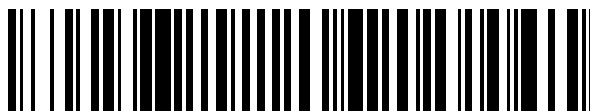


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 401 592**

51 Int. Cl.:

G07C 7/00 (2006.01)

G01P 1/12 (2006.01)

G07C 5/08 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **22.11.2005** **E 05818272 (6)**

97 Fecha y número de publicación de la concesión europea: **02.01.2013** **EP 1815256**

54 Título: **Unidad de tacógrafo electrónico para vehículo automóvil**

30 Prioridad:

22.11.2004 FR 0412379

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
22.04.2013

73 Titular/es:

ACTIA AUTOMOTIVE (100.0%)
5 rue Jorge Semprun
31432 Toulouse Cedex 4, FR

72 Inventor/es:

MALBERTI, LAURENT;
ROMON, ERIC y
KUNEGEL, JACQUES

74 Agente/Representante:

CURELL AGUILÁ, Mireia

ES 2 401 592 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Unidad de tacógrafo electrónico para vehículo automóvil.

La invención se refiere a una unidad de un aparato de control denominado tacógrafo, destinada a estar embarcada en un vehículo automóvil -en particular un vehículo de transporte de mercancías o de viajeros- con vistas a permitir el control de actividades de un conductor del vehículo. Se debe observar que el término "conductor" designa una persona que puede ejercer por turno actividades de chófer o de co-chófer (denominado también "acompañante") del vehículo. El tacógrafo comprende, además de esta unidad, por lo menos un sensor de movimiento del vehículo conectado a la unidad cuando ésta está embarcada.

En particular, un tacógrafo tiene por función registrar, almacenar, producir, imprimir y, eventualmente, intercambiar y visualizar, unos datos, denominados datos de conductor, relativos a las actividades de un conductor del vehículo, con vistas a permitir un control de estas actividades por un controlador.

Los tacógrafos utilizados actualmente en Europa son del tipo tacógrafo de discos gráficos, tal como el descrito por el documento US nº 4.782.691. Se trata de instrumentos analógicos y mecánicos que permiten retranscribir datos del conductor sobre un disco de papel por medio de un estilete.

Según una tendencia generalizada en el ámbito del automóvil, se han desarrollado por otra parte, unos tacógrafos electrónicos provistos en particular de circuitos con microprocesadores para el tratamiento y el almacenamiento de los datos del conductor. La introducción de la electrónica en los tacógrafos ha permitido contemplar la realización de novedosos equipos en el seno de la unidad de tacógrafo y la realización por parte de ésta de nuevas funciones. Así, por ejemplo, unos estudios se han referido a la sustitución de los discos gráficos conocidos (y utilizados todavía) por tarjetas inteligentes electrónicas. Éstos han desembocado en la concepción de unidades de tacógrafo, tales como la descrita por el documento US nº 4.644.368, provistas de dispositivos lector/registrator de tarjetas inteligentes.

El documento EP-A-0 592 166 y WO-A-02/31709 describen otros ejemplos de aparatos registradores de datos para vehículos según la técnica anterior.

Paralelamente, se ha hecho hincapié en la garantía de una mayor seguridad en el tratamiento de los datos, con el objetivo de evitar los fraudes. Una unidad de tacógrafo dispone ya, con este fin, de protecciones mecánicas (caja reforzada eventualmente provista de precintos de seguridad, etc.). La implantación de componentes electrónicos -y, en particular, de circuito(s) con microprocesador(es) y de lector(es) inteligentes- en la unidad de tacógrafo permite actualmente contemplar la utilización de protecciones electrónicas en el seno de la unidad, tales como unos mecanismos de seguridad criptográficos.

La invención pretende proporcionar un tacógrafo -y, más precisamente, una unidad de tacógrafo- electrónico securizado, en el que se garanticen particularmente:

- la autenticidad (verificación de la identidad) mutua de la unidad de tacógrafo y de ciertos medios externos a la unidad (tales como el sensor de movimiento y las tarjetas inteligentes) con los cuales la unidad está destinada a intercambiar datos; se debe observar que un medio es considerado como externo a la unidad cuando no está incorporado durante la concepción en la caja securizada de la unidad y es independiente o separable de la unidad,
- la autenticidad (verificación del origen) y la integridad de los datos intercambiados entre la unidad y ciertos medios externos a la unidad,
- la integridad, por firma electrónica, de datos descargados desde la unidad hacia unos dispositivos externos denominados dispositivos de descarga.

Para utilizar dichos mecanismos de seguridad, la unidad de tacógrafo debe conservar secretos criptográficos (claves de cifrado privadas o secretas para el encriptado y el desencriptado) e integrar unos algoritmos de cifrado correspondientes.

La invención pretende proporcionar una unidad de tacógrafo securizada, no sólo provista de dichos algoritmos y secretos criptográficos, sino además y sobre todo, provista de una protección electrónica reforzada apta para ofrecer un nivel elevado de resistencia a los ataques fraudulentos.

En efecto, a pesar de los esfuerzos desplegados en la técnica desde hace numerosos años, no se ha podido encontrar ninguna solución satisfactoria y fiable a este problema. El objetivo es no sólo ofrecer un control y una limitación del acceso a los datos gestionados por la unidad, en lectura y/o en escritura, sino también y sobre todo, garantizar el respeto de esta limitación permitiendo advertir cualquier falsificación de estos datos.

Un objetivo de la invención es proporcionar una unidad apta para resistir en gran medida a un ataque dirigido con

ayuda de medios sofisticados, ya se trate de medios utilizados directamente sobre los circuitos de la unidad o a distancia. La invención pretende, en particular, proporcionar una unidad que ofrezca un nivel de seguridad calificado E3 FORT según la metodología de evaluación ITSEC.

- 5 Otro objetivo de la invención es proporcionar una unidad de tacógrafo electrónico más competente asimismo en términos de funcionalidades.

Además, la invención pretende lograr los objetivos citados anteriormente a menor coste, proponiendo una unidad de tacógrafo de bajo precio de coste. En particular, la invención pretende proporcionar una unidad de tacógrafo que
10 cumpla estos objetivos a partir de medios y, en particular, de componentes electrónicos usuales y económicos o eventualmente nuevos pero de desarrollo y de fabricación poco costosos.

La invención se refiere a una unidad de tacógrafo destinada a ser embarcada en un vehículo automóvil y a estar conectada a por lo menos un sensor de movimiento del vehículo, comprendiendo la unidad por lo menos una tarjeta
15 con microprocesador(es), denominada tarjeta principal, para el tratamiento y el almacenamiento de datos, denominados datos tacográficos, que comprende por lo menos unos datos, denominados datos de conductor, relativos a actividades de un conductor de dicho vehículo. La unidad de tacógrafo está adaptada por otra parte para efectuar unas operaciones, denominadas operaciones de seguridad, que utilizan unos algoritmos de cifrado con fines de autenticación de por lo menos una parte de los datos tacográficos.

Se debe observar que los términos "algoritmos de cifrado" se pueden emplear para designar unos algoritmos de encriptado, unos algoritmos de desencriptado o ambos. Por otra parte, en la continuación de la descripción, los términos "datos de seguridad" designan unos datos adicionales memorizados y/o creados y/o calculados y/o
20 utilizados... en el marco de las operaciones de seguridad. Los datos de seguridad comprenden, en particular, unas claves de cifrado, unos certificados suministrados por organismos oficiales habilitados, unos atributos de seguridad generados por una operación de seguridad para una transmisión de datos, tales como una firma, una suma de control -denominada checksum-, etc. Algunos de estos datos, denominados datos secretos, son, por definición, secretos: conservados en el seno de la unidad de tacógrafo, deben permanecer inaccesibles a cualquier persona no autorizada (debiendo la unidad de tacógrafo ofrecer un nivel de resistencia elevado a los ataques que pretenden
25 obtener estos datos secretos); se trata esencialmente de claves de cifrado secretas -simétricas- y de claves de cifrado privadas.

La unidad de tacógrafo según la invención se caracteriza porque:

- 35 - la tarjeta principal comprende por lo menos un microprocesador, denominado microprocesador principal, para el tratamiento de los datos tacográficos,
- la unidad comprende por lo menos un circuito integrado protegido físicamente proveedor de servicios criptográficos, denominado circuito CSP, distinto del (de los) microprocesador(es) principal(es), estando en el
40 circuito CSP almacenados por lo menos unos datos denominados datos de seguridad secretos, estando este circuito CSP adaptado para realizar por lo menos una parte de las operaciones de seguridad cuando la unidad está embarcada en un vehículo.

