(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 735 805**

(51) Int. CI.:

G07B 15/04 (2006.01)
G07B 15/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.01.2017 E 17709787 (0)**

(97) Fecha y número de publicación de la concesión europea: **24.04.2019 EP 3238182**

(54) Título: **Dispositivo de a bordo para un vehículo**

(30) Prioridad:

14.01.2016 IT UB20169991

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.12.2019

(73) Titular/es:

AUTOSTRADE TECH S.P.A. (100.0%)
Via Alberto Bergamini, 50
00159 Roma, IT

(72) Inventor/es:

GARGIANI, LEONARDO

(74) Agente/Representante:

CURELL SUÑOL, S.L.P.

DESCRIPCIÓN

Dispositivo de a bordo para un vehículo.

Campo técnico de la invención

La presente invención se refiere, en general, al campo de los servicios telemáticos de tráfico. En particular, la presente invención se refiere a un dispositivo de a bordo para un vehículo, adecuado para su uso en un sistema que presta soporte a un servicio telemático de tráfico.

Técnica anterior

Se conocen sistemas que prestan soporte a servicios telemáticos de tráfico. Estos servicios comprenden tanto servicios para el usuario (tales como pago de peajes para el acceso a tramos de carreteras/autopistas, pago de tarifas de aparcamiento, etc.), como servicios de administrador (tales como el control del acceso a zonas urbanas con restricciones de tráfico, la monitorización del tráfico a lo largo del tramo de una carretera/autopista, etc.).

Generalmente, estos sistemas comprenden un dispositivo de a bordo (conocido también como “OBU”, es decir “On Board Unit” (“Unidad de A Bordo”)) adecuado para su instalación a bordo de un vehículo, y una pluralidad de dispositivos de carretera (conocidos, también, como “RSU” es decir “Road Side Units” (“Unidades de Carretera”)) adecuados para su instalación en la cuneta de la carretera, en pasarelas o puntos de acceso, o en áreas de peaje.

Generalmente, tanto el dispositivo de a bordo como los dispositivos de carretera están provistos de etapas respectivas de comunicación por radiofrecuencia (típicamente, etapas de DSRC, es decir “Dedicated Short Range Communication” (“Comunicación Dedicada de Corto Alcance”)) que permiten que el dispositivo de a bordo intercambie información con los dispositivos de carretera. Típicamente, estas etapas de comunicación por radiofrecuencia usan portadoras de radiofrecuencia, por ejemplo, en el intervalo de frecuencias comprendido entre 5 y 6 GHz.

Cada dispositivo de a bordo tiene, típicamente, un código de identificación exclusivo asociado OBU-ID, con el cual se configura por medio de software durante su fabricación. Por otra parte, cuando se asigna un dispositivo de a bordo a un usuario, el mismo se puede configurar con información sobre el usuario (por ejemplo, detalles personales) e información sobre el vehículo (matrícula, etcétera). La configuración de un dispositivo de a bordo conlleva también, generalmente, la carga de las aplicaciones de software que proporcionan los servicios telemáticos de tráfico a los que presta soporte el dispositivo.

Después de que se haya configurado e instalado a bordo un dispositivo de a bordo, puede que resulte necesario modificar su configuración, por ejemplo con el fin de actualizar o activar las aplicaciones de software ya presentes, o cargar aplicaciones nuevas, o eliminar o deshabilitar aquellas aplicaciones que ya no tienen interés para el usuario. Este es el caso correspondiente, por ejemplo, a cuando un usuario desea activar temporalmente un servicio de pago de peaje en un país extranjero. En este caso, la configuración del dispositivo de a bordo del usuario se debe modificar cargando y activando temporalmente una aplicación de software capaz de prestar soporte a este servicio.

Por otra parte, después de que se haya configurado e instalado a bordo un dispositivo de a bordo, puede que sea necesario llevar a cabo comprobaciones sobre su funcionamiento y pruebas diagnósticas, tales como una comprobación del nivel de carga de su batería. También podría resultar necesario comprobar la información de configuración (referente al usuario y/o al vehículo) almacenada por el dispositivo de a bordo.

Todas las operaciones antes mencionadas requieren acceso al dispositivo de a bordo con el fin de realizar la escritura o lectura de su memoria y son llevadas a cabo, generalmente, por medio de equipos provistos de etapas de comunicación por radiofrecuencia capaces de comunicarse con la etapa de comunicación presente en el dispositivo de a bordo. Estos equipos están presentes, en general, en los centros operativos gestionados por la empresa que proporciona el servicio telemático de tráfico o por la empresa que gestiona la carretera o la autopista a lo largo de la cual se proporciona el servicio telemático de tráfico. Por lo tanto, si un usuario desea modificar la configuración de su dispositivo de a bordo o comprobar el funcionamiento del mismo, en general debe dirigirse a uno de estos centros operativos.

El documento US 2014/0316685 describe un dispositivo de a bordo para un sistema que presta soporte a servicios telemáticos de tráfico, el cual comprende un módulo de comunicaciones de alcance cercano para su comunicación con un primer dispositivo de comunicaciones externo (por ejemplo, el teléfono móvil del usuario), un módulo de comunicaciones de alcance lejano (por ejemplo DSRC) para su comunicación con segundos dispositivos externos (por ejemplo, los dispositivos de carretera del sistema) y una memoria no volátil que es accesible por ambos módulos de comunicación. El módulo de comunicaciones de alcance cercano puede ser, por ejemplo, una etiqueta de NFC pasiva. Esta es alimentada por el teléfono móvil del usuario durante su comunicación y, de este modo, puede acceder a la memoria no volátil, y, al realizar esto, puede suministrar energía a la misma, incluso cuando el

resto del dispositivo de a bordo no se encuentra en condiciones operativas. Por lo tanto, el contenido de la memoria no volátil se puede leer y/o escribir por medio de la conexión entre el teléfono móvil del usuario y el módulo de comunicaciones del alcance cercano, con independencia de si el resto del dispositivo de a bordo está o no en modo operativo. De esta manera, es posible modificar la configuración del dispositivo de a bordo, por ejemplo, escribiendo datos de configuración en la memoria no volátil, mediante el teléfono móvil del usuario. De forma similar, es posible leer el contenido de la memoria no volátil mediante el teléfono móvil del usuario.

Otros documentos de la técnica anterior son el US 2014/316992 y US 2015/100394.

Breve descripción de la invención

El solicitante ha observado que el dispositivo de a bordo descrito por el documento US 2014/0316685 tiene una serie de inconvenientes.

En primer lugar, el solicitante ha observado que el módulo de comunicaciones de alcance cercano incluido en este dispositivo, debido a que tiene acceso directo a la memoria no volátil del dispositivo tanto durante la lectura como durante la escritura, reduce de forma desventajosa la seguridad del dispositivo de a bordo. En general, las tecnologías de corto alcance y campo cercano (tales como la tecnología NFC) tienen mecanismos para la autenticación y la protección de la conexión los cuales no son particularmente seguros, basándose la seguridad de la conexión, principalmente, en el hecho de tener un alcance de cobertura de solamente unos pocos centímetros. Por lo tanto, si, por ejemplo, un tercero tomara posesión del dispositivo de a bordo de un usuario, el mismo podría acceder al dispositivo de a bordo usando su propio teléfono móvil (u otro dispositivo equipado con un lector de NFC), y modificar, de este modo, la configuración del mismo, o leer información almacenada en él y usarla para clonar el dispositivo de a bordo (es decir, copiarla en otro dispositivo de a bordo).

Además, el acceso directo a la memoria no volátil por el módulo de comunicaciones de alcance cercano podría dar como resultado, de manera desventajosa, un uso ineficiente de los recursos computacionales y de almacenamiento del dispositivo de a bordo. De hecho, por ejemplo, el usuario podría decidir escribir datos de configuración en la memoria (o, de manera similar, leer datos de configuración de la memoria) no sabiendo que, precisamente en ese momento, el dispositivo de a bordo está ocupado en otra actividad prioritaria, por ejemplo un intercambio de datos con uno de los dispositivos de carretera. En este caso, la operación de escritura de datos de configuración iniciada por el usuario, aunque es de menor prioridad, podría privar de recursos computacionales, desventajosamente, a la actividad de mayor prioridad, con el riesgo de ralentizar o incluso detener su ejecución.

Teniendo en cuenta lo anterior, el objetivo de la presente invención es proporcionar un dispositivo de a bordo para un vehículo a motor, de acuerdo con la reivindicación independiente 1, que es adecuado para su uso en un sistema que presta soporte a un servicio telemático de tráfico y que resuelve los problemas antes mencionados.

En particular, el objetivo de la presente invención es proporcionar un dispositivo de a bordo para un vehículo a motor, de acuerdo con la reivindicación independiente 1, que es adecuado para su uso en un sistema que presta soporte a un servicio telemático de tráfico, que es más seguro y que usa de forma más eficiente sus recursos computacionales y de almacenamiento asociados.

