(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 530 229**

(51) Int. CI.:

G05B 19/042 (2006.01)
G06F 21/44 (2013.01)
G06F 21/73 (2013.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06F 21/57 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.01.2001 E 01101343 (0)**

(97) Fecha y número de publicación de la concesión europea: **07.01.2015 EP 1128242**

(54) Título: **Procedimiento de firma**

(30) Prioridad:

25.02.2000 DE 10008974

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.02.2015

(73) Titular/es:

BAYERISCHE MOTOREN WERKE AKTIENGESELLSCHAFT (100.0%)
PETUELRING 130
80809 MÜNCHEN, DE

(72) Inventor/es:

SCHMIDT, ERNST y
KUHLS, BURKHARD

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento de firma.

La invención concierne a un procedimiento para securizar la integridad de los datos de un software para un aparato de control de un vehículo automóvil.

Con la proporción creciente de la electrónica y las posibilidades de comunicación en y con un vehículo crecen también los requisitos que tienen que imponerse a la seguridad.

En las muy diferentes zonas del vehículo se utilizan microcontroladores de mando. Estos aparatos de control están unidos hoy en día frecuentemente uno con otro a través de un sistema de bus y existen generalmente posibilidades (por ejemplo enlace de diagnosis) para acceder desde fuera a este bus y para comunicarse con los distintos aparatos de control.

El funcionamiento de los aparatos de control viene determinado por programas de software. Hasta ahora, el software que se utiliza en un aparato de control (también: controlador) está archivado casi siempre en una memoria no programable (por ejemplo, en microprocesadores programados con máscara). Por tanto, no se puede realizar sin ciertas dificultades una manipulación del software. Por ejemplo, se puede reconocer el cambio completo de un módulo de memoria por otro módulo de memoria y reaccionar a este cambio de una manera correspondiente.

Sin embargo, debido a la utilización futura, en el vehículo, de aparatos de control programables, especialmente los llamados aparatos de control programables flash, se hace mayor el peligro de que se realicen manipulaciones no autorizadas en el software y, por tanto, en el funcionamiento de los aparatos de control. Así, el cambio de software por parte de personas no autorizadas podría llevarse a cabo de manera sencilla mediante una nueva programación con poco coste.

Sin embargo, por motivos de seguridad y para cumplir con los requisitos legales se tienen que adoptar medidas que impidan una variación del software original o autoricen esta variación solamente a personas autorizadas.

Por lo demás, en el futuro se podría manifestar como ventajoso perseguir un concepto de piezas iguales, en el que se emplea un mismo hardware en modelos diferentes. La diferencia en el funcionamiento reside entonces solamente en el software. En este concepto existe ciertamente la necesidad de que un determinado software solamente pueda ejecutarse en un vehículo individual y no pueda ser copiado de una manera sencilla.

Se conocen por el estado de la técnica un gran número de procedimientos y dispositivos de autentificación.

Así, en el documento US 5,844,986 se describe un procedimiento que se emplea para evitar una intervención no permitida en un sistema BIOS de un PC. Un coprocesador criptográfico, que contiene una memoria BIOS, realiza una autentificación y comprobación de una variación BIOS basándose en un llamado procedimiento de clave pública con una clave pública y una clave secreta. La comprobación se efectúa en este caso mediante una comprobación de una firma digital incrustada en el software que se quiere cargar.

Se conoce por el documento EP 0 816 970 un dispositivo para comprobar un software de empresa. Este dispositivo para autentificar una memoria PROM de arranque comprende una parte de memoria con un microcódigo. Un sector de autentificación comprende un generador hash que genera datos hash en respuesta a la ejecución del microcódigo.

El documento EP-A-0 939 012 propone un procedimiento para verificar la coherencia de informaciones que se cargan, a través de un aparato de carga remota, en un ordenador para controlar el funcionamiento de un equipo funcional de un automóvil. En este caso, el ordenador calcula una palabra de validación en base a las informaciones y compara la palabra de validación con una palabra de validación correspondiente almacenada en el ordenador de manera inaccesible para el aparato de carga remota. Para la verificación, el ordenador comprueba si la palabra de validación calculada por el ordenador coincide con la palabra de validación almacenada en el ordenador.

Sin embargo, con los procedimientos o dispositivos anteriores no es posible realizar directamente la comprobación de un software que se quiera cargar en un aparato de control de un vehículo automóvil.

El problema de la presente invención consiste en proporcionar un procedimiento para securizar la carga de un software auténtico en un aparato de control de un vehículo automóvil.

El problema se resuelve con las características de la reivindicación 1.

Según ésta, se genera primeramente un par de claves para el cifrado y descifrado de datos electrónicos. Por claves se entienden aquí en general parámetros de codificación y/o descodificación que son conocidos por algoritmos criptográficos en sí conocidos.

En el presente caso, el software es provisto de una firma (signatura) electrónica por medio de la primera clave. Para verificar la autenticidad del software se ha archivado una segunda clave correspondiente en o para el aparato de control en el cual deberá cargarse este software. Con esta segunda clave se puede comprobar la firma electrónica del software. Si la comprobación se desarrolla positivamente, se acepta entonces el software y éste puede ser aprovechado para controlar el aparato de control.

Como cifrado puede emplearse según una primera forma de realización un llamado procedimiento simétrico en el que ambas claves son idénticas. Por tanto, se trata aquí realmente de una sola clave que se emplea en sitios diferentes. Sin embargo, dado que tiene que contarse siempre con posibilidades de que se conozca una clave archivada en un aparato de control, el nivel de seguridad de un procedimiento simétrico no es óptimo. Por tanto, este procedimiento puede utilizarse únicamente cuando no están afectados procesos demasiados críticos para la seguridad. Para aumentar el nivel de seguridad se puede emplear una protección contra disparo adicional en forma de un hardware especial.

Según otra forma de realización preferida, se elige un procedimiento de cifrado asimétrico con una clave secreta y una clave pública. En este caso, la clave pública puede estar archivada en o para el aparato de control. Con la clave secreta se firmaría entonces el software. Como alternativa, el aparato de control o el propio vehículo puede generar también el par de claves asíncrono y archivar luego la clave secreta en el aparato de control. La clave pública tendría que ser entonces legible de modo que se pueda firmar con ella un software. Naturalmente, en la última alternativa habría que asegurarse de que la clave secreta no sea legible.

