

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 388 217**

51 Int. Cl.:
G06F 12/14 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 96 Número de solicitud europea: **02781227 .0**
- 96 Fecha de presentación: **07.10.2002**
- 97 Número de publicación de la solicitud: **1435040**
- 97 Fecha de publicación de la solicitud: **07.07.2004**

54 Título: **Procedimiento para codificar información dentro de los archivos de directorio en una tarjeta inteligente de circuito integrado**

30 Prioridad:
09.10.2001 US 972155

45 Fecha de publicación de la mención BOPI:
10.10.2012

45 Fecha de la publicación del folleto de la patente:
10.10.2012

73 Titular/es:
**ACTIVCARD IRELAND LIMITED
30 HERBERT STREET
DUBLIN 2, IE**

72 Inventor/es:
**BOYER, John y
HILLHOUSE, Robert D.**

74 Agente/Representante:
Curell Aguilá, Mireia

ES 2 388 217 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

Procedimiento para codificar información dentro de los archivos de directorio en una tarjeta inteligente de circuito integrado.

5

Campo de la invención

La presente invención se refiere a un procedimiento perfeccionado de codificación de datos en una tarjeta de circuito integrado (CI) y, más particularmente, a un procedimiento perfeccionado de codificación de datos en los archivos de directorio contenidos en una tarjeta inteligente de circuito integrado (CI) compatible con la norma PKCS15, tal como el definido en el preámbulo de la reivindicación 1, y a una tarjeta inteligente, tal como la definida en el preámbulo de la reivindicación 8.

10

Antecedentes de la invención

15

La tecnología de tarjeta inteligente (SC) permite el almacenamiento de información segura dentro de una tarjeta de circuito integrado. La información segura se almacena en un formato que exige claves y certificados de software para propósitos de autenticación a fin de recuperar la información. Una norma de codificación, conocida como PKCS15, establece cómo se representan estas claves y certificados en términos de archivos y directorios de tarjeta inteligente. El formato controla de forma segura el acceso externo a los archivos y directorios de la tarjeta inteligente durante el proceso de codificación de la información o de lectura de información de la tarjeta inteligente.

20

El formato compatible con PKCS15 para una tarjeta inteligente se documenta en la publicación "PKCS #15 v1.1: Cryptographic Token Information Syntax Standard", RSA Laboratories, 21 de diciembre de 1999. Cada tarjeta inteligente debe contener un archivo de directorio de objetos (ODF). Este archivo contiene punteros a otros archivos de directorio; por ejemplo cuando se almacenan claves criptográficas algunos de los archivos presentes son los archivos de directorio de clave privada (PrKDF), archivos de directorio de claves públicas (PuKDF), archivos de directorio de claves secretas (SKDF), archivos de directorio de certificados (CDF) y archivos de directorio de objetos de datos (DODF).

25

30

El archivo de directorio de clave privada se considera un directorio de identificadores de clave privada conocidos por la aplicación PKCS 15, y habitualmente almacena una clave privada. La tarjeta inteligente que contiene claves privadas debe disponer de por lo menos un archivo PrKDF. En algunos casos, este archivo de directorio de clave privada contiene punteros de referencias cruzadas a objetos de autenticación utilizados para proteger el acceso a las claves residentes en cualquier lugar de la tarjeta. Si existen claves privadas correspondientes a las claves públicas también residentes en la tarjeta, las claves públicas se almacenan dentro de un archivo de directorio de claves públicas (PuKDF). Entonces, las claves públicas y las claves privadas comparten el mismo identificador en la tarjeta.

35

Las tarjetas inteligentes que contienen claves secretas deben disponer de por lo menos un archivo de directorio de claves secretas (SKDF). El SKDF contiene atributos de clave generales, tales como etiquetas e identificaciones. En algunos casos, el SKDF también contiene punteros de referencia cruzada a objetos de autenticación utilizados para proteger el acceso a las claves. El archivo de directorio de certificados (CDF) se considera como un directorio de certificados conocido por la aplicación PKCS15, y en cada tarjeta inteligente debería estar presente por lo menos un CDF. El CDF contiene certificados o referencias a certificados. El archivo de directorio de objetos de datos (DODF) se considera un directorio de objetos de datos distintos a las claves o los certificados. Las tarjetas inteligentes que contienen dichos objetos de datos deben disponer de por lo menos un archivo DODF. Estos archivos contienen atributos de objetos de datos generales, tales como identificadores de la aplicación a la cual pertenece el objeto de datos y también punteros a los propios objetos de datos.

