo de usuario, por ejemplo, de un agente de la autoridad. Haciendo referencia a la figura 3B, el procedimiento 300B puede incluir establecer una conexión entre un dispositivo de usuario y un sistema a bordo de vehículo (310), recibir información de vehículo a partir del sistema a bordo de vehículo (322), extraer información a partir de la

información de vehículo recibida (324) y verificar la información extraída (326). El dispositivo de usuario puede necesitar acceder al sistema a bordo de vehículo 100. Sin embargo, mientras se establece la conexión entre el dispositivo de usuario y el sistema a bordo de vehículo 110 (310), el dispositivo de usuario del agente de la autoridad puede necesitar que el conductor facilite el establecimiento de la conexión. En otros casos, el sistema a bordo de vehículo 100 puede reservar un canal abierto para el acceso por parte de agentes de la autoridad. En estos casos, los agentes de la autoridad en patrulla pueden introducirse en el canal abierto y sin tener que detener a un vehículo en tránsito.

Una vez establecida la conexión, el sistema a bordo de vehículo 120 puede recibir información de usuario incluida en la identificación 122 digital en el dispositivo de usuario 120 a través de la conexión establecida (322). Por ejemplo, tal como se describe con respecto a la figura 1A, la información de vehículo puede incluir información de permiso de circulación de vehículo, información de cobertura de seguro, información de mantenimiento de vehículo, así como información de conductor. En particular, la información de conductor puede incluir un carnet de conducir digital del usuario.

El procedimiento 300B puede incluir extraer información a partir de la información de vehículo recibida (324). En algunos casos, el dispositivo de usuario del agente de la autoridad puede seleccionar una parte de la información de usuario/conductor para ver en una pantalla de dispositivo de usuario del agente de la autoridad. Por ejemplo, el dispositivo de usuario del agente de la autoridad puede elegir ver el carnet de conducir digital del conductor. En otros casos, el agente de la autoridad puede estar interesado únicamente en saber si el vehículo se ha registrado de manera adecuada y dispone del seguro mínimo requerido que no ha caducado. Hay ocasiones en las que el agente de la autoridad sólo está interesado en saber que el conductor del vehículo no es un sospechoso al que se le está buscando, aunque el vehículo pueda coincidir con el perfil o la descripción de un vehículo de fuga. El agente de la autoridad, en patrulla en la autopista, también puede preferir confirmar que determinados conductores de camiones tienen el carnet, cualificación y seguro apropiados sin tener que detener esos vehículos de gran tamaño.

El procedimiento 300B puede incluir verificar la información extraída (326). Por ejemplo, después de haberse extraído el carnet de conducir digital del conductor, el dispositivo de usuario de un agente de la autoridad puede elegir verificar la información con una fuente de autoridad, tal como un sistema de registros en el departamento de vehículos motorizados (u otra entidad que da servicio como representante). En esta situación, la verificación puede aprovechar la información de identidad en el DMV que se ha examinado. De manera similar, el dispositivo de usuario del agente de la autoridad puede verificar la información de permiso de circulación de vehículo o la información de estado del seguro.

El procedimiento también es aplicable en el contexto de vehículos autónomos. Haciendo referencia a las figuras 3C a 3E (que ilustran respectivamente los procedimientos 300C a 300E), puede establecerse una conexión entre un dispositivo de usuario y un sistema a bordo de vehículo (310); y después puede recibirse información de usuario a partir de un dispositivo de usuario (312) o puede recibirse la información de vehículo a partir del vehículo (322). Después de eso, el sistema a bordo de vehículo 110 y el dispositivo de usuario pueden interaccionar cada uno de manera inteligente para determinar (i) si la persona que intenta conducir el vehículo en un entorno de conducción compartida está autorizada para conducir; (ii) si la persona que espera al vehículo autónomo en un contexto de utilización compartida es el pasajero legítimo; y (iii) si el vehículo que se presenta es realmente el vehículo que se ha llamado.

En un contexto de conducción compartida, un grupo de conductores pueden compartir de manera conjunta la conducción de vehículos. Esta compartición puede surgir de la propiedad conjunta de un vehículo o a través de una entidad de alquiler que funciona con la naturaleza y el carácter de servicios de vehículos compartidos. En este contexto, el vehículo puede presentarse como un vehículo autónomo entregado a la puerta del conductor o en una ubicación elegida por el conductor. En una ilustración según la figura 3C, la información de usuario de la persona que intenta ocupar el asiento del conductor del vehículo puede compararse con información de conductores autorizados (334). La comparación puede realizarse de manera local en el sistema a bordo de vehículo. La comparación también puede realizarse de manera remota consultando una base de datos de la entidad de compartición. La comparación puede determinar si el usuario ha sido un miembro del club de compartición o si el usuario ha pagado para conducir el vehículo. Para que el conductor ocupe el asiento del conductor, el sistema a bordo de vehículo puede verificar para determinar que el usuario es un conductor autorizado y con carnet (336). La verificación puede incluir consultar en un sistema de registros y determinar que la información de carnet de conducir del usuario ya está en el sistema de registros. Gracias a la naturaleza aprobada de tal información en una fuente de autoridad tal como el DMV, el sistema a bordo de vehículo 110 puede determinar que la identidad afirmada es válida. En respuesta a determinar que el conductor es un usuario autorizado, el sistema a bordo de vehículo puede desbloquear el sistema de motor, el sistema de arranque, el sistema de frenos, así como otro sistema de control en el vehículo de modo que el usuario puede empezar a conducir el vehículo.

En un contexto de utilización compartida que utiliza vehículos autónomos, uno o más pasajeros pueden pedir el servicio. La petición puede ser en forma de llamar a un servicio de taxi u otras formas de servicio de utilización compartida. En el caso de vehículos autónomos, la petición puede conducir a la llegada de un vehículo sin conductor, tal como un coche sin conductor. En este contexto, se necesita implementar un mecanismo para que el

vehículo autónomo autentique al pasajero y para que el pasajero determine que el coche sin conductor es el que había llamado.

En una ilustración de la figura 3D, la información de usuario de la persona que espera recibir el servicio puede compararse con información de pasajeros abonados (344). La comparación puede realizarse de manera local en el sistema a bordo de vehículo. La comparación también puede realizarse de manera remota consultando una base de datos de la entidad de utilización compartida. La comparación puede determinar si el usuario ha sido un miembro del club de utilización compartida o si el usuario dispone de una cuenta lista para pagar para el servicio de utilización compartida. Para albergar al pasajero, el sistema a bordo de vehículo puede verificar para determinar que la información del usuario concuerda con información de pasajero, por ejemplo, a partir de una base de datos de abonados (344). La verificación puede incluir consultar un sistema de registros y determinar, por ejemplo, que la identidad ofrecida del usuario ya está en el sistema de registros. En respuesta a determinar que el conductor es un abonado actual y validar la identidad del usuario, el sistema a bordo de vehículo puede permitir que el usuario disfrute del servicio de utilización compartida.