Los algoritmos de cifrado con una clave secreta y una clave pública consisten en un llamado procedimiento de clave pública en el que la clave pública deberá ser públicamente conocida, mientras que la clave secreta es conocida solamente por un sitio autorizado, por ejemplo un centro de confianza. Tales algoritmos criptográficos son, por ejemplo, el algoritmo de Rivest, Shamir y Adleman (algoritmo RSA), un algoritmo de encriptado de datos (algoritmo DEA) y algoritmos similares. Con la clave secreta o la clave pública se puede generar – análogamente a la firma manuscrita – una firma digital para un documento electrónico. Solamente el propietario de la clave secreta o pública puede confeccionar una firma válida. La autenticidad del documento puede comprobarse después mediante la verificación de la firma por medio de la clave pública o secreta correspondiente. La clave secreta se denomina a veces también clave privada.

Un tercero no autorizado que no conozca la clave correcta no está en condiciones de proveer una firma válida. Si se carga entonces en un aparato de control un software manipulado y no firmado correctamente, esto es reconocido con la clave correspondiente y el aparato de control es puesto, por ejemplo, en un estado de incapacitado para funcionar.

Según otra forma de realización de la invención, se archiva la clave en el sector de arranque del aparato de control. El sector de arranque está casi siempre protegido de una manera especial y no puede sobrescribirse sin mayores dificultades. Según un perfeccionamiento, el sector de arranque puede ser “bloqueado” después de la inscripción y el ingreso de la clave, de modo que ya no sea posible un acceso adicional, especialmente una inscripción adicional. Se aseguraría así que la clave archivada en el sector de arranque estuviera protegida contra manipulación.

Para satisfacer los requisitos de una utilización de un software exclusivamente individual para un vehículo, el software previsto para un aparato de control de un vehículo determinado contiene informaciones individualizadoras del vehículo, por ejemplo el número del chasis u otros datos individuales del vehículo. Estas informaciones están asociadas al software o integradas en éste. Únicamente después de la asociación de estos datos al software o de su integración en el mismo, dicho software es firmado entonces con la clave prevista para ello. Un aparato de control acepta – como se ha descrito anteriormente – el software únicamente cuando se reconoce la firma como impecable con la otra clave asociada. Dado que la firma depende de la información individual del vehículo contenida en el software, ésta no pueda variarse posteriormente. Un software apto para ser ejecutado por un aparato de control de un vehículo puede alimentarse únicamente cuando no se haya variado la información individual del vehículo y ésta coincida realmente con la del vehículo. Por tanto, es imposible que un software individualizado de esta manera para un vehículo sea copiado en otro vehículo, ya que la información individual del vehículo no puede ser variada sin vulnerar la firma.

Para no tener que realizar una comprobación del software cada vez que se arranca un vehículo y se activan los aparatos de control, se realiza una comprobación de esta clase preferiblemente al menos durante la operación de carga. En el caso de un software impecablemente firmado, éste puede caracterizarse entonces de manera correspondiente, por ejemplo colocando en el aparato de control una bandera que no deberá ser influenciada en otras ocasiones. Después de la colocación de esta bandera el software queda aceptado también para otras activaciones. De esta manera, se pueden evitar retardos en el arranque normal del vehículo. Sin embargo, hay que asegurarse en este caso de que esta bandera no pueda ser influenciada desde fuera.

Para crear otro nivel de seguridad al cargar un software en las memorias del aparato de control, deberá ser posible según otra forma de realización de la invención, antes de la carga del software, un acceso a la memoria del aparato de control solamente con una autorización correspondiente. A este fin, antes del traspaso del software firmado está

prevista una “apertura” del aparato de control en un paso de solicitud. Cuando se emplean niveles de acceso diferentes en la solicitud, se podrían adjudicar, además, derechos de acceso diferentemente configurados. En el caso de un acceso de diagnóstico sería necesaria primeramente, por ejemplo, una solicitud, con lo cual el aparato de control reconoce a través de la información de acceso ingresada los derechos de acceso y el nivel de autorización ligado a ellos. Según la adjudicación de derechos, las autorizaciones de acceso pueden clasificarse desde no críticas hasta muy críticas. Según una forma de realización, se pide un código al aparato de control y se comprueba la validez de éste. A este fin, puede generarse, por ejemplo, en el aparato de control un número aleatorio que se devuelve después por el accedente en forma procesada, por ejemplo codificado o firmado de otra manera. En el aparato de control se comprueba entonces esta información, por ejemplo por medio de una clave de autentificación propia.

Es posible también configurar dinámicamente la adjudicación de derechos de acceso. Por ejemplo, se pueden proveer certificados de acceso de cuyas informaciones se desprenda el nivel de acceso. Si se acepta entonces un certificado de acceso, lo que puede ocurrir a su vez por la comprobación de una firma con una clave, se conceden entonces los derechos listados en el mismo.

Un aparato de control eventualmente previsto en exclusiva para el control de acceso no deberá estar dispuesto en forma libremente accesible en el vehículo frente a los restantes aparatos de control a causa de la función de seguridad central relativa a la adjudicación de derechos de autentificación, ya que mediante el desmontaje físico de un aparato de control se podrían esquivar los mecanismos de protección anteriormente descritos. Por tanto, es deseable una protección especial contra desmontaje, por ejemplo mecánica, de un aparato de control de seguridad de esta clase.

Además, se puede conseguir también un nivel de seguridad especial mediante la configuración de un conjunto de aparatos de control en el que están mutuamente conectados aparatos de control diferentes y éstos se condicionan unos a otros o se comprueban mutuamente.

Para excluir también el peligro de que se desmonte un aparato de control individual y se le sustituya por otro, puede ser conveniente, además, una protección propia contra desmontaje de los aparatos de control. A este fin, se realiza esporádicamente una prueba de autenticidad de los aparatos de control, por ejemplo en un vehículo en el que están integrados los aparatos de control. A este fin, se dirige una consulta a los aparatos de control, a la que éstos tienen que contestar con una información esperada determinada. Si la información realmente entregada por el aparato de control a comprobar no coincide con la información esperada o el aparato de control no contesta, se adoptan entonces unas medidas de securización adecuadas. En el caso de aparatos de control no críticos para la seguridad, el aparato de control puede ser excluido, por ejemplo, del conjunto de comunicación. Cuando el aparato de control es importante para el funcionamiento del vehículo, éste es entonces, por ejemplo, registrado, marcado o inscrito en una lista, de modo que al menos pueda comprenderse la manipulación en materia de software realizada en el respectivo aparato de control. En una forma de realización los aparatos de control tienen que contestar a la consulta por medio de una clave de autentificación secreta. Un aparato de control ilegalmente cambiado no dispone de esta clave y es entonces reconocido y tratado de manera correspondiente.