Se debe observar que el (los) circuito(s) CSP puede(n) estar soportado(s) por la tarjeta principal o por una o varias
45 tarjetas diferentes.

Así, la invención consiste en seleccionar y separar del conjunto de las operaciones realizadas por una unidad de tacógrafo por lo menos una parte de las operaciones relativas únicamente a la seguridad (operaciones que consisten
50 en autenticar y/o proteger ciertos datos por medio de algoritmos de cifrado, con el objetivo final de garantizar la autenticidad y la integridad de los datos del conductor), y en hacer ejecutar las operaciones de seguridad seleccionadas por un circuito específico, físicamente protegido. Para esto, en este circuito protegido se almacenan unos datos de seguridad secretos. Pueden estar almacenados asimismo los algoritmos de cifrado y/o unos datos de seguridad no secretos (tales como claves públicas) relativos a las operaciones de seguridad asignadas a dicho circuito CSP.

Dicha arquitectura electrónica permite garantizar un nivel de seguridad muy elevado, nunca alcanzado hasta el momento en una unidad de tacógrafo.

Como se explica a continuación, ofrece asimismo la posibilidad de utilizar unos componentes electrónicos habituales y poco onerosos.

Ventajosamente y según la invención, el (los) circuito(s) CSP está(n) dedicado(s) esencialmente a la realización de operaciones de seguridad, significando el término "esencialmente" que cada circuito CSP está dedicado a
65 operaciones de seguridad y, eventualmente, a unas operaciones puntuales que requieren poca capacidad de tratamiento y de almacenamiento, tales como el almacenamiento de datos temporales generados por el tratamiento de datos tacográficos. Un circuito proveedor de servicios criptográficos habitual y poco oneroso, que tenga una

pequeña capacidad de tratamiento y de almacenamiento se puede utilizar así a título de circuito CSP según la invención, teniendo cuenta de que éste está "descargado" de las funcionalidades de la unidad de tacógrafo que necesitan más capacidad.

Más particularmente, el (los) circuito(s) CSP está(n) dedicado(s) esencialmente a la realización de todas las operaciones de seguridad. Por tanto, el (los) microprocesador(es) principal(es) no ejecuta(n) ninguna operación de seguridad. Es posible utilizar así, a título de microprocesador principal, un microprocesador básico no protegido y, por tanto, poco oneroso, tal como, por ejemplo, un ordenador utilizado habitualmente en el campo del automóvil. Dicho ordenador clásico posee una capacidad de tratamiento y de almacenamiento suficiente para gestionar el conjunto de tareas (aparte de las operaciones de seguridad) reservadas a la unidad de tacógrafo.

En una versión preferida de la invención, la unidad de tacógrafo comprende un único circuito CSP, esencialmente dedicado a todas las operaciones de seguridad.

Ventajosamente y según la invención, la tarjeta principal de la unidad de tacógrafo comprende por lo menos una memoria, denominada memoria de aplicación, asociada a un microprocesador principal, en la que está almacenada una aplicación (uno o varios programas), denominada aplicación tacográfica, que se puede cargar en este microprocesador principal para el tratamiento de los datos tacográficos. Ventajosamente y según la invención, este microprocesador principal está adaptado para poder verificar la autenticidad y la integridad de por lo menos una parte de la aplicación tacográfica con ayuda de por lo menos una operación de seguridad realizada por un circuito CSP de la unidad de tacógrafo.

En particular, dicho microprocesador principal integra un programa de arranque protegido, físicamente inscrito en el microprocesador y adaptado para, durante una operación que pretende implementar por lo menos una de entre una aplicación tacográfica (primera o nueva) en la unidad, ordenar a dicho circuito CSP la ejecución de por lo menos una operación de seguridad con vistas a la autenticación de dicha aplicación o parte de aplicación tacográfica, y ordenar el registro de esta aplicación o parte de aplicación tacográfica en la memoria de aplicación únicamente si está considerada por el circuito CSP como auténtica e íntegra.

Dado que el programa de arranque está inscrito en duro (en el silicio) en el microprocesador principal, éste no puede ser modificado. Lo cual garantiza la orden por el microprocesador principal y la ejecución por el circuito CSP de la(s) operación(es) de seguridad mencionada(s) anteriormente. La aplicación tacográfica almacenada finalmente en la memoria de aplicación y utilizada por el (los) microprocesador(es) principal(es) es, por tanto, necesariamente auténtica e íntegra, es decir, ha sido concebida e implementada por un organismo habilitado, en un entorno securizado, según las especificaciones impuestas por las reglas y normas.

Además, está previsto preferentemente que la aplicación tacográfica almacenada en la memoria de aplicación esté adaptada a su vez para, cuando está cargada en el microprocesador principal para el tratamiento de los datos tacográficos, ordenar periódicamente al circuito CSP asociado la ejecución de por lo menos una operación de seguridad con vistas a su propia autenticación.

Ventajosamente y según la invención, cada circuito CSP está conectado a un microprocesador principal, estando dichos circuito CSP y microprocesador principal asociados adaptados para funcionar según una relación maestro/esclavo en la que el microprocesador principal es el maestro y el circuito CSP es el esclavo.

Así, todas las operaciones de seguridad ejecutadas por un circuito CSP lo son a petición del microprocesador principal asociado, que, para ello, transmite al circuito CSP unos datos para autenticar acompañados de por lo menos una orden de ejecución de una operación de seguridad correspondiente.

La unidad de tacógrafo según la invención comprende un dispositivo lector/registrador de tarjetas inteligentes, denominadas tarjetas tacográficas, apto para recibir por lo menos dos tarjetas tacográficas en paralelo.

En una versión preferida de la invención, la unidad de tacógrafo comprende asimismo una interfaz de conexión, denominada interfaz de tarjeta tacográfica, para una comunicación inalámbrica (y, en particular, a distancia) de la unidad con un dispositivo lector/registrador de tarjetas tacográficas externa a la unidad (en su versión más simple, este dispositivo externo está adaptado para recibir únicamente una sola tarjeta tacográfica a la vez).

Están previstos cuatro tipos de tarjetas tacográficas, perteneciendo cada tarjeta tacográfica a uno de estos tipos: las tarjetas de conductor, las tarjetas de controlador, las tarjetas de empresa y las tarjetas de taller. Cada tipo de tarjeta tacográfica da derecho, por una parte, a un acceso restringido a ciertos datos predeterminados almacenados en la unidad y, por otra parte, a la ejecución de ciertas operaciones predeterminadas según el tipo de tarjeta tacográfica. La inserción de una tarjeta tacográfica en el dispositivo lector/registrador de tarjetas (ya se trate del dispositivo de la unidad -denominado dispositivo integrado- o de un dispositivo externo apto para comunicarse con la unidad) permite abrir una sesión de funcionamiento de la unidad correspondiente al tipo de la tarjeta insertada.

De acuerdo con los objetivos fijados, se debe poder autenticar cualquier tarjeta tacográfica insertada en el

dispositivo lector/registrador de tarjetas (integrado o externo), al igual que los datos intercambiados entre dicha tarjeta tacográfica y la unidad de tacógrafo.

Con este fin, según la invención, el dispositivo lector/registrador está controlado por lo menos por un microprocesador principal de la unidad, al que está asociado un circuito CSP. Este microprocesador principal (o eventualmente estos microprocesadores principales) está adaptado para ordenar a dicho circuito CSP la ejecución de operaciones de seguridad con vistas a la autenticación mutua de la unidad y de una tarjeta tacográfica presente en el dispositivo lector/registrador de tarjetas (integrado o externo), y autorizar la apertura de una sesión de funcionamiento correspondiente únicamente si la unidad y la tarjeta tacográfica son consideradas como auténticas.

Una tarjeta de conductor autenticada proporciona así acceso a una sesión de funcionamiento denominada sesión de conductor; una tarjeta de taller autenticada proporciona acceso a una sesión de funcionamiento denominada sesión de taller; una tarjeta de controlador autenticada proporciona acceso a una sesión de funcionamiento denominada sesión de controlador; una tarjeta de empresa autenticada proporciona acceso a una sesión de funcionamiento denominada sesión de empresa.

Esta autenticación mutua entre tarjeta tacográfica y unidad se ejecuta preferentemente en cuanto se inserta una tarjeta en el dispositivo lector/registrador de tarjetas (tratándose en particular del dispositivo integrado). Con este fin, el microprocesador principal está adaptado para vigilar las inserciones y retiradas de tarjeta en el dispositivo lector/registrador y activar las operaciones de seguridad mencionadas anteriormente en cuanto se detecta una inserción de una tarjeta tacográfica en el dispositivo lector/registrador.