Cuando un vehículo autónomo llega para un servicio de utilización compartida, el pasajero puede desear determinar que el vehículo es realmente el que el usuario ha llamado. En una ilustración de la figura 3E, puede recibirse la información de vehículo a partir del vehículo (322). Entonces puede compararse esta información con una base de datos de abonados (354). La comparación puede realizarse de manera remota consultando una base de datos de la entidad de utilización compartida. La comparación puede determinar si el vehículo que acaba de llegar pertenece realmente a la entidad de utilización compartida. El vehículo puede llegar como un coche sin conductor o con un conductor. En algunos casos, padres o familiares del pasajero pueden desear determinar que el conductor tiene realmente carnet y cualificación adecuados. Esta verificación puede seguir generalmente las etapas expuestas en la figura 3D. En este caso, para que un pasajero escrupuloso verifique que el vehículo es legítimo para su utilización o conducción, puede verificarse la información de vehículo en un sistema de registros para determinar que el vehículo se ha registrado de manera adecuada.

Tal como se describe a lo largo de la presente memoria, los programas informáticos (también conocidos como programas, software, aplicaciones de software o código) incluyen instrucciones de máquina para un procesador programable y pueden implementarse en un lenguaje de programación orientado a objetos y/u orientado a procedimiento de alto nivel y/o en un lenguaje de ensamblaje/máquina. Tal como se utilizan en la presente memoria, los términos “medio legible por máquina” y “medio legible por ordenador” se refieren a cualquier producto de programa informático, aparato y/o dispositivo (por ejemplo, discos magnéticos, discos ópticos, memoria, dispositivos lógicos programables (PLD)) utilizados para proporcionar instrucciones de máquina y/o datos a un procesador programable, incluyendo un medio legible por máquina que recibe instrucciones de máquina como señal legible por máquina. El término “señal legible por máquina” se refiere a cualquier señal utilizada para proporcionar instrucciones de máquina y/o datos a un procesador programable.

Los procesadores adecuados para la ejecución de un programa de instrucciones incluyen, a modo de ejemplo, microprocesadores tanto de propósito general como especial, y el único procesador o uno de múltiples procesadores de cualquier clase de ordenador. Generalmente, un procesador recibirá instrucciones y datos a partir de una memoria de sólo lectura o una memoria de acceso aleatorio o ambas. Los elementos de un ordenador pueden incluir un procesador para ejecutar instrucciones y una o más memorias para almacenar instrucciones y datos. Generalmente, un ordenador también incluirá, o estará operativamente acoplado para comunicarse con, uno o más dispositivos de almacenamiento masivo para almacenar archivos de datos; tales dispositivos incluyen discos magnéticos, tales como discos duros internos y discos extraíbles; discos magnetoópticos; y discos ópticos. Los dispositivos de almacenamiento adecuados para implementar de manera tangible instrucciones de programa informático y datos incluyen todas las formas de memoria no volátil, incluyendo a modo de ejemplo dispositivos de memoria de semiconductor, tales como EPROM (memoria de sólo lectura programable y borrable), EEPROM (memoria de sólo lectura programable y borrable eléctricamente) y dispositivos de memoria flash; discos magnéticos tales como discos duros internos y discos extraíbles; discos magnetoópticos; y discos CD-ROM y DVD-ROM. El procesador y la memoria pueden complementarse por, o incorporarse en, ASIC (circuitos integrados específicos de aplicación).

Para proporcionar interacción con un usuario, los sistemas y las técnicas descritos en este caso pueden implementarse en un ordenador que presenta un dispositivo de visualización (por ejemplo, un monitor de CRT (tubo de rayos catódicos), de LCD (pantalla de cristal líquido), monitores de LED (diodo emisor de luz) o de OLED (diodo emisor de luz orgánico)) para visualizar información para el usuario y un teclado y un dispositivo de puntero (por ejemplo, un ratón o una bola rastreadora) mediante el cual el usuario puede proporcionar entrada al ordenador. También pueden utilizarse otras clases de dispositivos para proporcionar interacción con un usuario; por ejemplo, retroalimentación proporcionada al usuario puede ser cualquier forma de retroalimentación sensorial (por ejemplo, retroalimentación visual, retroalimentación auditiva o retroalimentación táctil); y la entrada a partir del usuario puede recibirse de cualquier forma, incluyendo entrada acústica, de voz o táctil.

Los sistemas y las técnicas descritos en este caso pueden implementarse en un sistema informático que incluye un componente de extremo posterior (por ejemplo, como servidor de datos) o que incluye un componente de

soporte intermedio (por ejemplo, un servidor de aplicación) o que incluye un componente de extremo delantero (por ejemplo, un ordenador de cliente que presenta una interfaz gráfica de usuario o un navegador de web a través del cual un usuario puede interaccionar con una implementación de los sistemas y técnicas descritos en este caso) o cualquier combinación de tales componentes de extremo posterior, de soporte intermedio o de extremo delantero. Los componentes del sistema pueden estar interconectados mediante cualquier forma o medio de comunicación de datos digitales (por ejemplo, una red de comunicación). Los ejemplos de redes de comunicación incluyen una red de área local ("LAN"), una red de área amplia ("WAN") e Internet.

El sistema informático puede incluir clientes y servidores. Un cliente y un servidor están generalmente remotos uno con respecto a otro y normalmente interaccionan a través de una red de comunicación. La relación de cliente y servidor surge gracias a programas informáticos que se ejecutan en los ordenadores respectivos y que presentan una relación de cliente-servidor entre sí.

Se han descrito varias implementaciones. No obstante, se entenderá que pueden realizarse diversas modificaciones sin alejarse del alcance de la invención. Por ejemplo, gran parte de este documento se ha descrito con respecto a aplicaciones de mensajería y mapeo, pero también pueden abordarse otras formas de aplicaciones gráficas, tales como guías de programa interactivas, navegación y aumento en páginas web y otras aplicaciones de este tipo.

Además, los flujos de lógica representados en las figuras no requieren el orden particular mostrado, o el orden secuencial, para lograr resultados deseables. Por consiguiente, otras formas de realización están dentro del alcance de las siguientes reivindicaciones.