La presente invención se explica seguidamente con más detalle ayudándose de ejemplos de realización y con referencia a los dibujos adjuntos. Los dibujos muestran en:

La figura 1, una representación esquemática de una estructura de aparato de control en un vehículo,

La figura 2a y la figura 2b, una representación esquemática del desarrollo de una firma digital de un software y su comprobación,

La figura 3a y la figura 3b, una representación del desarrollo de la firma digital del software de la figura 2, pero en otro modo de representación,

La figura 4, una representación del desarrollo de la provisión de una firma por un centro de confianza,

La figura 5, una representación de un algoritmo para un procedimiento de comprobación especial de informaciones individuales de un vehículo,

Las figuras 6a y 6b, un diagrama de bloques y de desarrollo para una autentificación con respecto a un aparato de control y

La figura 7, un diagrama de desarrollo para la realización de una inscripción de un software en un aparato de control.

En la figura 1 se representa en forma de diagrama de bloques una estructura de aparato de control con unidades conectadas en red unas con otras. La red de a bordo está constituida aquí por varias redes parciales (LWL-Most, sistema K-CAN, Powertrain-CAN, etc.) que poseen en parte velocidades de transmisión diferentes y que están unidas una con otra por medio de las llamadas pasarelas (módulo de pasarela central, pasarela de controlador).

Un bus de diagnóstico 16 está conectado directa o indirectamente con todas las demás redes por medio de la pasarela central 14. El bus de diagnóstico 16 representa uno de los enlaces más importantes con el entorno. A través de un testador de diagnóstico, que está conectado a una caja de enchufe OBD dispuesta en el extremo del bus de diagnóstico 16, y con intercalación de la pasarela central 14, se pueden activar todos los controladores, pasarelas y aparatos de control en el sistema completo.

Como alternativa, existe la posibilidad de acceder a los aparatos del vehículo a través de la red GSM 20 y un sistema telefónico 18 del vehículo. Es posible así en principio un acceso remoto a la red de a bordo del vehículo. El sistema telefónico 18 representa aquí también una pasarela entre la red de telefonía móvil (red GSM) y los abonados restantes del bus del vehículo.

En el bus del vehículo está integrado un sistema de acceso al coche (CAS) 22 que vigila la entrada en el vehículo. Incluye como función adicional un inmovilizador electrónico.

Una pasarela de controlador 21 representa una interfaz entre un reproductor de CDs y la red de a bordo. En la pasarela de controlador 21 se convierten también en mensajes las órdenes de entrada que imparte el conductor a través de los diferentes instrumentos, y estos mensajes se retransmiten a los respectivos aparatos de control activados.

Además, se representan varios aparatos de control (STG1 a STG5). El cometido de un aparato de control no solo consiste en el control de una unidad determinada en el vehículo, sino también en la comunicación entre los propios aparatos. La comunicación en el vehículo está “orientada a la radiodifusión”. Un generador de informaciones, que ha obtenido el acceso al bus, envía en principio sus informaciones a todos los aparatos de control. Se escucha para ello permanentemente el bus de datos que está unido con el controlador. Por el contrario, en la comunicación con el entorno, por ejemplo a través del bus de diagnóstico, se activa deliberadamente cada aparato de control con una dirección unívoca.

El software que determina la funcionalidad de la unidad de control estará alojado predominantemente en el futuro en una memoria programable, por ejemplo una memoria flash. En una programación flash solo se pueden borrar e inscribir de nuevo bloques completos. No es posible el borrado de bits individuales. Según los aparatos de control, se utilizan diferentes clases de microordenadores. Según los requisitos, éstos son procesadores de 8 bits, 16 bits o 32 bits. Todos estos aparatos de control o controladores están disponibles en variantes diferentes. Presentan, por ejemplo, una memoria flash en la placa electrónica o directamente integrada en el procesador.

El desarrollo de una securización de la integridad de los datos de un software para un aparato de control con una memoria flash se representa seguidamente con más detalle ayudándose de las figuras 2a y 2b.

En primer lugar, en un primer paso se proporciona por un único sitio autorizado, por ejemplo en un llamado centro de confianza, un par de claves constituido por una clave pública 58 y una clave secreta 52. Una clave es aquí un código electrónico con el que se puede cifrar y/o descifrar una información. Por ejemplo, se emplean en este caso unos algoritmos criptográficos conocidos, como los algoritmos RSA o DEA ya mencionados anteriormente, es decir, los llamados “algoritmos de clave pública” con pares de claves síncronos.

Se entrará primero en más detalles sobre el cifrado empleado. En el presente procedimiento de autentificación se prefiere un cifrado asíncrono. En el caso de claves simétricas, cada lado tiene que estar en posesión del “secreto”. Tan pronto como una clave síncrona, además de ser conocida por los sitios autorizados, es conocida también por terceros, no puede garantizarse una precaución de securización perfecta. Sin embargo, dado que en el presente procedimiento tiene que estar archivada en el aparato de control de un vehículo automóvil una clave del par de claves y, por tanto, no puede asegurarse el mantenerla en secreto, no es aconsejable la elección de un par de claves simétrico.

En contraste con el cifrado simétrico, W. Diffie y M. Hellman desarrollaron en 1976 la llamada criptografía de clave pública. En esta clase de cifrado se genera un par de claves con una clave pública y una clave secreta. Con la clave secreta se puede realizar una firma de un documento electrónico. Esta firma es singular y en general no puede ser comprendida. Con la clave pública se puede comprobar la firma.

El procedimiento de clave pública tiene la ventaja de que una clave del par de claves puede ser públicamente conocida. Sin embargo, dado que los procedimientos de clave pública actualmente conocidos son muy intensivos en cálculo, se emplean frecuentemente procedimientos híbridos, es decir, una combinación de procedimientos simétricos y asimétricos. En el procedimiento híbrido se intercambia entre las partes comunicantes una clave simétrica por medio de un procedimiento de clave pública. La comunicación propiamente dicha es cifrada entonces con la clave simétrica.

