(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 333 714**

(51) Int. Cl.:
B60R 25/04 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03797205 .6**
(96) Fecha de presentación : **23.07.2003**
(97) Número de publicación de la solicitud: **1532027**
(97) Fecha de publicación de la solicitud: **25.05.2005**

(54) Título: **Procedimiento para la protección frente a manipulaciones en un aparato de control para un componente de automóvil, y aparato de control.**

(30) Prioridad: **21.08.2002 DE 102 38 094**

(45) Fecha de publicación de la mención BOPI:
26.02.2010

(45) Fecha de la publicación del folleto de la patente:
26.02.2010

(73) Titular/es: **AUDI AG.**
85045 Ingolstadt, DE

(72) Inventor/es: **Feilen, Oliver y**
Stadtmüller, Rüdiger

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento para la protección frente a manipulaciones en un aparato de control para un componente de automóvil, y aparato de control.

La presente invención se refiere a un procedimiento para la protección de manipulaciones en un aparato de control para al menos un componente de automóvil así como a un aparato de control.

En automóviles se utilizan actualmente aparatos de control para el control de componentes individuales del automóvil, como por ejemplo el aparato de control del motor o el aparato de control de la caja de cambios. Las informaciones necesarias para el funcionamiento de tales aparatos de control, como por ejemplo programas y datos son depositadas codificadas o no codificadas en módulos de memoria (E^2PROM, Flash y similares). El procedimiento de codificación está depositado en este caso de manera independiente de una combinación de hardware fijo de módulos y, en general, en un medio de memoria que se puede escribir de nuevo.

El inconveniente de tales aparatos de control y de los programas utilizados es que pueden sustituirse módulos individuales de memoria, o bien se pueden sobrescribir los datos en los módulos de memoria a través de una interfaz de diagnosis o a través de acceso directo al módulo de memoria. La sustitución de un módulo de memoria o la sobrescritura de los datos y programas memorizados en este módulo de memoria puede conducir a que el componente del automóvil trabaje con otros datos característicos. Esto se realiza, por ejemplo, durante la llamada sintonización del chip, en la que se sustituyen módulos de memoria, que están asociados al aparato de control del motor o bien se modifican programas y datos memorizados en estos módulos de memoria, como datos característicos. De esta manera, se puede conseguir, por ejemplo, una elevación de la potencia o del par motor del motor. Si se realiza esta manipulación sin adaptar los otros componentes del automóvil, como refrigerador de aceite, turboalimentador o frenos, entonces se pueden producir daños en estos componentes del automóvil y estados críticos para la seguridad.

El documento DE 197 23 332 A1 describe un procedimiento para la protección de un microordenador configurado como aparato de control para un automóvil contra manipulaciones de un programa, en el que el microordenador presenta una memoria sólo de lectura y una memoria que se puede escribir de nuevo. En este caso, en la memoria sólo de lectura están depositados programas de control para un motor del automóvil. Módulos adicionales del programa así como datos que comprenden parámetros del motor están registrados en la memoria que se puede escribir de nuevo. En la memoria sólo de lectura está previsto un programa de verificación, que está en condiciones de investigar un contenido de la memoria que se puede escribir de nuevo para detectar modificaciones inadmisibles, por ejemplo un intercambio de datos.

El programa de la presente invención es, por lo tanto, crear un aparato de control para componentes de automóviles y un procedimiento para la protección de manipulaciones en un aparato de control, en el que no es posible una sustitución de un módulo de memoria y la modificación de los datos en el módulo de memoria, sin influir en la capacidad funcional del aparato de control o diagnosticar al menos la modificación y, dado el caso, representarla.

Este problema se soluciona a través de un procedimiento con las características de la reivindicación 1 de la patente y a través de un aparato de control con las características de la reivindicación 4 de la patente.

La invención se basa en el reconocimiento de que este cometido se puede solucionar cuando los datos y programas necesarios para el funcionamiento del aparato de control son depositados en diferentes memorias.