REIVINDICACIONES

1. Método implementado por ordenador que comprende:

establecer una conexión entre un dispositivo de usuario de un primer usuario y un sistema a bordo de un vehículo que está siendo conducido por el usuario (310);

solicitar acceso, a través de la conexión establecida, a información de usuario en el dispositivo de usuario;

en respuesta a la concesión de acceso, recuperar por lo menos una parte de la información de usuario a partir del dispositivo de usuario, incluyendo la parte de información de usuario un documento de identificación digital del primer usuario que había sido emitido por una entidad después de haber examinado al primer usuario, incluyendo el documento de identificación digital un elemento biométrico digital del primer usuario, así como una marca de agua digital que indica la entidad emisora (324);

conservar, en el sistema a bordo del vehículo, datos que codifican el documento de identificación digital del primer usuario de tal manera que, cuando el vehículo es inspeccionado por un agente de terceros, se presenta el documento de identificación digital del primer usuario al agente de terceros; y

autenticar, en el sistema a bordo del vehículo, un segundo usuario para desbloquear el vehículo y pasar a ser un conductor del vehículo verificando características de seguridad de un carnet de conducir digital y un elemento biométrico proporcionado por el segundo usuario con el documento de identificación digital del primer usuario conservado en el sistema a bordo del vehículo, en el que las características de seguridad del carnet de conducir digital incluyen una marca de agua digital, y en el que la verificación de las características de seguridad incluye

determinar si el carnet de conducir digital del segundo usuario que va a autenticarse es legítimo y válido, y, si el carnet de conducir digital es legítimo y válido, verificar información de identidad del carnet de conducir digital proporcionado con una base de datos de terceros, en el que los datos de terceros son una base de datos remota que incluye datos de identidad examinados por una autoridad externa; y

si la información de identidad se valida de acuerdo con los datos de identidad examinados, proporcionar acceso completo al segundo usuario autenticado para utilizar el vehículo.

2. Método según la reivindicación 1, que comprende:

hacer que se compare el elemento biométrico digital del documento de identificación digital del primer usuario con un usuario que conduce el vehículo, y hacer que se verifique información del documento de identificación digital en una base de datos de la entidad emisora.

3. Método según la reivindicación 1, en el que cuando el vehículo es inspeccionado por el agente de terceros, se visualiza el documento de identificación digital del primer usuario en un panel de visualización del sistema a bordo del vehículo.

4. Método según la reivindicación 1, en el que cuando el vehículo es inspeccionado por el agente de terceros, los datos que codifican el documento de identificación digital del primer usuario se transmiten desde el sistema a bordo del vehículo hasta un dispositivo de usuario del agente de terceros, de tal manera que el documento de identificación digital sea reproducido en una pantalla del dispositivo de usuario del agente de terceros.

5. Método según la reivindicación 1, en el que la recuperación de por lo menos la parte de la información de usuario a partir del dispositivo de usuario incluye

recuperar información del seguro del primer usuario a partir del dispositivo de usuario, indicando la información del seguro el estado del seguro actual del primer usuario, y

opcionalmente, en el que cuando el vehículo es inspeccionado por el agente de terceros, la información del seguro del primer usuario se transmite desde el sistema a bordo del vehículo hasta un dispositivo de usuario del agente de terceros para que la revise un agente de la autoridad.

6. Método según la reivindicación 1, en el que la recuperación de por lo menos la parte de la información de usuario a partir del dispositivo de usuario incluye la recuperación de información de vehículo a partir del dispositivo de usuario, comprendiendo la información de vehículo información de titularidad del vehículo e información de permiso de circulación del vehículo.

7. Método según la reivindicación 6, en el que cuando el vehículo es inspeccionado por el agente de terceros, la información de vehículo del primer usuario se transmite desde el sistema a bordo del vehículo hasta un dispositivo

de usuario del agente de terceros para que la revise el agente de terceros.

8. Método según la reivindicación 6, en el que la información de titularidad incluye información en un formato en cadena que muestra información de propiedad anterior e información de transferencia de titularidad del vehículo.

9. Método según la reivindicación 6, en el que la información de permiso de circulación incluye información en un formato en cadena que muestra información de permiso de circulación anterior del vehículo.

10. Sistema a bordo de un vehículo (110), incluyendo el sistema un procesador y una pantalla que pueden funcionar para realizar las operaciones del método según cualquiera de las reivindicaciones 1 a 9, en el que la conexión se establece entre el dispositivo de usuario (120) del primer usuario y el sistema a bordo del vehículo.

11. Sistema según la reivindicación 10, en el que la operación de establecer la conexión comprende o bien a) establecer una conexión cableada entre el sistema y el dispositivo de usuario del primer usuario o bien b) establecer una conexión inalámbrica entre el sistema y el dispositivo de usuario del primer usuario.

12. Medio legible por ordenador, que comprende un software que, cuando se ejecuta, hace que el ordenador realice las operaciones del método según cualquiera de las reivindicaciones 1 a 9.