Debido a la separación de las claves secreta y pública se pueden materializar procedimientos de autentificación y firmas digitales como se ha descrito anteriormente. Gracias a la posesión de la clave secreta se puede verificar unívocamente una identidad y se puede proveer una firma como en el caso de una firma manuscrita. Un

criptosistema de clave pública conocido es el procedimiento RSA ya mencionado anteriormente. Otros criptoprocedimientos de clave pública se basan en problemas en determinados grupos matemáticos para calcular logaritmos (problema de logaritmos discretos).

Para firmar digitalmente un documento, el único sitio autorizado cifra el documento con la clave secreta y agrega un valor de firma al documento. Para la verificación de la firma se descifra la firma con la clave pública y se compara el valor resultante con el valor del documento original. Si coinciden ambos valores del documento, la firma es entonces válida y se puede aceptar el software.

En el presente caso, una respectiva clave pública es almacenada por el sitio autorizado durante la producción de un vehículo en cada aparato de control del vehículo que deba ser modificado respecto del software (por ejemplo, el aparato de control de la caja de cambios).

Un cliente pide ahora a un distribuidor 100 (véase la figura 4) una función adicional determinada para su vehículo automóvil, por ejemplo una característica de cambio determinada para la selección de las etapas de multiplicación. Esta función puede materializarse por la carga de un nuevo software en el aparato de control de la caja de cambios del respectivo vehículo.

El distribuidor 100 proporciona seguidamente un software correspondiente 150 y lo envía, junto con el número de chasis del vehículo del cliente, al centro de confianza 104, que es el único autorizado para firmar (signar) este software. En el centro de confianza 104 se firma con la clave secreta el software juntamente con el número de chasis transmitido.

Este modo de proceder está representado también en la figura 2a (software 50, clave secreta 52), pero no se transmite aquí ningún número de chasis.

El software firmado 106 (véanse la figura 4 y el símbolo de referencia 56 en la figura 2a) se retransmite entonces al distribuidor 100, el cual lo puede cargar en el vehículo automóvil 12 del cliente.

La transmisión al centro de confianza 100, la operación de firma y la retransmisión pueden efectuarse con relativa rapidez por vía electrónica.

En el paso siguiente se carga el software firmado 56, 106, por parte del distribuidor 100, en el vehículo 12, o mejor en el aparato de control de la caja de cambios. La transmisión puede efectuarse a través del enchufe de diagnóstico y el bus de diagnóstico 16. Como alternativa, se puede efectuar también una carga controlada a distancia a través de la red GSM.

Durante la carga se efectúa primeramente una solicitud e identificación del distribuidor (véase el paso 500 en la figura 7). El distribuidor 100 envía para ello una dirección del aparato de control y un indicativo correspondiente al vehículo. En el caso de una identificación satisfactoria, se conecta el aparato de control (aquí: el aparato de control de la caja de cambios) dejándolo preparado para la inscripción del nuevo software. Es así posible la inscripción (también grabación en memoria flash) de un software nuevo en el aparato de control (véase 502 en la figura 7). Después de la carga del nuevo software en el aparato de control, el distribuidor 100 ha hecho su parte de la tarea.

En la operación siguiente el aparato de control 24 (figura 2), al ser activado, comprueba la firma del nuevo software cargado 56 por medio de la clave pública 58. Esto se explicará con detalle ayudándose de la figura 2b. Con la clave pública 58 se determina a partir de la firma en una unidad 60 del aparato de control 24 una magnitud que tiene que coincidir con el documento electrónico 62 que ha sido cifrado. Esta coincidencia se comprueba en un comparador 64. Cuando existe una coincidencia, se acepta el software cargado 50 y se hace funcionar el aparato de control 24 con este software. Si no existe coincidencia alguna, se marca el aparato de control 24 y se le archiva en una lista. En un diagnóstico se pueden recuperar después los datos de esta lista. Se proporciona entonces una nueva oportunidad para cargar un software correcto. Si no se carga un software correctamente firmado, el vehículo no puede seguir funcionando.

En las figuras 3a y 3b se han representado con algo más de precisión el cifrado y el descifrado. Durante la firma del software no se firma todo el software. Esto sería ineficiente. Por el contrario, se genera a partir del software, a través de una función hash en sí conocida, un llamado código hash 51 que consiste en una información digital de una longitud prefijada. Según las necesidades de seguridad, se puede elegir una longitud de, por ejemplo, 16 bits, 64 bits o 128 bits. Se firma entonces únicamente este código hash 51 (firma 54) y se agrega la firma al software 50. La firma del código hash es sensiblemente más eficiente que la firma de documentos de software largos.

Las funciones hash tienen entonces las siguientes propiedades esenciales: Es difícil encontrar para un valor hash dado un valor M de un documento (función unidireccional). Además, es difícil encontrar una colisión, es decir, dos valores con M y M' en los que sean iguales los valores hash (resistencia a las colisiones).

Durante la comprobación de la firma 50 se obtiene, aplicando la clave pública a la firma (símbolo de referencia 53 en la figura 3b), un valor hash 51' con el que se compara el valor hash real 51 del software 50 en un comparador 66. Si

coinciden ambos valores hash, se acepta el software 50. Se trata entonces de un software auténtico y el aparato de control puede hacerse funcionar con el software cargado. Si la comparación no es positiva, el aparato de control interrumpe su funcionamiento y espera hasta que haya sido cargado un software irreprochable con una firma correcta.

Aparte del desarrollo de autentificación anteriormente descrito se emplea frecuentemente también un llamado procedimiento de desafío-respuesta para la autentificación de una parte comunicante A frente a una parte comunicante B. En este caso, B envía primero a A un número aleatorio RND. A firma este número aleatorio por medio de su clave secreta y como respuesta envía a B este valor. B verifica la respuesta por medio de su clave pública y comprueba la autentificación de A.

Una autentificación de esta clase está representada en las figuras 6a y 6b. En la figura 6a se representa el bucle de comunicación entre un testador de diagnóstico y un aparato de control. En la autentificación según el procedimiento de desafío-respuesta un usuario envía primeramente por medio del testador de diagnóstico una información con un nivel de acceso determinado LI al aparato de control y solicita al aparato de control un número aleatorio (paso 400). El aparato de control contesta con la transmisión de un número aleatorio (paso 402). En el testador de diagnóstico se firma el número aleatorio con una clave secreta y después se envía el resultado nuevamente al aparato de control (paso 404). En el aparato de control se determina nuevamente el número aleatorio a partir de la firma con ayuda de la clave pública. Si el número así calculado coincide con el número aleatorio previamente transmitido por el aparato de control, se libera el acceso para este usuario con la etapa de seguridad deseada durante el periodo de tiempo del procedimiento de diagnóstico. Por tanto, el usuario, con una clasificación de seguridad correspondiente, puede inscribir un software en la memoria de un aparato de control.

