(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 376 229**

(51) Int. CI.:
***G06K 19/073*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03813629 .7**
(96) Fecha de presentación: **17.12.2003**
(97) Número de publicación de la solicitud: **1573665**
(97) Fecha de publicación de la solicitud: **14.09.2005**

(54) Título: **DISPOSITIVO OPTIMIZADO DE COMUNICACIÓN DE DATOS DIGITALES EN UNA TARJETA CON MICROCIRCUITO.**

(30) Prioridad:
**18.12.2002 FR 0216084**

(45) Fecha de publicación de la mención BOPI:
**12.03.2012**

(45) Fecha de la publicación del folleto de la patente:
**12.03.2012**

(73) Titular/es:
**OBERTHUR TECHNOLOGIES**
**50 quai Michelet**
**92300 Levallois-Perret, FR**

(72) Inventor/es:
**GOUESSANT, Hervé y**
**JAYET, Stéphane**

(74) Agente/Representante:
**Pérez Barquín, Eliana**

## DESCRIPCIÓN

Dispositivo optimizado de comunicación de datos digitales en una tarjeta con microcircuito

La presente invención se refiere a una tarjeta con microcircuito.

Más exactamente, la invención se refiere a una tarjeta con microcircuito adaptada:

- por un lado para procesar un flujo relativamente importante de datos digitales intercambiados con un dispositivo externo a la tarjeta; y

- por otro lado para implementar procedimientos de seguridad, por ejemplo funciones de verificación de la integridad de los datos digitales intercambiados con el dispositivo externo o funciones criptográficas de autenticación de un usuario de la tarjeta.

La invención también podrá utilizarse para la descompresión de un flujo de datos digitales encriptados.

Según una arquitectura conocida de dicha tarjeta, los datos digitales recibidos desde un puerto de entrada-salida de la tarjeta con microcircuito son leídos por un microprocesador y procesados cuando son recibidos. El microprocesador realiza los controles de seguridad mencionados anteriormente a medida que recibe los datos digitales.

Un problema fundamental de esta arquitectura es que el flujo de datos digitales que pueden ser intercambiados por la tarjeta está limitado por la frecuencia del microprocesador (generalmente del orden de 4 MHz para las tarjetas con microcircuito conocidas en el estado de la técnica).

En otros campos de la electrónica, para paliar los límites asociados a la frecuencia de un microprocesador, la transferencia de datos a alta velocidad es realizada a menudo por componentes denominados DMA (*Direct Memory Access*) [Acceso Directo a Memoria]. Estos componentes DMA son programados por un microprocesador para realizar una transferencia predeterminada, por ejemplo entre un puerto de entrada-salida y una memoria, no estando la transferencia, en cuanto a tal, realizada por el microprocesador.

Desgraciadamente, estos componentes DMA están dedicados a la transferencia de datos y no permiten realizar ningún procesamiento sobre los datos durante su transferencia. Por lo tanto, estos componentes no están, a priori, adaptados para la transferencia de datos sensibles que necesitan operaciones de seguridad, como es el caso para las tarjetas con microcircuito mencionadas anteriormente.

La solicitud de patente alemana DE19908285 A1 describe una tarjeta con chip cuya memoria es accesible por medio del microprocesador o directamente a través de una interfaz de memoria. El acceso directo está controlado después de la autenticación por el microprocesador.

La invención pretende, superando esta aparente incompatibilidad, permitir una transferencia de un flujo importante o rápido de datos seguros en una tarjeta con microcircuito mientras se mantiene un nivel de seguridad importante, esto gracias a una asociación original de un procesador y de un DMA.

La invención propone, a tal efecto, una tarjeta con microcircuito según la reivindicación 1.

De este modo, los datos recibidos desde el puerto de comunicación son transferidos por los medios de transferencia hacia una zona de memorización, no estando el flujo de esta transferencia limitado por la velocidad de los medios de control de flujo.

Por otro lado, durante esta transferencia, datos de seguridad obtenidos a partir de los datos digitales son comunicados por los medios de procesamiento a los medios de control de flujo, estando el flujo de estos datos de seguridad recibidos por los medios de control de flujo, limitado y siendo de todos modos muy inferior al flujo de datos digitales recibidos por la tarjeta.

