



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 313 944**

51 Int. Cl.:

G11C 5/00 (2006.01)

G11C 16/10 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **01904042 .7**

96 Fecha de presentación : **02.02.2001**

97 Número de publicación de la solicitud: **1258004**

97 Fecha de publicación de la solicitud: **20.11.2002**

54 Título: **Escritura en tiempo real asegurada para memoria no volátil.**

30 Prioridad: **11.02.2000 FR 00 01869**

45 Fecha de publicación de la mención BOPI:
16.03.2009

45 Fecha de la publicación del folleto de la patente:
16.03.2009

73 Titular/es: **Gemalto S.A.**
6, rue de la Verrerie
92190 Meudon, FR

72 Inventor/es: **Bringer, Laurence y**
Guterman, Pascal

74 Agente: **Cañadell Isern, Roberto**

ES 2 313 944 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

Escritura en tiempo real asegurada para memoria no volátil.

5 La presente invención concierne potencialmente cualquier tarjeta inteligente, o cualquier objeto electrónico portátil equivalente, que posea una memoria no volátil, por ejemplo, una memoria que pueda programarse y borrarse eléctricamente EEPROM o una memoria FLASH.

10 Las tarjetas inteligentes (smart card), llamadas también tarjetas de circuito integrado o tarjetas de microcontrolador, como la mayoría de los objetos electrónicos portátiles equivalentes, tales como calculadoras, organizadores, monederos electrónicos, juegos electrónicos, terminales radiotelefónicos, mandos a distancia; etc., almacenan distintos tipos de información en memoria no volátil.

15 No obstante, este almacenamiento de datos está sujeto, principalmente, en las aplicaciones a base de tarjeta inteligente, a distintas tensiones, como por ejemplo el tiempo de escritura y la seguridad.

El tiempo de escritura depende del tipo de la memoria. Es relativamente largo cuando la capa de aplicación en la tarjeta se somete a grandes dificultades temporales como, por ejemplo, durante las transacciones bancarias, o en tarjetas inteligentes sin contacto, etc.

20 En muchos casos, se considera que los datos confiados a la memoria no volátil son sensibles por la capa de aplicación. Por tanto, es importante que el proceso de escritura de estos datos se realice en condiciones seguras. Cualquier problema que se constatare durante la escritura de estos datos, como por ejemplo un fracaso de escritura, un fallo o una indisponibilidad de funcionamiento de la memoria, deberá señalarse, principalmente, en la capa de aplicación que tomará las medidas necesarias, tales como la anulación de la transacción; anulación de la tarjeta, etc.

Para realizar esta función de escritura, el sistema de explotación de la tarjeta inteligente proporciona un cierto número de servicios, que constituyen puntos de entrada informáticos, dedicados a la gestión de la memoria, los cuales llamamos a continuación "driver".

30 A continuación, la palabra "aplicación" designa el conjunto del programa informático que realiza las funcionalidades aplicativas soportadas por la tarjeta a nivel de su capa de aplicación. El driver agrupa subprogramas, principalmente, de escritura y lectura de datos contenidos en una capa de driver.

35 La figura 1 es un diagrama temporal que muestra, de izquierda a derecha, el desarrollo clásico de un proceso de escritura en una tarjeta inteligente, que fue solicitado por la aplicación y realizado por el driver. El proceso de escritura se divide generalmente en tres etapas:

40 - una etapa de inicialización IN el controlador que se ocupa de las funcionalidades de comando en escritura y en lectura de la memoria, como respuesta a una petición de escritura RE de la aplicación;

- una etapa de escritura EC para escribir un dato contenido en la petición RE, cuya duración depende de los resultados técnicos del controlador de memoria;

45 - una etapa de comprobación VE para verificar la exactitud del dato escrito en la memoria; la comprobación consiste en leer en la memoria el dato escrito en la etapa EC y en comparar el dato leído con el dato inicial contenido en la petición RE.

Seguidamente, el control del proceso de escritura lo comunica el driver a la aplicación transmitiéndole una respuesta de final RF después de que se haya terminado la última etapa de comprobación VE. Sabiendo que a menudo el conjunto del proceso de escritura es relativamente largo dependiendo de la tecnología utilizada para la fabricación de la memoria, los resultados de la aplicación resultan por tanto penalizados. La aplicación se suspende entonces hasta el final del proceso de escritura, tal y como se indica en SA entre dos tareas de aplicación sucesivas TA1 y TA2 en la figura 1. El documento US-A-5663910 muestra un proceso de escritura clásico.