La apertura de una sesión de funcionamiento permite la realización de operaciones cuya naturaleza depende del tipo de la sesión. Algunas de estas operaciones pueden conducir a intercambios de datos entre la tarjeta tacográfica y la unidad. En cada intercambio de datos entre la unidad de tacógrafo y una tarjeta tacográfica presente en el dispositivo lector/registrador de tarjetas (integrada o externo) y previamente autenticada, el microprocesador principal está adaptado para ordenar al circuito CSP la ejecución de por lo menos una operación de seguridad con vistas a la autenticación de dichos datos y tratar los datos intercambiados únicamente si son considerados como auténticos e íntegros.

En particular, el microprocesador principal está adaptado para:

- cuando se reciben datos (en particular, datos tacográficos) por la unidad desde dicha tarjeta tacográfica, ordenar al circuito CSP la ejecución de por lo menos una operación de seguridad con vistas a la autenticación de los datos recibidos, y tratar dichos datos únicamente si son considerados por el circuito CSP como auténticos e íntegros,
- cuando se deben transmitir datos por la unidad a dicha tarjeta tacográfica, ordenar al circuito CSP la ejecución de por lo menos una operación de seguridad con vistas a la protección de la totalidad de los datos a transmitir. La tarjeta tacográfica está adaptada, por otra parte, para ejecutar por lo menos una operación de seguridad con vistas a autenticar los datos transmitidos y tratar dichos datos únicamente si ésta los considera como auténticos e íntegros.

La unidad de tacógrafo debe poder autenticar, por otra parte, el sensor de movimiento con el cual se comunica cuando está embarcada en un vehículo, así como los datos, denominados datos de movimiento, que ésta recibe de dicho sensor. Se debe observar que los datos de movimiento son datos tacográficos.

Para su conexión al sensor de movimiento, la unidad de tacógrafo comprende una interfaz de conexión, denominada interfaz de sensor. Se debe observar que esta conexión es preferentemente filar, en cuyo caso la interfaz de sensor está constituida por uno o varios conectores. No obstante, ya no se excluye que esta conexión sea inalámbrica y que la interfaz de sensor comprenda (eventualmente en combinación con un conector) un dispositivo emisor-receptor de ondas electromagnéticas.

Por otra parte, según la invención, la tarjeta principal de la unidad comprende por lo menos un microprocesador principal conectado a dicha interfaz de sensor y al que está asociado un circuito CSP, estando dicho microprocesador principal adaptado para ordenar a dicho circuito CSP la ejecución de operaciones de seguridad con vistas, por una parte, a la autenticación mutua del sensor de movimiento y de la unidad y, por otra parte, a la autenticación de datos de movimiento recibidos del sensor de movimiento por la unidad, y tratar los datos de movimiento recibidos únicamente si el sensor de movimiento y la unidad son considerados como auténticos y si los datos recibidos son considerados como auténticos e íntegros.

En particular, el microprocesador principal está adaptado para:

- en el marco de una operación inicial denominada operación de emparejamiento de un sensor de movimiento y de la unidad de tacógrafo, ordenar al circuito CSP la ejecución de por lo menos una operación de seguridad con vistas a la autenticación mutua del sensor y de la unidad, y autorizar un intercambio ulterior de datos

entre dicho sensor y la unidad únicamente si éstos últimos son considerados como auténticos,

- en el marco de una operación periódica, denominada operación de control de los datos de movimiento, ordenar al circuito CSP la ejecución de por lo menos una operación de seguridad con vistas a la autenticación de datos, denominados datos de control, intercambiados entre el sensor y la unidad en el marco de esta operación de control, y autorizar el tratamiento de los datos de movimiento recibidos por la unidad en un periodo transcurrido únicamente si dichos datos de control son considerados como auténticos e íntegros. En otros términos, para garantizar la autenticidad y la integridad de los datos de movimiento sólo se verifica la autenticidad y la integridad de los datos de control.

Para una mayor seguridad, la operación de emparejamiento se puede realizar únicamente si está presente una tarjeta tacográfica de taller auténtica y autenticada en el dispositivo lector/registrador de tarjetas integrado en la unidad. En otros términos, el (los) microprocesador(es) principal(es) de la unidad está(n) adaptado(s) para autorizar la ejecución de una operación de emparejamiento únicamente en el marco de una sesión de taller (que se puede abrir únicamente por la autenticación de una tarjeta de taller).

Ventajosamente y según la invención, la unidad de tacógrafo comprende asimismo una interfaz de conexión, denominada interfaz de descarga, para la comunicación de la unidad con un dispositivo externo denominado dispositivo de descarga, en particular apto para memorizar datos tacográficos. La interfaz de descarga puede comprender un conector, con vistas a una conexión filar del dispositivo de descarga con la unidad, y/o un dispositivo emisor/receptor de ondas electromagnéticas, con vistas a una comunicación inalámbrica entre la unidad y un dispositivo de descarga eventualmente remoto.

Según la invención, se puede realizar una operación de descarga de datos por encargo de un usuario únicamente si está presente una tarjeta tacográfica de controlador, de taller o de empresa (con exclusión de una tarjeta de conductor) auténtica y autenticada en el dispositivo lector/registrador de tarjetas (integrado o externo). Con este fin, el (los) microprocesador(es) principal(es) está(n) adaptado(s) para autorizar la ejecución de una operación de descarga de datos hacia un dispositivo de descarga "conectado" a la unidad (conexión filar o inalámbrica) por medio de la interfaz de descarga únicamente en el marco de una sesión de controlador o de taller o de empresa (abierta por la autenticación de una tarjeta correspondiente).

Se debe observar que los datos cuya descarga está autorizada pueden diferir según la sesión de funcionamiento en curso.

Ventajosamente y según la invención, los datos tacográficos descargados se acompañan de un atributo de seguridad, tal como una firma electrónica, con vistas a su autenticación ulterior por el dispositivo de descarga o por otra herramienta. El microprocesador principal está adaptado asimismo para, en el marco de una operación de descarga de datos, ordenar al circuito CSP la ejecución de por lo menos una operación de seguridad con vistas a la protección de los datos a descargar.

Por otra parte, la unidad comprende asimismo de manera ventajosa una interfaz de conexión, denominada interfaz de calibrado, que comprende por lo menos un conector para la comunicación de la unidad con un dispositivo externo denominado dispositivo de calibrado con vistas al calibrado de la unidad.

Según la invención, se puede realizar una operación de calibrado, por encargo de un usuario, por medio de un dispositivo de calibrado conectado a la unidad por medio de la interfaz de calibrado, únicamente si está presente una tarjeta tacográfica de taller auténtica y autenticada en el dispositivo lector/registrador de tarjetas integrado en la unidad. Con este fin, el (los) microprocesador(es) principal(es) está(n) adaptado(s) para autorizar la ejecución de una operación de calibrado únicamente en el marco de una sesión de taller (abierta por la autenticación de una tarjeta de taller).

Durante una operación de calibrado, se transmiten a la unidad unos datos denominados datos de calibrado mediante el dispositivo de calibrado. Los datos de calibrado memorizados en la unidad al final de la operación de calibrado son datos tacográficos.

Ventajosamente y según la invención, un microprocesador principal de la unidad está adaptado para vigilar las inserciones y retiradas de tarjeta en el dispositivo lector/registrador de tarjetas (integrado o externo) y para, en cuanto se detecta una retirada de una tarjeta tacográfica del dispositivo lector/registrador, interrumpir cualquier operación en curso en la sesión de funcionamiento correspondiente. En particular, se interrumpen así las operaciones en curso de emparejamiento de sensor, de actualización de la aplicación tacográfica, de calibrado, de descarga de datos tacográfica y, por supuesto, de lectura/escritura en la tarjeta tacográfica (que ya no está conectada...).