Los medios de control de flujo, constituidos por ejemplo por un procesador, están entonces en condiciones de realizar, utilizando estos datos de seguridad, las operaciones necesarias de control de los medios de transferencia para garantizar que se respetan las restricciones de seguridad.
La invención permite, de este modo, aumentar el flujo de datos digitales procesados por la tarjeta con microcircuito, mientras se mantiene el nivel de seguridad de una tarjeta tradicional.

En una primera variante de realización de la tarjeta con microcircuito según la invención, los datos de seguridad mencionados anteriormente están constituidos, al menos en parte, por una parte de los datos digitales transferidos por la tarjeta.

En un modo preferido de esta primera variante de realización, los datos de seguridad comprenden datos de autenticación de una parte de los datos digitales recibidos por la tarjeta, estando los medios de control de flujo adaptados para verificar la validez de los datos digitales a partir de estos datos de autenticación y para controlar la transferencia en función del resultado de esta verificación.

De forma conocida, cuando la tarjeta recibe datos digitales transmitidos por un dispositivo externo, si los medios de control de flujo determinan que los datos de autenticación no son válidos, esto significa que los datos digitales no han sido enviados por un emisor autorizado.

En este caso, los medios de control de flujo pueden tomar una medida predeterminada, tal como bloquear la utilización de la tarjeta o enviar un mensaje de error.

En una realización preferida, para garantizar una utilización segura de la tarjeta, los medios de control de flujo ordenan la detención de la transferencia de los datos digitales por los medios de transferencia cuando los datos de autenticación no son válidos.

La tarjeta puede recibir, de este modo, un flujo importante de datos, estando una parte solamente de estos datos comunicada a los medios de control de flujo para garantizar la seguridad exigida.

En una segunda variante de realización, los medios de procesamiento están adaptados para insertar en los datos de seguridad un resultado de procesamiento calculado a partir de los datos digitales.

El resultado de procesamiento puede ser, por ejemplo, el resultado de una etapa de verificación de los datos de autenticación mencionados anteriormente por medios de cálculo comprendidos en los medios de procesamiento, por ejemplo medios criptográficos de la tarjeta con microcircuito. Este resultado es tenido en cuenta a continuación por los medios de control de flujo para verificar la integridad de los datos digitales y para controlar su transferencia por los medios de transferencia, de forma consecuente.

Esta etapa de autenticación puede consistir en verificar una firma, por ejemplo utilizando una clave criptográfica y una función de troceo según un algoritmo de tipo MD4, MD5 o SHA-1.

En esta variante, son los medios de control de flujo los que realizan las etapas de verificación de los datos de autenticación. A continuación pueden tomar una medida predeterminada tal como detener la transferencia de los datos digitales o bloquear la utilización de la tarjeta, en caso de utilización fraudulenta de la misma.

En una realización preferida, los medios de control de flujo realizan el control de la transferencia de los datos digitales modificando al menos un parámetro de funcionamiento de los medios de transferencia.

Por ejemplo, este parámetro de funcionamiento es una dirección de memorización des datos digitales en la zona de memorización.

De este modo, cuando el nivel de ocupación de un primer intervalo de la zona de memorización es superior a un umbral predeterminado, los medios de control de flujo pueden ajustar los parámetros de los medios de transferencia para que los datos digitales recibidos por los medios de transferencia sean memorizados en esta dirección.

El parámetro mencionado anteriormente también puede ser un parámetro que permita seleccionar el protocolo de comunicación entre los medios de entrada-salida y la zona de memorización. Este protocolo de comunicación puede estar, por ejemplo, adaptado a las transferencias de datos seguros.

Según diferentes variantes de realización de la tarjeta con microcircuito según la invención, los medios de procesamiento comprenden una unidad de compresión de los datos, una unidad de descompresión de los datos, una unidad de encriptado de los datos o una unidad de desencriptado de los datos.
En otra variante de realización, los medios de control de flujo están adaptados, además, para obtener datos preliminares directamente a partir de los medios de entrada-salida, siendo los datos preliminares tenidos en cuenta por la unidad de control de flujo para autorizar o rechazar la transferencia de los datos digitales por los medios de transferencia.

En un modo particular de esta variante de realización, estos datos preliminares comprenden datos de autenticación.

Esta realización permite obtener un nivel de seguridad suplementario, por ejemplo mediante el control de un código de autenticación, previamente a la transferencia de los datos digitales propiamente dichos. Al contrario que los datos de seguridad, este código de autenticación típicamente es verificado solamente una vez al comienzo de la sesión de transferencia. Puede requerir más tiempo de cálculo y, por lo tanto, emplear un algoritmo de autenticación complejo y que permite obtener un nivel de seguridad reforzado.