55 En el ámbito de la informática tradicional, la escritura de datos "en tiempo real" es una solución clásica que permite la ejecución de la escritura "en tiempo enmascarado" de los datos, es decir, sin bloquear el desarrollo de la aplicación. Esta solución se aplica más especialmente a los medios de almacenamiento de tipo disquete o disco duro.

60 En cambio, la escritura "en tiempo enmascarado" de los datos resulta mucho más difícil de aplicar en el marco de un sistema de explotación dedicado a una tarjeta inteligente. Por lo general, el sistema de explotación debe adaptarse a entornos materiales pobres, en particular, en términos de memoria de tipo RAM. Por esta razón, resulta imposible generalmente conservar en memoria el dato que debe escribirse con vistas a la verificación final.

65 La invención pone la mira en adaptar a una tarjeta inteligente o a un objeto electrónico portátil equivalente el concepto "de escritura tiempo real", sin pérdida de resultado en lo que se refiere a la seguridad del programa informático.

ES 2 313 944 T3

Con este fin, un procedimiento para escribir datos iniciales contenidos en una petición de escritura transmitida por un medio de tratamiento de datos a otro medio de control de escritura-lectura de una memoria no volátil en un objeto electrónico portátil de tipo tarjeta inteligente, se caracteriza por incluir las siguientes etapas:

- 5 - transmitir sólo un acuse de recibo por el medio de control a través del tratamiento de datos inmediatamente en respuesta a la petición de escritura si el medio de control está disponible para una escritura de datos iniciales en la memoria,
- 10 - realizar tareas en el medio de tratamiento de datos en respuesta al acuse de recibo simultáneamente a la escritura de los datos iniciales en datos escritos en la memoria,
- 15 - poner en espera hasta el final de la escritura el medio de tratamiento de datos si éste transmite otra petición de escritura antes del final de la escritura, y
- 15 - aceptar sólo otra petición de escritura después del final de la escritura de los datos iniciales en la memoria por el medio de control.

De este modo, las tareas relativas por lo menos a una aplicación en el medio de tratamiento de datos, como por ejemplo el procesador en el objeto electrónico portátil, se realizan en paralelo a la escritura de los datos iniciales en la memoria. No obstante, cualquier otra petición de escritura transmitida al driver en el medio de control sólo se realizará cuando la escritura de los datos iniciales llegue a su término. Esto significa que el acceso a los servicios del driver se realiza a través de un semáforo que controlará los accesos al proceso de escritura en el driver y que es capaz de administrar conflictos entre peticiones de escritura y retrasar la fecha de las peticiones de escritura posteriores mientras que el driver no haya sido reconocido como disponible.

25 La liberación del driver se señala a la aplicación desarrollada a través del tratamiento de datos por un medio de detección de final de escritura proporcionado en el objeto electrónico portátil para contar hacia atrás una duración predeterminada prácticamente en cuanto se transmite el acuse de recibo y señalar el final de la escritura cuando expire el plazo predeterminado. Según otra realización, la etapa de aceptar otra petición de escritura acompaña la desactivación de un medio de aumento de tensión interno a la memoria.

30 El medio de control según la invención también es capaz, de acuerdo con las dificultades de seguridad, de ejercer un control de integridad de los datos que deben escribirse, es decir, una comprobación de la integridad de los datos iniciales en comparación con los datos escritos que se producen entre la escritura de los datos iniciales y una lectura posterior de los datos escritos bajo el comando del medio de tratamiento de datos. La comprobación se produce ya sea justo o inmediatamente después de la escritura de los datos iniciales, en particular, antes de la etapa de aceptar otra petición de escritura, o bien después del final de la escritura, especialmente justo antes de la lectura posterior de los datos escritos.