En una versión preferida de la invención:

- la tarjeta principal comprende un único microprocesador principal para el tratamiento de los datos

tacográficos, al cual están conectados un circuito de alimentación eléctrica alimentado de manera permanente por una fuente eléctrica permanente del vehículo, una memoria de masa, denominada memoria de aplicación, de tipo electrónico y no volátil -y, en particular, de tipo flash- para el almacenamiento de por lo menos una aplicación tacográfica, una memoria de masa, denominada memoria de datos, de tipo electrónico y no volátil -y, en particular, de tipo flash- para el almacenamiento de datos tacográficos y, eventualmente, de otros datos, con exclusión de datos de seguridad secretos (las dos memorias definidas anteriormente pueden ser dos memorias distintas o una sola y misma memoria), un reloj en tiempo real con calendario, un conector de sensor y un conector (único), denominado conector de descarga/calibrado, para la conexión a la unidad de un dispositivo externo de calibrado o de un dispositivo externo de descarga, así como un dispositivo lector/registrador tal como se ha definido anteriormente,

- la unidad comprende un único circuito CSP dedicado a la realización de todas las operaciones de seguridad, estando dichos microprocesador principal y circuito CSP conectados y adaptados para funcionar según una relación maestro/esclavo en la que el microprocesador principal es el maestro y el circuito CSP es el esclavo,
- la unidad comprende asimismo una impresora, una pantalla de visualización y un dispositivo de captura de datos por un usuario (tal como un teclado).

La invención se refiere asimismo a una unidad de tacógrafo caracterizada en combinación por la totalidad o parte de las características mencionadas anterior y posteriormente.

La invención se extiende a un vehículo automóvil equipado con una unidad de tacógrafo de este tipo.

Otros objetivos, características y ventajas de la invención aparecerán con la lectura de la descripción siguiente, que se refiere a las figuras adjuntas que representan modos de realización preferidos de la invención, dados únicamente a título de ejemplos no limitativos, y en las que:

- la figura 1 es una vista en perspectiva de una unidad de tacógrafo según la invención,
- la figura 2 es una vista explosionada en perspectiva de una unidad de tacógrafo según la invención,
- la figura 3 es un esquema sinóptico que ilustra la arquitectura de esta unidad de tacógrafo y la organización de sus diferentes componentes, y
- la figura 4 es un organigrama que ilustra el desarrollo de una operación de seguridad según la invención.

La unidad de tacógrafo 1 según la invención comprende, en el seno de una caja securizada 2 reforzada (formada por varios elementos 2a, 2b, 2c) y provista de precintos de seguridad 50:

- una tarjeta principal 3 con microprocesador(es), que soporta un microprocesador principal 4, tal como los utilizados habitualmente en el campo del automóvil; como variante, dicha tarjeta soporta un grupo de microprocesadores en paralelo con vistas a asegurar una redundancia, o una pluralidad de microprocesadores independientes o conectados en serie que se reparten las funcionalidades del tacógrafo; la tarjeta principal 3 soporta asimismo un circuito CSP 20 proveedor de servicios criptográficos, conectado al microprocesador principal 4 según una relación maestro/esclavo en la que el microprocesador principal 4 es el maestro y el circuito CSP 20 es el esclavo; dicho circuito CSP está protegido físicamente; con este fin, posee unas características no sólo físicas, sino también funcionales (memoria apta para dispersar los secretos que contiene...), que garantizan su inviolabilidad; el circuito CSP 20 es, por ejemplo, un microprocesador CSP similar a los empleados para las tarjetas bancarias; el circuito CSP 20 integra una memoria protegida en la que están almacenados unos algoritmos de cifrado, unos datos de seguridad secretos (claves privadas y claves de sesión) y, eventualmente, otros datos de seguridad (claves públicas..., pudiendo como variante estos otros datos de seguridad ser almacenados en una memoria no protegida de la unidad) con vistas a la ejecución de operaciones de seguridad,
- una memoria de masa flash 5, denominada memoria de aplicación, conectada al microprocesador principal 4 y en la que se almacena una aplicación tacográfica que permite realizar todas las funcionalidades del tacógrafo, con exclusión de por lo menos una parte de las operaciones de seguridad y, preferentemente, con exclusión de todas las operaciones de seguridad a realizar para garantizar un nivel elevado de resistencia a los ataques fraudulentos; no obstante, se debe observar que la aplicación tacográfica integra unas órdenes que permiten activar la ejecución de las operaciones de seguridad; la memoria de aplicación 5 es de tipo no volátil,
- un circuito de alimentación eléctrica 6 conectado de forma permanente a una fuente eléctrica permanente del vehículo con vistas a alimentar el microprocesador principal 4 permanentemente cualquiera que sea la fase de explotación del vehículo en curso (fuera de contacto, después de contacto, motor parado, motor funcionando, vehículo parado, vehículo circulando...),

- un reloj en tiempo real con calendario 7 (fecha y hora) conectado al microprocesador principal 4 y que dispone preferentemente de una batería de repuesto,
- 5 - un dispositivo doble 8 lector/registrador de tarjetas tacográficas inteligentes, controlado por el microprocesador principal 4 y apto para recibir dos tarjetas tacográficas en paralelo. El dispositivo dispone de dos bloques 81, 82 sustancialmente idénticos, que comprenden cada uno:
 - 10 ■ una interfaz mecánica (de hendidura, corredera, carro deslizante...) de recepción de una tarjeta tacográfica, provista de un mecanismo motorizado controlado para el desplazamiento de una tarjeta 60 entre una posición de introducción/retirada y una posición enclavada de lectura/escritura,
 - 15 ■ un conector que permite la conexión entre el microprocesador principal 4 de la unidad y el chip 61 de una tarjeta tacográfica presente en posición enclavada de lectura/escritura,
 - 20 ■ por lo menos un órgano de detección de tarjeta en posición enclavada de lectura/escritura apto para transmitir una señal al microprocesador principal 4 cuando se detecta una tarjeta en posición enclavada de lectura/escritura,
- 25 - un dispositivo 16 emisor/receptor de ondas electromagnéticas, conectado al microprocesador principal 4 y que forma una interfaz de conexión, denominada interfaz de tarjetas, para la comunicación inalámbrica de la unidad con un dispositivo lector/registrador de tarjetas tacográficas externo a la unidad,
- un dispositivo 14 emisor/receptor de ondas electromagnéticas conectado al microprocesador principal 4 y que realiza una interfaz de conexión de la unidad 1 con un dispositivo de descarga remoto; como variante, un único y mismo dispositivo emisor/receptor realiza una interfaz de comunicación a la vez con un dispositivo lector/registrador de tarjetas y con un dispositivo de descarga de datos remotos,
- 30 - una pantalla de visualización 9, con retroiluminación, controlada por el microprocesador principal 4,
- una impresora 10 controlada por el microprocesador principal 4,
- un dispositivo 11 de captura de datos por un usuario, controlado por el microprocesador principal 4 y que comprende un teclado con teclas y/o una pantalla táctil,
- 35 - un conector 12 de sensor conectado al microprocesador principal 4, que realiza una interfaz de conexión de la unidad 1 con un sensor de movimiento con vistas a la recepción de datos de movimiento del vehículo,
- un conector 13 de descarga/calibrado conectado al microprocesador principal 4, que realiza una interfaz de conexión de la unidad 1 con un dispositivo de calibrado o un dispositivo de descarga, con vistas a la recepción de datos de calibrado (enviados por el dispositivo de calibrado) o a la descarga (con destino al dispositivo de descarga) de datos tacográficos,
- 40 - una pluralidad de conectores 15 conectados al microprocesador principal 4 para la conexión de la unidad a ciertos ordenadores o contactores del vehículo tales como el ordenador de velocidad, el contador kilométrico, el ordenador de régimen del motor, la red CAN de ordenadores del vehículo, con vistas a la transmisión de datos entre la unidad y estos ordenadores, así como otro conector 15 para la conexión del microprocesador principal 4 de la unidad a un indicador de aviso (señalización luminosa y/o sonora),
- 45 - una memoria de masa flash 17 de tipo no volátil, denominada memoria de datos, conectada al microprocesador principal 4 y en la que se almacenan los datos tacográficos, unos datos denominados datos de funcionamiento (índice de iluminación de la pantalla 9, zona de imagen de los tiques a imprimir por la impresora 10...) y unos datos denominados datos anexos (imprevistos, datos temporales...) y, eventualmente, unos datos de seguridad, con la condición de que no sean secretos (claves públicas, por ejemplo).
- 50
- 55

Además de la unidad 1, el tacógrafo comprende un sensor de movimiento del vehículo y unos cables de conexión que permiten conectar el sensor de movimiento y el conector de sensor 12 de la unidad embarcada. El sensor de movimiento está formado, en particular, por un elemento de detección de movimiento, por un microprocesador (al que está conectado el elemento de detección) y por un conector para la conexión del microprocesador del sensor a la unidad embarcada.