En otra realización preferida, estos datos preliminares comprenden una dirección de memorización de los datos digitales que serán transferidos por los medios de transferencia. En esta realización preferida, estos datos preliminares pueden comprender, además, datos de autenticación de esta dirección de memorización, esto para garantizar que la dirección de memorización no ha sido suministrada por un usuario no autorizado.

Según una realización particularmente ventajosa, la tarjeta con microcircuito comprende, además, medios de regulación adaptados para modificar una frecuencia del reloj aplicada a los medios de procesamiento en función de dichos datos de seguridad.

Esta característica permite, de este modo, limitar el consumo eléctrico de la tarjeta con microcircuito cuando la transferencia de datos digitales por los medios de transferencia debe interrumpirse.

La invención se entenderá mejor y otras ventajas quedarán más claras a la luz de la siguiente descripción de una tarjeta con microcircuito según su principio, que se da únicamente como ejemplo y hecha en referencia a los dibujos adjuntos, en los que:

- la figura 1 es un diagrama de bloques de una tarjeta con microcircuito según la técnica anterior;

- la figura 2 es un diagrama de bloques, análogo a la figura 1, que ilustra una posible realización de una tarjeta con microcircuito según la invención; y

- la figura 3 es un ejemplo de datos de seguridad según la invención.

La tarjeta 10 con microcircuito según la técnica anterior representada en la figura 1 comprende principalmente un procesador CPU asociado de forma convencional a cierto número de memorias (de tipo RAM, ROM, EEPROM), medios 12 de procesamiento y medios 14 de entrada-salida unidos, por ejemplo, a un terminal.

Los medios 12 de procesamiento comprenden una unidad 13 de cálculo adaptada para realizar el procesamiento propiamente dicho de los datos digitales, a saber por ejemplo operaciones de compresión, de descompresión, de encriptado o de desencriptado de estos datos.

En una realización preferida, los medios 14 de entrada-salida que permiten a la tarjeta 10 con microcircuito comunicarse con un terminal o una entidad electrónica externa, comprenden esencialmente una unidad de emisión recepción asíncrona de tipo UART.

Los medios 14 de entrada-salida también pueden estar adaptados para implementar protocolos de comunicación estandarizados y conocidos por el experto en la materia, a saber por ejemplo, los protocolos conocidos con las referencias “T=0”, “T=1” (ISO 7816), USB, FireWire o 12C.

Según la técnica anterior, cuando la tarjeta 10 con microcircuito recibe mediante la UART datos digitales que deben someterse a un procesamiento por la unidad 13 de cálculo de los medios 12 de procesamiento, la UART transmite un mensaje de interrupción al procesador CPU. El procesador CPU leerá entonces un registro de la UART y copiará los datos en la memoria RAM.

El procesador CPU inicializa entonces los medios 12 de procesamiento y a continuación leerá los datos a procesar en la memoria RAM y los copiará en un registro 16 de los medios 12 de procesamiento.
Para comunicarlo al terminal externo, el resultado calculado por los medios 12 de procesamiento es leído a continuación por el procesador CPU en el registro 16 y copiado en el registro UART por el procesador CPU.

Dicho modo de funcionamiento no es favorable para el procesamiento de datos digitales a alta velocidad por la tarjeta 10 con microcircuito. En efecto, la operación intermedia realizada por el procesador CPU de copia de los datos digitales en la zona de memorización RAM antes del procesamiento por los medios 12 de procesamiento es, muy particularmente, perjudicial.

Ahora bien, se desea aumentar la potencia de procesamiento de dicha tarjeta con microcircuito para procesar flujos importantes y continuos de datos en tiempo real.

Como ejemplo, se desea poder proceder al descifrado en tiempo real de datos digitales representativos de un sonido. Dichos datos son comprimidos según la norma MP3 y transmitidos a una velocidad de 128 kbits/s. La tarjeta con microcircuito encargada del descifrado en tiempo real necesita, por lo tanto, poder recibir y procesar información a alta velocidad.

A continuación se describirá una tarjeta con microcircuito según la invención y que permite resolver el problema anterior, en referencia a la figura 2.