40 La invención no efectúa la comprobación de integridad de los datos iniciales por simple lectura de los datos escritos y comparándolos luego con los datos iniciales cuando los recursos en memoria del objeto electrónico portátil, como tarjeta inteligente, son relativamente limitados y no permiten almacenar temporalmente el conjunto de los datos iniciales en el momento de su escritura en memoria. La comprobación de integridad según la invención puede entonces comprender una comparación de una firma de los datos iniciales con una firma de los datos escritos leídos. Cada firma puede deducirse de una codificación con redundancia cíclica de los datos correspondientes, o resultar de un picado de los datos relativos. De este modo, la ocupación memoria se reduce a una firma de datos obviamente más corta que los propios datos.

50 Sabido que la comprobación de integridad puede resultar costosa en tiempo para el medio de tratamiento de datos, la comprobación se opera "en diferido", en forma de una tarea de prioridad mínima, para no interferir con procesos sensibles, por ejemplo la gestión de un protocolo de comunicación en la capa de aplicación.

55 Cuando se produce un fallo de integridad de los datos escritos en comparación con los datos iniciales, puede activarse un medio de seguridad, como por ejemplo un gestor informático de seguridad, para impedir el uso normal del objeto electrónico portátil. De este modo, la ejecución de la comprobación no perturba las tareas en proceso en la aplicación, a veces sin interrupción, como los procesos vinculados a los protocolos de comunicación por ejemplo.

60 Para garantizar esta propiedad, la arquitectura informática del sistema de explotación en el medio de tratamiento de datos se adapta a esta dificultad utilizando un verdadero núcleo instantáneo simplificado capaz de arbitrar las prioridades asignadas a cada una de las tareas.

65 Otras características y ventajas de la presente invención se pondrán más de manifiesto cuando se lea la siguiente descripción de varias realizaciones preferidas de la invención en referencia a los dibujos anexos correspondientes en los que:

- la figura 1 es un diagrama temporal de un proceso de escritura en una memoria según la técnica anterior, ya comentada;

ES 2 313 944 T3

- la figura 2 es un bloque-diagrama esquemático de la arquitectura material de una tarjeta inteligente;

- la figura 3 es un diagrama temporal de un proceso de escritura en una memoria según la invención;

5 - la figura 4 es un algoritmo de un proceso de escritura según una primera realización de la invención; y

- la figura 5 es un algoritmo de proceso de escritura y lectura de datos según una segunda realización de la invención.

10

En referencia a la figura 2, un microcontrolador que constituye el “chip” de una tarjeta inteligente CP, o de cualquier objeto electrónico portátil equivalente, como por ejemplo un módulo de microprocesador denominado tarjeta inteligente SIM (Subscriber Identity Mobile) que se inserta en un terminal radiotelefónico, contiene principalmente de manera esquemática una unidad de tratamiento central CPU formada por un microprocesador PR, una memoria MO de tipo ROM que incluye un sistema de explotación OS de la tarjeta eventualmente completado por un navegador (browser) y algoritmos de aplicación de comunicación y autenticación específica, una memoria no volátil MNV de tipo EEPROM que con- tiene, en particular, los datos vinculados al dueño de la tarjeta, así como un número de identificación personal y un repertorio de nombres, y una memoria MA de tipo RAM destinada esencialmente al tratamiento de datos que deben recibirse de una estación de recepción de la tarjeta, tal como un terminal radiotelefónico o bancario que se transmitirá hacia la estación de recepción. Todos los componentes PR, MO MNV y MA están conectados entre sí por un bus interno BU.

25

Al tratarse de la invención, la tarjeta inteligente incluye, además, un controlador CM que pilota la memoria no volátil MNV para establecer comandos, como por ejemplo, la escritura, lectura y borrado de datos en la memoria, y para dirigir casillas de la memoria. El controlador de memoria CM obra recíprocamente con el procesador PR a medida del desarrollo de una aplicación por el intercambio de peticiones y respuestas a través del bus BU. En particular, el controlador CM contiene o está asociado al menos parcialmente a un driver DR, que pilota por lo menos el proceso de escritura y el proceso de lectura en la memoria MNV, a un verificador de firma VS y a un detector de final de escritura DFE. Los elementos DR, VS y CM se realizan en forma material y/o informática; si por lo menos un elemento está en

30

En la figura 3, observamos un diagrama temporal, comparable al de la técnica anterior de la figura 1, dónde una aplicación AP basada en el sistema de explotación OS se desarrolla con tareas sucesivas T1, T2 y T3, de izquierda a derecha. Se supone que la aplicación AP establece, hacia el final de la primera tarea T1, una petición de escritura RE1 que se transmite seguidamente al driver DR. La aplicación se desarrolla simultáneamente al proceso de escritura en el driver, el cual no interrumpe la aplicación como en la figura 1 y, de este modo, no bloquea el desarrollo de las siguientes tareas T2, T3 que suceden a la tarea T1 en la aplicación.

