(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 763 102**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.12.2016 PCT/FR2016/053318**

(87) Fecha y número de publicación internacional: **15.06.2017 WO17098189**

(96) Fecha de presentación y número de la solicitud europea: **09.12.2016 E 16825821 (8)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2019 EP 3387784**

(54) Título: **Método de personalización de un documento de seguridad**

(30) Prioridad:

10.12.2015 FR 1562108

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.05.2020

(73) Titular/es:

OBERTHUR TECHNOLOGIES (100.0%)
420 Rue d'Estienne d'Orves
92700 Colombes, FR

(72) Inventor/es:

BARREAU, CÉDRIC y
FERAUD, ALBAN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método de personalización de un documento de seguridad

Segundo plano tecnológico

La invención se refiere al ámbito de los documentos de seguridad, tales como las tarjetas bancarias o de identidad y los pasaportes electrónicos, y más concretamente trata sobre la personalización de dichos documentos.

Los documentos de seguridad son documentos que comprenden características físicas que permiten la autenticación fiable del portador del documento y del propio documento. En otras palabras, estas características físicas permiten, a partir de un protocolo de autenticación predeterminado, garantizar que un individuo es el propietario legítimo del documento de seguridad en cuestión y que el documento en sí es un documento auténtico. Estas características físicas (impresiones, materiales especiales, datos digitales grabados…) son generalmente difíciles de falsificar para proteger el documento electrónico contra cualquier acto de mala voluntad.

Los documentos de seguridad se presentan bajo diversas formas más o menos complejas. En particular, cabe señalar los documentos de seguridad denominados "electrónicos" en el sentido de que comprenden un módulo electrónico equipado con al menos una memoria, a diferencia de los documentos de seguridad clásicos, que están desprovistos de una memoria de este tipo. Las tarjetas de identidad, las tarjetas bancarias (generalmente las tarjetas inteligentes) o incluso los pasaportes electrónicos constituyen ejemplos comunes de documentos de seguridad.

Durante su fabricación, estos documentos de seguridad son generalmente personalizados. Esta etapa de personalización consiste en estampar, en y/o dentro el documento de seguridad, datos personales específicos del futuro propietario del documento. Estos datos personales son, por ejemplo, impresos o grabados en la superficie del documento. En el caso de los documentos de seguridad electrónicos, dichos datos personales también se pueden grabar en la memoria del módulo electrónico. Normalmente, durante la personalización de una tarjeta bancaria, el fabricante estampa los datos personales del titular en las caras de la tarjeta (apellido, nombre, número de tarjeta, etc.) y graba datos personales en el chip de la tarjeta.

La **figura 1** muestra esquemáticamente un método de personalización utilizado convencionalmente para personalizar un documento de seguridad. En este ejemplo, una primera entidad 2 (presente en un primer emplazamiento ST2) y una segunda entidad 4 (presente en un segundo emplazamiento ST4) cooperan juntas para realizar la personalización de un documento de seguridad 6.

Para ello, la entidad 2 recoge datos personales específicos del titular de un documento de seguridad 6 que se va a personalizar y, a continuación, convierte (E2) estos datos personales en datos de personalización PR que definen personalizaciones físicas (impresión, grabado, grabación de datos...) para aportarlas al documento de seguridad 6. La entidad 2 envía (E4) posteriormente estos datos de personalización PR a la entidad 4, que a continuación continúa el proceso en el emplazamiento ST4. Para ello, la entidad 4 recibe (E6) los datos de personalización PR y, a continuación, personaliza (E8) el documento de seguridad 6 a partir de los datos de personalización PR.

Sin embargo, este método conocido presenta un riesgo de que un documento de seguridad pueda eventualmente personalizarse con datos personales que no estaban destinados a él. Una entidad 4 puede en efecto personalizar erróneamente (o intencionadamente) el documento de seguridad 6 con datos de personalización asociados a una persona que no sea el propietario legítimo del documento de seguridad. El proceso de personalización se enfrenta hoy en día por lo tanto a importantes riesgos de fiabilidad y seguridad.

Por otra parte, existen problemas de seguridad en el caso de que varias entidades 4 diferentes compartan la responsabilidad de personalizar un conjunto de documentos de seguridad. Existe un riesgo en la medida de que varias entidades 4 (presentes en diferentes sitios) tengan acceso a los datos de personalización PR enviados por la entidad 2. Cuando los datos de personalización PR presentan un carácter confidencial, la dispersión de estos datos entre diversos actores capaces de procesarlos y utilizarlos es problemática.

Por otra parte, la entidad 4 encargada de la personalización goza generalmente de una relativa flexibilidad en cuanto a la elección de los documentos de seguridad en blanco que utiliza cuando realiza la personalización E8. En algunos casos, la entidad 4 tiene la posibilidad de elegir entre varias fuentes de suministro en el documento de seguridad 6. La entidad 2 o un tercero no dispone actualmente de los medios para garantizar que la entidad 4 realice adecuadamente la personalización E8 en un documento de seguridad 6 de un origen específico. Esto da como resultado una incertidumbre económica, especialmente para algunos fabricantes que desean asegurar su actividad de fabricación de documentos de seguridad.

El documento de publicación de solicitud de patente de EE.UU. 2008/0005567 A1 de Johnson describe la personalización de una tarjeta inteligente, o incluso de una aplicación, en base a un conjunto de instrucciones de personalización cifradas.

El documento de publicación de la solicitud de patente EP 1 544 706 A1 de Amador describe un método para cifrar un archivo de datos adecuados para la personalización de una tarjeta inteligente por medio de una clave raíz.

Por lo tanto, hoy en día existe una necesidad de más seguridad y fiabilidad en el proceso de personalización de un documento de seguridad.

Objetivo y resumen

Uno de los objetivos de la invención es remediar las deficiencias de la técnica anterior descritas anteriormente.

Para este propósito, la presente invención se refiere a un método de procesamiento de acuerdo con la reivindicación independiente 1.

La invención permite de forma ventajosa asegurar el proceso de personalización de un documento de seguridad. Para ello, se crea un enlace intrínseco entre los datos de personalización y el documento de seguridad. Esto es posible porque la información de diversificación (que permite cifrar y descifrar los datos de personalización) está presente dentro o en el documento de seguridad, bajo una forma apropiada cualquiera (dato digital grabado en una memoria, patrón físico presente en el documento, etc.). De esta forma, el análisis del documento de seguridad sólo permite recuperar la información de diversificación durante la personalización. En otras palabras, el fabricante que supervisa la personalización sólo puede obtener la información de diversificación DV a partir del propio documento de seguridad. Normalmente, la información de diversificación (y por lo tanto los datos de personalización correspondientes) sólo se pueden recuperar cuando comienza la personalización del documento de seguridad, reduciendo de este modo en gran medida los riesgos de seguridad mencionados anteriormente.