La unidad de tacógrafo tiene como función principal el tratamiento de datos del conductor, entre los cuales se pueden citar:

- la velocidad instantánea y la distancia recorrida entre dos paradas, calculándose estos datos a partir de los

datos de movimiento recogidos y transmitidos por el sensor de movimiento,

- las actividades del conductor (conducción -cuando el conductor conduce el vehículo- , trabajo, pausa/reposo, disponibilidad -cuando el "conductor", es decir, el titular de la tarjeta tacográfica es co-chófer), imponiéndose estos datos, según el caso, automáticamente (por la aplicación tacográfica) o siendo capturados manualmente por el conductor por medio del teclado 11,
- el tiempo de cada actividad,
- el lugar de comienzo y de final de las jornadas de trabajo, siendo estos datos capturados manualmente por el conductor,
- las condiciones particulares ("fuera de campo", trayecto en transbordador/tren), siendo estos datos capturados manualmente por el conductor.

Según la invención, las funciones atribuidas al microprocesador principal se refieren esencialmente a unas funciones de cálculo que se refieren a los datos del conductor, unas funciones más generales de gestión del conjunto de los datos tacográficos (datos de conductor, datos de movimiento, datos de controlador, datos de calibrado, datos de empresa...) y unas funciones de pilotaje de los diversos órganos de la unidad embarcada. Entre estas funciones se pueden citar:

- la generación y el tratamiento de datos de conductor y, en particular:
 - el tratamiento de los datos de movimiento del vehículo (que emanan del sensor de movimiento y se reciben por medio del conector de sensor) y, en particular, el cálculo de la velocidad y de la distancia recorrida, y la medición del tiempo,
 - el seguimiento de las actividades del conductor, el seguimiento de la situación de conducción,
 - el tratamiento de los datos de conductor capturados manualmente por el conductor (tales como el lugar de comienzo y de final de las jornadas de trabajo, las actividades del conductor y las condiciones particulares),
- la lectura de datos almacenados en las memorias de aplicación 5 y de datos 17, el registro y el almacenamiento de datos en estas memorias,
- el control del dispositivo 8 lector/registrador de tarjetas tacográfica con vistas, en particular, a la vigilancia de las inserciones y retiradas de tarjeta, la lectura de las tarjetas tacográficas, al registro y al almacenamiento de datos en las tarjetas tacográficas y, eventualmente, al accionamiento de los mecanismos de desplazamiento de tarjeta,
- el control de la pantalla de visualización 9,
- el control de la impresora 10,
- el tratamiento de los datos capturados manualmente por el conductor por medio del teclado 11,
- la emisión de avisos (envío de señales de aviso por medio de dispositivos emisores correspondientes, luminosas y/o sonoras),
- la detección de acontecimientos; se debe observar que, entre los acontecimientos, se pueden distinguir los relativos a las actividades del conductor (exceso de velocidad, solapamiento temporal, última sesión cerrada incorrectamente, conducción sin tarjeta apropiada, ...) de los relativos a la seguridad del tacógrafo (inserción de una tarjeta no válida, conflicto de tarjeta, inserción de una tarjeta en el curso de la conducción, interrupción de la alimentación eléctrica, error en los datos de movimiento, tentativa de ataque a la seguridad),
- la detección de las anomalías (anomalía en tarjeta, anomalía en aparato de control),
- la gestión de los enclavamientos de empresa (tratamiento de datos de empresas),
- el seguimiento de las actividades de control (entre ellas el tratamiento de los datos del controlador),
- el control de la interfaz de descarga/calibrado (conector y dispositivo emisor-receptor de ondas), la orden de descarga de datos hacia un dispositivo externo de descarga, el tratamiento de datos de calibrado recibidos,
- la realización de autotests,

- el control del circuito CSP 20, según una relación maestro/esclavo en la que el microprocesador principal es el maestro y el circuito CSP es el esclavo, y el mando de operaciones de seguridad, el tratamiento de los resultados de dichas operaciones de seguridad.

5 Ventajosamente y según la invención, las operaciones de seguridad con vistas a la autenticación mutua de la unidad y de una tarjeta tacográfica realizan, preferentemente, unos cálculos de cifrado por medio de claves asimétricas (claves privadas y públicas).

10 Se debe observar que se desencadena esta autenticación mutua por el microprocesador principal 4 cuando constata la inserción de una tarjeta tacográfica en una interfaz de recepción de tarjeta del dispositivo lector/registrador 8 o de un dispositivo externo remoto que se comunica con el microprocesador principal 4 por medio de la interfaz de tarjetas 16. El microprocesador principal 4 está adaptado en efecto para identificar las inserciones y las retiradas de la tarjeta en función de las señales que recibe del (de los) órgano(s) de detección de dicho dispositivo lector/registrador: la presencia de una tarjeta 60 en posición de lectura/escritura -recepción de una señal de detección- después de un periodo de ausencia de tarjeta -ninguna señal de detección- traduce la inserción de una tarjeta; la ausencia de tarjeta después de un periodo de presencia de tarjeta traduce la retirada de una tarjeta.

20 Para una mayor seguridad, la autenticación mutua de una tarjeta tacográfica presente en el dispositivo lector/registrador se activa asimismo de forma periódica (mientras que no se haya constatado ninguna retirada de tarjeta desde la autenticación precedente) mediante el microprocesador principal 4 y/o mediante la tarjeta tacográfica.

25 Ventajosamente y según la invención, las operaciones de seguridad con vistas a la autenticación de datos intercambiados entre la unidad y el sensor de movimiento o entre la unidad y una tarjeta tacográfica realizan preferentemente unos cálculos de cifrado por medio de claves de sesión, es decir, de claves simétricas (claves secretas). Estas claves de sesión comunes al circuito CSP 20 de la unidad y al medio externo (sensor de movimiento o tarjeta tacográfica) se establecen conjuntamente por los dos elementos en el marco de las operaciones de autenticación mutua de estos elementos o inmediatamente después de éstas. Las claves de sesión se almacenan en la memoria (protegida) del circuito CSP 20.

A título de ejemplo simplificado y no limitativo, la lectura de datos tacográficos sobre una tarjeta tacográfica previamente autenticada da lugar a las operaciones ilustradas en la figura 3, que permiten garantizar la integridad de los datos leídos (estas operaciones pretenden verificar que los datos recibidos por el microprocesador principal 4 corresponden a los enviados por la tarjeta tacográfica y que, por tanto, estos últimos no han sido falsificados durante la transmisión). El microprocesador principal 4 prepara la orden de lectura (etapa 30): el código de orden se abastece de datos, denominados datos anexos, necesarios para su ejecución, tales como la dirección y la longitud de los datos tacográficos a leer (con vistas a su localización en la memoria de la tarjeta tacográfica). Transmite (etapa 31) los datos anexos al circuito CSP 20 con una orden de ejecución de una operación de seguridad correspondiente, con vistas a proteger la integridad de dichos datos. El circuito CSP 20 calcula (etapa 32) una suma de control, denominada checksum, de los datos anexos, cifra (encripta) dicha checksum por medio de su clave de sesión y transmite (etapa 33) la checksum encriptada al microprocesador principal 4. El microprocesador principal 4 prepara (etapa 34) y transmite (etapa 35) la totalidad de la orden de lectura (código de orden + datos anexos + checksum) a la tarjeta tacográfica 60 (es decir, a su chip electrónico 61) a través del conector del dispositivo lector/registrador 8. La tarjeta tacográfica 60, 61 verifica la integridad de los datos recibidos (etapa 36) descifrando la checksum recibida por medio de su clave de sesión, calculando la checksum de los datos anexos recibidos y comparando los dos valores. Si estos últimos coinciden, la tarjeta tacográfica 60, 61 transmite (etapa 38) los datos tacográficos solicitados, después de haber calculado y cifrado previamente -por medio de su clave de sesión- su checksum (etapa 37). Cuando se reciben los datos (etapa 39), el microprocesador principal 4 transmite (etapa 40) al circuito CSP 20 los datos tacográficos y la checksum encriptada recibidos, así como una orden de ejecución de una operación de seguridad correspondiente que pretende verificar la integridad de los datos tacográficos recibidos. Ejecutando esta orden, el circuito CSP 20 calcula la checksum de los datos tacográficos y descifra la checksum encriptada que les acompaña por medio de su clave de sesión y compara los dos valores obtenidos (etapa 41). Si éstos coinciden, reenvía una señal de aprobación al microprocesador principal 4; en caso contrario, transmite a este último una señal de desaprobación (etapa 42). El microprocesador principal 4 explota los datos tacográficos únicamente si la señal recibida es una señal de aprobación (etapa 43). Si los datos tacográficos no se consideran como auténticos (señal de desaprobación), el microprocesador memoriza la anomalía y emite eventualmente una señal correspondiente a la atención del usuario (etapa 43).