Según formas de realización de la presente invención, este objetivo se logra con un dispositivo de a bordo para un vehículo, el cual comprende una etapa de comunicaciones por radiofrecuencia para su comunicación con los dispositivos de carretera, una etapa de comunicación de corto alcance para su comunicación con un dispositivo electrónico (por ejemplo, un teléfono móvil), situado en las proximidades del mismo, dos memorias y una unidad de procesado de datos que cooperan con ambas etapas de comunicación. Una primera memoria actúa como memoria operativa central accesible por parte de la unidad de procesado de datos solamente, y almacena por lo menos una primera clave de cifrado. Una segunda memoria es accesible directamente, en cambio, por la etapa de comunicaciones de corto alcance, está conectada eléctricamente a la misma o integrada en ella y almacena primeros datos referentes al dispositivo de a bordo. La etapa de comunicaciones de corto alcance está configurada para transmitir al dispositivo electrónico estos primeros datos, también en modo de alimentación suspendida o en caso de funcionamiento deficiente de la etapa de comunicaciones por radiofrecuencia. La etapa de comunicaciones de corto alcance está configurada además para recibir segundos datos cifrados desde el dispositivo electrónico y almacenarlos temporalmente en la segunda memoria. La unidad de procesado de datos está configurada para descifrar, tras la recepción de una señal de reactivación, estos segundos datos cifrados usando la clave de cifrado almacenada en la primera memoria operativa central y para almacenar los segundos datos en la primera memoria operativa central.

El dispositivo de a bordo es, de manera ventajosa, seguro, puesto que, en el momento de la recepción de datos desde el dispositivo electrónico por medio de la etapa de comunicaciones de corto alcance, los datos a descifrar y la clave de cifrado que es necesaria para descifrarlos están almacenados en dos memorias independientes físicamente, una de las cuales (a saber, aquella que almacena la clave) es accesible solamente por la unidad de procesado de datos, es decir, la etapa de comunicaciones de corto alcance no puede acceder directamente a ella. Por lo tanto, a pesar del hecho de que la etapa de comunicaciones de corto alcance permite establecer una

conexión no protegida entre el dispositivo electrónico y el dispositivo de a bordo, el dispositivo de a bordo es, de manera ventajosa, más seguro.

Además, el dispositivo de a bordo permite un uso más eficiente de sus recursos computacionales y de almacenamiento, puesto que la transferencia de los datos hacia la primera memoria operativa central y el procesado subsiguiente de los mismos se activan tras la recepción de la señal de reactivación en la unidad de procesado de datos. Esto permite una implementación de los mecanismos para gestionar la prioridad de las diversas operaciones que implican a la unidad de procesado de datos y a la primera memoria operativa central del dispositivo de a bordo, con lo cual, por ejemplo, para la actividad de procesado de datos recibidos desde la etapa de comunicaciones de corto alcance, la unidad de procesado de datos recibe señales de reactivación después de completar la ejecución de las actividades de mayor prioridad (por ejemplo, las actividades de intercambio de datos entre la etapa de comunicaciones por radiofrecuencia y dispositivos de carretera).

Según un primer aspecto, la presente invención proporciona un dispositivo de a bordo para un vehículo, siendo adecuado el dispositivo de a bordo para su uso en un sistema que proporciona un servicio telemático de tráfico, comprendiendo el dispositivo de a bordo:

- una etapa de comunicaciones por radiofrecuencia configurada para comunicarse con un dispositivo de carretera de dicho sistema;

- una etapa de comunicaciones de corto alcance configurada para comunicarse con un dispositivo electrónico ubicado en sus proximidades;

- una unidad de procesado de datos que coopera con la etapa de comunicaciones por radiofrecuencia y con la etapa de comunicaciones de corto alcance;

- una primera memoria operativa central accesible por la unidad de procesado de datos, almacenando la primera memoria operativa central por lo menos una clave de cifrado;

- una segunda memoria conectada eléctricamente a la etapa de comunicaciones de corto alcance o integrada en esta y accesible directamente por la etapa de comunicaciones de corto alcance, almacenando la segunda memoria unos primeros datos referentes al dispositivo de a bordo,

estando configurada la etapa de comunicaciones de corto alcance para transmitir al dispositivo electrónico los primeros datos, también en modo de alimentación suspendida o en caso de funcionamiento deficiente de la etapa de comunicaciones por radiofrecuencia y estando configurada además para recibir unos segundos datos cifrados desde el dispositivo electrónico y almacenarlos temporalmente en la segunda memoria, y

estando configurada la unidad de procesado de datos para descifrar, tras la recepción de una señal de reactivación, los segundos datos cifrados usando la por lo menos una clave de cifrado almacenada en la primera memoria operativa central y para almacenar los segundos datos en la primera memoria operativa central.

Preferentemente, la primera memoria operativa central se implementa dentro de la unidad de procesado de datos.

Alternativamente, la primera memoria operativa central se implementa fuera de la unidad de procesado de datos, y la primera memoria operativa central almacena un identificador de hardware UID_{120} de la unidad de procesado de datos de una manera no modificable y no borrable.

Preferentemente, el dispositivo comprende, también, una interfaz de cifrado de hardware entre la primera memoria operativa central y la unidad de procesado de datos.

Preferentemente, la etapa de comunicaciones de corto alcance está configurada para enviar dicha señal de reactivación a la unidad de procesado de datos.

De forma adicional o alternativa, el dispositivo comprende también un botón accesible manualmente desde el exterior del dispositivo, estando configurado el botón de manera que, cuando es presionado, dicha señal de reactivación se envía a la unidad de procesado de datos.

Preferentemente, los primeros datos se almacenan en la segunda memoria, cifrados con una clave privada de un mecanismo de cifrado asimétrico, y la etapa de comunicaciones de corto alcance está configurada para transmitir los primeros datos al dispositivo electrónico, cifrados con dicha clave privada. Los primeros datos puestos a disposición para su lectura y cifrados con la clave privada en la segunda memoria comprenden, preferentemente, datos de etiqueta del dispositivo de a bordo, que incluyen, en particular, su código de identificación exclusivo OBU-ID.

De acuerdo con una variante ventajosa, la etapa de comunicaciones de corto alcance está configurada para recibir

dichos primeros datos de un servidor central a través del dispositivo electrónico y de la etapa de comunicaciones de corto alcance en una forma cifrada con dicha clave privada, y para almacenar, directamente, de una manera permanente, los primeros datos cifrados en la segunda memoria, sin solicitar ninguna acción de la unidad de procesado de datos.

Según otra variante, la etapa de comunicaciones de corto alcance está configurada para recibir los primeros datos de un servidor central a través del dispositivo electrónico y de la etapa de comunicaciones de corto alcance en una forma no cifrada todavía con dicha clave privada, la primera memoria operativa central almacena también dicha clave privada, y la unidad de procesado de datos está configurada para cifrar dichos primeros datos con dicha clave cifrada y para almacenar, permanentemente, los primeros datos cifrados en la segunda memoria.

Preferentemente, la segunda memoria almacena, también, su identificador de hardware UID_{160}, almacenándose el identificador de hardware UID_{160} tanto no cifrado como cifrado con la clave privada junto con los primeros datos, y la etapa de comunicaciones de corto alcance está configurada para transmitir al dispositivo electrónico el identificador de hardware UID_{160} no cifrado y el identificador de hardware UID_{160} también cifrado con la clave privada junto con los primeros datos, para una autenticación adicional de los primeros datos por parte del dispositivo electrónico.

Preferentemente, los segundos datos son recibidos por la etapa de comunicaciones de corto alcance en una forma cifrada con una clave simétrica idéntica a la clave de cifrado almacenada en la primera memoria operativa central.

De acuerdo con una primera variante, la unidad de procesado de datos está configurada, tras la recepción de dicha señal de reactivación, para transferir, en primer lugar, los segundos datos cifrados desde la segunda memoria hasta la primera memoria operativa central y, a continuación, descifrarlos usando la clave de cifrado almacenada en la primera memoria operativa central.

De acuerdo con otra variante, la unidad de procesado de datos está configurada, tras la recepción de dicha señal de reactivación, para descifrar, en primer lugar, los segundos datos cifrados usando la clave de cifrado almacenada en la primera memoria operativa central y, a continuación, transferir los segundos datos descifrados hacia la primera memoria operativa central.

Preferentemente, los segundos datos cifrados se reciben en bloques cifrados independientes y la unidad de procesado de datos está configurada para iniciar el descifrado de los segundos datos cifrados únicamente después de recibir, en la segunda memoria, todos los bloques cifrados independientes.

Preferentemente, la unidad de procesado de datos está configurada para leer unos terceros datos almacenados en la primera memoria operativa central, para cifrar los terceros datos usando dicha clave de cifrado almacenada en la primera memoria operativa central, y para reenviar los terceros datos cifrados hacia la etapa de comunicaciones de corto alcance, estando configurada la etapa de comunicaciones de corto alcance para transmitir los terceros datos cifrados a un servidor central a través del dispositivo electrónico.

Preferentemente, la segunda memoria almacena, junto con dichos primeros datos, también un código de identificación exclusivo OBU-ID del dispositivo de a bordo, almacenándose el código de identificación exclusivo OBU-ID del dispositivo tanto no cifrado como cifrado con la clave simétrica, estando configurada la etapa de comunicaciones de corto alcance para transmitir, al servidor central, a través del dispositivo electrónico, también dicho código de identificación exclusivo OBU-ID tanto no cifrado como cifrado con la clave simétrica, de modo que se permita que el servidor central lleve a cabo la autenticación del dispositivo y el descifrado de dichos terceros datos.