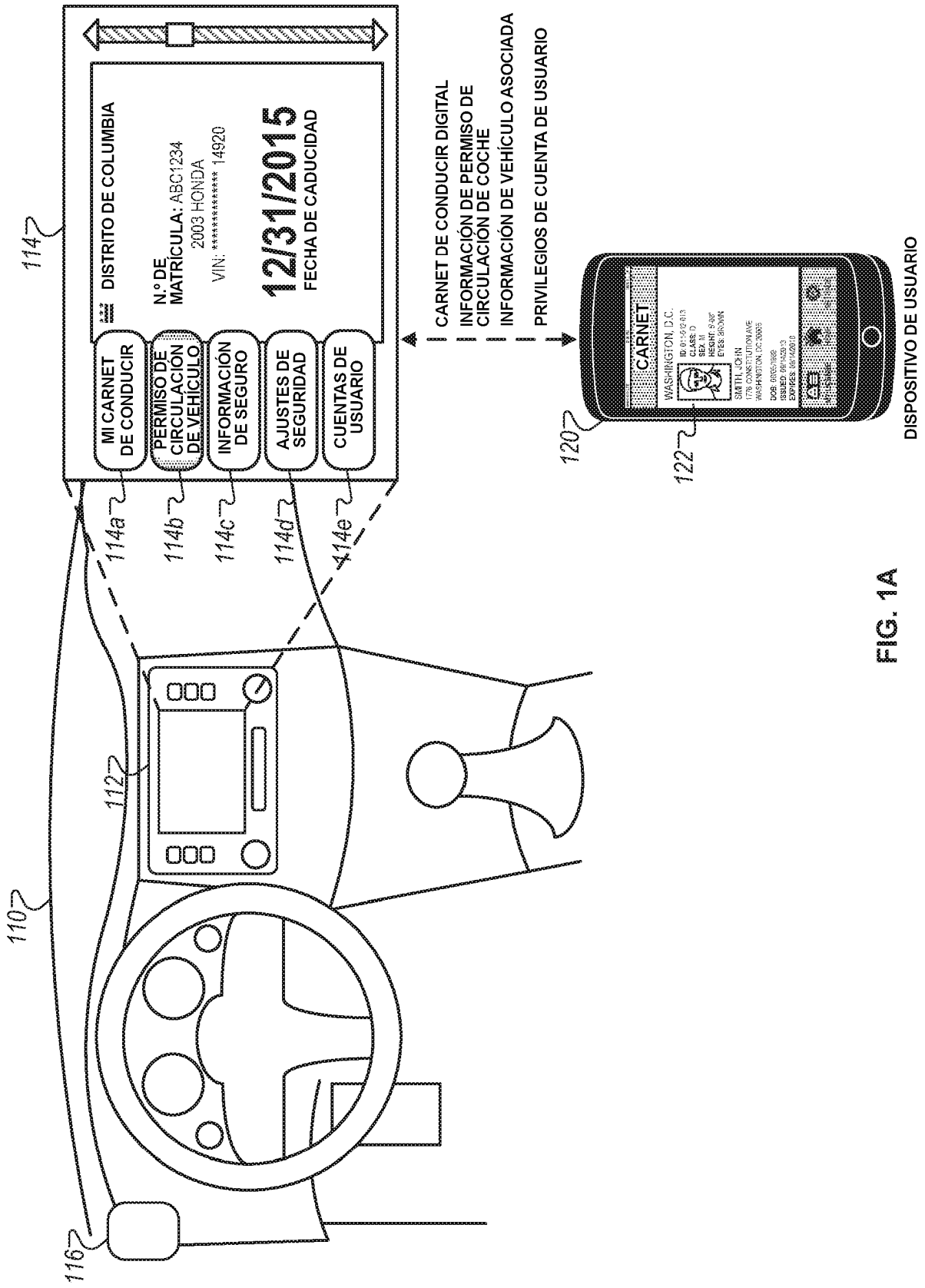
114
DISTRITO DE COLUMBIA
MI CARNET DE CONDUCIR
PERMISO DE CIRCULACIÓN DE VEHÍCULO
INFORMACIÓN DE SEGURO
AJUSTES DE SEGURIDAD
CUENTAS DE USUARIO
N.º DE MATRÍCULA: ABC1234
2003 HONDA
VIN: ********** 14920
12/31/2015
FECHA DE CADUCIDAD
114a
114b
114c
114d
114e
CARNET DE CONDUCIR DIGITAL
INFORMACIÓN DE PERMISO DE CIRCULACIÓN DE COCHE
INFORMACIÓN DE VEHÍCULO ASOCIADA
PRIVILEGIOS DE CUENTA DE USUARIO
120
CARNET
WASHINGTON, D.C.
122
110
112
116
DISPOSITIVO DE USUARIO

FIG. 1A

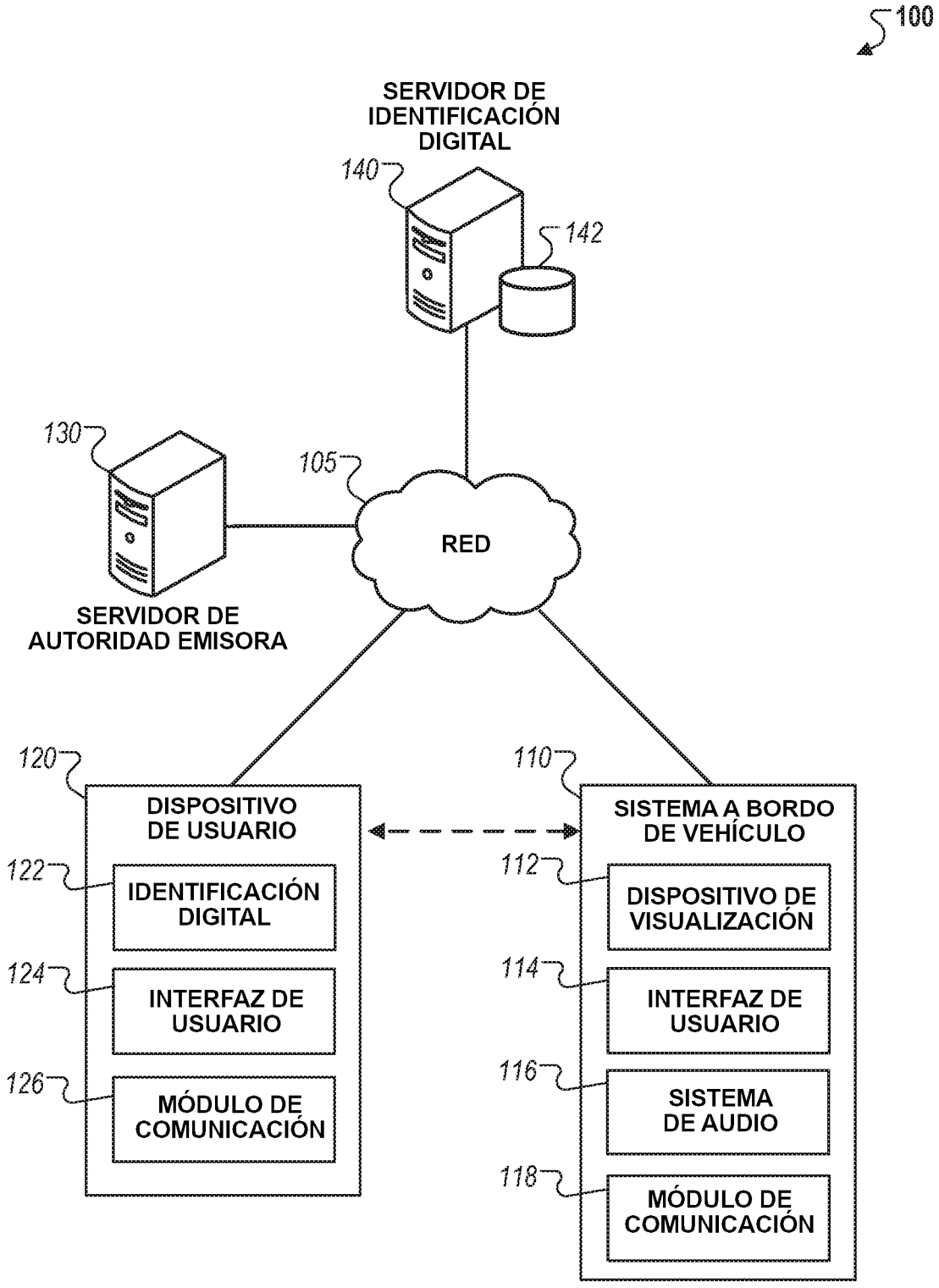
100
SERVIDOR DE IDENTIFICACIÓN DIGITAL
140
142
130
105
RED
SERVIDOR DE AUTORIDAD EMISORA
120
DISPOSITIVO DE USUARIO
122
IDENTIFICACIÓN DIGITAL
124
INTERFAZ DE USUARIO
126
MÓDULO DE COMUNICACIÓN
110
SISTEMA A BORDO DE VEHÍCULO
112
DISPOSITIVO DE VISUALIZACIÓN
114
INTERFAZ DE USUARIO
116
SISTEMA DE AUDIO
118
MÓDULO DE COMUNICACIÓN