60 Los datos de movimiento recibidos del sensor de movimiento son objeto asimismo de operaciones de seguridad con vistas a su autenticación. En efecto, el sensor de movimiento, previamente autenticado en el marco de una operación de emparejamiento con la unidad, emite continuamente unos impulsos que transmite a la unidad, emitiéndose cada impulso en el instante en el que el vehículo ha recorrido una distancia predeterminada desde el impulso anterior. El sensor de movimiento dispone por otra parte de un contador al que incrementa con cada impulso emitido. Asimismo, el microprocesador principal de la unidad dispone de un contador al que incrementa con cada

impulso recibido. Periódicamente, el microprocesador principal desencadena una operación securizada de comparación de los contadores de sensor y de unidad. La lectura del contador de sensor se efectúa, por ejemplo, como se ha explicado anteriormente con relación a la lectura de datos tacográficos en una tarjeta tacográfica: el valor del contador de sensor transmitido a la unidad es autenticado, en particular, por un atributo de seguridad de tipo checksum encriptada. Un valor relativo del contador de sensor y un valor relativo del contador de unidad (correspondiendo el valor relativo de un contador a la diferencia de valor del contador desde la última operación de comparación) son calculados por el microprocesador principal, y después comparados. Este procedimiento permite verificar la autenticidad y la integridad de los datos (impulsos) transmitidos por el sensor durante el periodo transcurrido desde la última operación de comparación.

Resulta evidente que la invención puede constituir el objeto de numerosas variantes con respecto a los modos de realización descritos anteriormente y representados en las figuras.

REIVINDICACIONES

1. Unidad de tacógrafo (1) destinada a ser embarcada en un vehículo automóvil y a ser conectada a por lo menos un sensor de movimiento del vehículo, comprendiendo la unidad por lo menos una tarjeta (3) con microprocesador(es), denominada tarjeta principal, para el tratamiento y el almacenamiento de datos, denominados datos tacográficos, que comprenden por lo menos unos datos, denominados datos de conductor, relativos a unas actividades de un conductor de dicho vehículo, estando dicha unidad de tacógrafo adaptada para efectuar unas operaciones, denominadas operaciones de seguridad, que utilizan unos algoritmos de cifrado con vistas a la autenticación de por lo menos una parte de los datos tacográficos, caracterizada porque:
 - dicha tarjeta principal (3) comprende por lo menos un microprocesador (4), denominado microprocesador principal, para el tratamiento de los datos tacográficos,
 - la unidad comprende por lo menos un circuito (20) físicamente protegido proveedor de servicios criptográficos, denominado circuito CSP, distinto del (de los) microprocesador(es) principal(es), circuito DSP en el cual están almacenados por lo menos unos datos denominados datos de seguridad secretos, estando este circuito CSP (20) adaptado para realizar por lo menos una parte de las operaciones de seguridad cuando la unidad está embarcada en un vehículo.
2. Unidad según la reivindicación 1, caracterizada porque la tarjeta principal (3) comprende por lo menos una memoria (5), denominada memoria de aplicación, asociada a un microprocesador principal (4), en la cual está almacenada una aplicación, denominada aplicación tacográfica, que puede ser cargada en este microprocesador principal para el tratamiento de los datos tacográficos, y porque este microprocesador principal está adaptado para poder verificar la autenticidad de por lo menos una parte de la aplicación tacográfica con ayuda de por lo menos una operación de seguridad realizada por un circuito CSP (20) de la unidad de tacógrafo.
3. Unidad según la reivindicación 2, caracterizada porque este microprocesador principal (4) integra un programa de arranque protegido, inscrito físicamente en el microprocesador y adaptado para, durante una operación que pretende implementar por lo menos una parte de una aplicación tacográfica en la unidad, ordenar a dicho circuito CSP (20) la ejecución de por lo menos una operación de seguridad con vistas a la autenticación de dicha aplicación o parte de aplicación tacográfica, y ordenar el registro de esta aplicación o parte de aplicación tacográfica en la memoria de aplicación (5) únicamente si está considerada por el circuito CSP como auténtica e íntegra.
4. Unidad según una de las reivindicaciones 2 o 3, caracterizada porque la aplicación tacográfica almacenada en la memoria de aplicación (5) está adaptada para, cuando está cargada en el microprocesador principal, ordenar periódicamente al circuito CSP (20) la ejecución de por lo menos una operación de seguridad con vistas a la autenticación de dicha aplicación tacográfica.
5. Unidad según una de las reivindicaciones 1 a 4, caracterizada porque el (los) circuito(s) CSP (20) está(n) dedicado(s) esencialmente a la realización de operaciones de seguridad.
6. Unidad según una de las reivindicaciones 1 a 5, caracterizada porque el (los) circuito(s) CSP (20) está(n) dedicado(s) esencialmente a la realización de todas las operaciones de seguridad.
7. Unidad según una de las reivindicaciones 1 a 6, caracterizada porque cada circuito CSP (20) está conectado a un microprocesador principal (4), estando dichos circuito CSP y microprocesador principal asociados adaptados para funcionar según una relación maestro/esclavo en la que el microprocesador principal es el maestro y el circuito CSP es el esclavo.
8. Unidad según una de las reivindicaciones 1 a 7, caracterizada porque el (los) circuito(s) CSP (20) está(n) soportado(s) por la tarjeta principal (3).
9. Unidad según una de las reivindicaciones 1 a 8, caracterizada porque:
 - la unidad comprende un dispositivo (8) lector/registrador de tarjetas inteligentes, denominadas tarjetas tacográficas, apto para recibir por lo menos dos tarjetas tacográficas en paralelo, perteneciendo cada tarjeta a un tipo de tarjeta predeterminado,
 - el dispositivo lector/registrador de tarjetas (8) está controlado por lo menos por un microprocesador principal (4) al cual está asociado un circuito CSP (20), estando dicho microprocesador principal adaptado para ordenar a dicho circuito CSP la ejecución de por lo menos una operación de seguridad con vistas a la autenticación mutua de la unidad y de una tarjeta tacográfica presente en el dispositivo lector/registrador de tarjetas, y para autorizar la apertura de una sesión de funcionamiento correspondiente al tipo de la tarjeta tacográfica presente únicamente si la unidad y dicha tarjeta son consideradas como auténticas.
10. Unidad según la reivindicación 9, caracterizada porque este microprocesador principal (4) está adaptado para

vigilar las inserciones y retiradas de tarjeta en el dispositivo (8) lector/registrador de tarjetas, y ordenar la ejecución de esta(s) operación(es) de seguridad en cuanto se detecta una inserción de una tarjeta tacográfica en el dispositivo lector/registrador de tarjetas.

5 11. Unidad según una de las reivindicaciones 1 a 10, caracterizada porque:

- la unidad comprende una interfaz de conexión (16), denominada interfaz de tarjeta, para una comunicación inalámbrica de la unidad con un dispositivo externo lector/registrador de tarjetas inteligentes, denominadas tarjetas tacográficas, perteneciendo cada tarjeta a un tipo de tarjeta predeterminado,
- dicho dispositivo lector/registrador externo está controlado por lo menos por un microprocesador principal (4) al que está asociado un circuito CSP (20), estando dicho microprocesador principal adaptado para ordenar a dicho circuito CSP la ejecución de por lo menos una operación de seguridad con vistas a la autenticación mutua de la unidad y de una tarjeta tacográfica presente en el dispositivo lector/registrador de tarjetas, y autorizar la apertura de una sesión de funcionamiento correspondiente al tipo de la tarjeta tacográfica presente únicamente si la unidad y dicha tarjeta son consideradas como auténticas.

12. Unidad según una de las reivindicaciones 9 a 11, caracterizada porque, en cada intercambio de datos entre la unidad (1) y una tarjeta tacográfica (60) presente en el dispositivo lector/registrador de tarjetas, dicho microprocesador principal (4) está adaptado para ordenar a dicho circuito CSP (20) la ejecución de por lo menos una operación de seguridad con vistas a la autenticación de dichos datos, y para tratar los datos intercambiados únicamente si éstos son considerados como auténticos e íntegros.

13. Unidad según la reivindicación 12, caracterizada porque el microprocesador principal (4) está adaptado para:

- cuando la unidad recibe datos desde dicha tarjeta tacográfica, ordenar a dicho circuito CSP (20) la ejecución de por lo menos una operación de seguridad con vistas a la autenticación de los datos recibidos, y para tratar dichos datos únicamente si éstos son considerados por el circuito CSP como auténticos e íntegros,
- cuando la unidad debe transmitir datos a dicha tarjeta tacográfica, ordenar a dicho circuito CSP (20) la ejecución de por lo menos una operación de seguridad con vistas a la protección de la integridad de los datos a transmitir.