40

45

50

Cada uno de los archivos de directorios (de clave privada, claves públicas, claves secretas, certificados u objetos de datos) ocupa una matriz permanente de memoria direccionable dentro de la tarjeta inteligente. En el procedimiento de codificación de la técnica anterior, las direcciones de los punteros se almacenan junto a una dirección inicial de memoria asignada al archivo del directorio de la tarjeta inteligente, y los datos de los punteros se almacenan en una dirección inicial de datos de puntero fija dentro de la memoria asignada al archivo del directorio de la tarjeta inteligente. Desgraciadamente, tras el proceso de codificación se obtienen dos bloques discontinuos de memoria no utilizada en el archivo de directorio, debido a la ubicación de la dirección inicial de datos de puntero.

55

La patente US nº 5.161.256 da a conocer una memoria de datos de una tarjeta CI constituida por un archivo de datos común utilizado para todas las aplicaciones, y una pluralidad de archivos de datos de aplicación utilizados independientemente para cada aplicación. Los archivos de datos comprenden una pluralidad de áreas. Se facilitan datos de identificación al archivo de datos y al área. Es posible prevenir la duplicación de definiciones verificando los datos de identificación. Si se utilizan datos distintos a los datos de identificación facilitados al archivo de datos común como datos de identificación para facilitar al archivo de datos de aplicación, el acceso a áreas del archivo de datos común y el archivo de datos de aplicación puede tener lugar conforme a los datos de mandato.

60

65

Considerando el objetivo anterior, el objeto de la presente invención es un procedimiento perfeccionado de codificación de información en la memoria permanente de una tarjeta inteligente. Este objeto se alcanza mediante las características del procedimiento según la reivindicación 1 y mediante las características de la tarjeta inteligente según la reivindicación 8.

5

En las reivindicaciones dependientes se describen otras características de la presente invención.

Por consiguiente, uno de los objetivos de la presente invención consiste en proporcionar un procedimiento perfeccionado de codificación de información en los archivos de directorio de una tarjeta inteligente, de tal forma que se disponga de un único bloque de memoria no utilizada en el archivo de directorio de la tarjeta inteligente tras la codificación, permitiendo dicho procedimiento perfeccionado la compatibilidad descendente con la aplicación compatible con PKCS15.

10

Sumario de la invención

15

Según la presente invención, está previsto un procedimiento de codificación de información en la memoria permanente de una tarjeta inteligente que comprende las etapas siguientes:

20

proporcionar un archivo de directorio que presenta una dirección inicial y una dirección final en la memoria permanente de la tarjeta inteligente;

proporcionar un objeto de datos para su almacenamiento en la tarjeta inteligente;

25

almacenar el objeto de datos entre la dirección inicial y la dirección final en por lo menos una última ubicación de memoria disponible del archivo de directorio, hallándose dicha última ubicación de memoria disponible más próxima a la dirección inicial del archivo de directorio que el objeto de datos almacenado previamente y

30

almacenar un puntero de datos entre la dirección inicial y la dirección final en por lo menos una primera ubicación de memoria disponible más próxima a la dirección inicial, indicando el puntero de datos la ubicación del objeto de datos,

en el que se dispone de un bloque continuo de memoria para el almacenamiento de un puntero de datos y los objetos de datos entre el último puntero de datos almacenado y la ubicación del objeto de datos indicada por el último puntero de datos almacenado.

35

Según otro aspecto de la presente invención, está previsto un procedimiento de codificación de información en la memoria permanente de una tarjeta inteligente, que comprende las etapas siguientes:

40

proporcionar un archivo de directorio que presenta una dirección inicial y una dirección final en la memoria permanente de la tarjeta inteligente;

proporcionar un objeto de datos para su almacenamiento en la tarjeta inteligente;

45

almacenar el objeto de datos entre la dirección inicial y la dirección final en por lo menos una última ubicación de memoria disponible próxima a la última ubicación de memoria disponible del archivo de directorio, hallándose dicha última ubicación de memoria disponible más próxima a la dirección inicial del archivo de directorio que el objeto de datos almacenado previamente y

50

almacenar un puntero de datos entre la dirección inicial y la dirección final en por lo menos una primera ubicación de memoria disponible cerca de la dirección inicial, indicando el puntero de datos la ubicación de un objeto de datos.

Según otro aspecto de la presente invención está prevista una tarjeta inteligente que comprende:

55

un archivo de directorio que presenta una dirección inicial y una dirección final en la memoria permanente de la tarjeta inteligente;

un objeto de datos almacenado en el archivo de directorio entre la dirección inicial y la dirección final;

60

un puntero de datos asociado al objeto de datos almacenado en el archivo de directorio entre la dirección inicial y la dirección final y

un bloque continuo de memoria disponible entre el último puntero de datos almacenado y la ubicación del objeto de datos indicada por el último puntero de datos almacenado, siendo operativo el bloque continuo de memoria disponible para almacenar el puntero de datos y los objetos de datos.