Por otra parte, incluso cuando se dispone de la información de diversificación, la entidad encargada de la personalización se ve limitada en el uso que puede hacer de ella para recuperar datos de personalización. De esta forma, gracias a la invención, una entidad encargada de personalizar un primer documento de seguridad sólo podrá utilizar la información de diversificación presente en dicho primer documento para personalizarlo, y posiblemente los documentos de seguridad pertenecientes al mismo lote que dicho primer documento de seguridad (dependiendo de si esta información de diversificación se asigna de forma única o colectiva a uno o varios documentos de seguridad).

En consecuencia, la invención tiene por objetivo también un programa informático en un soporte de información (o soporte de grabación), siendo este programa susceptible de implementarse en un dispositivo electrónico, en un terminal de lectura, o más generalmente en un ordenador, cuyo programa comprende instrucciones adaptadas a la implementación de las etapas de al menos uno de los métodos definidos anteriormente.

Este programa puede utilizar cualquier lenguaje de programación, y puede ser en forma de código fuente, código objeto o código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada, o en cualquier otra forma deseable.

La invención también se refiere a un sistema de personalización de un documento de seguridad de acuerdo con la reivindicación independiente 14.

El documento de seguridad definido en los modos de ejecución de los métodos y dispositivos anteriores puede ser una tarjeta inteligente, por ejemplo, conforme a la norma ISO/IEC 7816.

Breve descripción de los dibujos

Otras características y ventajas de la presente invención surgirán de la descripción dada a continuación, con referencia a los dibujos adjuntos que ilustran ejemplos de formas de realización desprovistas de cualquier carácter limitativo. En las figuras:

- La figura 1 ya descrita muestra, de forma esquemática, un método convencional de personalización de un documento de seguridad;

- La figura 2 muestra esquemáticamente la estructura de un sistema que comprende un dispositivo de procesamiento y un dispositivo de personalización, de acuerdo con una forma de realización particular de la invención;

- La figura 3 muestra esquemáticamente unos módulos implementados en el dispositivo de procesamiento de la figura 2, de acuerdo con una forma de realización particular de la invención;

- La figura 4 muestra esquemáticamente módulos implementados en el dispositivo de personalización de la figura 2, de acuerdo con una forma de realización particular de la invención;

- La figura 5 muestra, en forma de organigrama, las principales etapas de un método de procesamiento y un método de personalización implementados respectivamente por un dispositivo de procesamiento y un dispositivo de personalización, de acuerdo con una forma de realización particular de la invención;

- La figura 6 muestra esquemáticamente la estructura de un módulo electrónico de un documento de seguridad, de acuerdo con una forma de realización particular de la invención;

- Las figuras 7 y 8 muestran esquemáticamente una variante de la forma de realización de la invención; y

- La figura 9 muestra esquemáticamente una variante de la forma de realización de la invención.

Descripción detallada de varias formas de realización

Como se ha indicado anteriormente, la invención trata sobre la personalización de documentos de seguridad, tales como tarjetas bancarias o de identidad y pasaportes electrónicos, por ejemplo.

En los siguientes ejemplos de formas de realización, el documento de seguridad es una tarjeta inteligente (por ejemplo, conforme a la norma ISO/IEC 7816) que se puede, por ejemplo, utilizar como tarjeta bancaria para realizar operaciones bancarias. Sin embargo, se comprenderá que las tarjetas inteligentes distintas de las tarjetas bancarias y los documentos de seguridad distintos de una tarjeta inteligente se pueden considerar en el ámbito de la invención.

La invención propone asegurar la personalización de un documento de seguridad. Para ello, la invención, según sus diferentes formas de realización, requiere que los datos de personalización sean transmitidos bajo forma cifrada a la entidad encargada de la personalización, siendo realizada la cifrado de los datos de personalización a partir de una información llamada de diversificación asociada al documento de seguridad. Esta información de personalización está presente, por ejemplo, dentro y/o en el documento de seguridad que se va a personalizar. Esta información de personalización puede formar parte del propio documento de seguridad. La entidad encargada de la personalización entonces sólo puede descifrar los datos de personalización si tiene acceso al propio documento de seguridad dentro o en el que se encuentra la información de diversificación. La recuperación de la información de diversificación a partir del documento de seguridad permite descifrar los datos de personalización y, por lo tanto, personalizar el documento de seguridad en cuestión.

A menos que se indique lo contrario, los elementos comunes (o similares) con varias figuras tienen los mismos símbolos de referencia y presentan características idénticas (o similares), de modo que estos elementos comunes generalmente no se describen de nuevo en aras de la simplicidad.

La figura 2 muestra esquemáticamente la estructura de un dispositivo de procesamiento DA implementado bajo la supervisión de una entidad EA, así como la estructura de un dispositivo de personalización DB implementado bajo la supervisión de una entidad EB, de acuerdo con una forma de realización particular. En este caso, los dispositivos EA y EB pueden cooperar juntos para formar un sistema SY.

En el ejemplo considerado en este caso, el dispositivo de procesamiento DA puede preparar la personalización de un documento de seguridad C, es decir, una tarjeta inteligente en este ejemplo. El dispositivo de personalización DB (distinto del documento de seguridad C) puede personalizar la tarjeta inteligente C a partir de los datos de personalización transmitidos por el dispositivo de procesamiento DA.

Más específicamente, el dispositivo de procesamiento DA comprende en este caso un procesador 10, una memoria no volátil 12 y una interfaz de comunicación 14. El dispositivo DA muestra, por ejemplo, la arquitectura de un ordenador.

La memoria 12 es una memoria reescribible no volátil o memoria de sólo lectura (ROM), esta memoria constituye un soporte de grabación (o soporte de informaciones) conforme a una forma de realización particular, legible por el dispositivo de procesamiento DA, y en la cual se graba un programa informático PG1 conforme a una forma de realización particular. Este programa informático PG1 comprende instrucciones para la ejecución de las etapas de un método de procesamiento de acuerdo con una forma de realización particular.

La interfaz de comunicación 14 se puede comunicar con una interfaz de comunicación 24 del dispositivo de personalización DB, según se explica a continuación.

Según se muestra en la **figura 3**, el procesador 10, controlado por el programa informático PG1, y que coopera si es necesario con varios elementos de hardware del dispositivo de procesamiento DA (memorias, etc.), implementa una cierta

cantidad de módulos en este caso, a saber: un módulo de obtención M2, un módulo de cifrado M4 y un módulo de transmisión M6.

