(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 386 352**

(51) Int. CI.:

B60R 25/00 (2006.01)
B60R 25/04 (2006.01)
H04L 9/32 (2006.01)
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04730263 .3**
(96) Fecha de presentación: **29.04.2004**
(97) Número de publicación de la solicitud: **1740418**
(97) Fecha de publicación de la solicitud: **10.01.2007**

(54) Título: **Autenticación de un dispositivo externo a un vehículo**

(45) Fecha de publicación de la mención BOPI:
17.08.2012

(45) Fecha de la publicación del folleto de la patente:
17.08.2012

(73) Titular/es:
BAYERISCHE MOTOREN WERKE AKTIENGESELLSCHAFT
PETUELRING 130
80809 MÜNCHEN, DE

(72) Inventor/es:
KUHLS, Burkhard y
KIESSLING, Horst

(74) Agente/Representante:
Lehmann Novo, Isabel

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

Autenticación de un dispositivo externo a un vehículo.

La invención concierne especialmente a un procedimiento de autenticación de un dispositivo externo a un vehículo en un sistema de bus de un vehículo automóvil que presenta instrumentos de control, según el preámbulo de la reivindicación 1. El documento US 5 708 712 A revela las características del preámbulo de la reivindicación 1.

Para impedir manipulaciones en el control de desarrollo almacenado en los instrumentos de control o en el software correspondiente, que es ejecutado por uno o varios procesadores previstos en los instrumentos de control, es importante vigilar la autorización del acceso a los instrumentos de control. La autorización puede comprobarse con ayuda de medidas criptográficas.

Es desventajoso el hecho de que la realización de medidas criptográficas correspondientes carga al procesador o los procesadores del instrumento de control y a otros componentes de hardware del instrumento de control o bien requiere instrumentos de control más potentes y, por tanto, más caros. Esto se hace perceptible especialmente en un producto utilizado millones de veces, tal como ocurre con el instrumento de control de un vehículo automóvil.

El problema de la presente invención consiste especialmente en indicar un procedimiento que impida eficazmente y con poco coste una manipulación de un control de desarrollo almacenado en un instrumento de control.

Este problema se resuelve en el aspecto del procedimiento con las medidas indicadas en la reivindicación 1 y en el aspecto del dispositivo con la reivindicación de sistema independiente. Ejecuciones ventajosas de la invención son objeto de las reivindicaciones subordinadas.

Un aspecto esencial del procedimiento según la invención para autenticar un dispositivo externo a un vehículo en un sistema de bus de un vehículo automóvil que presenta instrumentos de control consiste en la realización de las medidas siguientes. En un primer paso un dispositivo de autenticación previsto en el sistema de bus transmite una consulta de autenticación al dispositivo externo al vehículo. El dispositivo externo al vehículo firma la consulta de autenticación con una clave secreta de un par de claves asimétricas, especialmente un par clave pública-clave secreta, y transmite la consulta de autenticación firmada o únicamente la firma al dispositivo de autenticación.

La consulta de autenticación consiste preferiblemente en un número aleatorio o similar generado por el dispositivo de autenticación, que se genera en particular solamente una vez. El dispositivo de autenticación consiste preferiblemente en un instrumento de control central que tiene acceso a la clave pública del par clave pública-clave secreta y que puede ejecutar un procedimiento de clave pública.

El dispositivo de autenticación obtiene, empleando el mismo algoritmo que el dispositivo externo al vehículo, una firma de la consulta de autenticación, descifra la firma transmitida por el dispositivo externo al vehículo mediante el empleo de la clave pública complementaria de la clave secreta y compara la firma obtenida con la transmitida.

En una ejecución de la invención se ha previsto que, en caso de una comparación positiva o de una coincidencia de las firmas, el dispositivo externo al vehículo gane, a través del dispositivo de autenticación, acceso de escritura y/o de lectura a una memoria de al menos unos de los instrumentos de control.

En una forma de realización preferida de la invención se posibilita en el dispositivo externo al vehículo que la memoria de uno o varios instrumentos de control sea provista de un nuevo control de desarrollo o software y/o de un nuevo código de liberación. El nuevo control de desarrollo puede consistir especialmente en un control de desarrollo que ha sido actualizado frente al control de desarrollo anterior, elimina problemas de software y/o habilita funciones adicionales del instrumento de control. El nuevo control de desarrollo puede consistir en un complemento del control de desarrollo ya almacenado en el instrumento de control, que habilita especialmente funciones adicionales del instrumento de control.