Breve descripción de los dibujos

A continuación, se describirá la presente invención haciendo referencia a los dibujos adjuntos, en los cuales:

5 la figura 1 es un diagrama de la técnica anterior de los archivos de directorio de una tarjeta inteligente de CI de la técnica anterior, así como de un procedimiento de la técnica anterior de codificación de datos en la tarjeta inteligente y

10 la figura 2 ilustra un procedimiento perfeccionado de codificación de datos en una tarjeta inteligente que da como resultado un único bloque continuo de memoria libre.

Descripción detallada de la invención

15 En la figura 1 de la técnica anterior, se representa una tarjeta inteligente (SC) de circuito integrado compatible con PKCS 15. La tarjeta inteligente comprende un archivo de directorio maestro (MF) 10, con un puntero a un archivo de directorio de objetos (ODF) 11. El ODF 11 contiene punteros a archivos de directorio de datos almacenados en la tarjeta inteligente, en particular un archivo de directorio de clave privada (PrKDF) 12, un archivo de directorio de claves públicas (PuKDF) 13, un archivo de directorio de claves secretas (SKDF) 14, un archivo de directorio de certificados (CDF) 15 y un archivo de directorio de objetos de datos (DODF) 16. La memoria facilitada a cada uno de estos archivos de directorio es permanente, direccionable por bytes y presenta una dirección inicial 22 y una dirección final 24.

25 La memoria para cada archivo de directorio de datos 17 comprende un espacio de memoria de puntero 18 y un espacio de memoria de datos de puntero 20. El espacio de memoria de puntero 18 está reservado para codificar direcciones de puntero, y el espacio de memoria de datos de puntero 20 está reservado para codificar datos de puntero. Se reserva un espacio de información de la memoria junto a la dirección inicial de la tarjeta inteligente 22 para los punteros 18. Se reserva un espacio de información de la memoria junto a la dirección inicial de los datos de puntero 23 para los datos de puntero 20. Unos punteros 18 correspondientes remiten a las entradas de datos de puntero 20, y entonces, por ejemplo, el puntero almacenado en el espacio de memoria de punteros "A" remite a una dirección de memoria que corresponde a los datos de puntero "A" almacenados en la memoria de datos de puntero. De esta manera cualquier referencia a los datos de puntero "A" se indexa en la memoria de punteros con el puntero "A".

35 Los punteros se codifican en secuencia en el espacio de memoria de punteros 18 empezando junto a la dirección inicial de la memoria 22, y los datos de puntero se codifican empezando por la dirección inicial de datos de puntero 23. A medida que se va codificando información en la memoria de los archivos de directorio de la tarjeta inteligente 17, la cantidad de memoria no utilizada se reduce, generándose dos bloques de memoria separados que no contienen datos. El primer bloque de memoria 19 que no contiene datos está situado entre la última entrada de puntero, la entrada "C", escrita en el espacio de memoria de punteros 18 y la dirección inicial de datos de puntero 23. El segundo bloque de memoria 21 que no contiene datos está situado entre la última entrada de datos de puntero, la entrada "C", escrita en el espacio de memoria de datos de puntero 20 y la dirección final de la memoria 24. Se generan de ese modo dos bloques de memoria no utilizada que no contienen datos. Debe tenerse en cuenta, por supuesto, que la memoria no utilizada se reserva para futuros usos de almacenamiento de datos.

45 La ubicación de la dirección inicial de los datos de puntero 23 para cada uno de los archivos de directorio de datos 17 es determinada por cuestiones de diseño, a fin de utilizar mejor la memoria disponible en el archivo de directorio. Durante la codificación de información en el archivo de directorio 17, el procedimiento de codificación de la técnica anterior limita la codificación a un número fijo de punteros o a una cantidad fija de datos de puntero, que deben determinarse antes de la codificación, debido a la ubicación de la dirección inicial de datos de puntero antes de la codificación. En cualquier caso, se generan dos bloques de memoria no consecutivos que no contienen datos codificados en el archivo de directorio 17.