El módulo de obtención M2 puede obtener datos de personalización DP para personalizar el documento de seguridad C. En el ejemplo considerado en este caso, el módulo de obtención M2 se configura para obtener datos personales específicos del futuro propietario del documento de seguridad C, y para convertir estos datos personales en datos de personalización DP.

El módulo de cifrado M4 puede cifrar los datos de personalización DP para producir datos cifrados DC, siendo realizado este cifrado a partir de una información de diversificación DV asociada al documento de seguridad C que se desea personalizar. Se supone en este caso que el módulo de cifrado M4 puede recuperar la información de diversificación DV de una manera apropiada. Cabe señalar que, en un ejemplo particular, estos datos de diversificación DV están presentes dentro y/o en el documento de seguridad C. En un ejemplo particular, la información de diversificación DV puede formar parte del propio documento de seguridad C (según se explica a continuación). Sin embargo, no es necesario que el módulo de cifrado M4 (y más generalmente el dispositivo DA) tenga acceso al propio documento de seguridad C para obtener la información de diversificación DV, pudiendo ser transmitida esta última por un tercero o accesible desde una base de datos, por ejemplo.

Como se indica a continuación, en un ejemplo particular, el módulo de cifrado M4 se configura para realizar la cifrado en un contenedor protegido tal como un HSM (Hardware Security Module HSM – módulo de hardware de seguridad).

El módulo de transmisión M6 puede transmitir los datos cifrados DC al dispositivo de personalización DB para permitir a este último personalizar el documento de seguridad C a partir de los datos cifrados DC y de la información de diversificación DV asociada al documento de seguridad C.

Según se muestra en la f**igura 2**, el dispositivo de personalización DB comprende un procesador 20, una memoria no volátil 22 y la interfaz de comunicación 24 ya mencionada anteriormente. Este dispositivo DB puede hacer que el documento de seguridad C se personalice a partir de los datos cifrados DC transmitidos por el dispositivo de procesamiento DA.

La memoria 22 es una memoria no volátil reescribible o una memoria de sólo lectura (ROM), esta memoria constituye un soporte de grabación (o soporte de informaciones) de acuerdo con una forma de realización particular, legible por el dispositivo de personalización DB, y en la cual se graba un programa informático PG2 de acuerdo con una forma de realización particular. Este programa informático PG2 contiene instrucciones para la ejecución de las etapas de un método de personalización de acuerdo con una forma de realización particular.

La interfaz de comunicación 24 se puede comunicar con la interfaz de comunicación 14 del dispositivo de personalización DA, como ya se indicó anteriormente.

Según se muestra en la **figura 4**, el procesador 20, controlado por el programa informático PG2, y que coopera si es necesario con varios elementos de hardware del dispositivo de personalización DB (memorias, etc.), implementa cierta cantidad de módulos en este caso, a saber: un módulo de recepción M20, un módulo de análisis M22, un módulo de descifrado M24 y un módulo de personalización M26.

El módulo de recepción M20 puede recibir los datos cifrados DC enviados por el dispositivo de procesamiento DA. La transmisión de datos cifrados DC del dispositivo DA al dispositivo DB se puede realizar por medio de un enlace de comunicación adecuado, por ejemplo, a través de una red de comunicación (Internet, etc.) o con la ayuda de un soporte adecuado (llave USB, etc.).

El módulo de análisis M22 puede analizar el documento de seguridad C para recuperar la información de diversificación DV asociada con el documento de seguridad C. La información de diversificación DV puede tomar varias formas dependiendo del caso de utilización.

En un ejemplo particular, la información de diversificación DV está presente dentro y/o en dicho documento C. Esta información de diversificación DV puede, por ejemplo, comprender al menos un patrón DV1 formado en la superficie del documento de seguridad C. Este patrón puede comprender, por ejemplo, al menos un carácter, símbolo y/o código gráfico (código de barras, código 2D, etc.). La información de diversificación DV también puede comprender al menos un dato DV2 grabado en una memoria incluida, si es necesario, en el documento de seguridad C, según se explica en detalle a continuación con referencia a la **figura 6.**

En un ejemplo particular, la información de diversificación DV forma parte del propio documento de seguridad C. En otras palabras, la información de diversificación DV puede comprender al menos una característica física que forme parte del documento de seguridad C. La información de diversificación DV está formada, por ejemplo, por al menos una

característica física no clonable del tipo PUF (por "Physical Unclonable Function") del documento de seguridad C. La información de diversificación DV puede, por ejemplo, comprender al menos un patrón formado por la estructura de la totalidad o parte del documento del documento de seguridad C. La información de diversificación DV puede estar formada, por ejemplo, total o parcialmente por un conjunto de fibras que formen parte del documento de seguridad C, presentando estas fibras una disposición o cualquier otra característica que caracterice el documento de seguridad C.

Asimismo, la naturaleza e implementación del análisis del documento C por el módulo de análisis M22 puede variar de acuerdo con el caso en cuestión. El módulo de análisis M22 puede, por ejemplo, utilizar una unidad de lectura óptica (no mostrada) capaz de realizar una detección óptica de la información de diversificación DV1 que figura en la superficie del documento de seguridad C. El módulo de análisis M22 también puede comprender una unidad de lectura de una memoria incluida, si es necesario, en el documento de seguridad C, según se indicó anteriormente.

En un ejemplo particular, la información de diversificación DV no se asocia al documento de seguridad C, sino a un individuo, por ejemplo, el titular legítimo (titular) del documento de seguridad C. En un ejemplo concreto, la información de diversificación DV comprende al menos una característica física del titular del documento de seguridad C, como por ejemplo una huella dactilar del titular, una huella del iris del titular…

El módulo de descifrado M24 puede descifrar los datos cifrados DC recibidos del dispositivo de procesamiento DA para obtener los datos de personalización DP. Este descifrado se realiza a partir de la información de diversificación DV recuperada por el módulo de análisis M22. Según se explica más detalladamente a continuación, según algunas formas de realización, el módulo de descifrado M24 no realiza por sí mismo el descifrado de los datos cifrados, sino que coopera con una entidad (por ejemplo, un contenedor protegido) externa al dispositivo de personalización DB para provocar el descifrado de los datos cifrados.

El módulo de personalización M26 puede causar la personalización del documento de seguridad C a partir de los datos de personalización DP recuperados por el módulo de descifrado M24. Para ello, el módulo de personalización M26 interactúa con todas las unidades de personalización (sistema de impresión, de grabado, de carbonización láser o de grabado, sistema de escritura en memoria, etc.) necesarias para la personalización deseada, estas unidades de personalización (no mostradas) pueden o no estar incluidas total o parcialmente en el dispositivo de personalización DB. Por ejemplo, el módulo de personalización M26 se puede configurar para enviar un comando de impresión a un sistema de impresión externo para realizar una personalización del documento de seguridad C mediante la impresión.