FIG. 1B

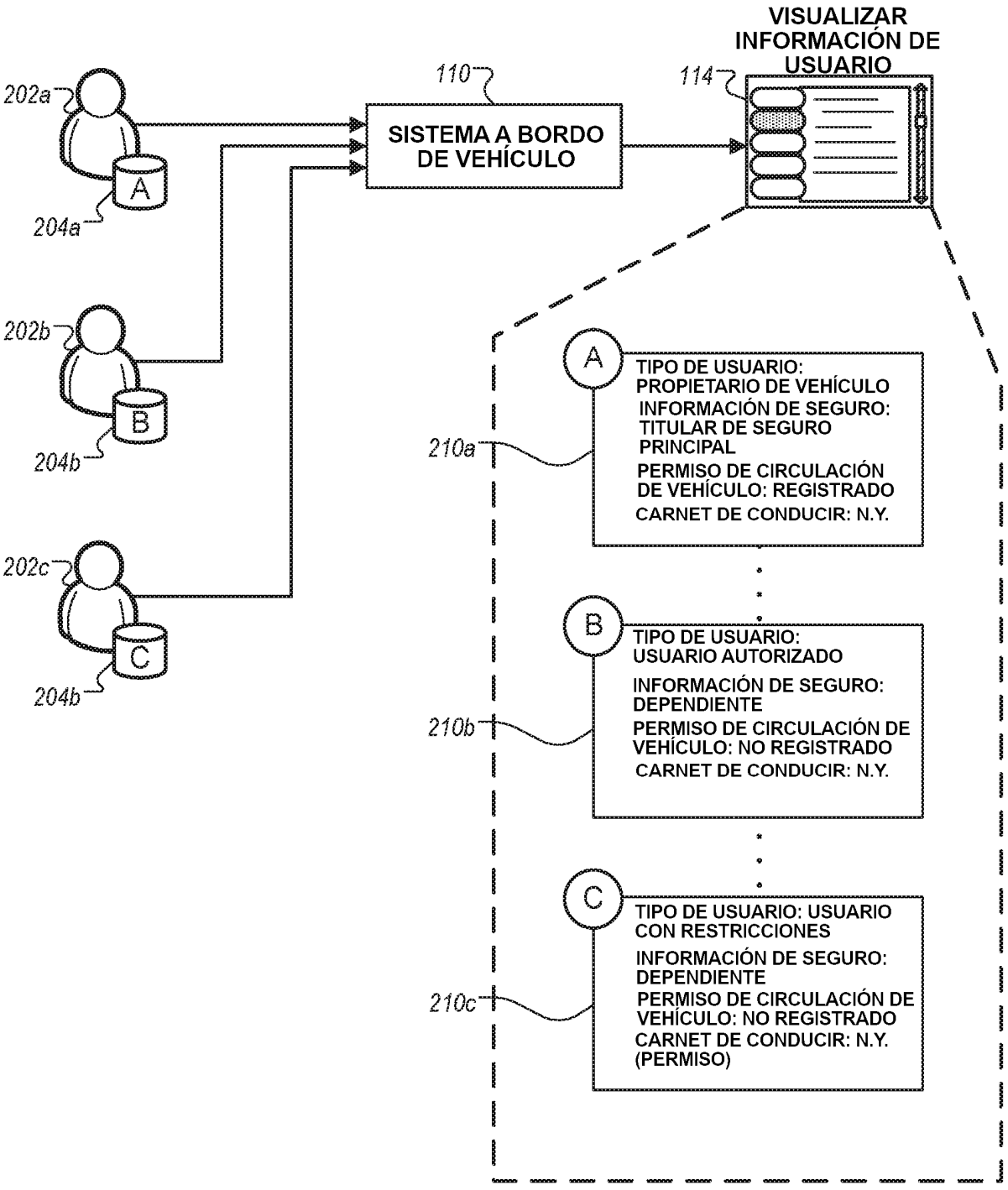
VISUALIZAR INFORMACIÓN DE USUARIO
110
114
SISTEMA A BORDO DE VEHÍCULO
202a
A
204a
202b
B
204b
202c
C
204b
A
TIPO DE USUARIO: PROPIETARIO DE VEHÍCULO
INFORMACIÓN DE SEGURO: TITULAR DE SEGURO PRINCIPAL
PERMISO DE CIRCULACIÓN DE VEHÍCULO: REGISTRADO
CARNET DE CONDUCIR: N.Y.
210a
B
TIPO DE USUARIO: USUARIO AUTORIZADO
INFORMACIÓN DE SEGURO: DEPENDIENTE
PERMISO DE CIRCULACIÓN DE VEHÍCULO: NO REGISTRADO
CARNET DE CONDUCIR: N.Y.
210b
C
TIPO DE USUARIO: USUARIO CON RESTRICCIONES
INFORMACIÓN DE SEGURO: DEPENDIENTE
PERMISO DE CIRCULACIÓN DE VEHÍCULO: NO REGISTRADO
CARNET DE CONDUCIR: N.Y. (PERMISO)
210c