55 Al diseñar el mapa de almacenamiento en memoria para una tarjeta inteligente que cumple la norma PKCS 15, surgen cuestiones contrapuestas. Son proporcionadas a título de ejemplo. Cuando se almacenan claves privadas en un área de datos, el espacio asignado a los punteros se basa en un número de claves máximo teórico. Cuando todas las claves son idénticas en cuanto a configuración, un cálculo matemático sencillo permite determinar la dirección inicial de los datos de puntero 23. En este caso, la memoria disponible dividida por la memoria necesaria para cada clave más la memoria necesaria para cada puntero determina el número máximo de claves que se pueden almacenar. Esto determina también la ubicación de la dirección inicial de los datos de puntero 23 que es por lo menos el número máximo de punteros multiplicado por la cantidad de espacio que necesita cada puntero empezando por el principio del archivo del directorio de datos. Desgraciadamente, cuando se admite más de un tamaño de clave, el cálculo no es tan sencillo. Entonces, o bien se admite el número máximo de claves (la utilización de la memoria se optimiza solo cuando todas las claves son del mismo tamaño y el más pequeño), o bien se admiten menos claves, siendo posible que se agote el espacio de punteros antes que el espacio de objetos de datos. Obviamente, en el primer caso de almacenamiento de claves de mayor tamaño, quedarán ubicaciones de puntero por utilizar.

Esta situación es problemática en la medida en que la norma PKCS 15 goza ya de una amplia implementación y aceptación, y en la dificultad que entraña actualmente diseñar de nuevo la memoria de datos de una tarjeta inteligente. El perfeccionamiento de una norma deficiente requiere la aceptación por el ente normativo y sus participantes. Esto constituye una tarea onerosa, cuya consecución a veces puede prolongarse durante años. Una estrategia alternativa consiste en diseñar un sistema de memoria perfeccionado retrocompatible. Desgraciadamente, dicha estrategia restringe considerablemente las opciones de diseño disponibles y a menudo resulta vana.

Un sistema de memoria perfeccionado retrocompatible debe permitir su lectura en cualquier dispositivo de lectura de tarjetas inteligentes según la norma PKCS15. No es necesario que la escritura de las tarjetas inteligentes cumpla fielmente la norma PKCS 15, siempre y cuando los datos puedan recuperarse mediante los sistemas PKCS15.

Una de dichas mejoras respecto del procedimiento de codificación de datos en la tarjeta inteligente de la técnica anterior se representa en la figura 2. En esta figura se representa un único archivo de directorio (DF) 25. La memoria facilitada al archivo de directorio presenta una dirección inicial 28 y una dirección final 29. Dentro de cada archivo de directorio de datos, existe un espacio de memoria de punteros 31 y un espacio de memoria de datos de objetos 33. El espacio de memoria de punteros 31 está reservado para almacenar direcciones de puntero, y el espacio de memoria de datos de objetos 33 está reservado para almacenar datos de puntero. El espacio de la memoria situado junto a la dirección inicial 28 se reserva para el almacenamiento de punteros 31. El espacio de la memoria situado junto a la dirección final 29 se reserva para los datos de puntero 27. Unos punteros 26 correspondientes remiten a las entradas de datos de objetos, y entonces, por ejemplo, el puntero almacenado en el espacio de memoria de punteros "A" remite a la dirección de los correspondientes datos de puntero "A" almacenados en el espacio de datos de la memoria de punteros. De esta manera el puntero "A" remite a todas las referencias a los datos de puntero "A" del espacio de memoria de punteros.

Los punteros se escriben en secuencia en el espacio de memoria de punteros empezando junto a la dirección inicial 28 y avanzando hacia la dirección final 29. Por consiguiente, en el espacio de memoria de punteros 31, el puntero "A" se halla en una dirección inferior al puntero "B". Por otro lado, los datos de objetos se codifican de una manera opuesta. El primer conjunto de datos de objetos 33 correspondiente al puntero "A" se codifica empezando junto a la dirección final de la memoria 29, y desde ahí los datos se escriben en secuencia desde una dirección superior hasta una dirección inferior y desde el final del objeto de datos hasta el principio, de tal manera que el objeto de datos mantiene el mismo orden compatible con la norma PKCS15. Por consiguiente, en el espacio de memoria de datos de puntero, los datos del puntero "A" se hallan en una dirección superior a los datos del puntero "B".

No se facilita ninguna dirección inicial de datos de puntero 23, puesto que los datos de objetos empiezan en la dirección final de la memoria 29 y avanzan hacia la dirección inicial de la memoria 28. A pesar de lo descrito acerca del almacenamiento de datos, comúnmente los objetos se escriben en la misma dirección progresiva que la empleada actualmente por los sistemas PKCS15. Las ubicaciones iniciales del objeto son determinadas por el tamaño del objeto y la última ubicación de datos disponible, de tal forma que los objetos se colocan al final del espacio de datos disponible.