De acuerdo con un segundo aspecto, la presente invención proporciona un sistema para proporcionar un servicio telemático de tráfico, comprendiendo el sistema una pluralidad de dispositivos de carretera, un dispositivo electrónico y un dispositivo de a bordo para un vehículo, estando configurado el dispositivo de a bordo para comunicarse tanto con la pluralidad de dispositivos de carretera como con el dispositivo electrónico, siendo el dispositivo de a bordo tal como se ha descrito anteriormente.

Breve descripción de los dibujos

La presente invención se pondrá más claramente de manifiesto a partir de la siguiente descripción, proporcionada a título de ejemplo no limitativo, y que debe leerse en referencia a los dibujos adjuntos, en los cuales:

- la figura 1 muestra, de forma esquemática, un sistema para proporcionar un servicio telemático de tráfico, que comprende un dispositivo de a bordo de acuerdo con una forma de realización de la presente invención; y

- la figura 2 muestra, de forma esquemática, un sistema para proporcionar un servicio telemático de tráfico, que comprende un dispositivo de a bordo de acuerdo con otra forma de realización de la presente invención.

Descripción detallada de formas de realización de la invención

La figura 1 muestra, de manera esquemática, un sistema para proporcionar un servicio telemático de tráfico, que comprende un dispositivo de a bordo de acuerdo con formas de realización de la presente invención. Este servicio telemático de tráfico puede ser un servicio para los usuarios (tal como el pago de peajes para acceder a tramos de carretera/autopista, el pago de tarifas de aparcamiento, etc.) o un servicio para el administrador (tal como el control de acceso a zonas urbanas con restricciones de tráfico, la monitorización de tráfico a lo largo de un tramo de una carretera/autopista, etc.).

El sistema comprende un dispositivo de a bordo 100, un dispositivo electrónico 210, una pluralidad de dispositivos de carretera (no mostrados en la figura 1 por motivos de simplicidad), una red de comunicaciones 600 y un servidor central 700 que se comunica con el dispositivo electrónico 210 por medio de la red de comunicaciones 600.

Preferentemente, el dispositivo de a bordo 100 es adecuado para su instalación a bordo de un vehículo (no mostrado en la figura 1 por motivos de simplicidad), por ejemplo, un vehículo a motor. Los dispositivos de carretera están configurados, en cambio, para su instalación en una posición fija, por ejemplo, a lo largo de la cuneta de una carretera, en un paso elevado o en una pasarela de acceso (por ejemplo, a un aparcamiento, una zona urbana, una sección de carretera o autopista, etc.).

Tal como se describirá de forma más detallada posteriormente, el dispositivo de a bordo 100 está configurado para comunicarse por radiocomunicaciones tanto con los dispositivos de carretera como con el dispositivo electrónico 210.

En particular, tal como se muestra en la figura 1, el dispositivo de a bordo 100 comprende, preferentemente, una batería 110, una unidad de procesado de datos 120, una primera memoria 130, una etapa de comunicaciones por radiofrecuencia 140, una etapa de comunicaciones de corto alcance 150 y una segunda memoria 160. El dispositivo de a bordo 100 puede comprender otros componentes (por ejemplo, componentes GNSS para posicionamiento por satélite) los cuales no se describirán de forma más detallada posteriormente en la presente memoria, ya que no son útiles a efectos de la presente descripción.

Preferentemente, la batería 110 está conectada eléctricamente, de manera directa o indirecta, a cada uno de los otros componentes del dispositivo de a bordo 100 (en particular, a la unidad de procesado de datos 120, a la primera memoria 130, a la etapa de radiofrecuencia 140 y a la etapa de comunicaciones de corto alcance 150), de manera que se alimenten cuando sea necesario y en caso de que así se requiera.

Preferentemente, la primera memoria 130 está conectada eléctricamente a la unidad de procesado de datos 120. La primera memoria 130 se puede implementar en el exterior o en el interior de la unidad de procesado de datos 120. En cualquier caso, la primera memoria 130 es accesible solamente por la unidad de procesado de datos 120 (en particular, no es accesible directamente por la etapa de comunicaciones de corto alcance 150).

En el caso de obtenerse externamente, la primera memoria 130 almacena, preferentemente, un identificador de hardware UID_{120} de la unidad de procesado de datos 120 (preferentemente, su número de chip) de una manera no modificable y no borrable. Este identificador de hardware UID_{120} es usado por la unidad de procesado 120 para comprobar la autenticidad de los datos leídos de la primera memoria 130. Ventajosamente, esto hace que resulte posible evitar que el contenido de la memoria operativa central de un dispositivo de a bordo sea clonado y transferido a otro dispositivo de a bordo.

A modo de medida de seguridad adicional, si la primera memoria 130 se implementa fuera de la unidad de procesado de datos 120, se proporciona una interfaz (no mostrada en los dibujos) entre la unidad 120 y la memoria 130, estando configurada dicha interfaz para llevar a cabo un cifrado por hardware de los datos que escribe la unidad 120 en la memoria 130, y un descifrado por hardware de los datos que lee la unidad 120 de la memoria 130. Por lo tanto, los datos almacenados en la memoria 130 quedan protegidos ventajosamente a nivel de hardware. Por ello, la primera memoria 130 es una memoria no volátil que actúa como una memoria operativa central segura del dispositivo de a bordo 100.

Preferentemente, la primera memoria 130 almacena el código de identificación exclusivo OBU-ID del dispositivo de a bordo 100 y, opcionalmente, información sobre el usuario que es propietario del vehículo y sobre el propio vehículo (por ejemplo, la matrícula y/o la clase de peaje del vehículo). Preferentemente, la primera memoria 130 también almacena las aplicaciones de software que proporcionan los servicios telemáticos de tráfico para el usuario y/o para el administrador soportados por el dispositivo de a bordo 100 y los datos generados por la comunicación del dispositivo de a bordo 100 con los dispositivos de carretera del sistema a través de la etapa de comunicaciones por radiofrecuencia 140 (por ejemplo, datos referentes a la posición del vehículo o tránsito del mismo a través de una vía de acceso).

La etapa de comunicaciones por radiofrecuencia 140 está configurada, preferentemente, para establecer enlaces

de radiocomunicaciones con los dispositivos de carretera. Por ejemplo, la etapa de radiofrecuencia 140 se puede implementar usando la tecnología de DSRC (Comunicaciones Dedicadas de Corto Alcance) la cual, como es sabido, comprende canales de radiocomunicaciones y procedimientos de autenticación, codificación y descodificación que han sido desarrollados, específicamente, para servicios telemáticos de tráfico, y usa bandas de frecuencia en el intervalo de 5.7 a 5.9 GHz.

La etapa de comunicaciones de corto alcance 150 está configurada, preferentemente, para prestar soporte a enlaces de radiocomunicaciones de corto alcance (máxima 10 cm) con el dispositivo electrónico 210.

El dispositivo electrónico 210 puede pertenecer al mismo usuario al que se ha asignado el dispositivo de a bordo 100, o puede pertenecer a terceros (por ejemplo, el administrador de la infraestructura de la carretera o autopista sobre la cual se proporciona el servicio telemático de tráfico al que presta soporte el dispositivo de a bordo 100, el administrador del servicio telemático de tráfico, o el organismo o autoridad responsable de monitorizar infracciones de tráfico). Preferentemente, el dispositivo electrónico 210 está provisto, también, de conectividad por cable o inalámbrica (por ejemplo, Wifi o red móvil) con la red de comunicaciones 600. Por ejemplo, el dispositivo electrónico 210 puede ser un teléfono inteligente, una tableta o un lector comercial genérico o diseñado especialmente. Preferentemente, el dispositivo electrónico 210 está provisto, también, de una interfaz de usuario 200 que comprende elementos de entrada y/o salida que comprenden, por ejemplo, botones pulsadores, cursores, pantalla táctil, etcétera. El dispositivo electrónico 210 comprende, también, una etapa de comunicaciones de corto alcance compatible con la etapa de comunicaciones de corto alcance 150 del dispositivo de a bordo 100.

Preferentemente, la etapa de comunicaciones de corto alcance 150 (y, por tanto, también la etapa correspondiente de comunicaciones de corto alcance del dispositivo electrónico 210) se implementa usando una tecnología de campo cercano, tal como la tecnología de RFID (Identificación por Radiofrecuencia) con corto alcance (es decir, radio inferior a 10 cm). De entre las diversas tecnologías de RFID, es posible usar, por ejemplo, la tecnología de NFC (Comunicación de Campo Cercano) que, como es sabido, funciona a la frecuencia de 13.56 MHz y puede alcanzar una velocidad de transmisión máxima de 424 kbit/s.

Preferentemente, la etapa de comunicaciones de corto alcance incluida en el dispositivo electrónico 210 está configurada como iniciador, mientras que la etapa de comunicaciones de corto alcance 150 está configurada como objetivo. En otras palabras, la etapa de comunicaciones de corto alcance 150 está configurada para recibir, desde la etapa de comunicaciones de corto alcance incluida en el dispositivo electrónico 210, una portadora de radiocomunicaciones, a partir de la cual extrae su propio suministro de alimentación.