35

La figura 4 indica las etapas principales E1 a E7 que se encuentran a raíz de una petición de escritura RE establecida por la aplicación AP según una primera realización de la invención.

40

En la primera etapa E1, el driver inicia un proceso de escritura relativo a datos iniciales DI contenidos en la petición RE, SI el driver DR no tiene ninguna tarea de escritura, tal y como se indica en RE1 en la figura 3; como dijimos anteriormente, la aplicación AP continúa desarrollándose en paralelo al proceso de escritura. El driver confirma el lanzamiento inminente de la escritura en la siguiente etapa E2, transmitiendo un acuse de recibo AC a la aplicación.

45

En cambio, tal y como se indica en la etapa E3, si la petición de escritura RE se produce en curso del proceso de escritura, como la petición RE2 hacia la mitad de la tarea T2, o como la petición RE3 hacia el principio de la tarea T3 (figura 3), la aplicación AP se interrumpe hasta el final del proceso de escritura en curso, indicada por una señal de final de escritura FE del detector DFE; la petición RE1 o RE2 se pone en espera y se inscribe en una fila de espera del driver que se leerá en cuanto se termine el proceso de escritura en curso.

50

De este modo, si a las etapas del proceso que suceden a las etapas de inicialización E1 y E2, la tarea siguiente T2 no requiere ninguna escritura, ésta se realizará sin interrupción y sin ser diferida, al igual que la técnica anterior. Por ejemplo, una tarea T2 en la aplicación AP que consiste en enviar una respuesta hacia una estación de recepción de la tarjeta inteligente o en recibir una petición desde la estación de recepción no será perturbada por el proceso de escritura en curso.

55

En la etapa E2, simultáneamente al establecimiento de la respuesta AC, el detector de final de escritura DFE está activo cuando, según una primera variante, el detector de final de escritura DFE no está incluido directamente en el controlador CM de la memoria MNV y se encuentra en forma de un contador de cuenta hacia atrás (timer) de una duración predeterminada DP, es decir, un contador hacia atrás de impulso de reloj. Programado previamente a una duración predeterminada especificada de la escritura memoria, el detector de final de escritura DFE está activado con el controlador CM por el procesador PR a raíz de la petición RE1.

60

Según una segunda variante, el detector de final de escritura está implementado en el controlador MC de la memoria no volátil MNV embarcada en el microcircuito. En este ejemplo, la parada del proceso de escritura caracterizado por la reinicialización de registros y la desactivación de una “bomba de carga” aumenta la tensión de alimentación de la

65

tarjeta para pasar a una tensión más elevada de programación interna de una memoria reprogramable de tipo EEPROM, necesaria, en particular, para la escritura, es automática.

Después de la etapa E4 que sucede a la etapa E2, el driver DR escribe los datos iniciales DI contenidos en la petición RE1 en la casilla designada de la memoria MNV. El driver comprueba a continuación los datos escritos en la etapa E5, la cual es esencial desde un punto de vista de seguridad. En el transcurso de la etapa E5, el driver DR lee los datos escritos DE y el verificador VS los compara con los datos DI inicialmente contenidos en la petición RE1, antes de la etapa de escritura propiamente dicha E4. La comparación en el verificador VS es, en realidad, la comparación de una firma S(DI) de los datos iniciales antes de la escritura establecida por el driver y de una firma S(DE) de los datos leídos después de la escritura. Las firmas S(DI) y S(DE) se calculan según un mismo algoritmo de comprobación; la firma S(DI) de los datos iniciales en la petición RE1 se calcula inmediatamente en espera del cálculo de la firma S(DE) de los datos escritos correspondientes, y seguidamente se leen en la memoria. Estas firmas tienen ventajosamente una longitud obviamente inferior a la de los datos.

Por ejemplo, cada una de las firmas S(DI) y S(DE) se deduce de una codificación de redundancia cíclica CRC (Cyclic Redundancy Check) realizada muy rápidamente por el verificador VS sin intervención del procesador PR.