A continuación, se describe la individualización del software para un vehículo determinado. Ya al hacer referencia al proceso de firma según la figura 4 se mencionó que se transmite con el software una identificación del vehículo que corresponde únicamente a un vehículo determinado. Se firma entonces el software juntamente con la identificación del vehículo (por ejemplo, el número del chasis) y se reenvía el paquete al distribuidor. La firma entra entonces en el código hash (descrito en la forma de realización según las figuras 3a y 3b) e influye también decisivamente sobre la firma.

El aparato de control acepta solamente – como ya se ha descrito antes – un software correctamente firmado. Si la firma es correcta, se comprueba también si la identificación de vehículo asociada al software coincide realmente con la del vehículo. Si ocurriera esto, se liberaría entonces el software. Con este modo de proceder se puede emplear el software individualizado de vehículo solamente en un vehículo de destino determinado. Para otro vehículo se tiene que adquirir nuevamente otro software provisto de una firma individual.

Para poder realizar una individualización de un software, el número del chasis deberá ser incorporado ya durante la fabricación en los aparatos de control correspondiente de una manera no manipulable. El número del chasis tiene que estar presente todavía en el aparato de control incluso después de un borrado de una memoria. Esto puede materializarse registrando el número del chasis en una memoria no volátil y no recambiable, por ejemplo en el sistema de acceso al coche ya mencionado más arriba y especialmente protegido.

El modo de proceder siguiente según la figura 5 asegura una consulta no manipulable. Además del número del chasis, se necesita otro par de claves individual del vehículo consistente en una clave secreta IFSs y una clave pública IFSp. La asociación del número del chasis y las dos claves se efectúa en un puesto central, es decir, en el centro de confianza. La clave secreta IFSs está almacenada en un sistema 210 de acceso al coche, concretamente en forma no legible.

El número del chasis ya se encuentra también hoy en la zona de acceso del sistema 210 de acceso al coche.

En el nuevo software que se debe cargar se archiva ahora también, además del número del chasis, la clave pública IFSp 202 individual del vehículo (paso 200 en la figura 5). Seguidamente, se securiza todo el software en el centro de confianza por medio de la firma 204. Después de la carga del software en el aparato de control se comprueba primeramente la naturaleza correcta de la firma 204.

Seguidamente, el aparato de control 206 comprueba, por medio de la consulta de desafío-respuesta anteriormente descrita, si el número de chasis incluido en el software coincide con el del vehículo. A este fin, el aparato de control 206 envía el número de chasis FGNsw contenido en el software y un número aleatorio RANDOM al sistema 210 de acceso al coche. El número de chasis almacenado FGN es comparado allí con el número de chasis recibido FGNsw. A continuación, se firman los dos valores con la clave secreta IFSs y se les reenvía nuevamente al aparato de control 206. El aparato de control 206 puede comprobar ahora con la clave pública IFSp el envío firmado y comparar los valores obtenidos con el valor de desafío que se envió al principio al sistema de acceso al coche. Si coincide los valores, se puede aceptar entonces el software (paso 216, o.k.). En caso contrario, no se acepta el software (paso 218, no).

Como variante de este procedimiento, en lugar de un par de claves individual IFSs y IFSp se puede emplear también

un par de claves correspondiente, no individualizado para el vehículo, que esté ya almacenado en el vehículo. Se suprime así la administración de esta clave. Asimismo, es posible, naturalmente, un mecanismo correspondiente con un procedimiento criptográfico simétrico. Esto tiene ciertamente ventajas de procesamiento, pero trae consigo el peligro de la extracción de la clave asimétrica de los aparatos de control.

Naturalmente, en todos los procedimientos anteriormente citados hay que asegurarse absolutamente de que las claves secretas del centro de confianza permanezcan también secretas. En conjunto, la criptografía antes citada ofrece una buena posibilidad de cargar solamente el software correcto en vehículos o en determinados vehículos y, por tanto, prevenir manipulaciones no autorizadas.

REIVINDICACIONES

1. Procedimiento para securizar la integridad de los datos de un software para un aparato de control de un vehículo automóvil, en el que se puede almacenar en una memoria del aparato de control un software que influye en el funcionamiento del aparato de control, **caracterizado** por los pasos de

habilitar un par de claves para el cifrado y descifrado de datos electrónicos,

archivar una primera clave en o para un aparato de control del vehículo automóvil,

firmar con la segunda clave un software que se quiere cargar,

cargar el software firmado en la memoria del aparato de control,

comprobar la firma del software por medio de la clave archivada en o para el aparato de control y aceptar el software cargado cuando la comprobación se desarrolle con un resultado positivo,

añadir al software al menos una información individual de un vehículo que contiene el aparato de control,

firmar el software juntamente con la al menos una información individual del vehículo,

por que, aparte de la comprobación de la firma del software, se comprueba también la información individual del vehículo, por que se acepta el software en el aparato de control solamente cuando la información individual de vehículo del software coincide con la del vehículo, y

por que la firma depende de la información individual del vehículo contenida en el software.

2. Procedimiento según la reivindicación 1, **caracterizado** por que se emplea un par de claves asimétrico en el que ambas clases son iguales.

3. Procedimiento según la reivindicación 1, **caracterizado** por que se emplea un par de claves asimétrico con una clave secreta y una clave pública.

4. Procedimiento según la reivindicación 3, **caracterizado** por que la clave pública está archivada en o para el aparato de control y se firma el software con la clave secreta.

5. Procedimiento según la reivindicación 3, **caracterizado** por que el vehículo, especialmente el o un aparato de control del vehículo, genera un par de claves síncrono, por que se archiva la clave secreta en el vehículo, especialmente en un aparato de control, y por que se puede extraer del vehículo la clave pública para firmar un software.

6. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que la clave archivada en el aparato de control se archiva en el sector de arranque de un ordenador.

7. Procedimiento según la reivindicación 6, **caracterizado** por que el sector de la rutina de arranque se bloquea después de la inscripción y el ingreso de la clave y está así protegido contra un acceso adicional, especialmente un acceso de inscripción.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que se reproduce primeramente el software sobre una información de longitud determinada y se firma luego esta información.