La configuración de la etapa de comunicaciones de corto alcance 150 en forma de lector resulta ventajosa, ya que permite reducir la complejidad electrónica y el software de la unidad de a bordo. También permite que la etapa de comunicaciones de corto alcance 150 funcione (y, por lo tanto, se comunique con la etapa correspondiente de comunicaciones de corto alcance incluida en el dispositivo electrónico 210) también cuando la batería 110 del dispositivo de a bordo 100 está completamente descargada, o cuando el resto del dispositivo de a bordo (en particular, la unidad de procesado de datos 120, la primera memoria 130 y la etapa de radiofrecuencia 140) está dañado o, en cualquier caso, no está funcionando.

La segunda memoria 160 puede estar conectada eléctricamente a la etapa de comunicaciones de corto alcance 150. Alternativamente, la segunda memoria 160 puede estar integrada en la etapa de comunicaciones de corto alcance 150. En ambos casos, la segunda memoria 160 es accesible directamente por la etapa de comunicaciones de corto alcance 150 la cual puede llevar a cabo sobre la misma tanto operaciones de escritura como operaciones de lectura también sin implicar a la unidad de procesado 120, según se describirá de forma más detallada posteriormente en la presente memoria. La segunda memoria 160 es, preferentemente, una memoria no volátil capaz de mantener los datos incluso cuando no está alimentada eléctricamente. Por ejemplo, la segunda memoria 16 puede ser una memoria del tipo E^2PROM.

La segunda memoria 160 almacena, de manera preferente permanentemente, un conjunto de datos básicos referentes al dispositivo de a bordo 100, que comprenden un código de identificación exclusivo OBU-ID del dispositivo de a bordo 100 y, opcionalmente, información sobre el usuario y/o el vehículo. Además, la segunda memoria 160 es adecuada para almacenar, de una manera temporal o transitoria, datos enviados por el servidor central 700 y destinados a la unidad de procesado de datos 120 y/o a la primera memoria 130, tal como se describirá de forma más detallada posteriormente en la presente memoria.

Con el fin de establecer un enlace de radiocomunicaciones entre el dispositivo de a bordo 100 y el dispositivo electrónico 210, los dos dispositivos se acercan entre sí (a una distancia inferior a 10 cm). El protocolo de comunicaciones por medio del cual funcionan la etapa de comunicaciones de corto alcance 150 y la etapa de corto alcance correspondiente incluida en el dispositivo electrónico 210 establece, así, de manera automática, un enlace de radiocomunicaciones. El enlace de radiocomunicaciones así establecido es, preferentemente, un enlace bidireccional de punto-a-punto el cual permite un intercambio bidireccional de datos entre el dispositivo de a bordo 100 y el dispositivo electrónico 210.

En particular, por medio del enlace de radiocomunicaciones de corto alcance entre el dispositivo electrónico 210 y el dispositivo de a bordo 100, la etapa de comunicaciones de corto alcance 150 puede transmitir al dispositivo electrónico 210 datos leídos de la segunda memoria 160 o de otros componentes del dispositivo de a bordo 100, permitiendo, de este modo, la lectura de estos datos desde el dispositivo de a bordo 100 por medio del dispositivo electrónico 210.

Opcionalmente, los datos leídos se pueden visualizar en forma de textos o gráficos sobre la interfaz de usuario 200 del dispositivo electrónico 210. De manera adicional o alternativa, los datos leídos se pueden transmitir desde el dispositivo electrónico 210 al servidor central 700 a través de la red de comunicaciones 600.

Estas operaciones de lectura puede permitir que el usuario del dispositivo electrónico 210 (que puede ser el usuario al que se ha asignado el dispositivo de a bordo 110 o el personal del proveedor del servicio telemático de tráfico al que presta soporte el dispositivo de a bordo 100) lleve a cabo, por ejemplo, comprobaciones diagnósticas o pruebas de funcionamiento del dispositivo de a bordo 100 (por ejemplo, comprobación del nivel de carga de su batería 110) o la comprobación de la información de configuración sobre el usuario y/o el vehículo a motor almacenada por el dispositivo de a bordo 100.

Si los datos que van a ser leídos están almacenados en la segunda memoria 160 (como en el caso, por ejemplo, de los datos básicos antes mencionados), la etapa de comunicaciones de corto alcance 150 puede leerlos, ventajosamente, incluso si la batería 110 está completamente descargada, o cuando la unidad de procesado de datos 120 y/o la primera memoria 130 no están funcionando. Por lo tanto, los datos básicos almacenados en la segunda memoria 160 pueden ser leídos, ventajosamente, por medio del dispositivo electrónico 210, con independencia de si el dispositivo de a bordo 100 está funcionando o no. Por ello, la segunda memoria 160 lleva a cabo sustancialmente, de manera ventajosa, una función de etiqueta electrónica.

En cambio, si los datos que van a ser leídos no están almacenados en la segunda memoria 160, la etapa de comunicaciones de corto alcance 150 puede leerlos únicamente si la batería 110 está cargada y el dispositivo de a bordo 100 (por lo menos la unidad de procesado de datos 120 y la primera memoria 130) está funcionando correctamente.

Para iniciar una operación de lectura, preferentemente el dispositivo electrónico 210 envía una señal de orden a la etapa de comunicaciones de corto alcance 150.

Si la operación de lectura se refiere a datos almacenados en la segunda memoria 160 (por ejemplo, los datos básicos antes mencionados), la etapa de comunicaciones de corto alcance 150 recupera los datos requeridos de la segunda memoria 160, y los envía al dispositivo electrónico 210, sin solicitar ninguna acción por parte de la unidad de procesado de datos 120.

En cambio, si la operación de lectura se refiere a datos que no están almacenados en la segunda memoria 160 (operación para la cual, según se ha mencionado anteriormente, la batería 110 debe estar suficientemente cargada), la etapa de comunicaciones de corto alcance 150 reenvía la señal de orden a la unidad de procesado de datos 120 la cual recupera los datos requeridos (por ejemplo, de la primera memoria 130), y los envía a la etapa de comunicaciones de corto alcance 150 la cual, a su vez, los reenvía al dispositivo electrónico 210. Preferentemente, esta señal de orden viene precedida por una señal de reactivación la cual activa la unidad de procesado de datos 120.

Además de las operaciones de lectura, por medio del enlace de radiocomunicaciones de corto alcance entre el dispositivo electrónico 210 y el dispositivo de a bordo 100, la etapa de comunicaciones de corto alcance 150 puede recibir, del dispositivo electrónico 210, datos que deben ser suministrados a los otros componentes del dispositivo de a bordo 100 (en particular, a la unidad de procesado de datos 120 y/o a la primera memoria 130 y/o a la segunda memoria 160), permitiendo, así, la escritura de estos datos en el dispositivo de a bordo 100 a través del dispositivo electrónico 210.

Estas operaciones de escritura pueden permitir, por ejemplo, que el usuario del dispositivo electrónico 210 (que puede ser el usuario al que se ha asignado el dispositivo de a bordo 100 o el personal del proveedor del servicio telemático de tráfico al que presta soporte el dispositivo de a bordo 100) modifique la configuración del dispositivo de a bordo 100, por ejemplo actualizando o activando las aplicaciones de software que ya están presentes o cargando aplicaciones nuevas o eliminando o desactivando aquellas aplicaciones que ya no tienen interés para el usuario. Por lo tanto, estas operaciones de escritura se pueden realizar ventajosamente sin tener que visitar un centro operativo de servicio al cliente.

Una operación de escritura prevé, preferentemente, que el servidor central 700 transmita los datos que deben ser escritos al dispositivo de a bordo 100 a través de la red de comunicaciones 600 y el dispositivo electrónico 210.

Preferentemente, el dispositivo electrónico 210 no lleva a cabo ningún procesado de los datos, ejecutando meramente una función de transductor entre la conexión con la red de comunicaciones 600 (por ejemplo, Wi-Fi o

red móvil) y el enlace de radiocomunicaciones de corto alcance con el dispositivo de a bordo 100 (por ejemplo, NFC). Los datos transmitidos sobre el enlace de radiocomunicaciones de corto alcance entre el dispositivo electrónico 210 y el dispositivo de a bordo 100 son, por lo tanto, iguales que los datos transmitidos sobre la red de comunicaciones 600 entre el servidor central 700 y el dispositivo electrónico 210.

Deberá indicarse que el establecimiento del enlace de radiocomunicaciones de corto alcance no requiere ningún ajuste manual o ningún procedimiento de emparejamiento, y, por lo tanto, es muy rápido (aproximadamente 1/10^{ésima} de un segundo). Además, puesto que el enlace de corto alcance tiene un radio máximo de 10 cm, el mismo no se ve expuesto, intrínsecamente, al riesgo de rastreo (*sniffing*) de los datos transmitidos los cuales, en cualquiera de los casos, según se explicará posteriormente, están preferentemente cifrados por el servidor central 700.