Según otro ejemplo, cada una de las firmas S(DI) y S(DE) resulta de un picado de datos correspondientes, es decir, resulta de una toma de partes predeterminadas de los datos correspondientes, y las firmas que resultan de los datos iniciales picados y los datos escritos y seguidamente leídos y picados se comparan.

El verificador VS puede implantarse en lógica cableada, tal y como se muestra en la figura 2, o aplicado en forma de programa informático en la memoria ROM MO.

Si la prueba de comprobación revela un defecto de integridad de datos escritos DE en comparación con los datos iniciales DI de la etapa E5, se activa un medio de seguridad, por ejemplo un gestor de seguridad aplicado en la memoria MO de la tarjeta inteligente, como se indica en la etapa E6, con el fin de realizar una tarea de ayuda.

La tarea de ayuda consiste, por ejemplo, en prohibir toda comunicación entre la tarjeta inteligente CP y la estación de recepción de tarjeta, en la cual se introdujo la tarjeta y hacer que la tarjeta no sea válida de este modo, u ordenar la nueva escritura de los datos iniciales por ejemplo interrumpiendo la aplicación AP, o transferir el proceso de escritura de datos iniciales al driver hacia otra memoria de la tarjeta.

El final del proceso de escritura con comprobación lo constata en la etapa E7 el detector de final de escritura DFE que lo señala al controlador CM después del final del proceso de escritura anterior. El controlador se encuentra entonces en estado de aceptar otra petición de escritura, eventualmente ya en espera como la petición RE2 que se muestra en la figura 3.

Como variante, el controlador CM genera una señal de final de escritura FE en forma de una interrupción transmitida a la aplicación AP. Cuando el detector DFE es el contador hacia atrás de la duración citada anteriormente, su paso a cero, que corresponde a la expiración de la duración predeterminada DP, es indicado por la señal FE al procesador de PR que detiene el controlador CM. Cuando el detector DFE está implementado directamente en el controlador CM, éste genera automáticamente la señal FE para transmitirla al procesador PR después de un retraso predeterminado que sucede a la desactivación de la "bomba de carga" necesario para la escritura, dicho retraso está disponible para la comprobación.

Según otra realización, la etapa de comprobación E5 con la etapa de seguridad E6 no está incluida en el proceso de escritura entre las etapas E4 y E7, sino al principio del proceso de lectura posterior de los datos escritos en la memoria MNV por el procesador PR, como se demuestra en E10 en la figura 5. La etapa E10 sucede a una petición de lectura RL de la aplicación AP, aplicada por el procesador PR al driver DR a través del bus BU. La petición de lectura RL es validada por el driver DR en una etapa E8 para la lectura, de manera análoga a la etapa E1, o se pone en espera hasta el final de un proceso de lectura en curso en una etapa E9, cuando el driver DR trata una petición de escritura.

A continuación, después de la comprobación positiva en la etapa E10, el proceso de lectura se prosigue de una manera conocida en una etapa E11.

Referencias citadas en la descripción

Esta lista de referencias citadas por el solicitante tiene como objeto solamente ayudar al lector, y no forma parte del documento de patente europea. A pesar de que se ha tenido mucho cuidado en su concepción, no pueden excluirse errores u omisiones, por tanto la OEP rehúsa toda responsabilidad a este respecto.

Documentos patentes citados en la descripción

- US 5663910 A

REIVINDICACIONES

5 1. Procedimiento para escribir datos iniciales contenidos en una petición de escritura (RE1) transmitida por un medio de tratamiento de datos (PR, AP) a un medio de control de escritura-lectura (CM, DR) de una memoria no volátil (MNV) en un objeto electrónico portátil (CP), **caracterizado** por comprender las siguientes etapas:

10 - transmitir solamente (E1, E2) un acuse de recibo (AC) por el medio de control (CM, DR) al medio de tratamiento de datos (PR, AP) inmediatamente como respuesta a la petición de escritura (RE1) si el medio de control está disponible para una escritura (E4) de los datos iniciales (DI) en la memoria,

- realizar tareas (T2, T3) en el medio de tratamiento de datos en respuesta al acuse de recibo simultáneamente a la escritura (E4) de datos iniciales (DI) en datos escritos (DE) en la memoria,

15 - poner en espera (E3) hasta el final de la escritura el medio de tratamiento de datos (PR, AP) si este transmite otra petición de escritura (RE2) antes del final de la escritura, y

- aceptar solamente (E7) otra petición de escritura (RE2) después del final de la escritura de los datos iniciales en la memoria (MNV) por el medio de control.