9. Procedimiento según la reivindicación 8, **caracterizado** por que se elige como función de reproducción una función hash.

10. Procedimiento según la reivindicación 1, **caracterizado** por que se genera un par de claves propio (par de claves individual del vehículo) para comprobar la información individual del vehículo, estando presentes en una unidad de seguridad del vehículo la información individual del vehículo y una primera clave del par de claves propio, estando archivada también en el software, junto a la información individual del vehículo, la segunda clave del par de claves propio y comprobándose en una rutina separada en el vehículo si coinciden las dos claves del par de claves propio, para aceptar, en caso afirmativo, el software cargado.

11. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que se comprueba el software al menos durante la primera activación del aparato de control y se le marca entonces de manera correspondiente.

12. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que, en caso de un acceso externo al aparato de control, una unidad de acceso comprueba si existe una autorización para el acceso.

13. Procedimiento según la reivindicación 12, **caracterizado** por que se solicita un código a un aparato de control y se comprueba la naturaleza correcta de este código.

14. Procedimiento según la reivindicación 12 ó 13, **caracterizado** por que un aparato de control emite un número aleatorio que ha de ser firmado por el accedente, y por que se comprueba la firma en el aparato de control, especialmente por medio de una clave de autentificación.

15. Procedimiento según cualquiera de las reivindicaciones 12 a 14, **caracterizado** por que, al consultar la autorización de acceso, se verifica un nivel de autorización y se aceptan o no se aceptan acciones de acceso en función del nivel de autorización.

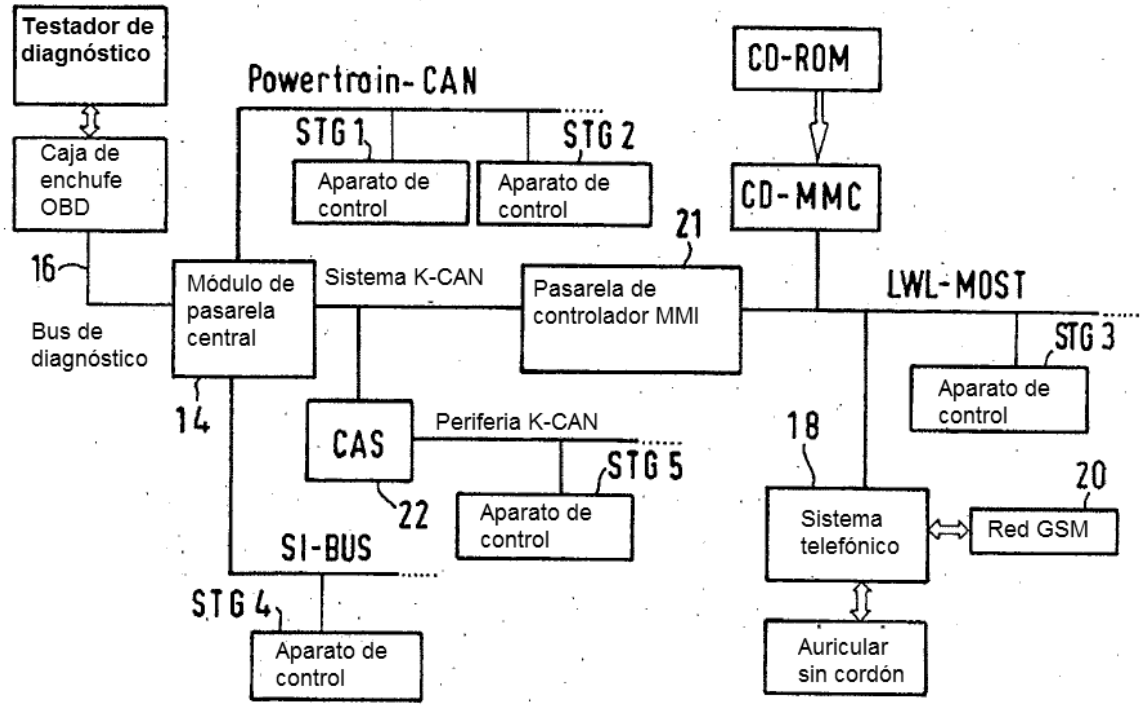
16. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que un equipo de seguridad realiza en un vehículo al menos esporádicamente una comprobación de autentificación de un aparato de control y registra el aparato de control en caso de resultado negativo.

17. Procedimiento según la reivindicación 16, **caracterizado** por que en el aparato de control está archivado un código secreto individual de dicho aparato de control.

18. Procedimiento según la reivindicación 16 o 17, **caracterizado** por que el equipo de seguridad consulta una característica específica del aparato de control y comprueba la autenticidad de ésta.

19. Procedimiento según cualquiera de las reivindicaciones 16 a 18, **caracterizado** por que se emplea en la comprobación de autenticidad una clave archivada en el equipo de seguridad y/o una clave archivada en el aparato de control.

FIG.1


Testador de diagnóstico
Caja de enchufe OBD
16
Bus de diagnóstico
Powertrain-CAN
STG 1
Aparato de control
STG 2
Aparato de control
Módulo de pasarela central
14
Sistema K-CAN
Pasarela de controlador MMI
21
CD-ROM
CD-MMC
LWL-MOST
STG 3
Aparato de control
CAS
22
Periferia K-CAN
STG 5
Aparato de control
SI-BUS
STG 4
Aparato de control
18
Sistema telefónico
20
Red GSM
Auricular sin cordón