El problema en que se basa la invención se soluciona, por lo tanto, a través de un procedimiento para la protección contra manipulaciones en un aparato de control para al menos un componente de automóvil, en el que el código necesario para el funcionamiento del aparato de control se divide en, al menos, un código maestro, que comprende informaciones esenciales para la función del aparato de control, y, al menos un sub-código, que comprende otras informaciones para el funcionamiento del aparato de control, en el que al menos el código maestro es depositado en una zona del microordenador protegida contra lectura, que solamente se puede escribir una vez y el código maestro supervisa la manipulación del sub-código.

A través de la división del código, que es necesario para el funcionamiento del aparato de control, se puede hacer accesible, por un lado, una parte que debe reprogramarse o bien actualizarse, por ejemplo, en caso de reparaciones, sin que debe ser accesible la parte, que contiene informaciones esenciales para el funcionamiento del aparato de control. Además, a través de la división del código es posible un registro del código en diferentes memoria, lo que implica una elevación de la seguridad contra manipulaciones. El código maestro puede representar, por ejemplo, el programa de control propiamente dicho, que comprende el cálculo de la carga del motor y el número de revoluciones y de las variables de ajuste y los valores de ajuste para el acceso a campos característicos y la generación de señales de control para actuadores conectados del aparato de control. En el sub-código puede estar contenido entonces el programa, por ejemplo, para medidas que mejora del escape de gases y la comodidad. Ambos códigos pueden contener adicional o alternativamente datos.

De acuerdo con la invención, se deposita el código maestro en una zona OTP (one-time-programmable) del microordenador protegida contra lectura, que solamente se puede escribir una vez. De esta manera se imposibilita, por

una parte, una modificación no autorizada del código maestro y, por otra parte, se puede evitar una multiplicación del software, que es necesario para el funcionamiento del aparato de control.

El sub-código se puede depositar en una zona del microordenador que se puede escribir de nuevo o en una zona que se puede escribir de nuevo de un módulo de memoria externo. De esta manera se puede actualizar o reprogramar el sub-código. Pero a través de la función de supervisión contenida en el código maestro contra manipulación en el sub-código se puede evitar una modificación no permitida del sub-código.

Además, el problema en que se basa la invención se soluciona por medio de un aparato de control para un componente de automóvil, que comprende, al menos, un microordenador (μC) y, al menos, un módulo de memoria, en el que el código necesario para el funcionamiento del aparato de control está dividido en al menos un código maestro, que comprende informaciones esenciales para la función del aparato de control y al menos un sub-código, que comprende otras informaciones para el funcionamiento del aparato de control, y al menos el código maestro está depositado en una zona del microordenador protegida contra lectura, que solamente se puede escribir una vez y el código maestro contiene un módulo de función del software para la detección de la manipulación dentro del sub-código.

El módulo de función del software puede comprender, por ejemplo, una formación lineal de sumas de control o CRC, una formación de valor Hash o un procedimiento de codificación.

Con preferencia, al menos una parte del sub-código está depositada codificada en una zona que se puede escribir de nuevo y el código maestro sirve para la generación de una clave para la decodificación. La parte del sub-código, que está depositada codificada, puede representar, por ejemplo, una huella dactilar.

Las características y detalles, que se describen con relación al procedimiento según la invención, se aplican de manera correspondiente para el aparato de control según la invención y a la inversa.

A continuación se describirá la invención con la ayuda de los dibujos adjuntos, que se refieren a posibles ejemplos de realización de la invención. En este caso:

La figura 1 muestra una representación esquemática en bloques de una forma de realización del aparato de control según la invención; y

La figura 2 muestra una representación esquemática en bloques de otra forma de realización del aparato de control según la invención.