Esta manera de codificar los datos en el archivo de directorio 25 da como resultado un único bloque de memoria no utilizada 32 que no contiene datos. Este bloque único de memoria no utilizada 32 está situado entre el último puntero codificado situado dentro del espacio de memoria de punteros 31 y el último conjunto de datos de objetos codificados situado dentro del espacio de memoria de datos de objetos 33.

En consecuencia, la ubicación de la dirección inicial de los datos de puntero 23 ya no está sujeta a ninguna limitación, puesto que deja de ser necesaria, y tampoco se desperdicia espacio de la memoria a causa de insuficiente espacio en una sola de las dos áreas de memoria, la de datos de puntero y la de datos de objeto. Este único bloque continuo de memoria no utilizada 32 del archivo de directorio permite codificar aplicaciones y aprovechar mejor el espacio de memoria contenido en el archivo de directorio, eliminando el espacio de memoria vacío no consecutivo del archivo de directorio.

Convenientemente, el formato es retrocompatible con los procedimientos de lectura y codificación PKCS 15, ya que los punteros del espacio de memoria de punteros siguen remitiendo a la correspondiente información almacenada en el espacio de memoria de datos de puntero. Con el procedimiento perfeccionado, se puede codificar más información dentro de cada archivo de directorio, puesto que el procedimiento de codificación perfeccionado permite mejorar la gestión de la memoria del archivo de directorio.

Por ejemplo, la cantidad total de memoria permanente asignada al DODF es de 100 bytes. Los objetos de datos almacenados en el DODF son de 19 bytes o 39 bytes de longitud. Si se encuentran cinco punteros de datos a objetos de datos almacenados en el DODF y cinco objetos de datos de 19 bytes almacenados en el DODF, la cantidad de espacio total utilizada realmente en el DODF es de 100 bytes en el sistema de la técnica anterior. Si, por ejemplo, en el DODF se encuentran tres punteros de datos a objetos de datos, un objeto de datos de 19 bytes y dos objetos de datos de 39 bytes almacenados, en este caso también se utiliza realmente un total de 100 bytes de espacio del DODF en el sistema de la técnica anterior. En la técnica anterior, si el número de punteros a objetos de datos del DODF se establece en cinco en el momento de la inicialización del archivo de directorio, entonces sólo se

5 escriben cinco objetos de datos de 19 bytes en el DODF o un objeto de datos de 39 bytes y dos objetos de datos de 19 bytes, lo cual deja 18 bytes de datos sin utilizar dentro del archivo de directorio, en los cuales no se escribe ningún dato, puesto que los objetos de datos tienen un tamaño mínimo de 19 bytes. No obstante, según la presente invención, la limitación a la cantidad de espacio de punteros no existiría, puesto que el espacio de datos de puntero y el espacio de datos de objetos comparten la misma parte de memoria continua dentro del DODF. Convenientemente, si en la presente invención es necesario cambiar el tamaño del objeto de datos, es posible adaptar el objeto de datos a medida para que ocupe la cantidad exacta de memoria libre en el DODF, puesto que los datos de puntero y los datos de objetos comparten el mismo espacio de memoria.

REIVINDICACIONES

1. Procedimiento de codificación de información en la memoria permanente de una tarjeta inteligente que comprende las etapas siguientes:

5 proporcionar un archivo de directorio (25) que presenta una dirección inicial (28) y una dirección final (29) dentro de la memoria permanente de la tarjeta inteligente, soportando la tarjeta inteligente la recuperación de los objetos de datos según la norma PKCS15;

10 proporcionar un objeto de datos (27) para su almacenamiento en el interior de la tarjeta inteligente;

almacenar el objeto de datos (27) entre la dirección inicial y la dirección final en por lo menos una última ubicación de memoria disponible en el interior del archivo de directorio, encontrándose la última ubicación de memoria disponible más próxima a la dirección inicial del archivo de directorio que un objeto de datos almacenado previamente,

15 caracterizado porque:

20 el objeto de datos se escribe secuencialmente en la memoria empezando desde una dirección superior del objeto de datos almacenado previamente hasta una dirección inferior más próxima a la dirección inicial; y

almacenar un puntero de datos (26) entre la dirección inicial y la dirección final en por lo menos la más próxima primera ubicación de memoria disponible a la dirección inicial, resultando el puntero de datos indicativo de una ubicación de objeto de datos, escribiéndose el puntero de datos secuencialmente en la memoria empezando en la proximidad de la dirección inicial (28) y avanzando hacia la dirección final (29) de una manera opuesta a la del objeto de datos,

25 en el que puede disponerse de un bloque continuo (32) de memoria para el almacenamiento en el mismo de punteros de datos y objetos de datos entre un último puntero de datos almacenado y la ubicación del objeto de datos indicada por el último puntero de datos almacenado.