20 2. Procedimiento conforme a la reivindicación 1, según el cual un medio de detección de final de escritura (DFE) se suministra en el objeto electrónico portátil (CP) para contar hacia atrás una duración predeterminada (DP) prácticamente en cuanto el acuse de recibo (AC) se transmite (E2) e indicar el final de la escritura (E7) cuando expire la duración predeterminada.

25 3. Procedimiento conforme a la reivindicación 1, según el cual la etapa de aceptar (E7) otra petición de escritura acompaña la desactivación de un medio de aumento de tensión interna en la memoria (MNV).

30 4. Procedimiento conforme a cualquiera de las reivindicaciones 1 a 3, que comprende una verificación (E5, E10) de la integridad de los datos iniciales (DI) en comparación con los datos escritos (DE) que tienen lugar entre la escritura de los datos iniciales (E4) y una lectura posterior (E11) de los datos escritos (DE).

5. Procedimiento conforme a la reivindicación 4, según el cual la comprobación (E5) se produce justo después de la escritura (E4) de los datos iniciales (DI).

35 6. Procedimiento conforme a la reivindicación 4, según el cual la comprobación (E10) se produce justo antes de la lectura posterior (E11) de los datos escritos (DE).

40 7. Procedimiento conforme a cualquiera de las reivindicaciones 4 a 6, según el cual la comprobación incluye una comparación de una firma (S(DI)) de los datos iniciales con una firma (S(DE)) de los datos escritos leídos en la memoria (MNV).

8. Procedimiento conforme a la reivindicación 7, según el cual se deduce cada firma de una codificación con redundancia cíclica de los datos correspondientes.

45 9. Procedimiento conforme a la reivindicación 7, según el cual cada firma resulta de un picado de los datos correspondientes.

50 10. Procedimiento conforme a cualquiera de las reivindicaciones 4 a 9, que incluye la activación de un medio de seguridad (E6) en respuesta a un defecto de integridad de los datos escritos (DE) en comparación con los datos iniciales (DI).

55 11. Objeto electrónico portátil (CP) que incluye un medio de tratamiento de datos (PR), una memoria no volátil (MNV) y un medio de control de escritura-lectura (CM) de la memoria no volátil (MNV), **caracterizado** porque el medio de control (CM) y el medio de tratamiento de datos (PR) están en condiciones de aplicar el procedimiento según cualquiera de las reivindicaciones 1 a 10.

60 12. Objeto electrónico portátil (CP) conforme a la reivindicación 11, **caracterizado** por ser de tipo tarjeta inteligente.

FIG.1

(Técnica anterior)