Según la presente invención, los medios 12 de procesamiento comprenden medios DMA de transferencia de los datos digitales entre el puerto 14 de comunicación y una zona 18 de memorización.

En el ejemplo de la figura 2 descrito en este documento, la zona 18 de memorización es una memoria viva RAM.

En otras realizaciones, la zona 18 de memorización puede seleccionarse entre diferentes tipos de memorias reescribibles, a saber por ejemplo, una memoria Flash, una memoria de tipo EEPROM o un disco duro.

En otra variante de realización, la zona 18 de memorización es un puerto de la unidad 13 de cálculo de los medios 12 de procesamiento.

En la realización preferida descrita en este documento, estos medios DMA de transferencia comprenden un componente electrónico dedicado conocido por el experto en la materia llamado DMA (*Direct Memory Access*).

De forma conocida, dichos componentes se programan mediante la escritura de parámetros en registros de configuración.

Como ejemplo no limitante, dichos parámetros comprenden la dirección de un puerto de los medios 14 de entrada-salida, la dirección de un intervalo de la zona 18 de memorización en el que deben memorizarse los datos digitales, y parámetros representativos de un criterio de detención de la transferencia.

Sea como fuere, la tarjeta con microcircuito según la invención comprende además medios 26 de control de flujo adaptados para controlar la transferencia de los datos digitales por los medios DMA de transferencia.

En particular, cuando los datos digitales deben ser transferidos hacia una zona 18 de memorización de tipo EEPROM, los medios 26 de control de flujo están adaptados para controlar un generador de tensión o cualquier otro medio que permita aplicar una tensión eléctrica suficiente a la memoria EEPROM para que ésta sea accesible en escritura.

En la realización descrita en referencia a la figura 2, los medios 26 de control de flujo están constituidos por un procesador CPU, el cual está asociado convencionalmente a estas diferentes memorias (RAM, ROM, EEPROM) como en el caso de la figura 1.

El ajuste de parámetros de los medios DMA de transferencia por los medios 26 de control de flujo se representa esquemáticamente mediante las señales 20 en la figura 2.

Según la presente invención, los medios 12 de procesamiento también comprenden medios 22 de comunicación entre su unidad 13 de cálculo y los medios 26 de control de flujo.

Estos medios 22 de comunicación permiten el intercambio de datos de seguridad entre los medios 12 de procesamiento y los medios 26 de control de flujo, obteniéndose estos datos de seguridad a partir de los datos digitales DATA transferidos por los medios DMA de transferencia.

Cronológicamente, una vez programados los medios DMA de transferencia por los medios 26 de control de flujo por medio de las señales 20, los medios DMA de transferencia realizan la transferencia de los datos digitales entre los medios 14 de entrada-salida y la zona 18 de memorización. La unidad 13 de cálculo de los medios 12 de procesamiento obtiene a continuación los datos DATA_CTRL de seguridad a partir de los datos digitales DATA memorizados en la zona 18 de memorización y los comunica a los medios 26 de control de flujo por los medios 22 de comunicación.

Un ejemplo de datos DATA_CTRL de seguridad, en una realización preferida, se da en la figura 3.

Los datos DATA_CTRL de seguridad comprenden una parte P1 de los datos digitales y los datos de autenticación AUTH calculados a partir de los datos digitales de la parte P1.

En una primera variante de realización, los datos de autenticación AUTH forman una firma de P1. Típicamente, se trata de los datos P1 a los que se ha aplicado una función de troceo conocida tal como MD4, MD5 o SHA-1 y, a continuación, un algoritmo de encriptado. Para ello, puede utilizarse un algoritmo de encriptado con clave simétrica tal como el algoritmo DES (*Data Encryption Standard*) [Estándar de Encriptado de Datos] o un algoritmo con clave asimétrica tal como el algoritmo RSA (del nombre de sus inventores Rivest, Shamir y Adelman).

En esta variante, al recibir estos datos DATA_CTRL de seguridad, los medios 26 de control de flujo desencriptan en primer lugar la firma AUTH con la clave de desencriptado y obtienen un primer resultado HASH1. Los medios 26 de control de flujo aplican a continuación la función de troceo a la parte P1 y obtienen un segundo resultado HASH2.

Los medios 26 de control de flujo comparan a continuación el primer resultado HASH1 y el segundo resultado HASH2.