Como ya se indicó, el documento de seguridad C se puede presentar de acuerdo con varias formas. Puede ser o no un documento de seguridad electrónico, que se presenta por ejemplo bajo la forma de una cartilla o una tarjeta.

Según se muestra en la **figura 2**, en este caso se supone que el documento C es una tarjeta inteligente, por ejemplo, de un tipo de tarjeta bancaría, que comprende un módulo electrónico 30 ilustrado en detalle en la f**igura 6**. Por ejemplo, la tarjeta inteligente C puede ser conforme con la norma ISO/IEC 7816.

Más específicamente, el módulo electrónico 30 comprende en este ejemplo el procesador 40, una memoria no volátil 42 en la que se puede grabar una información de diversificación DV2, y una memoria no volátil 43 en la que se puede grabar una clave maestra K1, cuya naturaleza y uso se explicarán a continuación.

El módulo electrónico 30 puede ser, por ejemplo, un módulo de identidad de suscriptor *integrado*, designado de otro modo con la apelación eUICC por "*embedded Universal Integrated Circuit Chip*".

En una forma de realización, el módulo electrónico 30 puede contener, en la memoria no volátil 42 y/o 43, la resultante de la diversificación de la clave maestra K1 por la información de diversificación DV1 y/o DV2.

Las memorias no volátiles 40 y 42 pueden ser la misma memoria física.

Como ya se indicó, el patrón DV1 formado en la superficie de la tarjeta C constituye un primer ejemplo de información de diversificación DV. La información DV2 almacenada en la memoria 42 constituye un segundo ejemplo de información de diversificación DV. De acuerdo con una forma de realización particular, la información de diversificación DV comprende DV1 y DV2.

Además, la **figura 2** muestra en este caso una personalización 32a de la tarjeta inteligente C realizada por impresión o grabado, por ejemplo. Otros tipos de personalización de la tarjeta inteligente C son posibles, tal como la personalización eléctrica del módulo electrónico 30 en el presente caso. La personalización realizada por la entidad DB también puede comprender una configuración específica del módulo electrónico 30 o la grabación de datos de personalización en el módulo electrónico 30.

Ahora se describe una forma de realización particular con referencia a la f**igura 5**. Más concretamente, el dispositivo de procesamiento DA implementa un método de procesamiento para preparar la personalización del documento de seguridad C, ejecutando el programa informático PG1. Del mismo modo, el dispositivo de personalización DB implementa un método de personalización ejecutando el programa informático PG2.

En el transcurso de una etapa A2, el módulo de obtención M2 del dispositivo de procesamiento DA obtiene los datos de personalización DP ya mencionados anteriormente, definiendo estos datos una personalización del documento de seguridad C a realizar. Para ello, el módulo de obtención M2 obtiene, por ejemplo, datos personales asociados al futuro titular del documento de seguridad C y, a continuación, convierte estos datos personales en datos de personalización DP que se pueden utilizar por el dispositivo de personalización DB.

En el transcurso de una etapa A4, el módulo de cifrado M4 cifra (o encripta) los datos de personalización DP, a partir de la información de diversificación DV, para producir los datos cifrados DC. Los datos de personalización DP se asocian (o enlazan) de este modo al documento de seguridad C que se va a personalizar.

Para recuperar la información de diversificación DV, el dispositivo de procesamiento de DA no tiene necesariamente que tener acceso al documento de seguridad C en sí. Normalmente, la entidad EA que supervisa la ejecución del dispositivo de procesamiento DA no tiene el documento de seguridad C en su poder durante la realización del método de procesamiento para preparar la personalización del documento de seguridad C.

La información de diversificación DV puede, por ejemplo, ser transmitida por un tercero al dispositivo de procesamiento DA, o ser accesible, por ejemplo, desde una base de datos externa al dispositivo de procesamiento DA; pudiendo ser el soporte utilizado, por ejemplo, un contenedor protegido tal como un HSM (Hardware Security Module – módulo de hardware de seguridad).

En este ejemplo, se supone que la información DV2 grabada en el módulo electrónico 30 de la tarjeta C constituye la información de diversificación DV. Alternativamente, el patrón DV1 se podría utilizar como información de diversificación DV (o DV1 y DV2 en combinación).

En una forma de realización particular, durante el cifrado A4, los datos de personalización DP se cifran a partir de una clave maestra de cifrado K1 en combinación con la información de diversificación DV. La clave maestra K1 (o "master key" en inglés) se almacena, por ejemplo, en una memoria no volátil del dispositivo de procesamiento DA.

El módulo de transmisión M6 envía (A6) a continuación los datos cifrados DC al dispositivo de personalización DB para que éste último pueda personalizar el documento de seguridad C a partir de estos datos cifrados DC y la información de diversificación DV asociada al documento de seguridad.

El módulo de recepción M20 del dispositivo de personalización DP recibe la información cifrada DC en el transcurso de una etapa B6.

Por otra parte, el módulo de análisis M22 analiza (B8) el documento de seguridad C para recuperar la información de diversificación DV presente dentro o en el documento de seguridad C, a saber: la información DV2 almacenada en la memoria 42 en este ejemplo. Para ello, el módulo de análisis M22 efectúa una lectura de la memoria 42 del módulo 30 para recuperar la información DV2. Cabe señalar que la recuperación de la información de diversificación DV mediante el dispositivo de personalización DB sólo es posible en este caso en la medida en que el módulo electrónico 30 sea accesible para lectura por el módulo de análisis M22.

De manera más general, es necesario generalmente que la entidad EB esté en posesión del propio documento de seguridad C para que se pueda realizar el análisis B8.

La etapa de análisis B8 se puede realizar, si es necesario, antes de la etapa de recepción B6.

En el transcurso de una etapa B10, el módulo de descifrado M24 descifra (o desencripta) los datos cifrados DC para obtener los datos de personalización DP. Este descifrado B10 se realiza a partir de la información de diversificación DV (es decir, la información DV2) recuperada en la etapa B8.

Como se describió anteriormente, en una forma de realización particular, los datos de personalización DP se cifran, durante el cifrado A4, a partir de una clave maestra de cifrado K1 en combinación con la información de diversificación DV. Siempre en esta forma de realización, durante el descifrado B10, los datos cifrados DC se pueden descifrar a partir de una clave maestra de descifrado K1a en combinación con la información de diversificación DV. Esta clave maestra de descifrado K1a se almacena, por ejemplo, en la memoria no volátil 43 del módulo electrónico 30.