El código de liberación puede consistir especialmente en datos que liberan, especialmente dentro de un plazo temporal, un control de desarrollo o software mantenido preparado para su desarrollo en el instrumento de control o en otro sitio del vehículo. Esto quiere decir que el control de desarrollo o software ya almacenado en el vehículo se puede ejecutar únicamente después de la habilitación del código de liberación en el vehículo.

En una forma de realización alternativa o complementaria de la invención se han previsto las medidas siguientes para autenticar instrumentos de control o para comprobar si se trata de instrumentos de control autorizados en el sistema de bus. En un primer paso un primer instrumento de control de un gran número de instrumentos de control del vehículo automóvil transmite una consulta de autenticación al dispositivo de autenticación a través del sistema de bus.

La consulta de autenticación consiste preferiblemente en un número aleatorio o similar generado por el instrumento de control, el cual se genera únicamente una sola vez. El dispositivo de autenticación es tal que tiene acceso a una

clave criptográfica simétrica y puede ejecutar un procedimiento criptográfico simétrico.

La ejecución de un procedimiento criptográfico simétrico somete a los recursos del instrumento de control o del dispositivo de autenticación, especialmente al procesador, a una carga netamente más pequeña que en el caso de un procedimiento asimétrico, de modo que la autenticación de los instrumentos de control en un vehículo frente al dispositivo de autenticación puede efectuarse a un coste netamente menor cuando se emplea la invención.

El dispositivo de autenticación firma la consulta de autenticación empleando una primera clave simétrica y transmite la consulta de autenticación firmada o únicamente la firma al primer instrumento de control. El firmado o la generación de la firma se realiza aplicando un algoritmo hash a la consulta de autenticación o a los datos de autenticación. El algoritmo hash suministra un valor hash que es característico de los datos de autenticación concretos. El valor hash se cifra con la primera clave simétrica y el valor hash cifrado se agrega a la consulta de autenticación o a los datos de autenticación y, junto con la consulta de autenticación, se le transmite al primer instrumento de control. Como alternativa, se puede transmitir también únicamente la firma o el valor hash cifrado al primer instrumento de control, puesto que allí se ha generado ciertamente y está así ya presente la consulta de autenticación.

El primer instrumento de control compara la firma transmitida con una firma obtenida por el primer instrumento de control aplicando la clave simétrica a la consulta de autentificación. La firma puede ser obtenida por el primer instrumento de control haciendo que el mismo algoritmo hash que ha sido aplicado por el dispositivo de autenticación a la consulta de autenticación para obtener la firma sea aplicado también por el primer instrumento de control a la consulta de autenticación. Se obtiene nuevamente un valor hash. Este valor hash o la firma formada a base del valor hash empleando la clave simétrica se compara con la firma transmitida o con el valor hash obtenido nuevamente a partir de la firma transmitida empleando la clave simétrica.

En caso de una comparación positiva o una coincidencia de las firmas o valores hash, el primer instrumento de control y el dispositivo de autenticación se consideran como recíprocamente autenticados, es decir que para el instrumento de control se considera el dispositivo de autenticación como auténtico o autorizado, y viceversa. De manera correspondiente, en caso de una comparación positiva o una coincidencia, se hace preferiblemente que el primer instrumento de control esté preparado para funcionar. Como alternativa o como complemento, se podría otorgar al dispositivo de autenticación un acceso de escritura y/o de lectura a una memoria electrónica del primer instrumento de control.

En un ejemplo de realización preferido de la invención se ha previsto que uno o varios instrumentos de control adicionales del sistema de bus realicen de la manera descrita la autenticación con el dispositivo de autenticación. Por tanto, gracias a estas medidas se puede comprobar si se encuentran en el sistema de bus instrumentos de control no autorizados o un dispositivo de autenticación no autorizado.

En otro ejemplo de realización de la invención se realiza sucesivamente la autenticación de los instrumentos de control frente al dispositivo de autenticación. Esto reduce los recursos de hardware necesarios.