En una realización preferida de esta primera variante, cuando estos resultados HASH1 y HASH2 difieren, los medios 26 de control de flujo ordenan la detención de la transferencia de los datos digitales mediante el envío de una señal de detención.

En la realización preferida, los medios 12 de procesamiento insertan en los datos DATA_CTRL de seguridad un resultado de procesamiento de los datos digitales DATA por la unidad 13 de cálculo.

Este resultado de procesamiento es, por ejemplo, la dirección en la cual una parte de los datos digitales DATA es memorizada por los medios DMA de transferencia en la zona 18 de memorización, estando los medios 26 de control de flujo entonces adaptados para leer los datos de esta parte, y para verificar su validez, y para controlar la transferencia de los datos digitales DATA por los medios DMA de transferencia en función del resultado de esta verificación.

En una realización en la que los medios 12 de procesamiento comprenden medios criptográficos 13, este resultado de procesamiento es el resultado, obtenido por la unidad criptográfica 13, de una etapa de autenticación de los datos digitales DATA.

Como variante, el resultado de procesamiento es el resultado, obtenido por los medios criptográficos 13, de una etapa de verificación de una firma de los datos digitales DATA.

Esta etapa de verificación puede ser, por ejemplo, el desencriptado de los datos AUTH, realizándose este desencriptado utilizando un algoritmo RSA para obtener un resultado similar al primer resultado HASH1.

En una realización preferida, los medios 26 de control de flujo están adaptados además para obtener datos preliminares directamente a partir de los medios 14 de entrada-salida, mediante la trayectoria 24 de datos representada en la figura 2.

Como variante, los datos preliminares son obtenidos por los medios 26 de control de flujo a partir de un segundo puerto de entrada-salida, por ejemplo utilizando el protocolo conocido con la referencia “T=0” (ISO 7816), estando los medios 14 de entrada-salida reservados para la transferencia de los datos digitales DATA por los medios DMA de transferencia.
La trayectoria 24 de datos también puede ser una trayectoria de datos bidireccional utilizada por los medios 26 de control de flujo para comunicar información a un dispositivo externo a la tarjeta con microcircuito. Esta información puede estar constituida, por ejemplo, por un mensaje de error emitido por los medios 26 de control de flujo cuando estos detectan, a partir de la información de seguridad, la presencia de datos digitales erróneos.

Esta información también puede estar constituida por un flujo de datos que salen de la tarjeta con microcircuito, siendo este flujo de datos el resultado del procesamiento, por los medios 12 de procesamiento, de los datos digitales DATA recibidos por la tarjeta.

Estos datos preliminares comprenden, por ejemplo, datos PASSWD de autenticación, teniéndose estos datos preliminares, sean cuales fueran, en cuenta para controlar la transferencia de los datos digitales por los medios DMA de transferencia.

De este modo, por ejemplo si los datos PASSWD de autenticación no se ajustan a una regla de control predeterminada, pudiendo estar esta regla memorizada en la memoria ROM, los medios 26 de control de flujo no programan a los medios DMA de transferencia para realizar la transferencia de datos digitales entre los medios 14 de entrada-salida y la zona 18 de memorización.

Preferentemente, los datos preliminares comprenden una dirección de memorización de los datos digitales.

En una variante de realización, la tarjeta con microcircuito comprende medios de regulación PLL adaptados para modificar una frecuencia del reloj aplicada a los medios 12 de procesamiento en función de los datos de control DATA_CTRL.

Estos medios de regulación PLL pueden estar constituidos, por ejemplo, por un componente de tipo PLL (*Phase Lock Looping*, en inglés [Bucle de Enganche en Fase]) conocido por el experto en la materia y que permite derivar señales de diferentes frecuencias del reloj, a partir de una señal de un reloj externo no representado.

En la realización preferida, estos medios de regulación PLL están controlados por los medios 26 de control de flujo para ajustar el consumo eléctrico de los medios 12 de procesamiento en función del flujo de datos digitales DATA.

Según la realización seleccionada, los medios DMA de transferencia pueden ser unidireccionales o bidireccionales. La invención se aplica en particular para controlar la transferencia de datos digitales encriptados DATA a partir de la zona 18 de memorización hacia los medios 14 de entrada-salida.