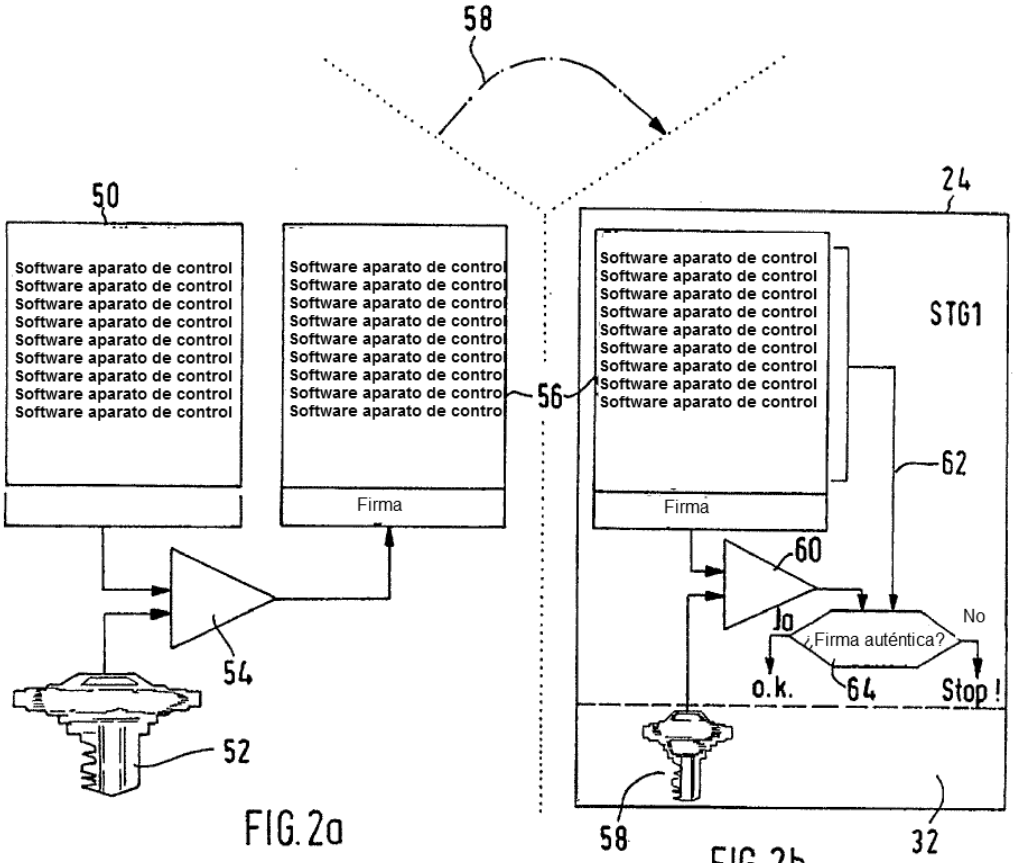


FIG. 2a

FIG. 2b

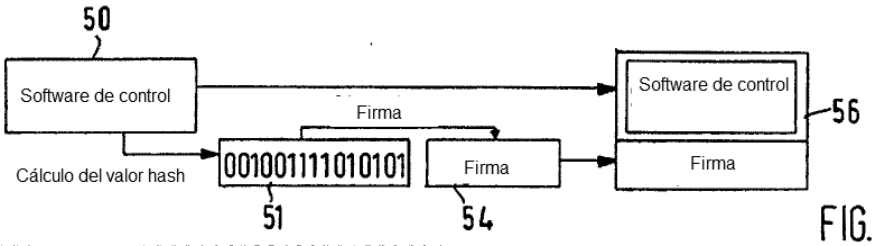
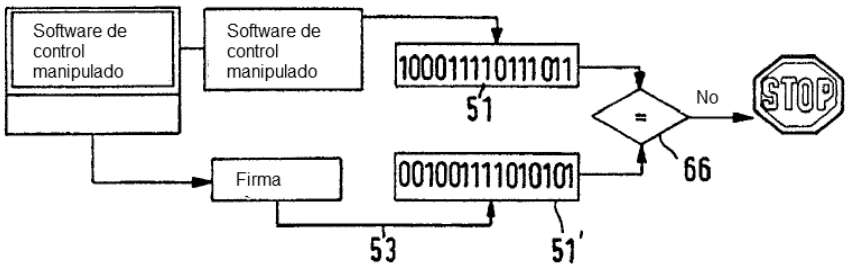


FIG. 3a

FIG. 3b



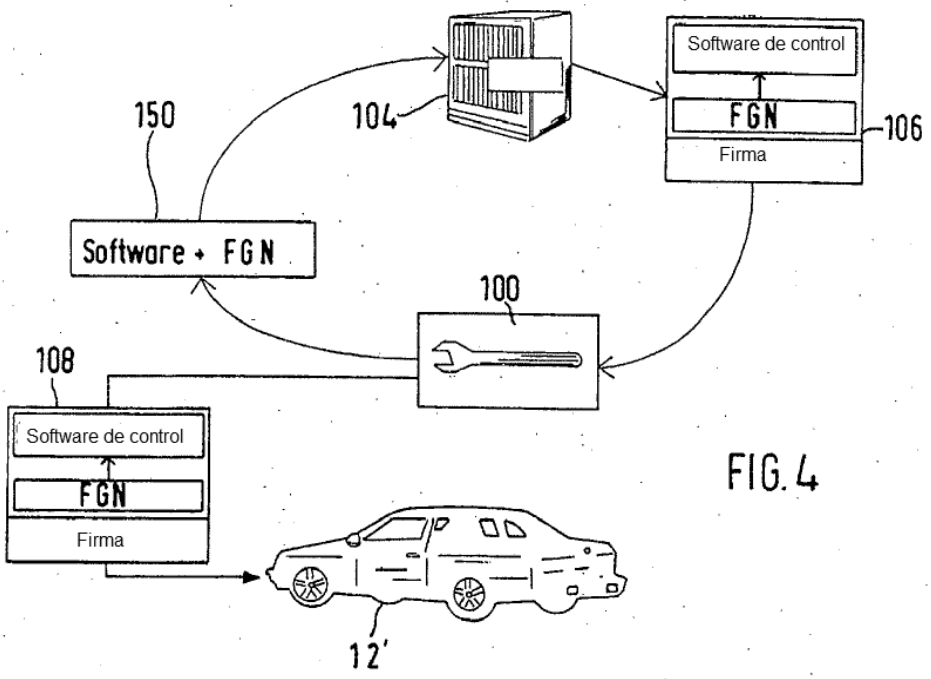

150
104
Software de control
FGN
106
Firma
Software + FGN
100
108
Software de control
FGN
Firma
12'