En un ejemplo de realización de la invención se ha previsto que el vehículo automóvil pueda ser puesto en funcionamiento tan sólo cuando prácticamente todos los instrumentos de control del sistema de bus hayan realizado el procedimiento de autenticación con resultado de comparación positivo. Se puede garantizar así la seguridad de funcionamiento del sistema de bus o la compatibilidad de los abonados del bus. Asimismo, esta medida aumenta la protección contra robo del vehículo automóvil equipado con el sistema de bus de la invención cuando está integrado un inmovilizador en el sistema de bus o en los instrumentos de control.

En otro ejemplo de realización de la invención se ha previsto que la ejecución del procedimiento de autenticación se efectúe en cada caso antes del arranque del vehículo, preferiblemente después de la apertura del vehículo. Gracias a esta medida se comprueban la seguridad funcional, la compatibilidad, etc. no sólo una sola vez, sino periódicamente.

En un ejemplo de realización de la invención se ejecuta antes del arranque del vehículo el procedimiento de autenticación según la invención para prácticamente tan sólo los instrumentos de control que tienen que estar disponibles al arrancar el vehículo, a fin de que el vehículo, tras un corto tiempo de marcha de calentamiento - en caso de que sea necesario -, esté preparado para funcionar. El procedimiento de autenticación según la invención puede ejecutarse luego para los demás instrumentos de control después del proceso de arranque del vehículo, sin que se dificulte la puesta en funcionamiento del vehículo automóvil.

En otro ejemplo de realización de la invención se ha previsto que prácticamente todos los instrumentos de control empleen la misma clave simétrica para la ejecución del procedimiento de autenticación. Esta medida hace que sea más sencilla la administración de las claves y, además, tiene la ventaja de que los instrumentos de control del vehículo correspondiente están así asociados uno a otro.

En un ejemplo de realización de la invención se ha previsto que la clave asimétrica varíe de un vehículo a otro y que

un instrumento de control de un primer vehículo, al ejecutar el procedimiento de autenticación según la invención, acceda a una primera clave simétrica y el mismo instrumento de un segundo vehículo, al ejecutar el procedimiento, acceda a una segunda clave simétrica, o bien emplee una clave de esta clase.

La clave simétrica está preferiblemente "alojada" en el sistema de bus de tal manera que pueda ser leída únicamente por el dispositivo de autenticación y por los instrumentos de control implicados en el procedimiento, es decir que permanezca secreta, y no pueda ser variada sin autorización. En una ejecución de la invención la clave simétrica está almacenada en la respectiva zona de carga no externamente legible o variable de cada instrumento de control y en la zona correspondiente del dispositivo de autenticación.

Como quiera que la clave simétrica varía de un vehículo a otro, es relativamente inocuo el espionaje de la clave simétrica de un vehículo concreto. Por supuesto, esto sería completamente diferente en el caso de espionaje de una clave simétrica de un vehículo que "case" con todos los vehículos del mismo tipo.

En un ejemplo de realización de la invención se ha previsto que el procedimiento según la invención se desarrolle en dirección contraria, es decir que el dispositivo de autenticación transmita una consulta de autenticación al primer instrumento de control, y el primer instrumento de control firme la consulta de autenticación con la primera clave simétrica y transmita la consulta de autenticación firmada al dispositivo de autenticación.

En este caso, se desplaza la comparación del instrumento de control al dispositivo de autenticación. Esto va acompañado de una descarga de recursos de cada instrumento de control y una carga de recursos del dispositivo de autenticación. La múltiple descarga de recursos frente a una única carga de recursos conduce a ahorros de costes de hardware.

La invención hace posible un sistema de bus de un vehículo automóvil con instrumentos de control en el que está previsto en el sistema de bus un dispositivo de autenticación y se ejecuta en el sistema de bus un procedimiento conforme a la invención. Asimismo, la invención hace posible un producto de programa informático para la autenticación de un dispositivo externo a un vehículo en un sistema de bus de un vehículo automóvil que presenta instrumentos de control, cuyo producto permite que se desarrolle un procedimiento según una o varias de las reivindicaciones de procedimiento siguientes.