**REIVINDICACIONES**

1. Tarjeta con microcircuito que comprende:

- medios (14) de entrada-salida adaptados para recibir un flujo continuo de datos digitales (DATA);
- medios (12) de procesamiento de estos datos; y
- medios (26) de control de flujo,

estando la tarjeta con microcircuito caracterizada porque los medios (12) de procesamiento comprenden:

- medios (DMA) de transferencia de dicho flujo continuo de datos digitales (DATA) entre los medios (14) de entrada-salida y una zona (18) de memorización; y
- medios (20) de comunicación, con los medios (26) de control de flujo, de datos (DATACTRL) de seguridad obtenidos a partir de dichos datos digitales (DATA),

estando los medios (26) de control de flujo adaptados para controlar la transferencia del flujo continuo de datos digitales (DATA) por los medios (DMA) de transferencia, teniendo en cuenta dichos datos (DATACTRL) de seguridad.

2. Tarjeta con microcircuito según la reivindicación 1, caracterizada porque dichos datos (DATA_CTRL) de seguridad están constituidos al menos en parte por una parte de dichos datos digitales (DATA).

3. Tarjeta con microcircuito según la reivindicación 2, caracterizada porque dichos datos (DATA_CTRL) de seguridad comprenden datos (AUTH) de autenticación de una parte (P1) de los datos digitales recibidos por la tarjeta, estando los medios (26) de control de flujo adaptados para verificar la validez de dichos datos digitales (DATA) a partir de estos datos (AUTH) de autenticación y para controlar dicha transferencia en función del resultado de esta verificación.

4. Tarjeta con microcircuito según una cualquiera de las reivindicaciones 1 a 3, caracterizada porque dichos medios (12) de procesamiento están adaptados para insertar en dichos datos (DATA_CTRL) de seguridad, un resultado de procesamiento de dichos datos digitales (DATA).

5. Tarjeta con microcircuito según la reivindicación 4, caracterizada porque dicho resultado de procesamiento es el resultado de una etapa de autenticación de dichos datos digitales.

6. Tarjeta con microcircuito según una cualquiera de las reivindicaciones 1 a 5, caracterizada porque los medios de control de flujo están adaptados para modificar al menos un parámetro de funcionamiento de dichos medios (DMA) de transferencia.

7. Tarjeta con microcircuito según la reivindicación 6, caracterizada porque dicho parámetro se selecciona entre una dirección de dicha zona (18) de memorización y un parámetro de selección de un protocolo de comunicación entre los medios (14) de entrada-salida y la zona (18) de memorización.

8. Tarjeta con microcircuito según una cualquiera de las reivindicaciones 1 a 7, caracterizada porque dichos medios (12) de procesamiento comprenden una unidad (13) de compresión de datos, una unidad de descompresión de datos, una unidad de encriptado de datos o una unidad de desencriptado de datos.

9. Tarjeta con microcircuito según una cualquiera de las reivindicaciones 1 a 8, caracterizada porque dichos medios (26) de control de flujo están adaptados para detener la transferencia de los datos digitales (DATA) por dichos medios (DMA) de transferencia cuando detectan, a partir de dichos datos (DATA_CTRL) de seguridad, la presencia de datos de autenticación no válidos entre dichos datos digitales (DATA).

10. Tarjeta con microcircuito según una cualquiera de las reivindicaciones 1 a 9, caracterizada porque los medios (26) de control de flujo están adaptados, además, para obtener datos preliminares directamente a partir de los medios (14) de entrada-salida, siendo los datos preliminares tenidos en cuenta también por los medios (26) de control de flujo para autorizar o rechazar la transferencia de los datos digitales (DATA) por los medios (DMA) de transferencia.

11. Tarjeta con microcircuito según la reivindicación 10, caracterizada porque dichos datos preliminares comprenden datos de autenticación (PASSWD).

12. Tarjeta con microcircuito según la reivindicación 10 u 11, caracterizada porque dichos datos preliminares

comprenden una dirección de memorización de dichos datos digitales.

13. Tarjeta con microcircuito según una cualquiera de las reivindicaciones 1 a 12, caracterizada porque comprende además medios de regulación (PLL) adaptados para modificar una frecuencia del reloj aplicada a los medios (12) de procesamiento en función de dichos datos (DATA_CTRL) de seguridad.

14. Tarjeta con microcircuito según una cualquiera de las reivindicaciones 1 a 13, caracterizada porque dichos medios (DMA) de transferencia comprenden un componente DMA.