FIG. 4

FIG.5

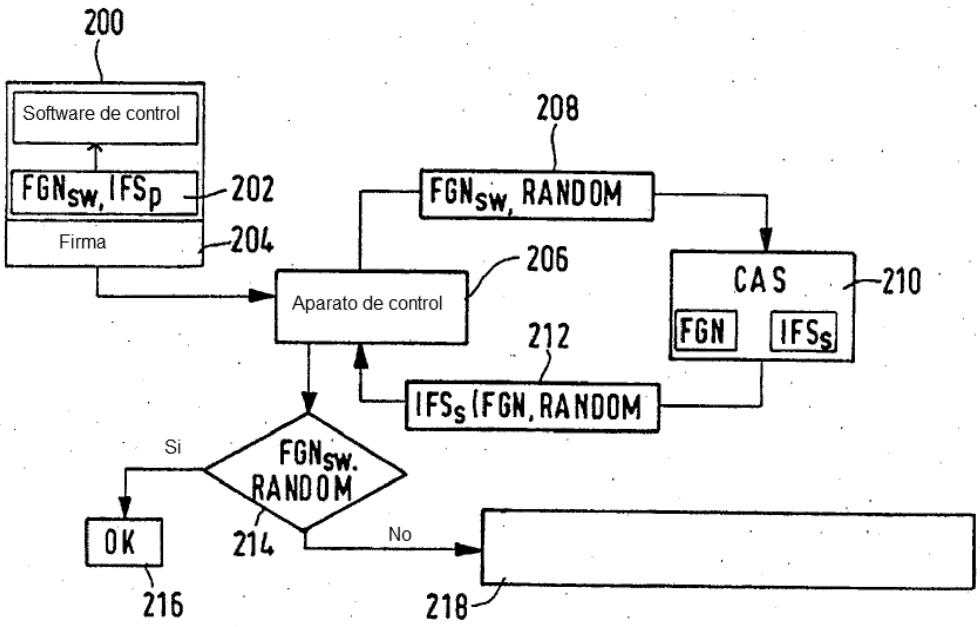

200
Software de control
FGNsw, IFSp
202
Firma
204
208
FGNsw, RANDOM
206
Aparato de control
CAS
210
FGN
IFSs
212
IFSs (FGN, RANDOM
Si
FGNsw. RANDOM
214
OK
216
No
218

FIG. 6a,

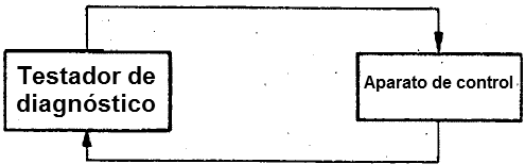

Testador de diagnóstico
Aparato de control

FIG. 6b,

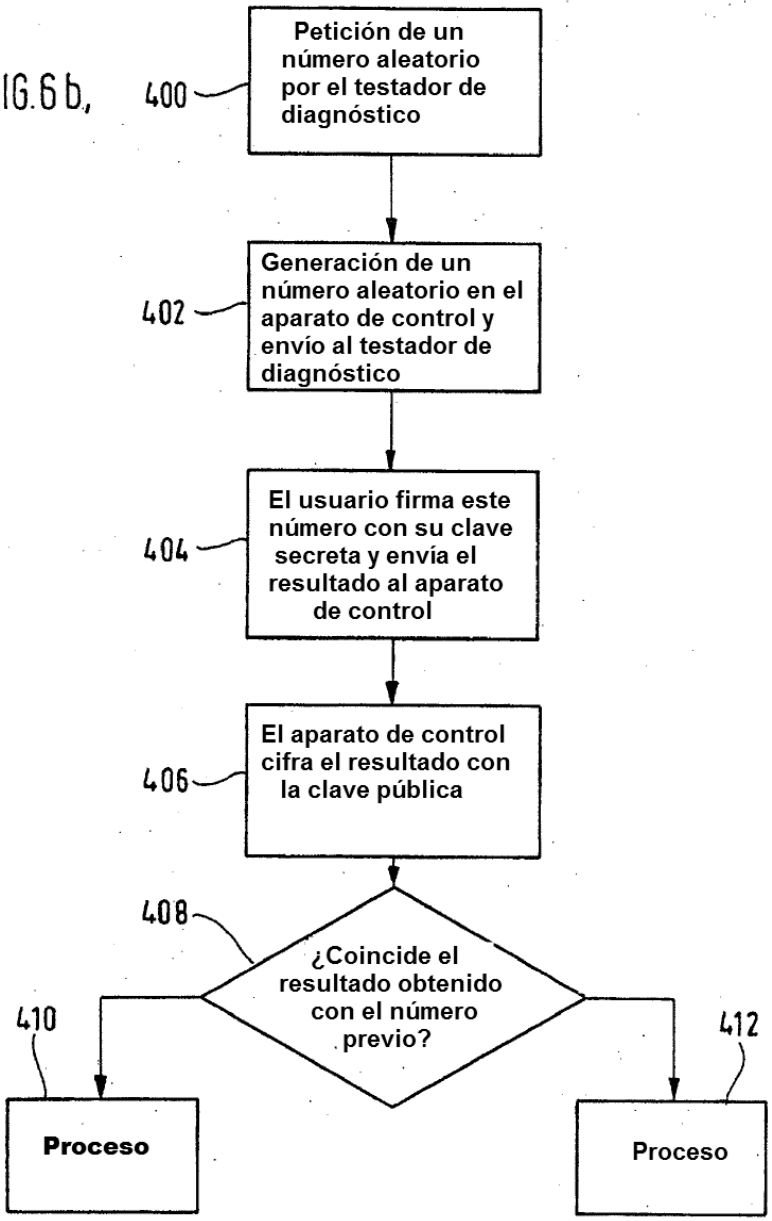
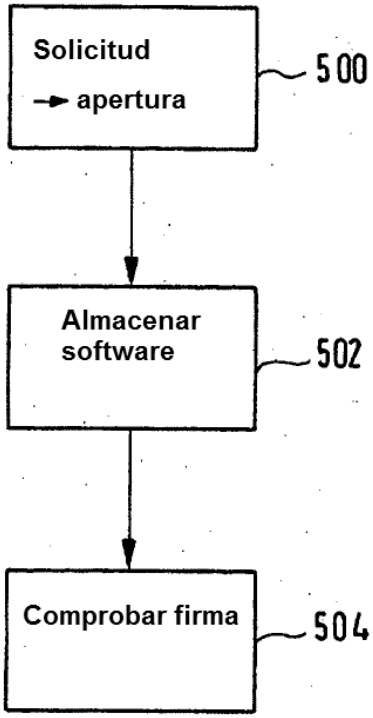

400
Petición de un número aleatorio por el testador de diagnóstico
402
Generación de un número aleatorio en el aparato de control y envío al testador de diagnóstico
404
El usuario firma este número con su clave secreta y envía el resultado al aparato de control
406
El aparato de control cifra el resultado con la clave pública
408
¿Coincide el resultado obtenido con el número previo?
410
Proceso
412
Proceso

FIG. 7


Solicitud
apertura
500
Almacenar
software
502
Comprobar firma
504