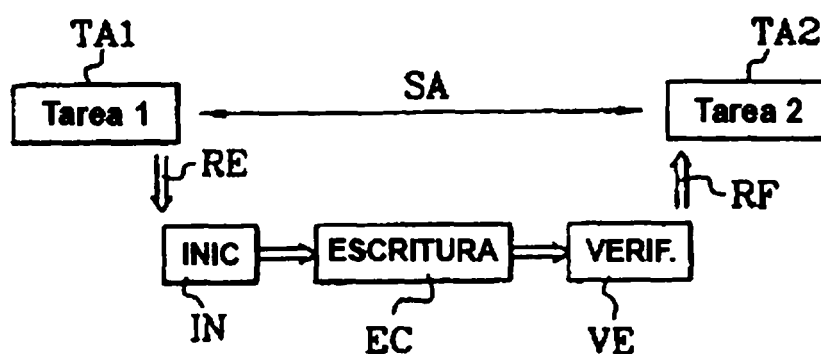


FIG.3

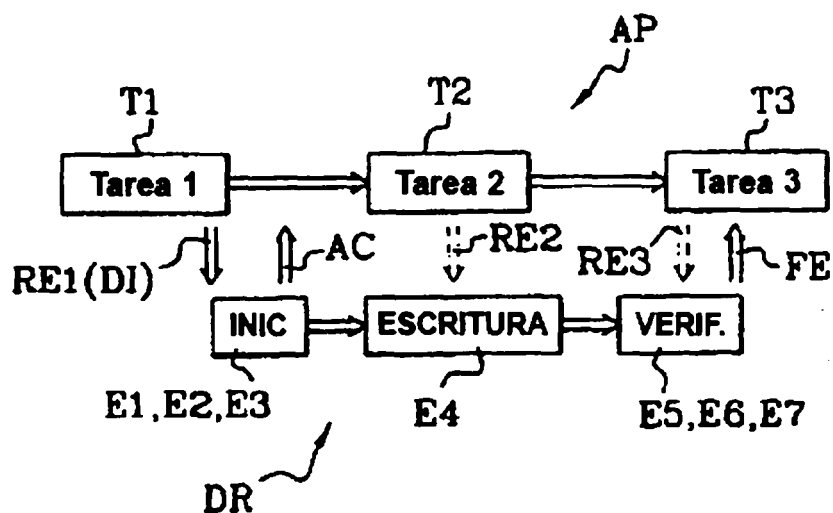


FIG.2