De acuerdo con una primera forma de realización, las claves maestras K1 y K1a utilizadas respectivamente por el cifrado A4 y el descifrado B10 son idénticas (en el caso del cifrado simétrico). De acuerdo con una segunda forma de realización,

las claves maestras K1 y K1a son claves maestras emparejadas que son diferentes entre sí (en el caso de un cifrado asimétrico). En este último caso, la clave maestra de cifrado K1 sólo permite realizar el cifrado, mientras que la clave maestra de descifrado K1a sólo permite realizar el descifrado.

En el transcurso de una etapa B12, el módulo de personalización M26 a continuación provoca la personalización del documento de seguridad C a partir de los datos de personalización DP recuperados en la etapa de descifrado B10. La personalización puede comprender, por ejemplo, una modificación física en la superficie del documento de seguridad C o incluso una configuración eléctrica del módulo electrónico 30. La personalización B12 puede comprender, por ejemplo, la formación (mediante impresión, grabado, carbonización láser, etc.) en la superficie del documento de seguridad C de patrones 32a (caracteres, símbolos, número de serie, fotos, etc.). La personalización B12 también puede comprender la grabación de datos de personalización DP (o cualquier otra configuración eléctrica apropiada) en una memoria del módulo electrónico 30.

Cabe señalar que el módulo de personalización M26 puede incluir los sistemas de impresión, de grabado en relieve, de lectura de memoria, etc., necesarios para la personalización deseada. Alternativamente, el módulo de personalización M26 se puede configurar para enviar al menos un comando necesario para activar la operación de personalización adecuada.

La invención permite de forma ventajosa asegurar el proceso de personalización de un documento de seguridad. Para ello, se crea un enlace intrínseco entre los datos de personalización y el documento de seguridad. Esto es posible porque la información de diversificación (que se utiliza para cifrar y descifrar los datos de personalización) está asociada al documento de seguridad. Un vínculo de este tipo es posible, en particular, cuando la información de diversificación está presente en el documento de seguridad dentro o en el documento de seguridad, en cualquier forma apropiada (datos digitales grabados en una memoria, patrón físico presente en el documento, PUF, etc.). Por lo tanto, sólo el análisis del documento de seguridad permite recuperar la información de diversificación durante la personalización. En otras palabras, el fabricante EB que supervisa la personalización sólo puede obtener la información de diversificación DV a partir del propio documento de seguridad. Normalmente, la entidad EB sólo podrá recuperar la información de diversificación DV (y, por lo tanto, los datos de personalización correspondientes) cuando proceda con la personalización del documento de seguridad en cuestión.

Por otra parte, incluso cuando está en posesión de la información de diversificación DV, la entidad EB está limitada en la utilización que puede hacer para recuperar los datos de personalización. Por lo tanto, gracias a la invención, la entidad EB encargada de personalizar un primer documento de seguridad sólo podrá utilizar la información de diversificación DV presente en dicho primer documento para personalizarlo, y posiblemente los documentos de seguridad pertenecientes al mismo lote que dicho primer documento de seguridad.

En un ejemplo particular, una información de diversificación DV se asigna de forma única a un documento de seguridad C determinado, de modo que la obtención de la información de diversificación DV a partir de un documento de seguridad no permita obtener datos de personalización destinados a otros documentos de seguridad. Alternativamente, la misma información de diversificación se atribuye de forma colectiva a varios (por ejemplo, al menos un lote) de documentos de seguridad. El análisis de un documento de seguridad permite entonces recuperar datos de diversificación válidos para la personalización de un conjunto de documentos de seguridad.

Por otra parte, la invención tiene como consecuencia que la entidad EB encargada de realizar la personalización no tenga más la posibilidad de elegir entre varias fuentes de suministro para obtener el documento de seguridad. Sólo el documento de seguridad conocido por la entidad EA (y cuyos datos de diversificación son conocidos por ella) pone a la entidad EB en posición de descifrar los datos cifrados necesarios para personalizar el documento de seguridad en cuestión.

De acuerdo con una forma de realización descrita en referencia a las f**iguras 7** y **8**, el dispositivo de procesamiento DA puede utilizar un contenedor protegido H1 para realizar el cifrado A4. Del mismo modo, el dispositivo de personalización DB puede utilizar un contenedor protegido H2 para realizar el descifrado B10.

Un contenedor protegido (o caja fuerte digital) puede grabar claves criptográficas y, si es necesario, realizar operaciones de cifrado o descifrado con la ayuda de dichas claves. Un contenedor protegido puede ser del tipo HSM (por "*Hardware Security Module*") o se puede presentar bajo la forma de una tarjeta inteligente (o "*batchcard" en* inglés).

De acuerdo con un ejemplo particular, el contenedor protegido H1 está contenido en la memoria del dispositivo de procesamiento DA. De acuerdo con otro ejemplo de forma de realización, el dispositivo de procesamiento DA puede cooperar con el contenedor protegido H1 situado esta vez fuera del dispositivo de procesamiento DA, para realizar el cifrado A4.

Del mismo modo, de acuerdo con un ejemplo particular, el contenedor protegido H2 está contenido en la memoria del dispositivo de personalización DB. De acuerdo con otro ejemplo de forma de realización, el dispositivo de personalización

DB puede cooperar con el contenedor protegido H2 situado esta vez fuera del dispositivo de personalización DB, para realizar el descifrado B10.

Según se muestra en la f**igura 7**, el contenedor protegido H1 contiene en la memoria la clave maestra de cifrado K1 según se mencionó anteriormente. Durante el transcurso del cifrado A4, el dispositivo de procesamiento DA (más específicamente el módulo de cifrado M4) envía (S2) la información de diversificación DV al contenedor protegido H1. A partir de la información de diversificación DV y de la clave maestra de cifrado K1 contenida en la memoria, el contenedor protegido H1 determina (S4) una clave derivada K2 realizando una función criptográfica F2 tomando como entrada DV y K1. El dispositivo de procesamiento DA también envía (S6) los datos de personalización DP al contenedor protegido H1. A partir de la clave derivada K2 y de los datos de personalización DP, el contenedor protegido H1 produce (S8) los datos cifrados DC realizando una función criptográfica F4 tomando como entrada K2 y DP. Una vez producidos, estos datos cifrados DC son entregados (S10) por H1 al dispositivo de procesamiento DA.

De acuerdo con una variante de forma de realización, la clave maestra de cifrado K1 no se almacena en el contenedor protegido H1, sino que éste último puede recibir esta clave maestra K1 desde el exterior (de DA, por ejemplo) para determinar la clave derivada K2 de la clave maestra K2 en combinación con la información de diversificación DV.