Una vez que los datos que deben escribirse han sido recibidos a través del enlace de radiocomunicaciones de corto alcance, la etapa de comunicaciones de corto alcance 150 los guarda, preferentemente, de manera temporal en la segunda memoria 160. Con el fin de evitar cualquier sobreescritura o acceso no autorizado a la segunda memoria 160, se proporciona preferentemente un mecanismo de protección de escritura de código de paso. Alternativamente, es posible proporcionar, en la segunda memoria 160, una o más áreas que están protegidas o tienen una función de escritura habilitada únicamente por la unidad de procesado de datos 120 y no por la etapa de comunicaciones de corto alcance 150.

Si la operación de escritura se refiere a datos que se van a almacenar permanentemente en la segunda memoria 160 (por ejemplo, los datos básicos antes mencionados), la etapa de comunicaciones de corto alcance 150 puede identificar y almacenar dichos datos directamente, de una manera permanente, en la segunda memoria 160 (sin requerir ninguna acción por parte de la unidad de procesado de datos 120), por ejemplo en una posición de dirección de la segunda memoria 160 dedicada al almacenamiento permanente de los datos básicos. Alternativamente, la etapa de comunicaciones de corto alcance 150 puede reenviar los datos que deben ser escritos, de una manera transparente, a la unidad de procesado de datos 120, la cual identifica dichos datos y los transfiere de vuelta a la segunda memoria 160, por ejemplo en la posición de dirección de la segunda memoria 160 dedicada al almacenamiento permanente de datos básicos.

En cambio, si la operación de escritura se refiere a los datos destinados a la unidad de procesado de datos 120 y/o a la primera memoria 130 (por ejemplo, los datos de configuración antes mencionados), la etapa de comunicaciones de corto alcance 150 reenvía dichos datos, preferentemente, de una manera transparente, a la unidad de procesado de datos 120, la cual los procesa y, si fuera necesario, los escribe en la primera memoria 130.

Deberá indicarse que, si la operación de escritura involucra a la unidad de procesado de datos 120, la batería 110 debe estar cargada. Por otro lado, si la unidad de procesado de datos 120 no está implicada, la operación de escritura se puede llevar a cabo incluso si la batería 110 está descargada.

Preferentemente, si la unidad de procesado de datos 120 está involucrada en la operación de escritura, la misma, preferentemente, inicia el procesado de los datos que se deben escribir tras la recepción de una señal de reactivación. Esta señal de reactivación se puede enviar a la unidad de procesado de datos 120 por parte de la etapa de comunicaciones de corto alcance 150 o por parte del usuario del dispositivo de a bordo 100, por ejemplo por medio de un botón especial al cual se puede acceder manualmente en el exterior del dispositivo de a bordo 100.

De acuerdo con una variante ventajosa, el dispositivo de a bordo 100 puede estar provisto de uno o más indicadores (por ejemplo, indicadores de luz LED) diseñados para proporcionar al usuario una realimentación visual en relación con el resultado de la operación de escritura de datos en el dispositivo de a bordo 100. Por ejemplo, el dispositivo de a bordo 100 puede estar provisto de un indicador de luz configurado para señalizar al usuario si la operación de escritura de los datos en la primera memoria 130 se ha completado satisfactoriamente.

Resumiendo, el dispositivo de a bordo 100 de acuerdo con la presente invención puede funcionar sustancialmente, por lo tanto, en tres configuraciones de funcionamiento diferentes:

- primera configuración de funcionamiento: lectura, por medio de un enlace de radiocomunicaciones de corto alcance con el dispositivo electrónico 210, de datos básicos almacenados en la segunda memoria 160 (función de etiqueta electrónica);

- segunda configuración de funcionamiento: lectura, por medio de un enlace de radiocomunicaciones de corto alcance con el dispositivo electrónico 210, de datos no almacenados en la segunda memoria 160. Esta configuración de funcionamiento es útil, en general, con la finalidad de verificar el funcionamiento del dispositivo de a bordo 100, con fines diagnósticos y, de manera general, con el fin de leer los datos contenidos en la primera memoria 130; y

- tercera configuración de funcionamiento: escritura, por medio de un enlace de radiocomunicaciones de corto alcance con el dispositivo electrónico 210, de datos en la primera memoria 130 o en la segunda memoria 160. Esta configuración de funcionamiento es en general útil con el fin de configurar el dispositivo de a bordo 100 (por ejemplo, para modificar los datos de etiqueta, actualizar o activar las aplicaciones de software ya presentes, o cargar aplicaciones nuevas, o para eliminar o deshabilitar aquellas aplicaciones que ya no tienen interés para el usuario, véase el ejemplo antes mencionado en el que el usuario desea activar temporalmente un servicio de pago de peaje en un país extranjero).

El sistema mostrado en la figura 1 está configurado, preferentemente, para proporcionar una conexión segura entre el dispositivo de a bordo 100 y el dispositivo electrónico 210 y, opcionalmente, entre el servidor central 700 y el dispositivo de a bordo 100. Con este fin, un mecanismo para garantizar la autenticidad de los datos leídos de la segunda memoria 160 (concretamente, de manera que el dispositivo electrónico 210 y/o el servidor central 700 puedan estar seguros de que los datos leídos se refieren realmente al dispositivo de a bordo 100 y no han sido clonados, en cambio, por otro dispositivo de a bordo) y un mecanismo para proteger los datos intercambiados entre el servidor central 700 y el dispositivo de a bordo 100.

Preferentemente, el mecanismo para garantizar la autenticidad de los datos leídos de la segunda memoria 160 (por ejemplo, los datos básicos del dispositivo de a bordo 100) se basa en un cifrado asimétrico de los datos puestos a disposición durante la lectura por medio de un almacenamiento permanente en la segunda memoria 160.

En particular, los datos que se pueden leer de la segunda memoria 160 se almacenan en la segunda memoria 160 cifrados con una clave privada. Para no tener que guardar la clave privada almacenada en el dispositivo de a bordo 100, el servidor central 700 envía, preferentemente, al dispositivo de a bordo 100, los datos que deben volverse legibles de la segunda memoria 160 en una forma ya cifrada con la clave privada. En este caso, tras la recepción de los datos cifrados con clave privada desde el servidor central 700, la etapa de comunicaciones de corto alcance 150 puede almacenarlos directamente en la segunda memoria 160, sin solicitar ninguna acción por parte de la unidad de procesado de datos 120.

Alternativamente, el servidor central 700 puede enviar al dispositivo de a bordo 100 los datos que deben volverse legibles de la segunda memoria en una forma no cifrada todavía con clave privada. En este caso, tras la recepción de los datos no cifrados con clave privada desde el servidor central 700, la etapa de comunicaciones de corto alcance 150 los reenvía, preferentemente, a la unidad de procesado de datos 120 la cual los cifra con clave privada y los almacena permanentemente en la segunda memoria 160. Por lo tanto, en este segundo caso, se requieren una acción por parte de la unidad de procesado de datos 120 y el almacenamiento de la clave privada en la primera memoria 130.

Si, posteriormente, el dispositivo electrónico 210 o el servidor central 700 solicita la lectura de estos datos, dichos datos son transmitidos, cifrados con clave privada, hacia el dispositivo electrónico 210 por medio de la etapa de comunicaciones de corto alcance 150. Durante esta operación, no se envía ninguna orden a la unidad de procesado de datos 120 del dispositivo de a bordo 100, la cual no se requiere para llevar a cabo operaciones de lectura desde la segunda memoria 160.

Por lo tanto, de acuerdo con una primera variante, el dispositivo electrónico 210 usa, preferentemente, la clave pública para descifrar los datos leídos que están cifrados con clave privada. La clave pública, puesto que se puede distribuir libremente, se guarda, de manera preferente, localmente en el dispositivo electrónico 210 (por ejemplo, dentro de una aplicación ejecutada por el dispositivo 210 para gestionar la lectura de datos desde el dispositivo 100), liberando, de este modo, al dispositivo electrónico 210 de la necesidad de conectarse al servidor central 700 durante toda la operación de lectura de los datos almacenados por la segunda memoria 160.

Opcionalmente, es posible proporcionar una autenticación adicional de los datos leídos, basándose en un identificador de hardware UID_{160} de la memoria 160 (por ejemplo, su número de chip). Según esta variante, el identificador de hardware UID_{160} es escrito, preferentemente, por el fabricante de la memoria 160 en un área específica de la misma, de manera que este queda almacenado permanentemente y está disponible en el modo de solo lectura y, por lo tanto, no puede ser modificado. Preferentemente, en la segunda memoria 160, el identificador de hardware UID_{160} se almacena tanto no cifrado como cifrado con clave privada junto con los datos que deben volverse legibles (por ejemplo, los datos básicos) guardados permanentemente en la segunda memoria 160 (que contiene, tal como se ha descrito anteriormente, el identificador OBU-ID y, opcionalmente, datos sobre el usuario y/o el vehículo).

El identificador de hardware UID_{160} se transmite, preferentemente, al dispositivo electrónico 210 sin cifrar, junto con los datos que deben ser leídos, cifrados con clave privada.