14. Unidad según una de las reivindicaciones 1 a 13, que comprende una interfaz de conexión (12), denominada interfaz de sensor, para la conexión de la unidad al sensor de movimiento, caracterizada porque la tarjeta principal (3) comprende por lo menos un microprocesador principal (4) conectado a dicha interfaz de sensor (12) y al que está asociado un circuito CSP (20), estando dicho microprocesador principal (4) adaptado para ordenar a dicho circuito CSP (20) la ejecución de operaciones de seguridad con vistas, por una parte, a la autenticación mutua del sensor de movimiento y de la unidad y, por otra parte, a la autenticación de los datos de movimiento recibidos del sensor de movimiento por la unidad, y para tratar los datos de movimiento recibidos únicamente si el sensor de movimiento y la unidad son considerados como auténticos y si los datos recibidos son considerados como auténticos e íntegros.

15. Unidad según la reivindicación 14, caracterizada porque dicho microprocesador principal (4) está adaptado para:

- en el marco de una operación inicial denominada operación de emparejamiento de un sensor de movimiento y de la unidad, ordenar a dicho circuito CSP (20) la ejecución de por lo menos una operación de seguridad con vistas a la autenticación mutua del sensor y de la unidad, y para autorizar un intercambio ulterior de datos entre dicho sensor y la unidad únicamente si estos últimos son considerados como auténticos,
- en el marco de una operación periódica, denominada operación de control de los datos de movimiento, ordenar al circuito CSP (20) la ejecución de por lo menos una operación de seguridad con vistas a la autenticación de datos, denominados datos de control, intercambiados entre el sensor y la unidad en el marco de esta operación de control, y autorizar el tratamiento de los datos de movimiento recibidos por la unidad en un periodo transcurrido únicamente si dichos datos de control son considerados como auténticos e íntegros.

16. Unidad según las reivindicaciones 15 y 9, caracterizada porque el (los) microprocesador(es) (4) está(n) adaptado(s) para autorizar la ejecución de una operación de emparejamiento únicamente en el marco de una sesión de taller.

17. Unidad según una de las reivindicaciones 1 a 16 y según una de las reivindicaciones 9 u 11, caracterizada porque:

- comprende una interfaz de conexión (13, 14), denominada interfaz de descarga, para la comunicación de la unidad con un dispositivo externo denominado dispositivo de descarga, apto para memorizar datos tacográficos,

- el (los) microprocesador(es) principal(es) (4) está(n) adaptado(s) para autorizar la ejecución de una operación de descarga de datos hacia un dispositivo de descarga conectado a la unidad por medio de la interfaz de descarga únicamente en el marco de una sesión de controlador o de taller o de empresa.

18. Unidad según una de las reivindicaciones 1 a 17 y según la reivindicación 9, caracterizada porque:

- comprende una interfaz de conexión (13, 14), denominada interfaz de calibrado, para la comunicación de la unidad con un dispositivo externo denominado dispositivo de calibrado,
- el (los) microprocesador(es) principal(es) (4) está(n) adaptado(s) para autorizar la ejecución de una operación de calibrado de la unidad, por medio de un dispositivo de calibrado conectado a la unidad por medio de la interfaz de calibrado, únicamente en el marco de una sesión de taller.

19. Unidad según una de las reivindicaciones 1 a 18 y según la reivindicación 9, caracterizada porque un microprocesador principal (4) de la unidad está adaptado para vigilar las inserciones y retiradas de la tarjeta en el dispositivo (8) lector/registrador de tarjetas y para, en cuanto se detecta una retirada de una tarjeta tacográfica del dispositivo lector/registrado, interrumpir cualquier operación en curso en la sesión de funcionamiento correspondiente.

20. Unidad según una de las reivindicaciones 1 a 19, caracterizada porque:

- la tarjeta principal (3) comprende un único microprocesador principal (4) para el tratamiento de los datos tacográficos, al cual están conectados un circuito de alimentación eléctrica (6) alimentado de manera permanente por una fuente eléctrica permanente del vehículo, una memoria de masa (5), denominada memoria de aplicación, de tipo no volátil para el almacenamiento de por lo menos una aplicación denominada aplicación tacográfica, una memoria de masa (17), denominada memoria de datos, de tipo no volátil para el almacenamiento por lo menos de los datos tacográficos, un reloj en tiempo real con calendario (7), un dispositivo (8) lector/registrador de tarjetas inteligentes, denominadas tarjetas tacográficas, apto para recibir por lo menos dos tarjetas tacográficas en paralelo, un conector (12), denominado conector de sensor, para la conexión de la unidad al sensor de movimiento, un conector (13), denominado conector de descarga/calibrado, para la conexión a la unidad de un dispositivo externo de calibrado o de un dispositivo externo de descarga,
- la unidad comprende un único circuito CSP (20), dedicado a la realización de todas las operaciones de seguridad, estando dichos microprocesador principal (4) y circuito CSP (20) conectados y adaptados para funcionar según una relación maestro/esclavo en la que el microprocesador principal es el maestro y el circuito CSP es el esclavo,
- la unidad comprende una impresora (10), una pantalla de visualización (9), un dispositivo (11) de captura de datos por un usuario.

21. Vehículo automóvil, caracterizado porque está equipado con una unidad de tacógrafo según una de las reivindicaciones 1 a 20.