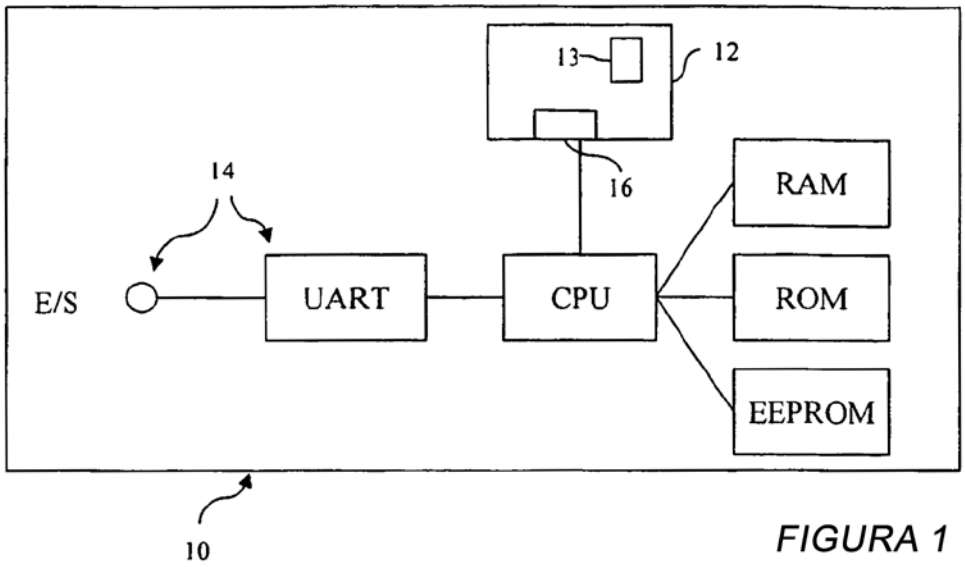


FIGURA 1

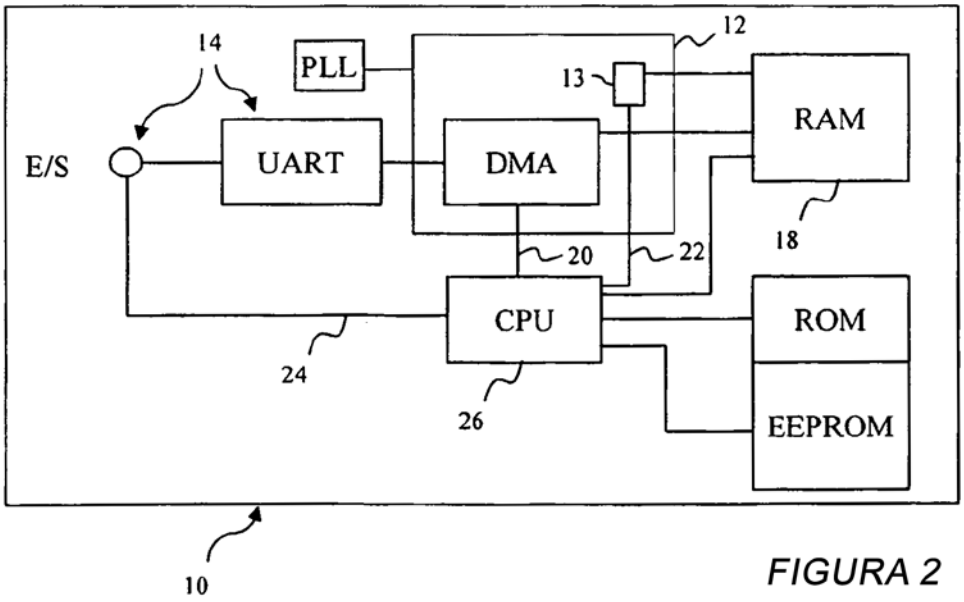


FIGURA 2

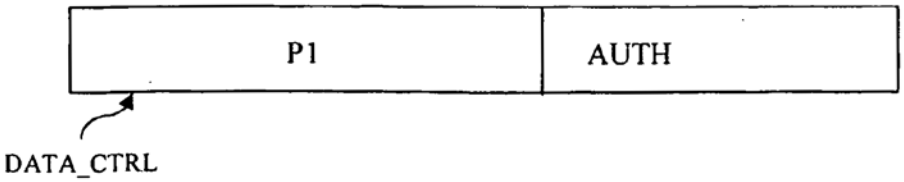


FIGURA 3