Después de llevar a cabo el descifrado de los datos que se deben leer con clave pública, el dispositivo electrónico 210 compara, preferentemente, el identificador de hardware UID_{160} recibido sin cifrar con el identificador de hardware UID_{160} obtenido a partir del descifrado con clave pública. Si los dos identificadores de hardware coinciden,

los datos que deben ser leídos se autentican adicionalmente.

De esta manera, es posible evitar, de forma ventajosa, que la segunda memoria 160 sea clonada y se transfiera a otro dispositivo de a bordo. Si el contenido de la segunda memoria 160 del dispositivo de a bordo 100 se fuera a copiar a otro dispositivo de a bordo, la falta de correspondencia entre los dos identificadores de hardware sería detectada y, por lo tanto, los datos leídos no se autenticarían. Por lo tanto, se garantiza, de manera ventajosa, la incapacidad de clonación de los datos almacenados en la segunda memoria 160, a saber, la imposibilidad de copiar estos datos en la memoria de otro dispositivo de a bordo.

Como alternativa al cifrado asimétrico, es posible prever un cifrado simétrico de los datos almacenados permanentemente por la segunda memoria 160. De esta manera, la clave privada (que es la misma para el cifrado y el descifrado) es conocida, de manera preferente, solamente para el servidor central 700 y para el dispositivo de a bordo 100. Por lo tanto, la lectura de estos datos en modo de etiqueta electrónica por parte del dispositivo electrónico 210 requiere, en cualquier caso, el reenvío de los datos al servidor central 700 el cual los descifra con la clave privada conocida por él y, si son autenticados, los retrasmite sin cifrar al dispositivo electrónico 210.

En cambio, con respecto al mecanismo para proteger los datos transmitidos desde el servidor central 700 hasta el dispositivo de a bordo 100, el mismo se basa, preferentemente, en un cifrado simétrico de los datos transmitidos. Este cifrado simétrico usa una misma clave privada para cifrar y descifrar los datos, debiendo ser conocida, por ello, dicha clave tanto para el servidor central 700 como para el dispositivo de a bordo 100. En particular, la clave privada se almacena en la primera memoria 130 del dispositivo de a bordo 100, preferentemente en un área no borrable y no modificable de la primera memoria 130.

En referencia, por ejemplo, a una operación para escribir datos en la primera memoria 130, el servidor central 700 cifra, preferentemente, los datos que se deben escribir con la clave privada, y los transmite al dispositivo electrónico 210 en el que, tal como se ha descrito anteriormente, los mismos son guardados temporalmente en la segunda memoria 160.

Si la batería 110 y la unidad de procesado de datos 120 están operativas y funcionando, la unidad de procesado de datos 120, preferentemente (tras la recepción de una señal de reactivación, según se ha descrito anteriormente), descifra los datos que se deben escribir usando la clave privada almacenada en la primera memoria 130 y los almacena en la primera memoria 130. Esta operación se puede llevar a cabo de diferentes maneras.

Según una primera variante, la unidad de procesado de datos 120 en primer lugar transfiere los datos cifrados desde la segunda memoria 162 a la primera memoria 130 y, a continuación, los descifra, usando la clave simétrica almacenada en la primera memoria 130.

De acuerdo con una segunda variante, la unidad de procesado de datos 120 en primer lugar recupera la clave simétrica de la primera memoria 130, a continuación, la usa para descifrar los datos (por ejemplo, guardados temporalmente en una memoria RAM interna asociada), y, finalmente, los transfiere a la primera memoria 130.

Deberá indicarse que, en ambas variantes, en cualquier caso, los datos a descifrar y la clave privada que se usa para descifrar dichos datos residen en dos memorias independientes físicamente, una de las cuales (concretamente la primera memoria 130 que almacena la clave privada) es accesible solamente para la unidad de procesado de datos 120 y, por lo tanto, no es accesible directamente por parte de la etapa de comunicaciones de corto alcance 150. Por lo tanto, a pesar del hecho de que la etapa de comunicaciones de corto alcance 150 permite el establecimiento de una conexión no protegida entre el dispositivo electrónico 210 y el dispositivo de a bordo 100, el dispositivo de a bordo 100 es, ventajosamente, muy seguro.

Además, de acuerdo con una variante ventajosa, el servidor central 700 divide los datos que se deben escribir en bloques (antes o después de llevar a cabo el cifrado de clave simétrica de dichos datos), y el mismo, a continuación, los transmite al dispositivo de a bordo 100 por medio del dispositivo electrónico 210. Preferentemente, antes de iniciar el descifrado de los datos que se deben escribir en la primera memoria 130 según se ha descrito anteriormente, la unidad de procesado de datos 120 espera a la recepción de todos los bloques cifrados en la segunda memoria 160. Esto, de manera ventajosa, hace que aumente adicionalmente la seguridad y la fiabilidad de la comunicación entre el servidor central 700 y el dispositivo de a bordo 100 puesto que los bloques, antes de ser escritos en la memoria 130, deben ser descifrados por un proceso que es totalmente externo a la memoria 160 en la cual están almacenados temporalmente.

La seguridad de la clave privada usada para el cifrado simétrico se garantiza, preferentemente, según la manera que se describe a continuación.

Preferentemente, en la fábrica del dispositivo de a bordo 100 se lleva a cabo una personalización, comprendiendo esta operación las siguientes etapas:

(i) leer, por medio de la etapa de comunicaciones por radiofrecuencia 140, un identificador exclusivo del

dispositivo de a bordo 100, por ejemplo, su código de identificación exclusivo OBU-ID;

(ii) transmitir el código OBU-ID a la entrada de un servidor seguro (por ejemplo, del tipo HSM – Hardware Security Module (Módulo de Seguridad de Hardware)). Este servidor seguro almacena (de una manera no accesible desde el exterior) por lo menos una clave maestra, sobre la base de la cual, a continuación, calcula por lo menos una clave derivada usando el código OBU-ID recibido como diversificador. A continuación, el servidor seguro proporciona, en su salida, la por lo menos una clave derivada calculada. Preferentemente, el servidor seguro almacena una clave de administración maestra *MAdBTKey* y una clave de aplicación maestra *MApBTKey* sobre cuya base calcula, respectivamente, una clave de administración derivada *DAdBTKey* y una clave de aplicación derivada *DApBTKey*, usando el código OBUI-ID recibido como diversificador. Las dos claves derivadas, a las que da salida el servidor seguro, se pueden usar para diferentes aplicaciones.

(iii) almacenar la por lo menos una clave derivada en el dispositivo de a bordo 100. Tal como ya se ha mencionado, esta operación se lleva a cabo preferentemente en la fábrica, enviándose la por lo menos una clave derivada al dispositivo de a bordo 100 por medio de la etapa de comunicaciones por radiofrecuencia 140. A continuación, la(s) clave(s) derivada(s) se almacena(n) en la primera memoria 130 de manera que quede(n) protegida(s) (no legible(s)), no modificable(s) y no borrable(s) sin la acción de la unidad de procesado 120.

Durante la operación del dispositivo de a bordo 100, en relación con la transmisión de los datos que se deben escribir desde el servidor central 700 al dispositivo de a bordo 100, el servidor central 700 usa, preferentemente, un segundo servidor de HSM seguro (que contiene, también la(s) clave(s) maestra(s)), suministrándole el código de identificación exclusivo OBU-ID del dispositivo de a bordo 100 y obteniendo, a partir del mismo, la clave derivada específica que se debe usar para la comunicación con el dispositivo de a bordo 100. Los datos transmitidos, cifrados por el servidor central 700 con la clave derivada, son recibidos según se ha descrito anteriormente por la unidad de procesado de datos 120 la cual, usando la clave derivada adecuada almacenada en su primera memoria 130, descifra los datos recibidos los cuales se almacenan finalmente en la primera memoria 130.

En el caso de la transmisión de datos desde el dispositivo de a bordo 100 hasta el servidor central 700, es necesario permitir que el dispositivo de a bordo 100 sea identificado por el servidor central 700 de manera que el servidor central 700 pueda calcular (por medio del segundo servidor seguro) la clave derivada necesaria para el descifrado de los datos recibidos desde el dispositivo de a bordo 100. Esto requiere un intercambio de datos entre el dispositivo de a bordo 100 y el servidor central 700, lo cual se describirá, a continuación, de manera más detallada, en referencia a la figura 2.

Una primera etapa prevé, preferentemente, que el dispositivo electrónico 210, después de registrarse (abrir sesión) en el servidor central 700, obtenga, a partir del dispositivo de a bordo 100, por medio del enlace de corto alcance con la etapa de comunicaciones de corto alcance 150, los siguientes datos leídos de la segunda memoria 160:

- el código de identificación exclusivo OBU-ID del dispositivo de a bordo 100 sin cifrar (de modo que permita que el servidor central 700 calcule la clave derivada);
- el código OBU-ID cifrado con la clave derivada (para garantizar la autenticación); y
- los datos que deben transmitirse cifrados por la unidad de procesado de datos 120 con la clave derivada.

A continuación, estos datos se envían al servidor central 700 a través de la red de comunicaciones 600 (la figura 2 muestra, por motivos de simplicidad, un repetidor 800 de la red de comunicaciones 600).