30 2. Procedimiento según la reivindicación 1, que comprende las etapas siguientes:

35 almacenar el objeto de datos (27) entre la dirección inicial y la dirección final en por lo menos una ubicación de memoria disponible próxima a la última ubicación de memoria disponible en el interior del archivo de directorio, encontrándose la última ubicación de memoria disponible más próxima a una dirección inicial del archivo de directorio que un objeto de datos almacenado previamente; y

40 almacenar el puntero de datos (26) entre la dirección inicial y la dirección final en por lo menos una ubicación de memoria disponible próxima a la dirección inicial, resultando el puntero de datos indicativo de una ubicación de un objeto de datos.

45 3. Procedimiento según la reivindicación 1 o 2, en el que la aplicación del procedimiento da como resultado un bloque continuo (32) de memoria disponible entre el último puntero de datos almacenado y la ubicación de objeto de datos indicada por el último puntero de datos almacenado.

50 4. Procedimiento según cualquiera de las reivindicaciones 1 y 3, en el que el puntero de datos (26) comprende una dirección es determinada sustrayendo el tamaño del objeto de datos de la última dirección de ubicación de memoria disponible.

55 5. Procedimiento según cualquiera de las reivindicaciones 1 y 4, en el que la última dirección de ubicación de memoria disponible es determinada como la dirección en el interior del último puntero de datos menos una ubicación de dirección.

6. Procedimiento según cualquiera de las reivindicaciones 1 y 2, en el que la dirección inicial de la memoria es inferior a la dirección final de la memoria.

60 7. Procedimiento según cualquiera de las reivindicaciones 1 y 2, en el que la dirección inicial de la memoria es superior a la dirección final de la memoria y en el que el sentido de avance en la memoria es desde los valores de dirección superiores hacia los valores de dirección inferiores.

8. Tarjeta inteligente que comprende:

65 un archivo de directorio (25) que presenta una dirección inicial (28) y una dirección final (29) dentro de la memoria permanente de la tarjeta inteligente, soportando la tarjeta inteligente la recuperación de los objetos de datos según la

norma PKCS15;

un objeto de datos (27) almacenado en el interior del archivo de directorio entre la dirección inicial y la dirección final;

5 un puntero de datos (26) asociado al objeto de datos almacenado en el interior del archivo de directorio y entre la dirección inicial y la dirección final;

caracterizada porque:

10 el objeto de datos se escribe secuencialmente en la memoria empezando desde una dirección superior de un objeto de datos almacenado previamente hasta una dirección inferior más próxima a la dirección inicial;

el puntero de datos se escribe secuencialmente en la memoria empezando en la proximidad de la dirección inicial (28) y avanzando hacia la dirección final (29) de una manera opuesta a la del objeto de datos; y

15 presenta un bloque continuo (32) de memoria disponible entre un último puntero de datos almacenado y la ubicación de objeto de datos indicada por el último puntero de datos almacenado, sirviendo el bloque continuo de memoria disponible para almacenar en la misma los punteros de datos y los objetos de datos.

20 9. Tarjeta inteligente según la reivindicación 8, en la que:

el objeto de datos (27) es almacenado en por lo menos una última ubicación de memoria disponible en el interior del archivo de directorio; y

25 el puntero de datos asociado (26) es almacenado en por lo menos la más próxima primera ubicación de memoria disponible a la dirección inicial y entre la dirección inicial (28) y la dirección final (29).

10. Tarjeta inteligente según la reivindicación 8, en la que:

30 una pluralidad de objetos de datos (27) se almacena en un bloque de memoria contiguo que comprende por lo menos una última ubicación de memoria disponible en el interior del archivo de directorio; y

35 una pluralidad de punteros de datos asociados (26) se almacena en un bloque de memoria contiguo que comprende por lo menos la más próxima primera ubicación de memoria disponible a la dirección inicial y entre la dirección inicial y la dirección final.

11. Tarjeta inteligente según la reivindicación 8, en la que:

40 una pluralidad de objetos de datos (27) se almacena en un bloque de memoria contiguo que comprende una ubicación de memoria próxima a la última ubicación de memoria disponible en el interior del archivo de directorio; y

una pluralidad de punteros de datos asociados (26) se almacena en un bloque de memoria contiguo que comprende una ubicación de memoria próxima a por lo menos la más próxima primera ubicación de memoria disponible a la dirección inicial y entre la dirección inicial y la dirección final.