En la figura 1 se representa una forma de realización de un aparato de control de acuerdo con la invención. La estructura de aparatos de control, como por ejemplo aparatos de control de motor, se conoce desde hace mucho tiempo a partir del estado de la técnica, de manera que solamente se describe aquí en la medida necesaria para la comprensión de la invención. El aparato de control 1 comprende, en la forma de realización representada, un microordenador μC, una memoria Flash 2 y una EEPROM (E^2PROM) 3. La memoria Flash 2 y la memoria (E^2PROM) 3 presenta, respectivamente, una zona OTP 21, 31. éstas están configuradas con preferencia no protegidas contra lectura. También está prevista una zona OTP 11 en el μC.

Los módulos de memoria Flash 2, E^2PROM 3 están provistos en la forma de realización representada con números de identificación ID específicos de los componentes. Éstos se describen, en general, en el fabricante del módulo y se depositan en las zonas OTP 21, 31 de los módulos individuales.

En el proceso de fabricación del aparato de control, durante la primera puesta en servicio del aparato de control, se leen por el microordenador μC las ID de los módulos de memoria 2, 3 individuales y se depositan en una zona OTP 11 del μC que se puede escribir una vez. A partir de este instante, la función del aparato de control 1 solamente es posible en combinación con las ID conocidas por el μC de los módulos de memoria externos 2, 3.

En cada puesta en servicio siguiente del aparato de control 1 se leen de nuevo por el μC las ID de todos los módulos de memoria 2, 3 conectados con éste. En una unidad de comparación se pueden comparar entonces estas ID actuales con las identificaciones originales, que están depositadas en la zona OTP 11 del μM. Si se comprueba en esta comparación que una de las ID no coincide con una de las ID originales, entonces se impide la función del aparato de control o se diagnostica al menos la modificación y, dado el caso, se representa.

El código para el funcionamiento del aparato de control está dividido en un código maestro (MC) y un sub-código (SC). El código maestro MC contiene funcionalidades elementales, esenciales para el funcionamiento del aparato de control, por ejemplo el programa para la generación de señales para actuadores conectados (no representados) del aparato de control o el programa para el cálculo de las variables de ajuste y valores de ajuste. El código maestro MC puede comprender, además, datos. En el sub-código SC están contenidos otros programas y datos. El aparato de control solamente es capaz de funcionar utilizando ambos códigos MC y SC. En la forma de realización representada, el sub-código SC está contenido en una zona de la memoria Flash 2 que se puede escribir de nuevo. El código maestro MC está contenido en una zona OTP 11 del microordenador μC. El código maestro está protegido con preferencia contra lectura a través de contacto. Esto se puede conseguir, por ejemplo, físicamente a través de una aleación de un

tramo de transistor o según la técnica de circuitos. El sub-código SC se puede modificar o sobrescribir, en oposición al código maestro MC. Esto permite una actualización del sub-código o una reprogramación.

El μC presenta, además, un número de identificación μC-ID. También éste está depositado en una zona OTP del μC protegida contra lectura. En la E^2PROM están depositados otros datos para el funcionamiento del aparato de control en una zona que se puede escribir de nuevo. Estos datos pueden ser, por ejemplo, valores de adaptación así como números de revoluciones de marcha en ralentí en un aparato de control del motor.

Durante la inicialización del aparato de control, el microordenador μC aprende los números de identificación depositados en la zona OTP 21, 31 de los módulos de memoria 2, 3 y, por lo tanto, no variables y los deposita en una zona OTP del microordenador μC, que puede estar configurada opcionalmente también protegida contra lectura.

Desde este instante, el microordenador μC conoce los módulos de memoria 2, 3 conectados con éste a través de su ID.