FIG. 2

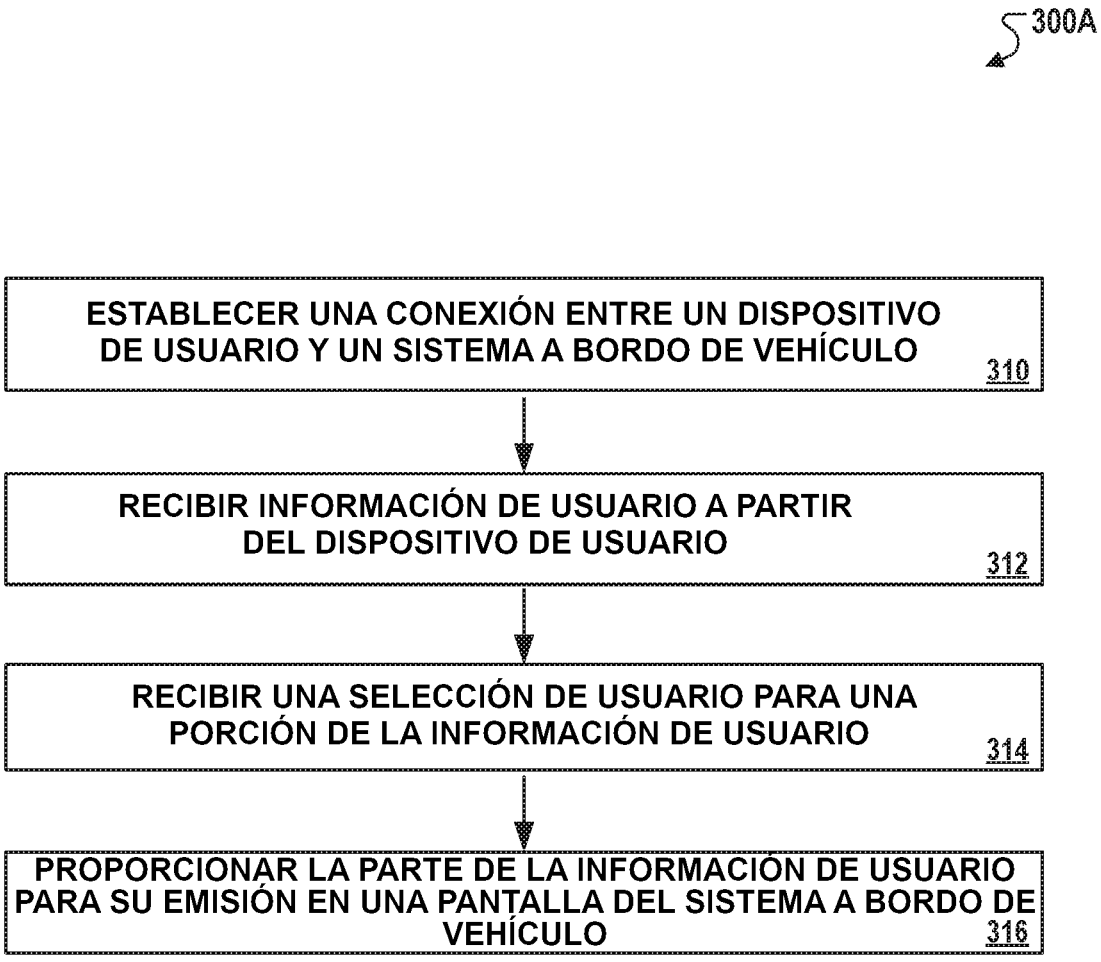
300A
ESTABLECER UNA CONEXIÓN ENTRE UN DISPOSITIVO DE USUARIO Y UN SISTEMA A BORDO DE VEHÍCULO
310
RECIBIR INFORMACIÓN DE USUARIO A PARTIR DEL DISPOSITIVO DE USUARIO
312
RECIBIR UNA SELECCIÓN DE USUARIO PARA UNA PORCIÓN DE LA INFORMACIÓN DE USUARIO
314
PROPORCIONAR LA PARTE DE LA INFORMACIÓN DE USUARIO PARA SU EMISIÓN EN UNA PANTALLA DEL SISTEMA A BORDO DE VEHÍCULO
316

FIG. 3A

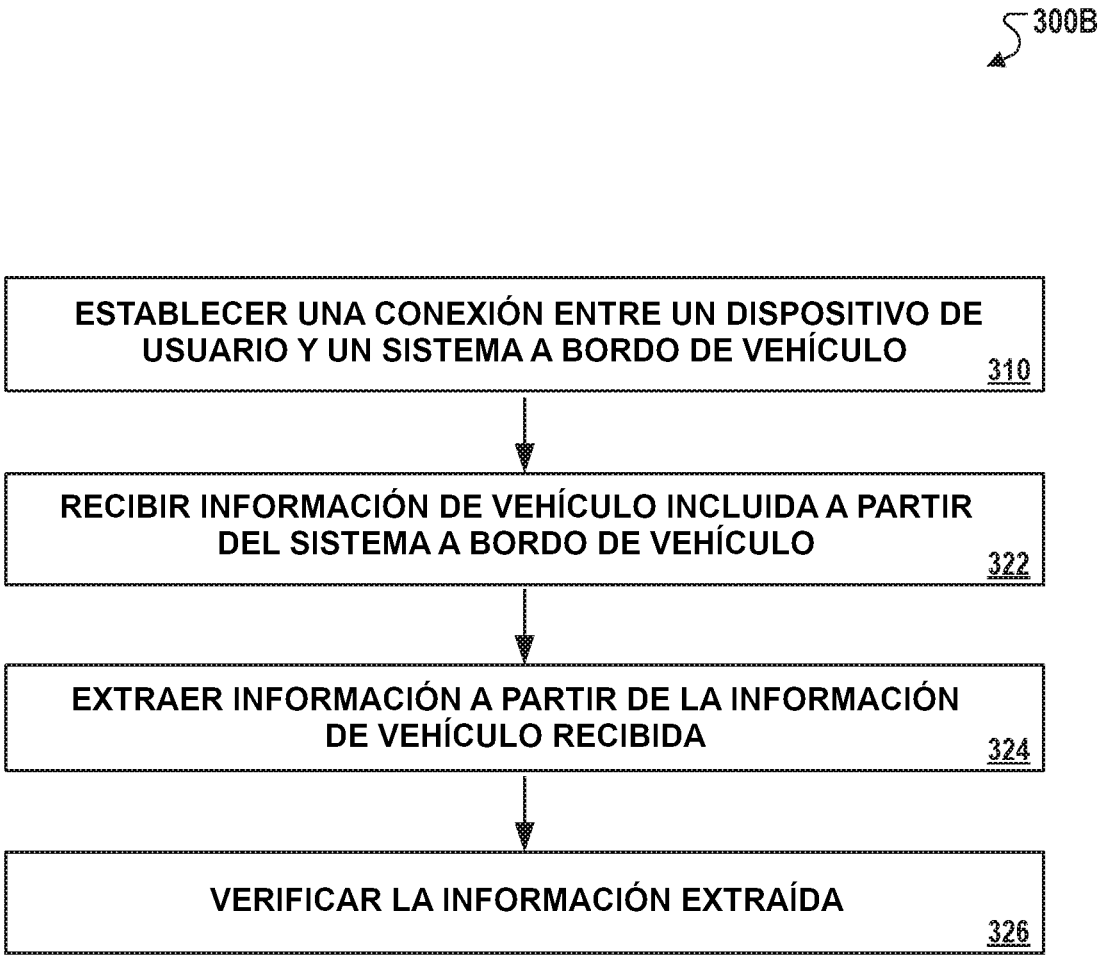
300B
ESTABLECER UNA CONEXIÓN ENTRE UN DISPOSITIVO DE USUARIO Y UN SISTEMA A BORDO DE VEHÍCULO
310
RECIBIR INFORMACIÓN DE VEHÍCULO INCLUIDA A PARTIR DEL SISTEMA A BORDO DE VEHÍCULO
322
EXTRAER INFORMACIÓN A PARTIR DE LA INFORMACIÓN DE VEHÍCULO RECIBIDA
324
VERIFICAR LA INFORMACIÓN EXTRAÍDA
326