REIVINDICACIONES

1. Procedimiento de autenticación de un dispositivo externo a un vehículo en un sistema de bus de un vehículo automóvil que presenta instrumentos de control, en el que

- en el sistema de bus está previsto un dispositivo de autenticación,
- el dispositivo de autenticación transmite una consulta de autenticación al dispositivo externo al vehículo,
- el dispositivo externo al vehículo firma la consulta de autenticación con una clave secreta de un par de claves asimétricas, especialmente un par clave pública-clave secreta, y transmite la consulta de autenticación firmada al dispositivo de autenticación,
- el dispositivo de autenticación obtiene una firma de la consulta de autenticación empleando el mismo algoritmo que el dispositivo externo al vehículo, y **caracterizado** porque
- se descifra la firma transmitida por el dispositivo externo al vehículo empleando la clave pública complementaria de la clave secreta y se compara la firma obtenida con la transmitida.

2. Procedimiento según la reivindicación 1, **caracterizado** porque, en caso de una comparación positiva o un coincidencia, el dispositivo externo al vehículo adquiere, a través del dispositivo de autenticación, acceso de escritura y/o de lectura a una memoria de al menos uno de los instrumentos de control.

3. Procedimiento según la reivindicación 1 ó 2, **caracterizado** porque

- para la autenticación de los instrumentos de control, un primer instrumento de control transmite una consulta de autenticación al dispositivo de autenticación a través del sistema de bus,
- el dispositivo de autenticación firma la consulta de autenticación empleando una primera clave simétrica y transmite la consulta de autenticación firmada o únicamente la firma al primer instrumento de control,
- el primer instrumento de control compara la firma transmitida de la consulta de autenticación con una firma obtenida por el primer instrumento de control aplicando la clave simétrica a la consulta de autenticación, y/o
- el primer instrumento de control descifra la firma transmitida de la consulta de autentificación empleando la primera clave simétrica y se obtiene un primer valor hash, y el primer instrumento de control aplica un algoritmo hash a la consulta de autenticación, con lo que se obtiene un segundo valor hash, y
- en caso de una comparación positiva o una coincidencia de las firmas y/o de los valores hash, se hace que el primer instrumento de control quede preparado para funcionar.

4. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** porque uno o varios instrumentos de control adicionales del sistema de bus ejecutan el procedimiento de autenticación según la reivindicación 3.

5. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** porque el vehículo automóvil puede ponerse en funcionamiento tan solo cuando prácticamente todos los instrumentos de control del sistema de bus han ejecutado el procedimiento de autenticación según la reivindicación 3 con un resultado de comparación positivo.

6. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** porque la ejecución del procedimiento de autenticación se realiza cada vez antes del arranque del vehículo, preferiblemente después de la apertura del vehículo.

7. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** porque prácticamente todos los instrumentos de control emplean la misma clave simétrica para la ejecución del procedimiento de autenticación según la reivindicación 3.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** porque la clave simétrica varía de un vehículo a otro y un instrumento de control de un vehículo emplea, para la ejecución del procedimiento según la reivindicación 3, una primera clave simétrica y el mismo instrumento de control de un segundo vehículo emplea, para la ejecución del procedimiento según la reivindicación 3, una segunda clave simétrica.

9. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** porque el procedimiento según la reivindicación 3 se desarrolla en dirección contraria, es decir que el dispositivo de autenticación transmite una consulta de autenticación al primer instrumento de control, y el primer instrumento de control firma la consulta de autenticación con la primera clave simétrica y transmite la consulta de autenticación firmada o únicamente la firma al

dispositivo de autenticación.

10. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** porque el procedimiento según la reivindicación 1 se desarrolla en dirección contraria, es decir que el dispositivo externo al vehículo ejecuta las medidas realizadas por el dispositivo de autenticación y el dispositivo de autenticación ejecuta las medidas realizadas por el dispositivo externo al vehículo.

11. Sistema de bus de un vehículo automóvil con instrumentos de control, **caracterizado** porque en el sistema de bus está previsto un dispositivo de autenticación y en el sistema de bus se ejecuta un procedimiento según cualquiera de las reivindicaciones de procedimiento anteriores.

12. Producto de programa informático para autenticar un dispositivo externo a un vehículo en un sistema de bus de un vehículo automóvil que presenta instrumentos de control, **caracterizado** porque el producto de programa informático permite que se desarrolle un procedimiento según una o varias de las reivindicaciones de procedimiento anteriores.