Adicionalmente, las ID de los módulos de memoria depositadas en el microordenador pueden servir también para la codificación de datos o programas. Así, por ejemplo, los datos depositados en la E^2PROM pueden ser codificados a través de un procedimiento de codificación simétrica, en el que la clave comprende al menos una parte de la ID de al menos uno de los módulos de memoria 2, 3. En un aparato de control de motor, en la E^2PROM pueden estar registrados, por ejemplo, valores de aprendizaje, datos de fabricación y valores de adaptación. Para la codificación son adecuados, en principio, todos los procedimientos de codificación simétrica, que permiten la incorporación de una identificación específica del aparato de control. Con preferencia, los datos de la E^2PROM son codificados por medio de una clave, que comprende, adicional o alternativamente a la ID de los módulos de memoria externos, la ID del microordenador μC. De esta manera se consigue una codificación específica de los aparatos de control, que hace imposible una sustitución de la E^2PROM o una sobrescritura de los datos memorizados en ella o bien impide el funcionamiento del aparato de control después de tal manipulación. La clave es depositada con preferencia en la memoria RAM del microordenador μC. De esta manera se forma la clave con cada aceleración del aparato de control incorporando una identificación específica de los aparatos de control (por ejemplo, la ID del μC y, dado el caso, las ID de los módulos de memoria) y, por lo tanto, es específica de los aparatos de control.

Además, el sub-código SC puede estar depositado total o parcialmente codificado en la memoria Flash 2. También para esta codificación se puede integrar la ID de los módulos de memoria individuales o del microordenador o bien una parte de esta ID en la clave. La decodificación de los datos en el sub-código se realiza a través del código maestro. Puesto que éste está depositado en una zona del microordenador protegida contra lectura, se puede impedir una lectura del programa y, por lo tanto, una reproducción del software.

La supervisión del sub-código frente a manipulación, que se asegura a través del μC en el código maestro, se puede realizar también a través de otros procedimientos distintos a la codificación. Así, por ejemplo, se puede utilizar adicional o alternativamente la formación lineal de sumas de control o CRC o formación de valor Hash. Para el reconocimiento de una manipulación realizada de los datos y, dado el caso, de partes del sub-código se forman sumas de control lineales, por ejemplo a través de zonas seleccionadas y se incorpora el resultado codificado como huella dactilar en el sub-código. El código maestro calcula en el funcionamiento de los aparatos de control, por ejemplo, en una señal en el terminal 15 a través de la misma zona definida anteriormente, el valor comparativo (por ejemplo, suma de control lineal) y lo verifica frente a un valor de referencia decodificado, depositado codificado en el sub-código. Se puede seleccionar opcionalmente el tipo de reconocimiento de la manipulación.

Después del reconocimiento de una manipulación se introducen medidas por el código maestro, que conducen, dado el caso, al fallo de los aparatos de control.

En la figura 2 se muestra otra forma de realización del aparato de control de acuerdo con la invención. En esta forma de realización, los módulos de memoria 2 y 3 están integrados en el microordenador μC. El μC presenta en este caso una memoria Flash incrustada, de manera que se emula la E^2PROM. Esta configuración del aparato de control presenta, en efecto, la ventaja de que se puede impedir de forma fiable una sustitución de los módulos de memoria, pero los datos en la emulación de la E^2PROM solamente se pueden sobrescribir en bloques.

El procedimiento para la protección contra manipulación se realiza en este aparato de control con memoria interna esencialmente como se ha descrito anteriormente para aparatos de control con memorias externas. También aquí se pueden depositar codificados especialmente los datos de la E^2PROM emulada y se pueden decodificar por medio de una clave, que comprende una identificación individual del aparato de control, como la μC-ID y/o la Flash-ID. De la misma manera, de pueden decodificar los datos o huellas dactilares codificadas contenidas en el sub-código, que está depositado en la memoria Flash del μC, por medio del código maestro. También aquí se integra en la clave con preferencia una identificación específica de los aparatos de control.

La invención no está limitada a las formas de realización representadas. Así, por ejemplo, como identificación de los módulos individuales de la memoria se puede contemplar, por ejemplo, la fecha de fabricación del aparato de control. De esta manera se puede impedir una manipulación durante el tiempo de garantía.

El aparato de control puede representar en el sentido de esta invención, por ejemplo, un aparato de control del motor, un aparato de control de la caja de cambios o también un instrumento combinado.

Con un procedimiento de acuerdo con la invención y el aparato de control de acuerdo con la invención se pueden conseguir, frente a los aparatos de control convencionales, un gran número de ventajas.