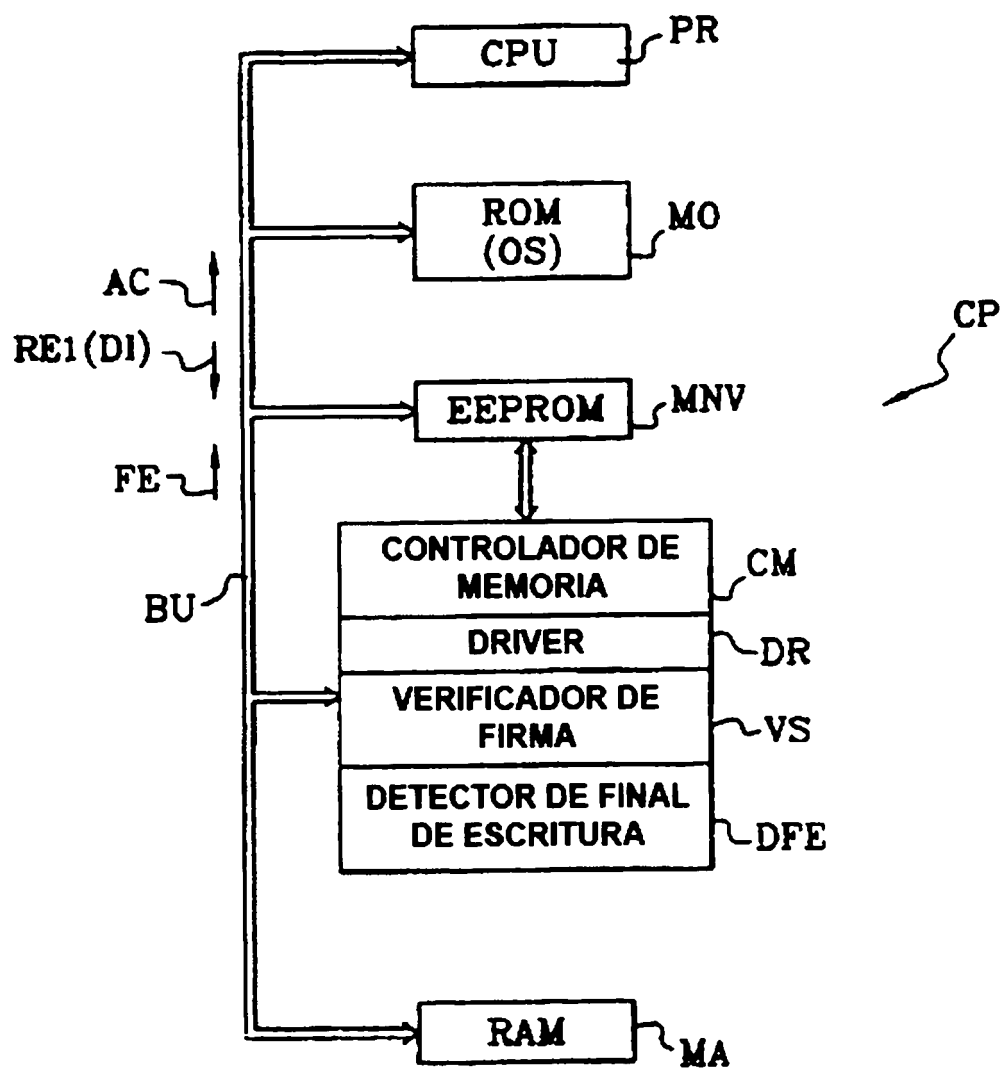


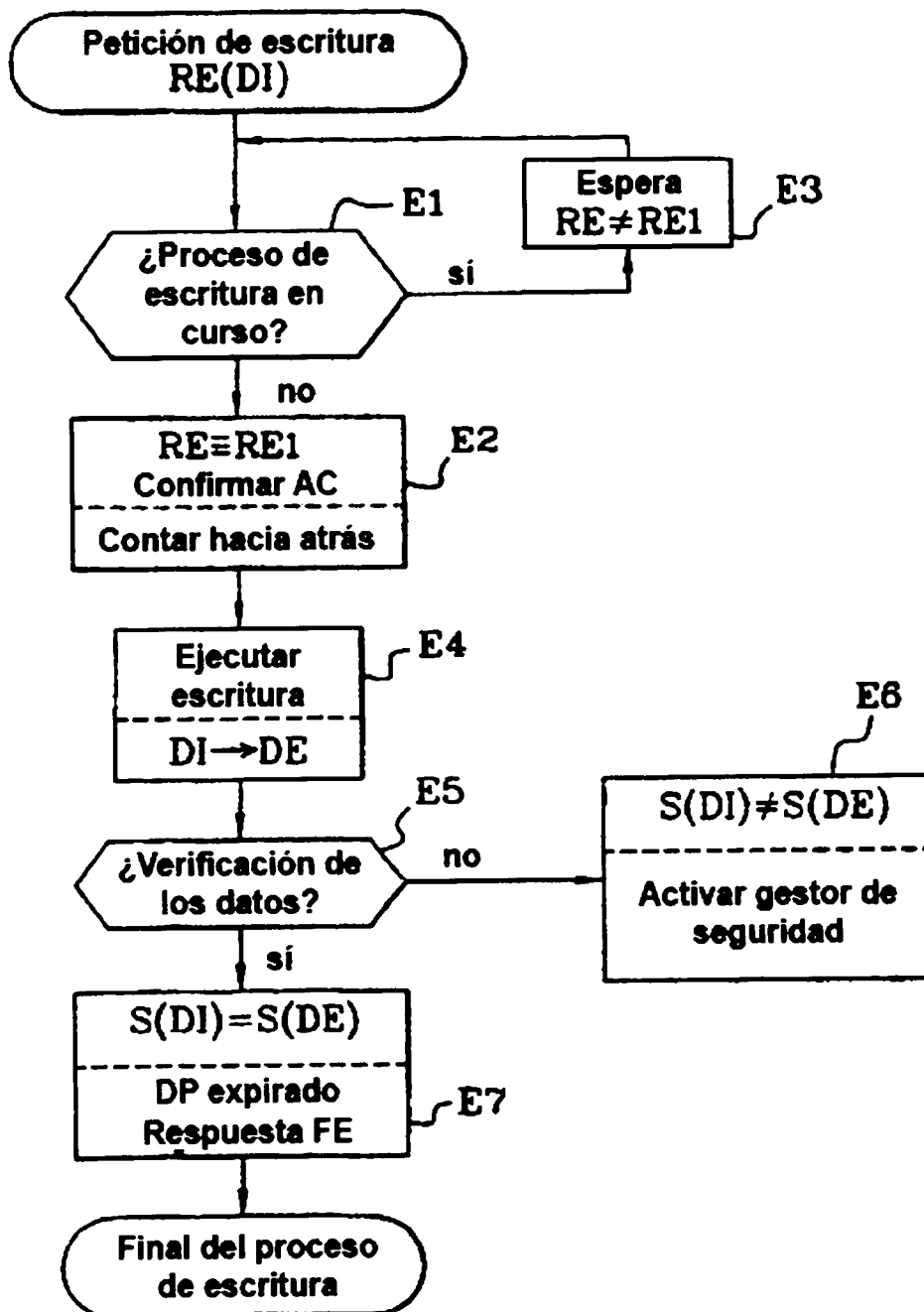
FIG.4

FIG.5