FIG. 3B

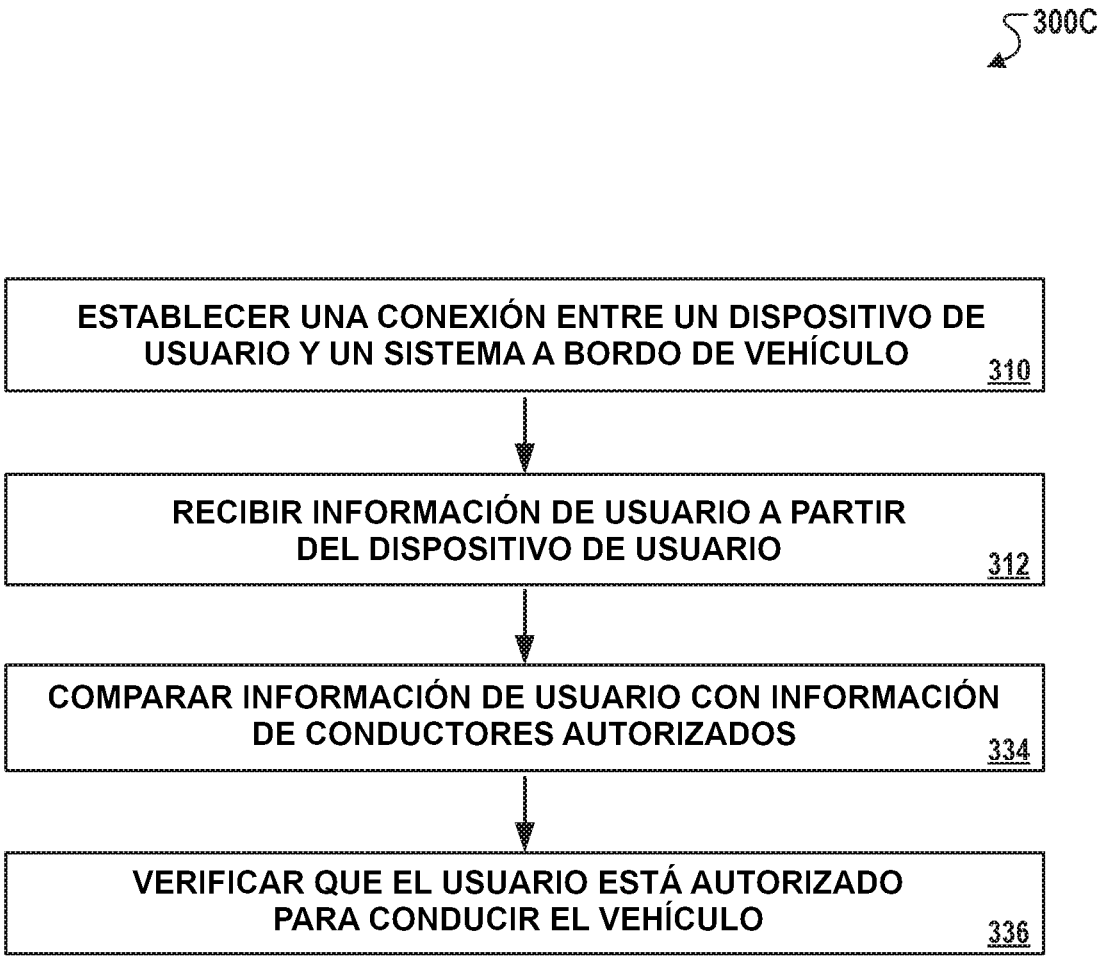
300C
ESTABLECER UNA CONEXIÓN ENTRE UN DISPOSITIVO DE USUARIO Y UN SISTEMA A BORDO DE VEHÍCULO
310
RECIBIR INFORMACIÓN DE USUARIO A PARTIR DEL DISPOSITIVO DE USUARIO
312
COMPARAR INFORMACIÓN DE USUARIO CON INFORMACIÓN DE CONDUCTORES AUTORIZADOS
334
VERIFICAR QUE EL USUARIO ESTÁ AUTORIZADO PARA CONDUCIR EL VEHÍCULO
336