Una vez que se han recibido los datos antes mencionados, el servidor central 700 usa, preferentemente, el segundo servidor de HSM seguro antes mencionado (indicado con el número de referencia 710 en la figura 2), suministrándole el código de identificación exclusivo OBU-ID del dispositivo de a bordo 100 recibido sin cifrar y obteniendo, a partir del mismo, la clave derivada específica que se usará para la comunicación con el dispositivo de a bordo 100.

Una vez que se ha obtenido la clave derivada, el servidor central 700 descifra los datos recibidos y valida que sean correctos.

Los datos de configuración enviados desde el servidor central 700 al dispositivo de a bordo 100 y cifrados con clave derivada también pueden comprender datos que se almacenarán en la segunda memoria 160, de manera que permanezcan legibles por el dispositivo electrónico 210 por medio de las radiocomunicaciones de corto alcance. Estos datos pueden haber sido cifrados ya o no por medio del servidor central 700 con el fin de autenticarlo, según se ha descrito anteriormente.

La unidad de procesado de datos 120, una vez que se ha descifrado el mensaje con la clave derivada, identifica

los datos que se van a poner a disposición para su lectura, y establece si los mismos ya están cifrados con vistas a su autenticación. Si es así, los almacena permanentemente en la segunda memoria 160. En caso negativo, recupera, de la primera memoria 130, la clave privada del cifrado asimétrico destinado a permitir la autenticación de los datos leídos, la usa para cifrar los datos y los almacena permanentemente en la segunda memoria 160.

Opcionalmente, para la comunicación entre el servidor central 700 y el dispositivo de a bordo 100 también puede usarse una clave de sesión. Preferentemente, el emisor (a saber, el servidor central 700 si se escriben datos en el dispositivo de a bordo 100, o el dispositivo de a bordo 100 si se leen datos del dispositivo de a bordo 100) calcula una clave de sesión, por ejemplo, sobre la base de la clave derivada y un número aleatorio. La clave de sesión se vuelve a calcular (y, por lo tanto, es diferente) para cada sesión de comunicaciones.

El emisor usa, preferentemente, la clave de sesión calculada para cifrar adicionalmente los datos que se van a transmitir, ya cifrados con la clave derivada del mecanismo de cifrado simétrico. El emisor, también preferentemente, cifra la clave de sesión calculada, usando, por ejemplo, la clave pública del destinatario (a saber, el dispositivo de a bordo 100 si se escriben datos, o el dispositivo central 700 si se leen datos), y envía también esto al destinatario.

El destinatario, tras la recepción de los datos y la clave de sesión cifrada, descifra la clave de sesión usando la clave privada asociada y, a continuación, usa la clave de sesión para descifrar los datos recibidos (que se descifrarán, adicionalmente, usando la clave derivada).

Este mecanismo es ventajoso puesto que representa una solución que es menos compleja, desde un punto de vista computacional, en comparación con el cifrado asimétrico de todos los datos intercambiados entre el servidor central 700 y el dispositivo de a bordo 100, y que permite reducir significativamente el tiempo de cálculo necesario para el cifrado y el descifrado de los datos intercambiados.

De acuerdo con una serie de variantes, la protección con la clave de sesión se usa únicamente sobre el enlace entre el dispositivo electrónico 210 y el servidor central 700. En este caso, la gestión de las claves de sesión se confía al dispositivo electrónico 210 y no al dispositivo de a bordo 100.

Si el dispositivo de a bordo 100 está equipado con una interfaz de conexión de datos (por ejemplo, si es un dispositivo satelital equipado, también, con tecnología de radiocomunicaciones o Bluetooth), la escritura de los datos en la segunda memoria 160 (y, a continuación, en la memoria 130) puede ser gestionada por la unidad de procesado de datos 120, intercomunicada, en este caso, con la interfaz de conexión de datos (por ejemplo, el módem interno de tecnología de radiocomunicaciones o la interfaz Bluetooth). En este caso, la etapa de comunicaciones de corto alcance 150 se puede usar simplemente para la función de lectura de datos de la memoria 160.

Las ventajas del dispositivo de a bordo 100 son evidentes a partir de la descripción anterior.

El dispositivo de a bordo descrito, además de permitir la lectura de datos (por ejemplo, con fines de verificación o diagnóstico) y la escritura de datos (por ejemplo, con fines relativos a la configuración) por parte del dispositivo electrónico 210, permite, de hecho, gestionar el intercambio de datos con el dispositivo electrónico 210 y el servidor central 700 de una manera particularmente segura.

REIVINDICACIONES

1. Dispositivo de a bordo (100) para un vehículo, siendo adecuado dicho dispositivo de a bordo (100) para su uso en un sistema que proporciona un servicio telemático de tráfico, comprendiendo dicho dispositivo de a bordo (100):

- una etapa de comunicaciones por radiofrecuencia (140) configurada para comunicarse con un dispositivo de carretera de dicho sistema;

- una etapa de comunicaciones de corto alcance (150) configurada para comunicarse con un dispositivo electrónico (210) ubicado en sus proximidades;

- una unidad de procesado de datos (120) que coopera con dicha etapa de comunicaciones por radiofrecuencia (140) y con dicha etapa de comunicaciones de corto alcance (150),

- una primera memoria operativa central (130) accesible por dicha unidad de procesado de datos (120), almacenando dicha primera memoria operativa central (130) por lo menos una clave de cifrado;

- una segunda memoria (160) conectada eléctricamente a dicha etapa de comunicaciones de corto alcance (150) o integrada en esta y accesible directamente por dicha etapa de comunicaciones de corto alcance (150), almacenando dicha segunda memoria (160) unos primeros datos referentes a dicho dispositivo de a bordo (100); y

en el que dicha etapa de comunicaciones de corto alcance (150) está configurada para transmitir a dicho dispositivo electrónico (210) dichos primeros datos, también en modo de alimentación suspendida o en caso de funcionamiento deficiente de dicha etapa de comunicaciones por radiofrecuencia (140) y está configurada además para recibir unos segundos datos cifrados desde dicho dispositivo electrónico (210) y almacenarlos temporalmente en dicha segunda memoria (160);

y en el que dicha unidad de procesado de datos (120) está configurada para descifrar, tras la recepción de una señal de reactivación, dichos segundos datos cifrados usando dicha clave de cifrado almacenada en dicha primera memoria operativa central (130) y para almacenar dichos segundos datos en dicha primera memoria operativa central (130).

2. Dispositivo (100) según la reivindicación 1, en el que dicha primera memoria operativa central (130) se implementa dentro de dicha unidad de procesado de datos (120).

3. Dispositivo (100) según la reivindicación 1, en el que dicha primera memoria operativa central (130) se implementa fuera de dicha unidad de procesado de datos (120), y en el que dicha primera memoria operativa central (130) almacena un identificador de hardware UID_{120} de dicha unidad de procesado de datos (120) de una manera no modificable y no borrable.

4. Dispositivo (100) según la reivindicación 3, que comprende también una interfaz de cifrado de hardware entre dicha primera memoria operativa central (130) y dicha unidad de procesado de datos (120).

5. Dispositivo (100) según cualquiera de las reivindicaciones anteriores, en el que dicha etapa de comunicaciones de corto alcance (150) está configurada para enviar dicha señal de reactivación a dicha unidad de procesado de datos (120).

6. Dispositivo (100) según cualquiera de las reivindicaciones anteriores, en el que dicho dispositivo (100) comprende además un botón accesible manualmente desde el exterior de dicho dispositivo (100), estando configurado dicho botón de manera que, cuando es presionado, dicha señal de reactivación se envía a dicha unidad de procesado de datos (120).

7. Dispositivo (100) según cualquiera de las reivindicaciones anteriores, en el que dichos primeros datos se almacenan en dicha segunda memoria (160) en una forma cifrada con una clave privada de un mecanismo de cifrado asimétrico, y en el que dicha etapa de comunicaciones de corto alcance (150) está configurada para transmitir dichos primeros datos a dicho dispositivo electrónico (210) en una forma cifrada con dicha clave privada.

8. Dispositivo (100) según la reivindicación 7, en el que dicha etapa de comunicaciones de corto alcance (150) está configurada para recibir dichos primeros datos de un servidor central (700) a través de dicho dispositivo electrónico (210) y de dicha etapa de comunicaciones de corto alcance (150) en una forma ya cifrada con dicha clave privada, y para almacenar, directamente, de una manera permanente, dichos primeros datos cifrados en dicha segunda memoria (160), sin solicitar ninguna acción de dicha unidad de procesado de datos (120).

9. Dispositivo (100) según la reivindicación 7, en el que dicha etapa de comunicaciones de corto alcance (150) está configurada para recibir dichos primeros datos de un servidor central (700) a través de dicho dispositivo

electrónico (210) y de dicha etapa de comunicaciones de corto alcance (150) en una forma no cifrada todavía con dicha clave privada, en el que dicha primera memoria operativa central (130) almacena dicha clave privada, y en el que dicha unidad de procesado de datos (120) está configurada para cifrar dichos primeros datos con dicha clave cifrada y para almacenar, de una manera permanente, dichos primeros datos cifrados en dicha segunda memoria (160).