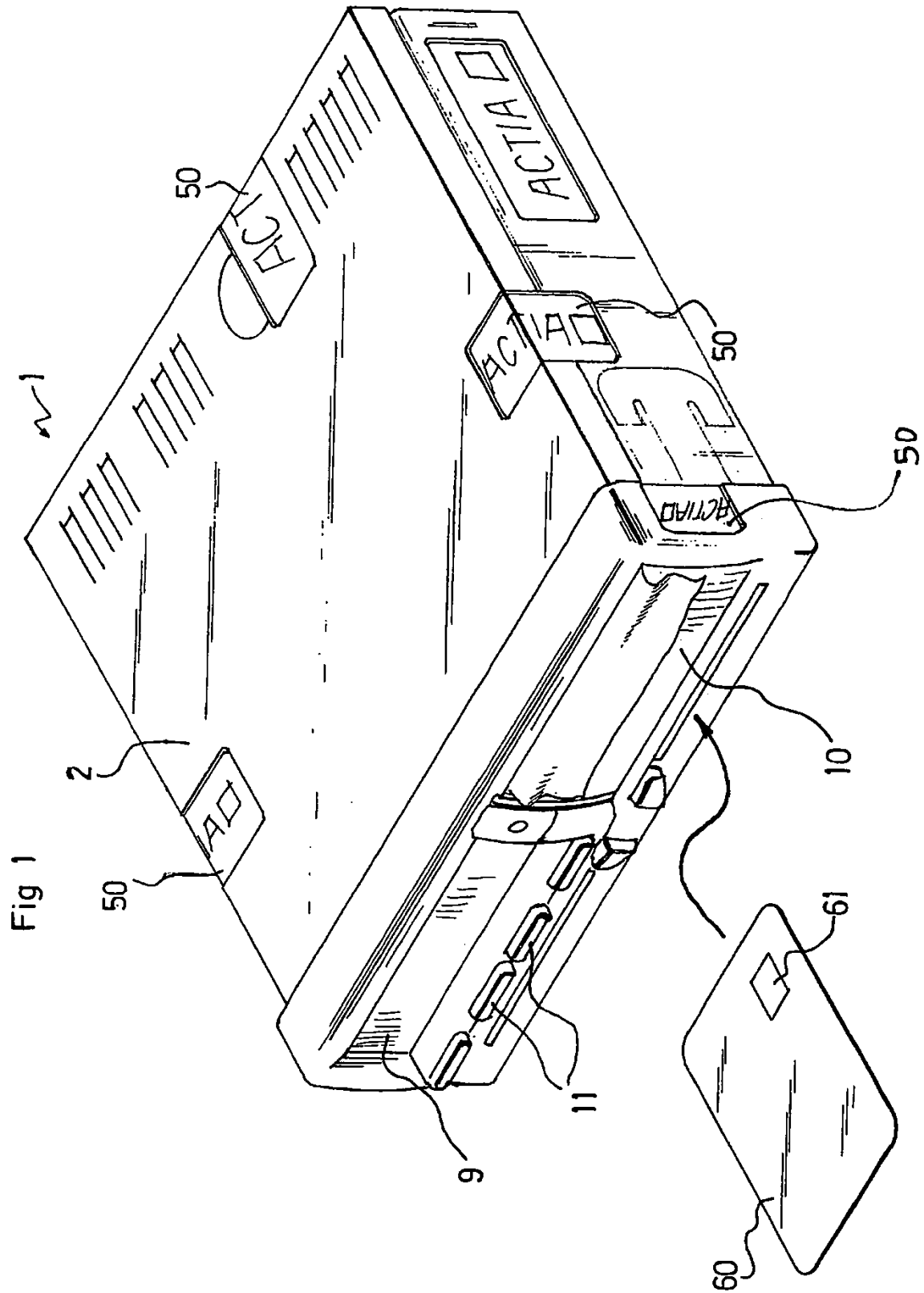
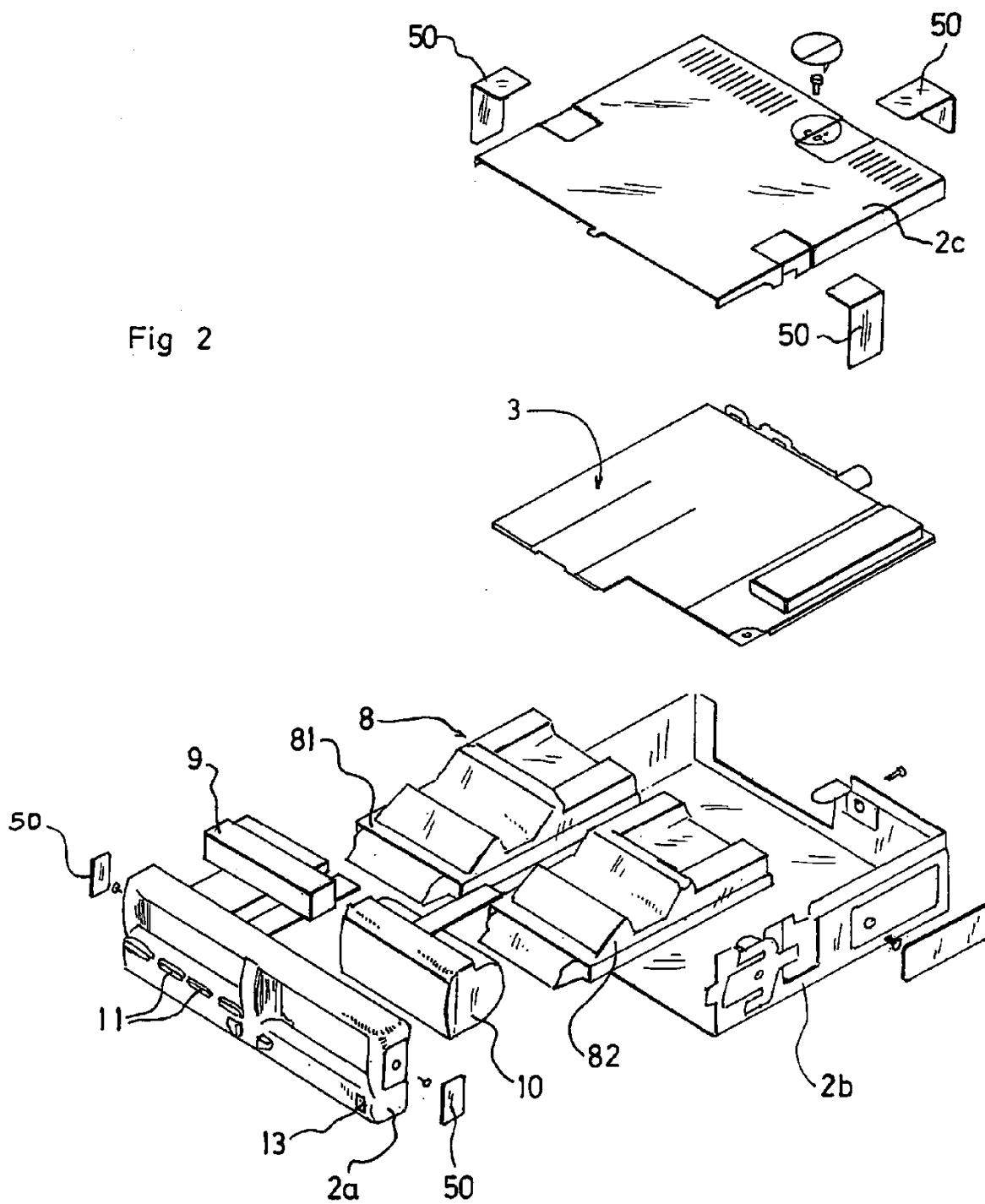


Fig 2



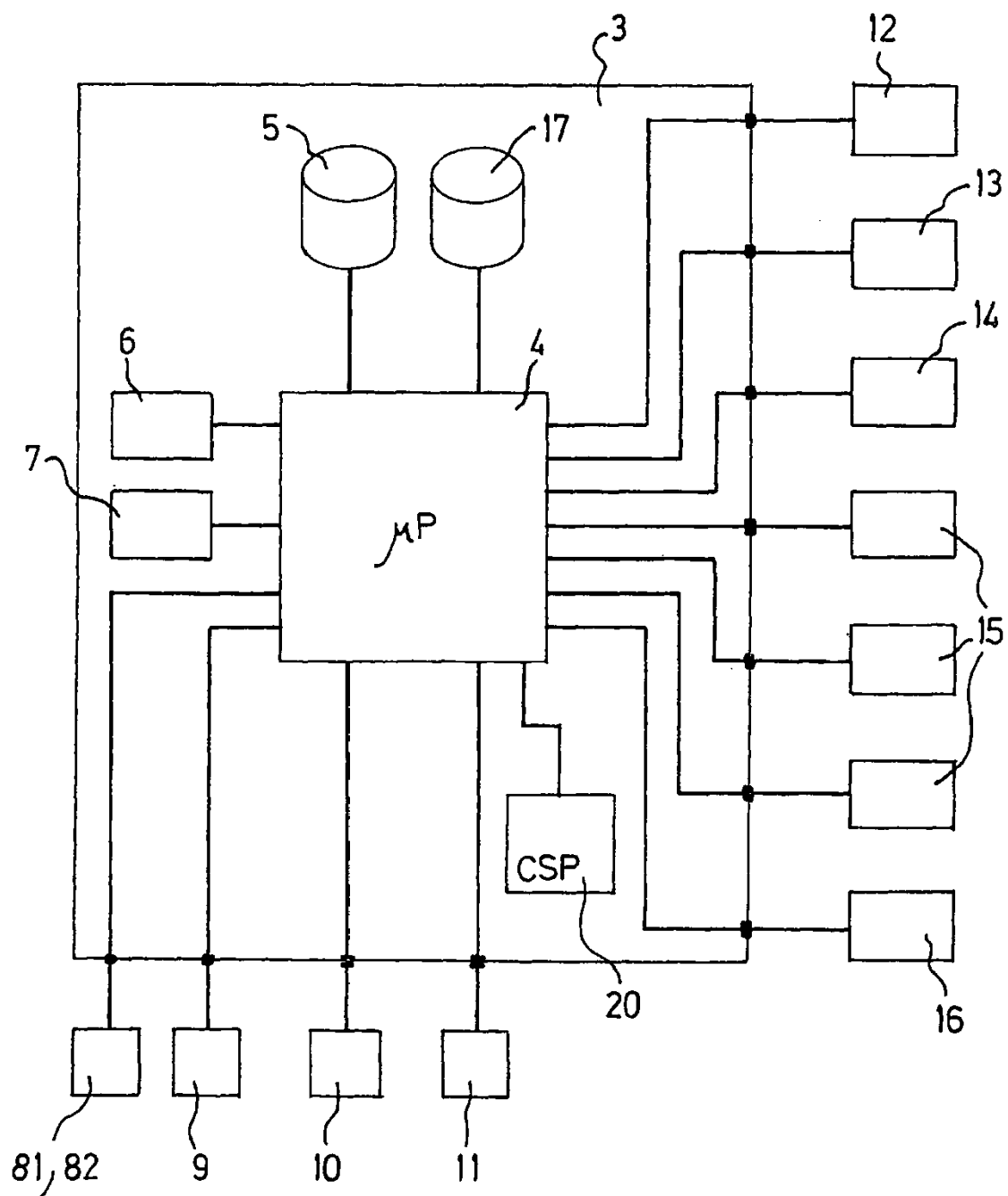


Fig 3

Fig 4