Con el aparato de control de acuerdo con la invención se puede impedir de manera fiable una sustitución de alguno o varios módulos, puesto que a través de una sustitución de este tipo se puede impedir la función del aparato de control. No es posible la lectura de una parte del programa o bien de los datos, que son forzosamente necesarios para la función del control, cuando esta parte está depositada en la zona OTP protegida contra lectura. De esta manera se puede impedir una reproducción o bien una modificación del software. Tampoco es posible el acceso a datos confidenciales a través del contacto del módulo, cuando éstos están depositados en la zona OTP protegida contra lectura del μC. De manera especialmente segura se puede proteger el aparato de control contra manipulación porque solamente se puede ejecutar en la combinación de código maestro y sub-código. Una modificación del sub-código depositado en la memoria reprogramable, dado el caso externa, por ejemplo Flash conduce, sin una adaptación del código maestro, a un fallo de los aparatos de control. Además, los datos que están depositados, por ejemplo, en una E^2PROM, se pueden codificar de manera específica de los aparatos de control. También la decodificación de tales datos se puede realizar en función de una identificación del aparato de control. Se puede crear seguridad adicional porque la codificación y decodificación se realiza en función de la combinación de los módulos individuales con las ID conocidas por el μC.

Por lo tanto, en resumen, se puede establecer que a través de la división del código en un código maestro y un sub-código se puede evitar de manera fiable la manipulación de aparatos de control, como por ejemplo la sintonización del chip en aparatos de control del motor.

REIVINDICACIONES

1. Procedimiento para la protección contra manipulaciones en un aparato de control para al menos un componente de automóvil, que comprende, al menos, un microordenador (μC) y al menos un módulo de memoria (2, 3), en el que el código necesario para el funcionamiento del aparato de control (1) se divide en, al menos, un código maestro (MC), que comprende informaciones esenciales para la función del aparato de control (1) y, al menos un sub-código (SC), que comprende otras informaciones para el funcionamiento del aparato de control (1), en el que al menos el código maestro (1) es depositado en una zona (11) del microordenador (μC), que solamente se puede escribir una vez y el código maestro (MC) supervisa la manipulación del sub-código (SC), **caracterizado** porque la zona (11) del microordenador (μC) que solamente se puede escribir una vez está configurada protegida contra lectura.

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado** porque el sub-código (SC) es depositado en una zona del microordenador que se puede escribir de nuevo.

3. Procedimiento de acuerdo con la reivindicación 1, **caracterizado** porque el sub-código (SC) es depositado en una zona que se puede escribir de nuevo de al menos un módulo de memoria externo (2).

4. Aparato de control para un componente de automóvil, que comprende, al menos, un microordenador (μC) y, al menos, un módulo de memoria (2, 3), en el que el código necesario para el funcionamiento del aparato de control (1) está dividido en al menos un código maestro (MC), que comprende informaciones esenciales para la función del aparato de control (1) y al menos un sub-código (SC), que comprende otras informaciones para el funcionamiento del aparato de control (1), y al menos el código maestro (MC) está depositado en una zona (11) del microordenador (μC) protegida contra lectura, que solamente se puede escribir una vez y el código maestro (MC) contiene un módulo de función del software para la detección de la manipulación dentro del sub-código (SC).

5. Aparato de control de acuerdo con la reivindicación 4, **caracterizado** porque el sub-código (SC) está depositado en una zona del microordenador (μC) que se puede escribir de nuevo.

6. Aparato de control de acuerdo con la reivindicación 4, **caracterizado** porque el sub-código (SC) está depositado en una zona que se puede escribir de nuevo de al menos un módulo de memoria externo (2, 3).

7. Aparato de control de acuerdo con una de las reivindicaciones 4 a 6, **caracterizado** porque al menos una parte del sub-código (SC) está depositada codificada en una zona que se puede escribir de nuevo y el código maestro (MC) sirve para la generación de una clave para la decodificación.