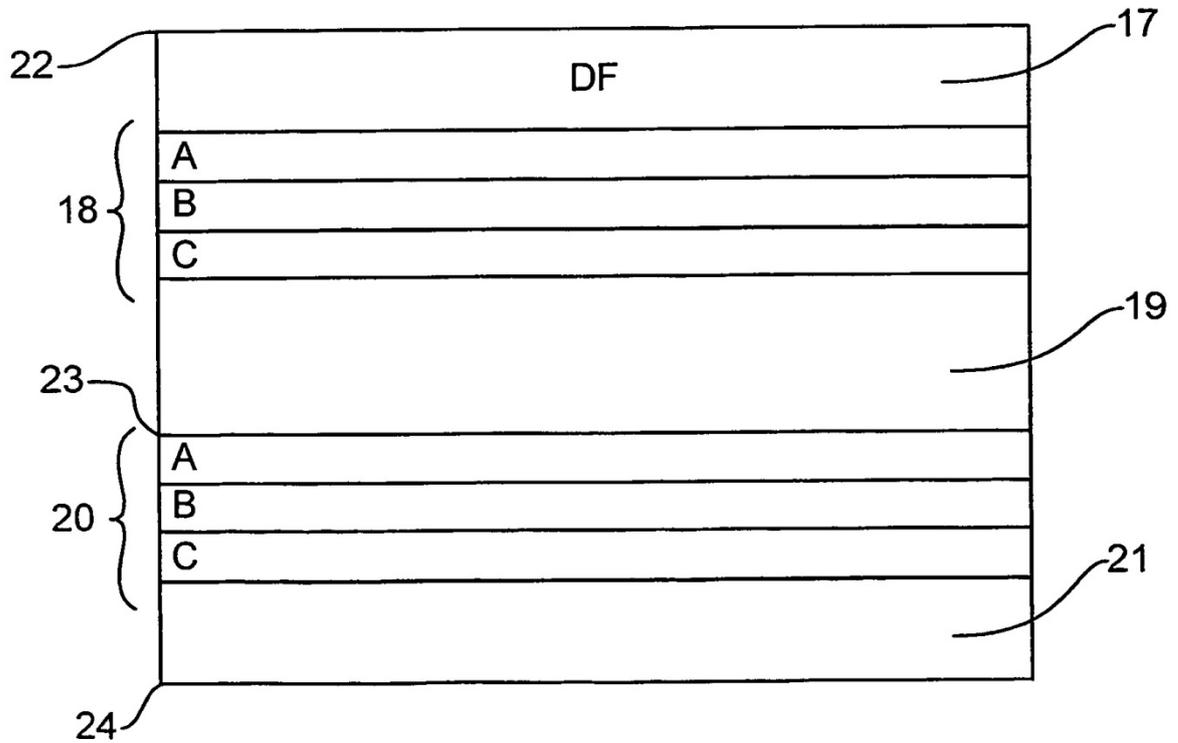
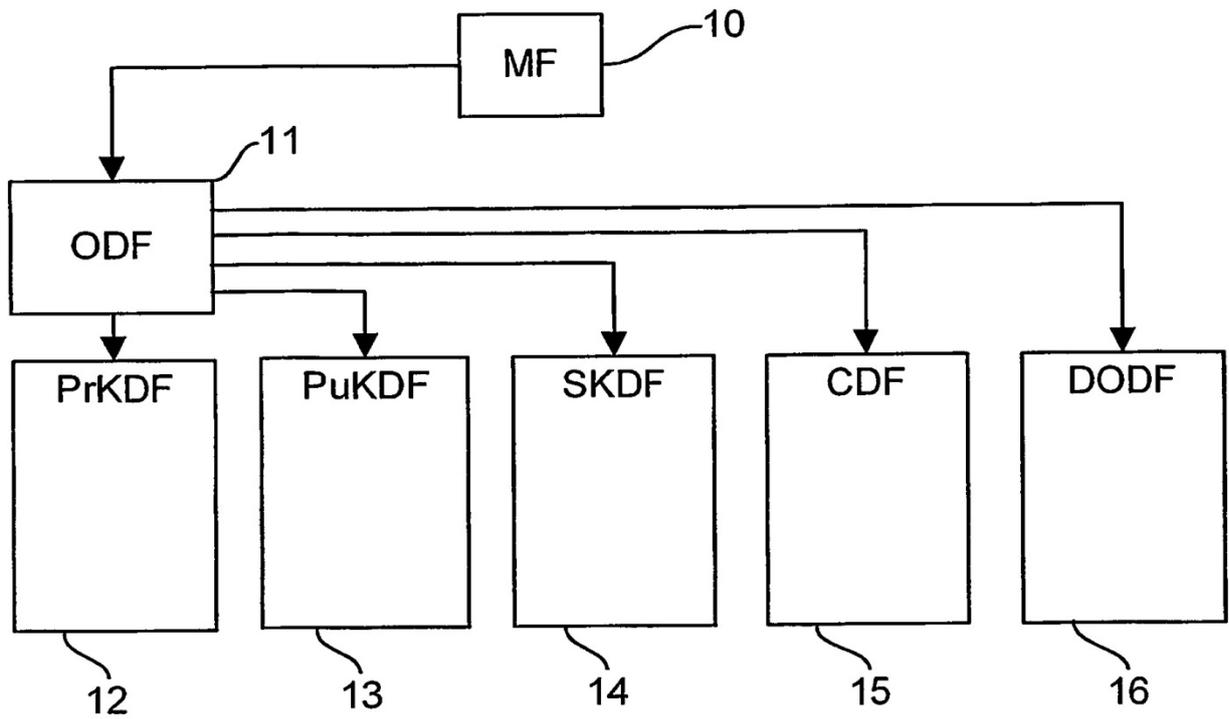