Según se muestra en la f**igura 8,** el contenedor protegido H2 actúa de manera similar al contenedor protegido H1 para realizar el descifrado B10.

Más específicamente, el contenedor protegido H2 contiene en memoria la clave maestra de descifrado K1a ya mencionada anteriormente. En el transcurso del descifrado B10, el dispositivo de personalización DB (más específicamente el módulo de descifrado M24) envía (S20) la información de diversificación DV recuperada durante el análisis B8 al contenedor protegido H2. A partir de la información de diversificación DV y de la clave maestra de descifrado K1a contenida en la memoria, el contenedor protegido H2 determina (S22) la clave derivada K2a ya mencionada anteriormente realizando la función criptográfica F2a tomando como entrada DV y K1a.

De acuerdo con un primer ejemplo, las claves maestras K1 y K1a son idénticas (cifrado asimétrico). En este caso, las funciones F2 y F2a realizadas por los contenedores H1 y H2 respectivamente son idénticas, y las claves derivadas K2 y K2a obtenidas al ejecutar las funciones F2 y F2a respectivamente son idénticas.

De acuerdo con un segundo ejemplo, las claves maestras K1 y K1a son claves emparejadas distintas entre sí (cifrado asimétrico). En este caso, las funciones F2 y F2a ejecutadas por los contenedores H1 y H2 respectivamente son diferentes, y las claves derivadas K2 y K2a obtenidas al ejecutar las funciones F2 y F2a respectivamente son diferentes.

De acuerdo con una variante de forma de realización, la clave maestra de descifrado K1a no se graba en el contenedor protegido H2, pero éste último puede recibir esta clave maestra K1a desde el exterior (desde la DB, por ejemplo) para determinar la clave derivada K2a a partir de la clave maestra K1a en combinación con la información de diversificación DV.

Según se muestra en la **figura 8**, el dispositivo de personalización DB también envía (S24) los datos cifrados DC al contenedor protegido H2. A partir de la clave derivada K2a y de los datos cifrados DC, el contenedor protegido H2 produce (S26) los datos de personalización DP realizando una función criptográfica F6 tomando como entradas K2a y DC. Una vez producidos, estos datos de personalización DP son entregados (S28) por H2 al dispositivo de personalización DB.

La utilización de contenedores protegidos permite asegurar los medios criptográficos (en particular las claves maestras K1 y K2) necesarios para cifrar y descifrar los datos de personalización. En efecto, confiar una clave maestra K1, K1a sin protección a una tercera entidad puede presentar un riesgo en la medida en que es posible, a partir de una clave maestra de este tipo, realizar ingeniería inversa para recuperar información sensible. Gracias a la utilización de contenedores protegidos, una entidad encargada de personalizar un documento de seguridad no tendrá acceso directo a la propia clave maestra (estando esta contenida en dicho contenedor de forma segura). La utilización de contenedores protegidos permite cifrar o descifrar de forma segura los datos de personalización.

Sin embargo, en algunos casos, un riesgo persiste cuando una entidad tiene en su poder un contenedor protegido que contiene dicha clave maestra. De hecho, en la hipótesis de que se despliegen recursos suficientes en este sentido, siempre es probable que se obtengan datos sensibles de un contenedor protegido de este tipo. Por ejemplo, la entidad EA (o un tercero) puede, por ejemplo, no tener la suficiente confianza en la entidad EB como para dejarla de manera prolongada en un contenedor protegido de este tipo.

Para paliar este problema, de acuerdo con una forma de realización particular, la presente invención propone que el contenedor protegido que permite el descifrado de datos cifrados esté a su vez contenido en una memoria del documento de seguridad que se desea personalizar.

Más concretamente, de acuerdo con una forma de realización particular, el contenedor protegido H2, descrito anteriormente con referencia a la f**igura 8**, está incluido en el documento de seguridad C, más concretamente en el módulo electrónico 30 en el ejemplo considerado en este caso. El dispositivo de personalización DP puede cooperar con el módulo electrónico 30 del documento de seguridad C para permitir la ejecución de las etapas S20 a S28 ya descritas.

En esta forma de realización particular, el dispositivo de personalización DB, y más generalmente la entidad EB que lo supervisa, tiene acceso al contenedor protegido H2 - y por lo tanto indirectamente a la clave maestra K1 - sólo cuando posee el documento de seguridad C que se va a personalizar. En ausencia del documento de seguridad C, el contenedor protegido H2 está fuera del alcance de la entidad EB, reduciendo de este modo los riesgos de seguridad mencionados anteriormente.

En los ejemplos descritos con referencia a la **figura 8**, el contenedor protegido H2 puede implementar la función criptográfica F6, mientras que el contenedor protegido H2 se puede implementar en el documento de seguridad C si es necesario. De acuerdo con una variante de forma de realización ilustrada en la **figura 9**, el contenedor protegido H2, que se puede implementar en el módulo electrónico 30 del documento de seguridad C si es necesario, contiene la clave maestra de descifrado K1a y puede realizar la función criptográfica F2a para obtener la clave derivada K2a. En cambio, la función criptográfica F6 se ejecuta fuera del documento de seguridad C y, por tanto, fuera del contenedor protegido H2. En este caso, el contenedor protegido H2 se configura, por ejemplo, para transmitir (S23) la clave derivada K2a a un terminal T externo al documento de seguridad C y, por tanto, externo al contenedor protegido H2. El terminal externo T puede ser, por ejemplo, el dispositivo de procesamiento DB. El terminal externo T puede ejecutar la función F6 a partir de la clave derivada K2a y de los datos cifrados DC, para obtener (S27) los datos de personalización DP. Si es necesario, el terminal externo T puede transmitir (S29) los datos de personalización DP al dispositivo de procesamiento DB. Esta forma de realización es ventajosa cuando el documento de seguridad C que se va a personalizar no dispone de los recursos necesarios para realizar la operación de descifrado.

En un ejemplo particular, cuando el contenedor protegido H2 que contiene la clave maestra de cifrado K1a se implementa en el documento C, el dispositivo de personalización DB, y más generalmente la entidad EB que lo supervisa, tiene acceso a la clave derivada K2a, y por lo tanto indirectamente a la clave maestra de descifrado K1a, sólo cuando posee el documento de seguridad C que se va a personalizar. En ausencia del documento de seguridad C, la clave maestra de descifrado K1a y la clave derivada K2a están fuera del alcance de la entidad EB, reduciendo de este modo los riesgos de seguridad mencionados anteriormente.