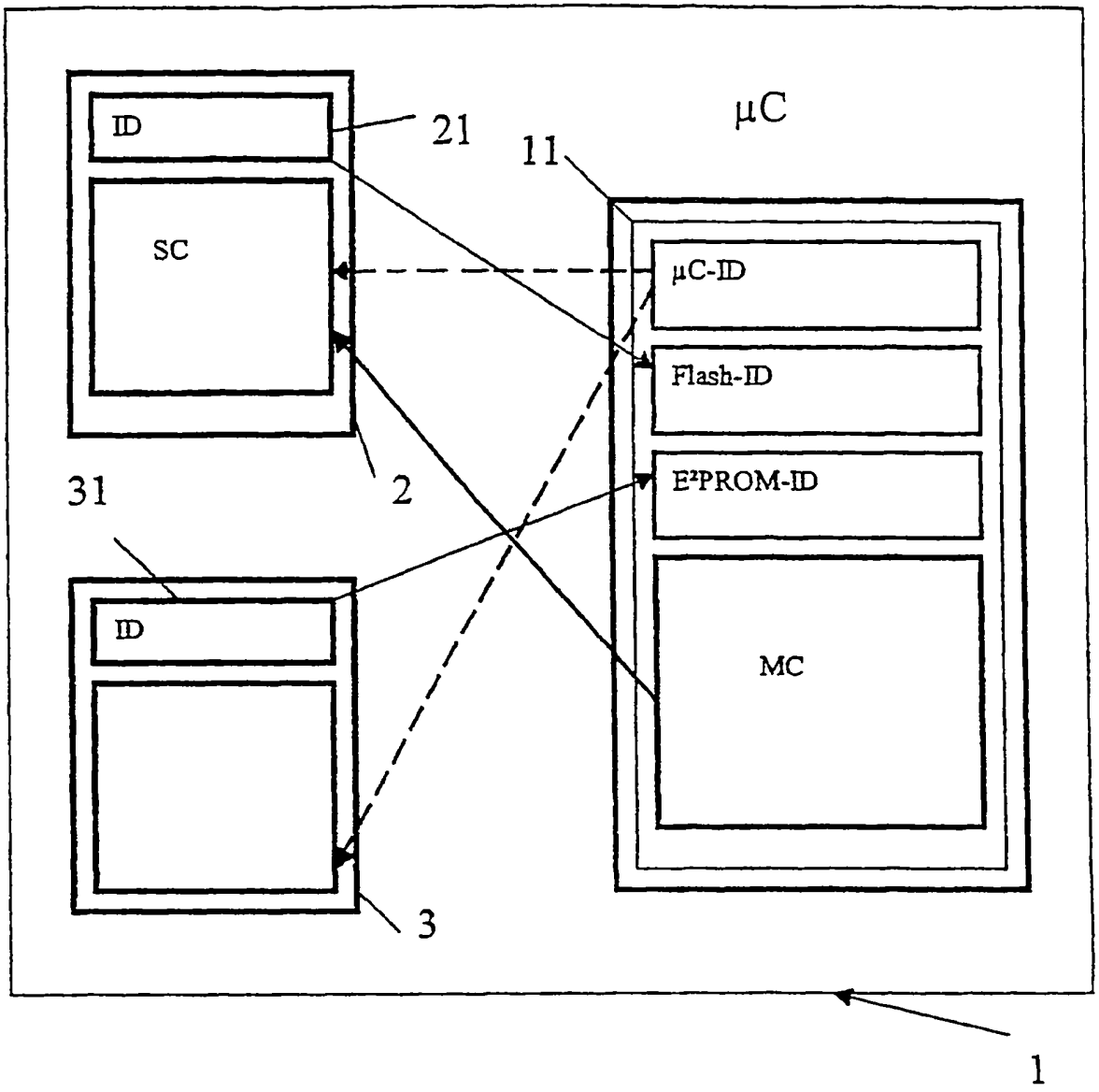

FIG. 1