10. Dispositivo (100) según cualquiera de las reivindicaciones 7 a 9, en el que dicha segunda memoria (160) almacena también un identificador de hardware UID_{160} de dicha segunda memoria (160), almacenándose dicho identificador de hardware UID_{160} tanto no cifrado como cifrado con dicha clave privada junto con dichos primeros datos, y en el que dicha etapa de comunicaciones de corto alcance (150) está configurada para transmitir a dicho dispositivo electrónico (210) dicho identificador de hardware UID_{160} no cifrado y dicho identificador de hardware UID_{160} también cifrado con dicha clave privada junto con dichos primeros datos, para una autenticación adicional de dichos primeros datos por parte de dicho dispositivo electrónico (210).

11. Dispositivo (100) según cualquiera de las reivindicaciones anteriores, en el que dichos segundos datos son recibidos por dicha etapa de comunicaciones de corto alcance en una forma cifrada con una clave simétrica idéntica a dicha clave de cifrado almacenada en dicha primera memoria operativa central (130).

12. Dispositivo (100) según cualquiera de las reivindicaciones anteriores, en el que dicha unidad de procesado de datos (120) está configurada, tras la recepción de dicha señal de reactivación, para transferir, en primer lugar, dichos segundos datos cifrados desde dicha segunda memoria (160) hasta dicha primera memoria operativa central (130) y, a continuación, descifrarlos usando dicha clave de cifrado almacenada en dicha primera memoria operativa central (130).

13. Dispositivo (100) según cualquiera de las reivindicaciones 1 a 12, en el que dicha unidad de procesado de datos (120) está configurada, tras la recepción de dicha señal de reactivación, para descifrar, en primer lugar, dichos segundos datos cifrados usando dicha clave de cifrado almacenada en dicha primera memoria operativa central (130) y, a continuación, transferir dichos segundos datos descifrados hacia dicha primera memoria operativa central (130).

14. Dispositivo (100) según una de las reivindicaciones anteriores, en el que dichos segundos datos cifrados se reciben en bloques cifrados independientes y en el que dicha unidad de procesado de datos (120) está configurada para iniciar el descifrado de dichos segundos datos cifrados únicamente después de recibir, en dicha segunda memoria (160), la totalidad de dichos bloques cifrados independientes.

15. Dispositivo (100) según cualquiera de las reivindicaciones anteriores, en el que dicha unidad de procesado de datos (120) está configurada para leer unos terceros datos almacenados en dicha primera memoria operativa central (130), para cifrar dichos terceros datos usando dicha clave de cifrado almacenada en dicha primera memoria operativa central (130), y para reenviar dichos terceros datos cifrados hacia dicha etapa de comunicaciones de corto alcance (150), estando configurada dicha etapa de comunicaciones de corto alcance (150) para transmitir dichos terceros datos cifrados a un servidor central (700) por medio de dicho dispositivo electrónico (210).

16. Dispositivo (100) según la reivindicación 15, en el que dicha segunda memoria (160) almacena, junto con dichos primeros datos, también un código de identificación exclusivo OBU-ID de dicho dispositivo (100), almacenándose dicho código de identificación exclusivo OBU-ID de dicho dispositivo (100) tanto no cifrado como cifrado con dicha clave simétrica, estando configurada dicha etapa de comunicaciones de corto alcance (150) para transmitir a dicho servidor central (700), a través de dicho dispositivo electrónico (210), también dicho código de identificación exclusivo OBU-ID tanto no cifrado como cifrado con dicha clave simétrica, de modo que permita que dicho servidor central (700) lleve a cabo la autenticación de dicho dispositivo (700) y el descifrado de dichos terceros datos.

17. Sistema para proporcionar un servicio telemático de tráfico, que comprende una pluralidad de dispositivos de carretera, un dispositivo electrónico (210) y un dispositivo de a bordo (100) para un vehículo, estando configurado dicho dispositivo de a bordo (100) para comunicarse tanto con dicha pluralidad de dispositivos de carretera como con dicho dispositivo electrónico (210), siendo dicho dispositivo de a bordo (100) según cualquiera de las reivindicaciones 1 a 16.

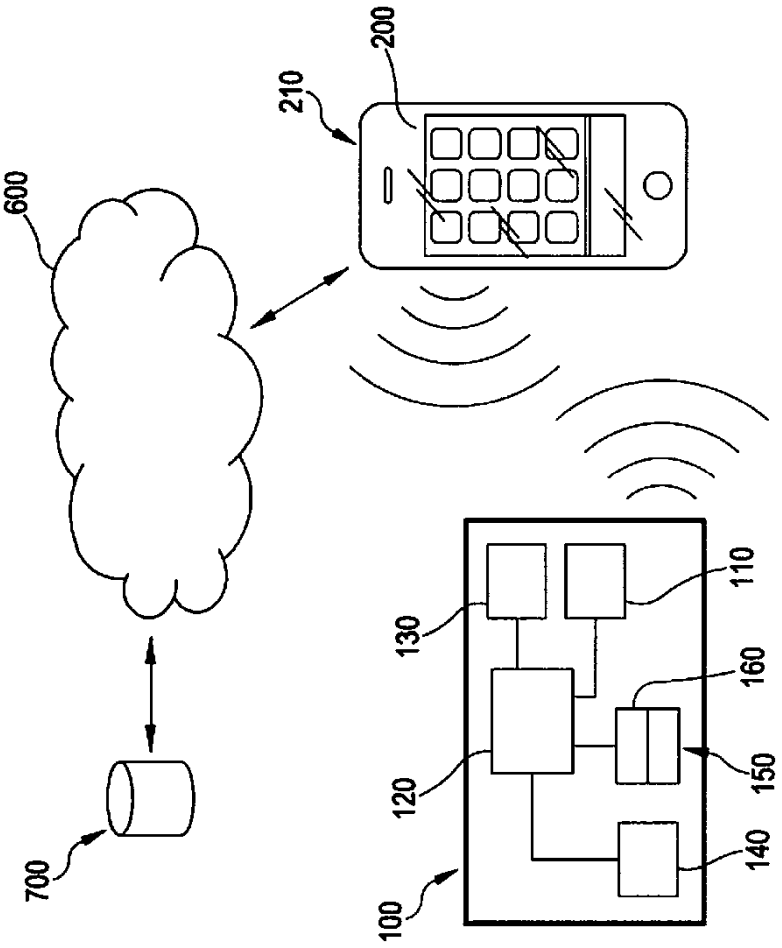

Fig. 1

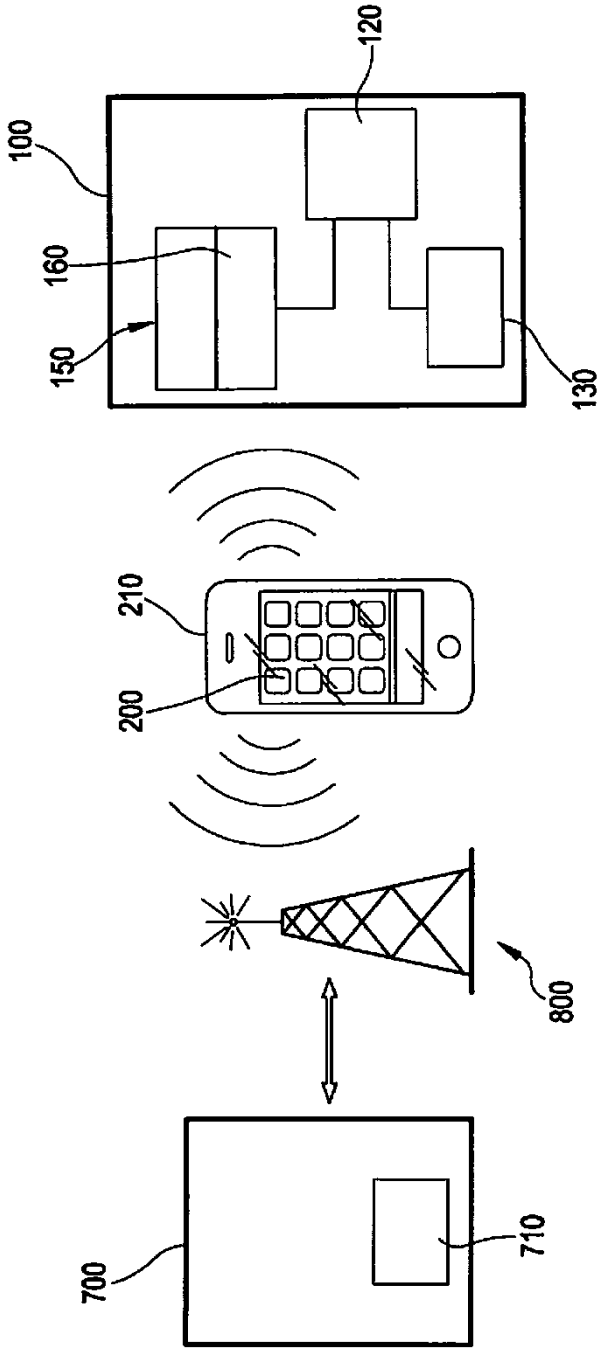

Fig. 2