De acuerdo con una variante de la forma de realización descrita anteriormente con referencia a la **figura 9**, la clave maestra de descifrado K1a no se graba en el contenedor protegido H2, pero este último puede recibir esta clave maestra K1a (de la BD, por ejemplo) para determinar la clave derivada K2a a partir de la clave maestra K1a y la información de diversificación DV.

De acuerdo con una forma de realización particular, el contenedor H1 (respectivamente H2) no realiza la función F2 (respectivamente F2a), ni contiene K1 (respectivamente K1a). Contiene sólo la clave K2 (respectivamente K2a).

De acuerdo con una forma de realización particular, los contenedores H1 y H2 no realizan las funciones F2 y F2a respectivamente, ni contienen K1 y K1a respectivamente. Únicamente contienen las claves K2 y K2a respectivamente.

Por ejemplo, los contenedores protegidos H1 y H2 pueden cada uno recibir la clave derivada K2 y K2a respectivamente desde el exterior para realizar las funciones F4 y F6 respectivamente.

Según se describió anteriormente, la invención permite realizar una personalización de forma segura de un documento de seguridad. Cabe señalar, sin embargo, que se pueden considerar otras aplicaciones de la invención. En efecto, es posible utilizar la invención para un fin distinto de la personalización de un documento de seguridad.

De forma más general, la invención tiene por objetivo transmitir de forma segura datos asociados a un documento de seguridad desde una primera entidad hacia una segunda entidad.

El experto en la técnica comprenderá que las formas de realización y las variantes descritas anteriormente sólo constituyen ejemplos no limitativos de implementación de la invención. En particular, el experto en la técnica podrá considerar cualquier adaptación o combinación de las formas de realización y variantes descritas anteriormente para dar respuesta a una necesidad muy particular.

De acuerdo con una forma de realización, la invención se implementa por medio de componentes de software y/o hardware. Con esta óptica, el término "módulo" empleado en esta presentación se puede referir tanto a un componente de software, así como a un componente de hardware o a un conjunto de componentes de hardware y software.

REIVINDICACIONES

1. Método de personalización, implementado por un sistema (SY) que comprende un dispositivo de procesamiento (DA) y un dispositivo de personalización (DB), para personalizar un documento de seguridad (C), comprendiendo dicho método las siguientes etapas realizadas por el dispositivo de procesamiento (DA):

- obtención (A2) de datos de personalización (DP) para personalizar el documento de seguridad;

- cifrado (A4) de los datos de personalización, a partir de una información de diversificación (DV) asociada al documento de seguridad, para producir datos cifrados (DC), en los que, durante el cifrado, los datos de personalización (DP) se cifran a partir de una clave maestra de cifrado (K1) en combinación con la información de diversificación; y

- transmisión (A6) de los datos cifrados a un dispositivo de personalización (DB) para permitir a este último personalizar el documento de seguridad a partir de los datos cifrados y la información de diversificación;

comprendiendo dicho método además las siguientes etapas realizadas por el dispositivo de personalización (DB):

- recepción (B6) de los datos numéricos (CC);

- análisis (B8) del documento de seguridad para recuperar la información de diversificación (DV) asociada a dicho documento de seguridad;

- descifrado (B10) de los datos cifrados de una clave maestra de descifrado (K1a) en combinación con la información de diversificación para obtener datos de personalización (DP); y

- personalización (B12) del documento de seguridad a partir de los datos de personalización, que comprende una modificación física en la superficie del documento de seguridad (C).

2. Método de acuerdo con la reivindicación 1, en donde la información de diversificación (DV) está presente dentro o en el documento de seguridad (C).

3. Método de acuerdo con la reivindicación 1 o 2, en donde la clave maestra de cifrado (K1) se empareja con la clave maestra de descifrado (K1a) distinta de la clave maestra de cifrado (K1).

4. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en donde el dispositivo de procesamiento utiliza un contenedor protegido (H1) para realizar dicho cifrado, siendo grabada la clave maestra de cifrado (K1) en el contenedor protegido,

en el que dicho contenedor protegido:

- determina una clave derivada (K2) a partir de la información de diversificación y la clave maestra de cifrado (K1), y

- cifra, a partir de la clave derivada (K2), los datos de personalización (DP) para producir los datos cifrados (DC).

5. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en donde el documento de seguridad comprende una memoria (42) en la que se graba al menos una parte (DV2) de la información de diversificación, comprendiendo el análisis la lectura de la memoria para recuperar dicha al menos una parte de la información de diversificación.

6. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en donde el dispositivo de personalización (DB) coopera con un contenedor protegido (H2) para causar dicho descifrado,

en donde dicho contenedor protegido descifra (S26) los datos cifrados (DC) recibidos por el dispositivo de personalización para obtener dichos datos de personalización (DP).

7. Método de acuerdo con la reivindicación 6, en donde el contenedor protegido (H2):

- determina (S22) una clave derivada (K2a) a partir de la clave maestra de descifrado (K1a) y a partir de la información de diversificación (DV) recuperadas por el dispositivo de personalización (DB) durante dicho análisis; y

- descifra (S26), a partir de la clave derivada (K2a), los datos cifrados (DC) recibidos por el dispositivo de personalización para obtener dichos datos de personalización (DP).

8. Método de acuerdo con la reivindicación 6, cooperando el dispositivo de personalización (DB) con el contenedor protegido (H2) para provocar dicho descifrado,

en donde dicho contenedor protegido:

- determina (S22) una clave derivada (K2a) a partir de la clave maestra de descifrado (K1a) y a partir de la información de diversificación (DV) recuperada por el dispositivo de personalización (DB) durante dicho análisis; y

- transmite la clave derivada (K2a) a un terminal externo para que éste último descifre (S27) los datos cifrados (DC) para obtener dichos datos de personalización (DP).

9. Método de acuerdo con una cualquiera de las reivindicaciones 6 a 8, en donde el documento de seguridad (C) comprende un módulo electrónico (30) que puede implementar el contenedor protegido (H2).

10. Método de acuerdo con una cualquiera de las reivindicaciones 6 o 9 siendo grabada la clave maestra de descifrado (K1a) en el contenedor protegido (H2).

11. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 10, en donde al menos una parte de la información de diversificación recuperada durante dicho análisis comprende un patrón (DV1) formado en la superficie del documento de seguridad.

12. Programa informático (PG1; PG2) que comprende instrucciones para la ejecución de las etapas de un método de acuerdo con una cualquiera de las reivindicaciones 1 a 11 cuando dicho programa se ejecuta mediante un ordenador.