FIG. 3C

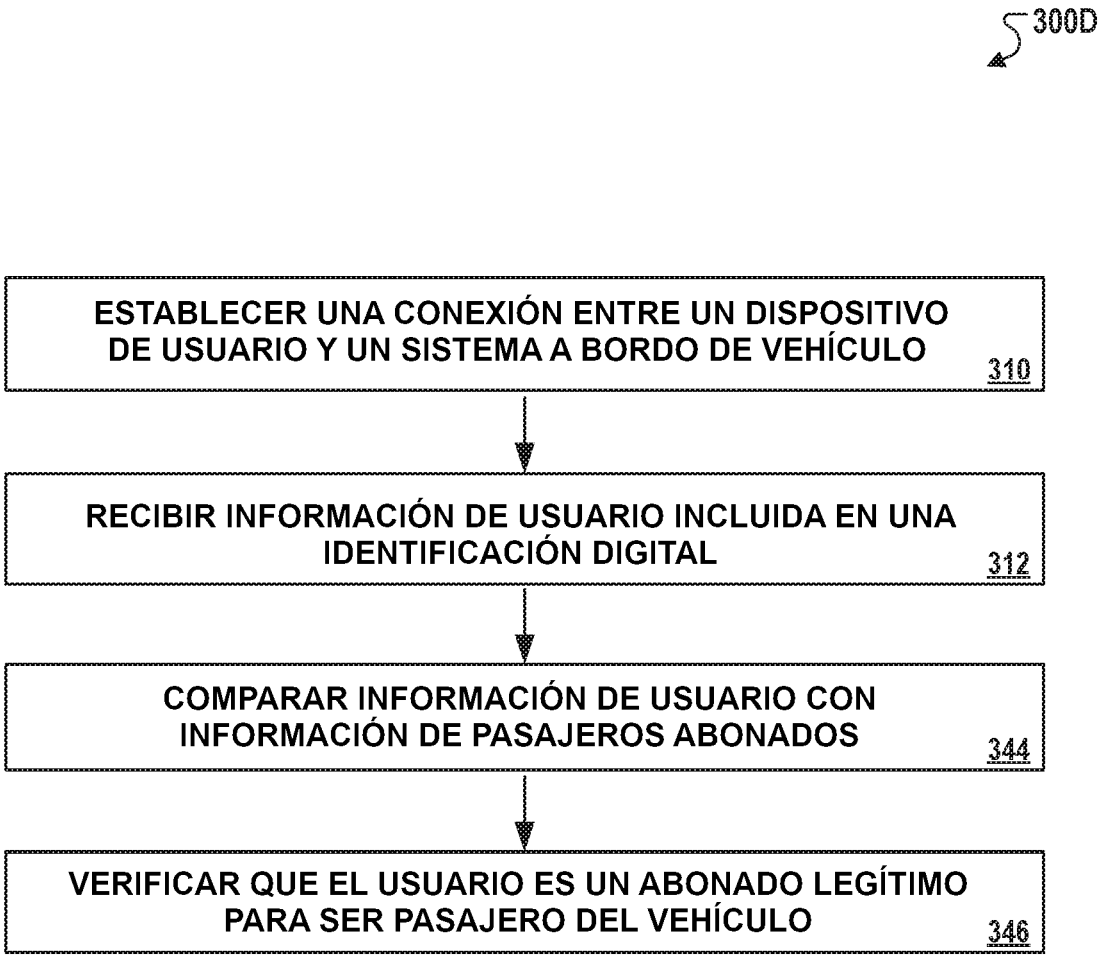
300D
ESTABLECER UNA CONEXIÓN ENTRE UN DISPOSITIVO DE USUARIO Y UN SISTEMA A BORDO DE VEHÍCULO
310
RECIBIR INFORMACIÓN DE USUARIO INCLUIDA EN UNA IDENTIFICACIÓN DIGITAL
312
COMPARAR INFORMACIÓN DE USUARIO CON INFORMACIÓN DE PASAJEROS ABONADOS
344
VERIFICAR QUE EL USUARIO ES UN ABONADO LEGÍTIMO PARA SER PASAJERO DEL VEHÍCULO
346

FIG. 3D

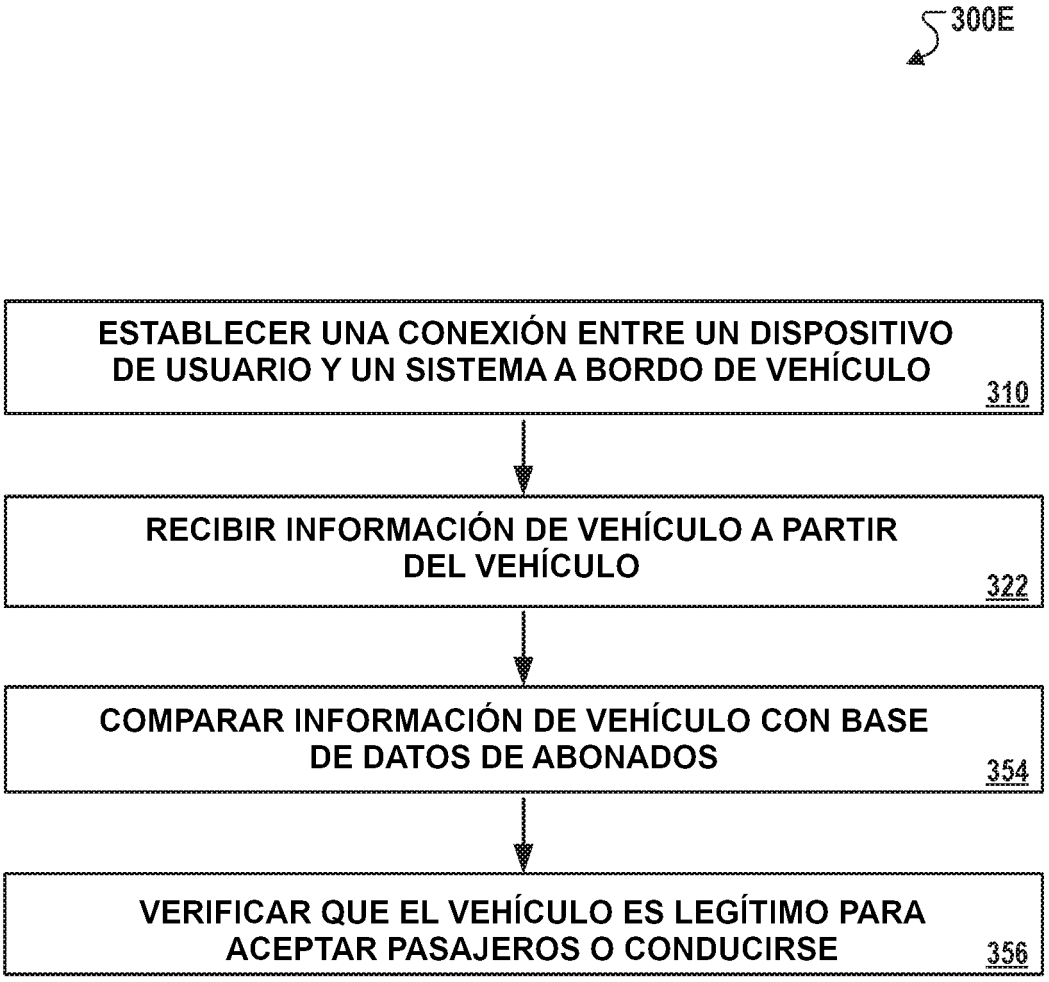
300E
ESTABLECER UNA CONEXIÓN ENTRE UN DISPOSITIVO DE USUARIO Y UN SISTEMA A BORDO DE VEHÍCULO
310
RECIBIR INFORMACIÓN DE VEHÍCULO A PARTIR DEL VEHÍCULO
322
COMPARAR INFORMACIÓN DE VEHÍCULO CON BASE DE DATOS DE ABONADOS
354
VERIFICAR QUE EL VEHÍCULO ES LEGÍTIMO PARA ACEPTAR PASAJEROS O CONDUCIRSE
356

FIG. 3E