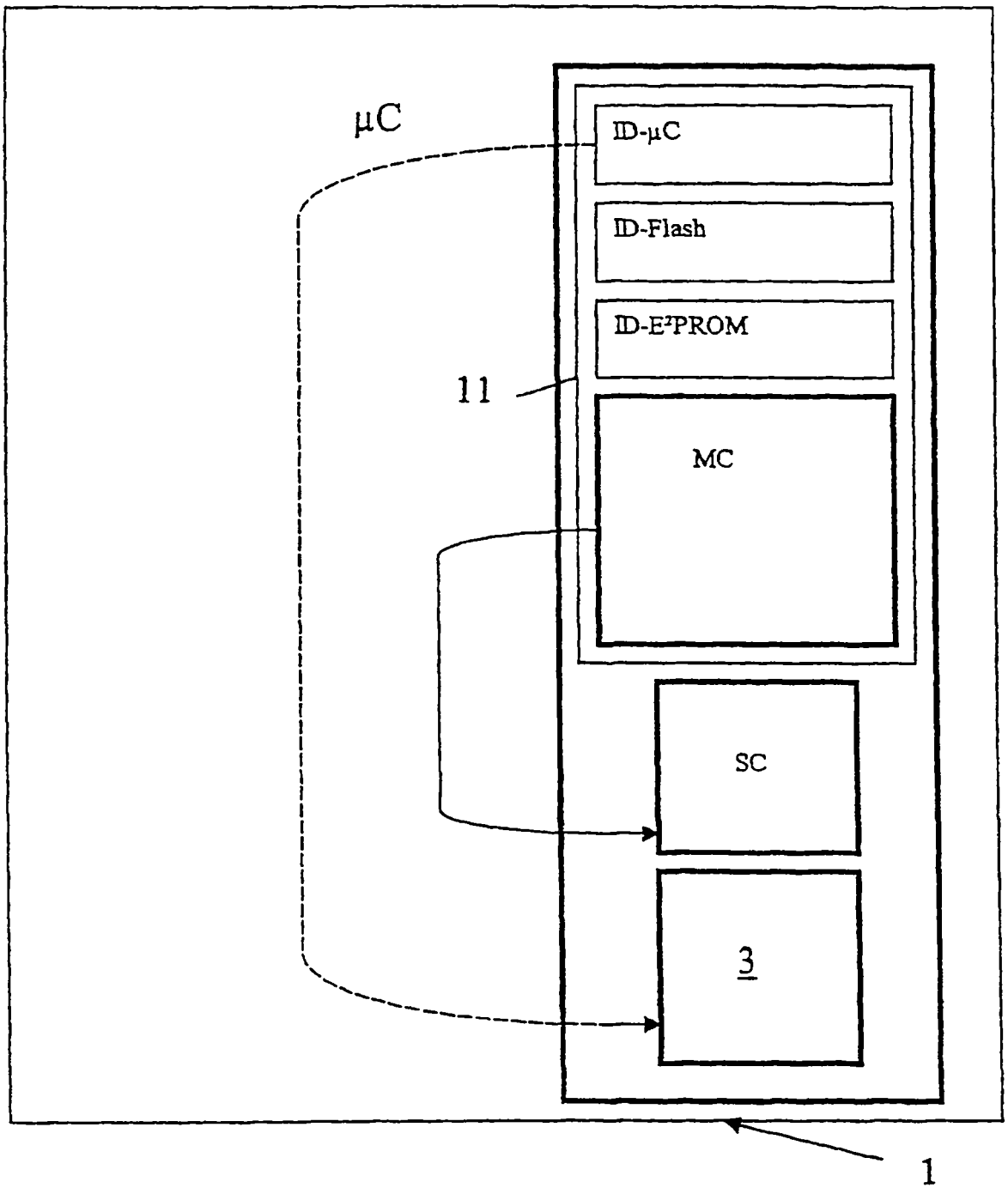

FIG. 2