Fig. 1
(TÉCNICA ANTERIOR)

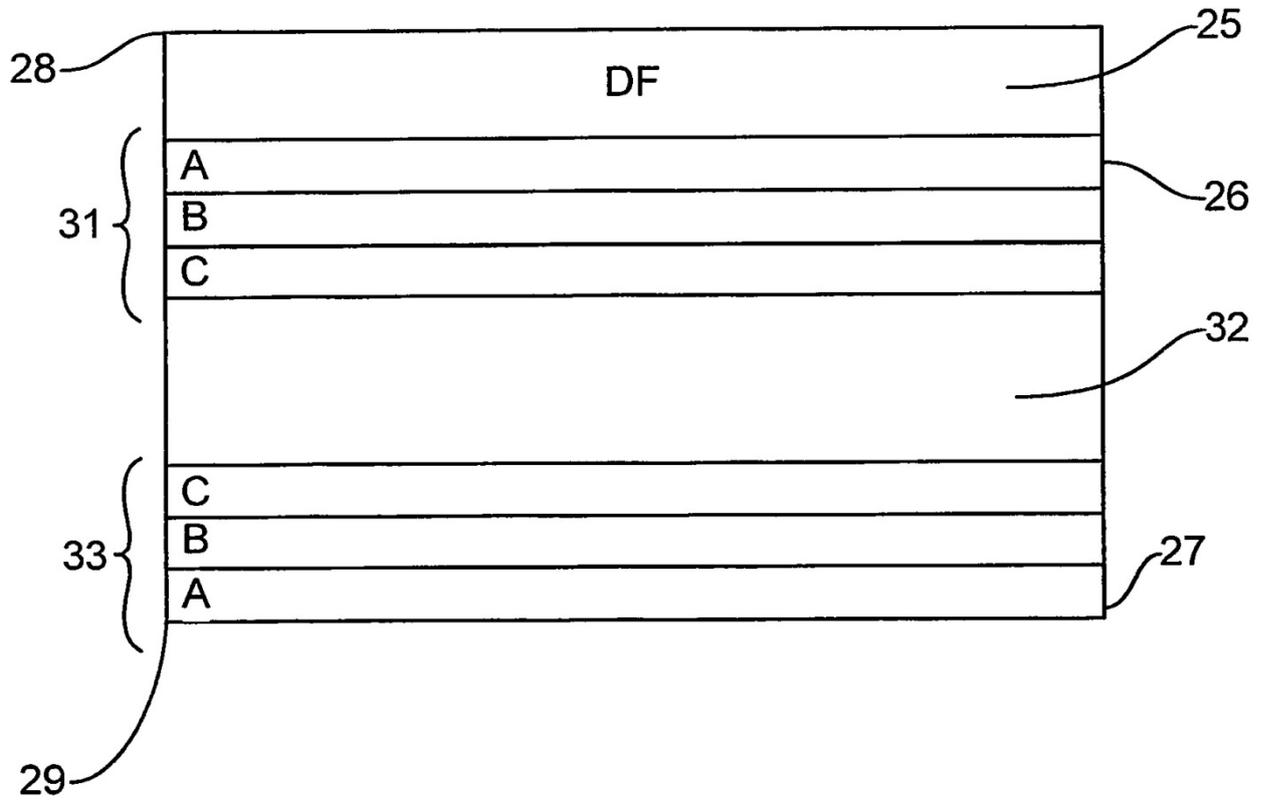


Fig. 2