13. Sistema (SY) que comprende un dispositivo de procesamiento (DA) y un dispositivo de personalización (DB), para personalizar un documento de seguridad (C), comprendiendo el dispositivo de procesamiento (DA):

- un módulo de obtención (M2) configurado para obtener datos de personalización para personalizar el documento de seguridad;

- un módulo de cifrado (M4) configurado para cifrar los datos de personalización a partir de una información de diversificación (DV) asociada al documento de seguridad o a un individuo, para producir datos cifrados, en donde el módulo de cifrado se configura para cifrar los datos de personalización (DP) a partir de una clave maestra de cifrado (K1) en combinación con la información de diversificación; y

- un módulo de transmisión (M6) configurado para transmitir los datos cifrados a un dispositivo de personalización para permitir a este último personalizar el documento de seguridad a partir de los datos cifrados y la información de diversificación;

comprendiendo el dispositivo de personalización (DB):

- un módulo de recepción (M20) configurado para recibir los datos cifrados;

- un módulo de análisis (M22) configurado para analizar el documento de seguridad para recuperar la información de diversificación asociada a dicho documento de seguridad;

- un módulo de descifrado (M24) configurado para descifrar los datos cifrados a partir de una clave maestra de descifrado (K1a) en combinación con la información de diversificación para obtener datos de personalización (DP); y

- un módulo de personalización (M26) configurado para personalizar el documento de seguridad a partir de los datos de personalización, realizando una modificación física en la superficie del documento de seguridad (C).

14. Sistema de acuerdo con la reivindicación 13, en donde al menos parte de la información de diversificación recuperada por el módulo de análisis comprende un patrón (DV1) formado en la superficie del documento de seguridad.

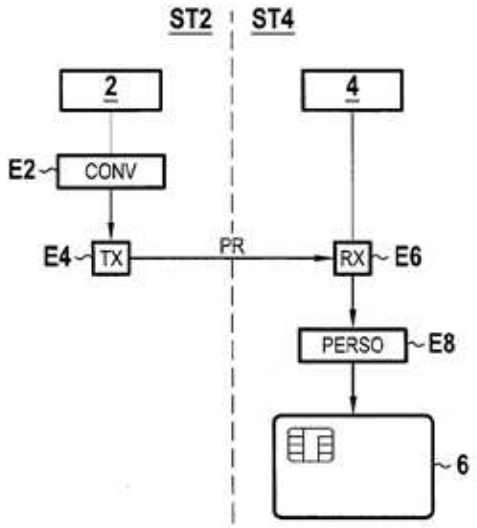

FIG.1

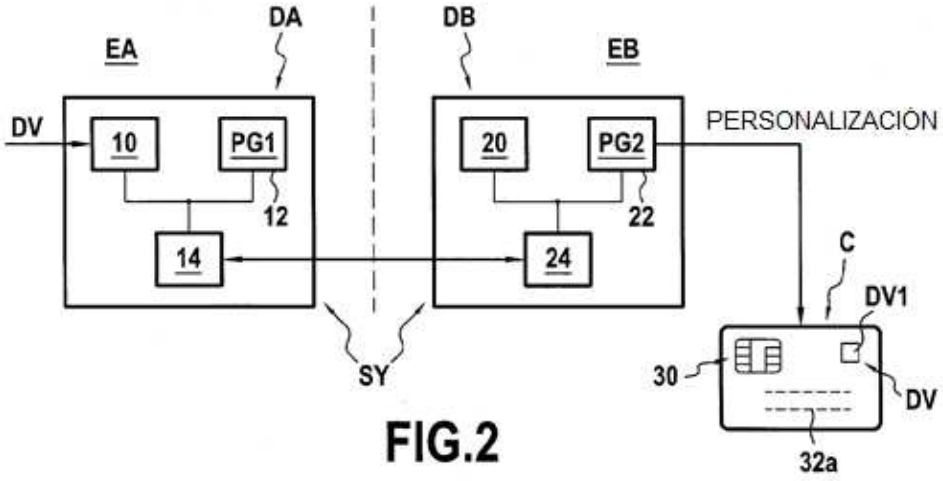

FIG.2

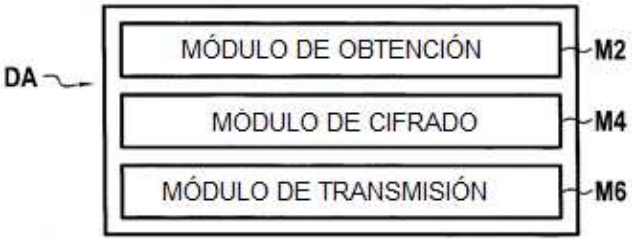

FIG.3

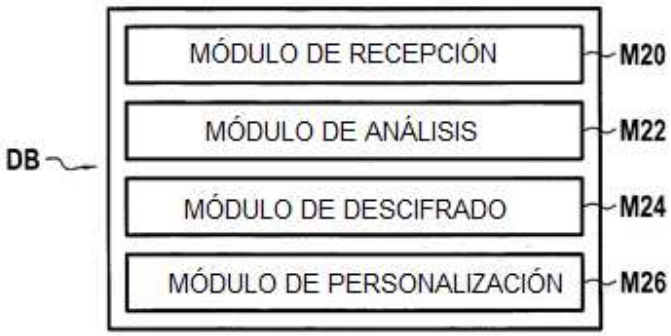

FIG.4

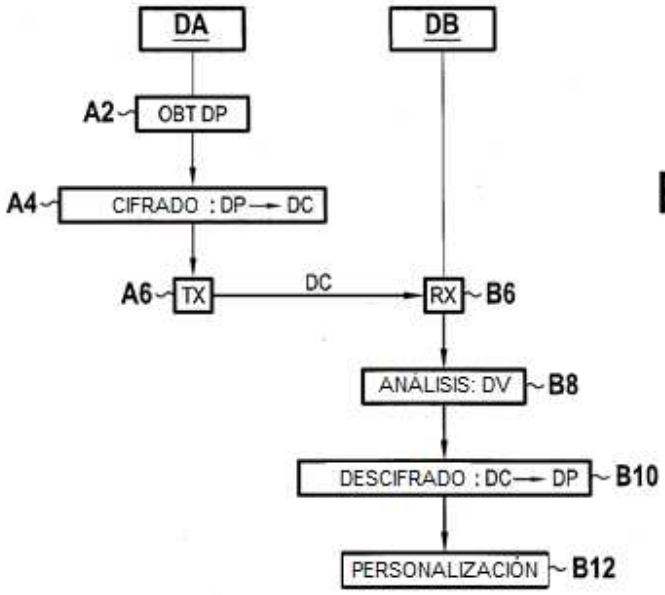

FIG.5

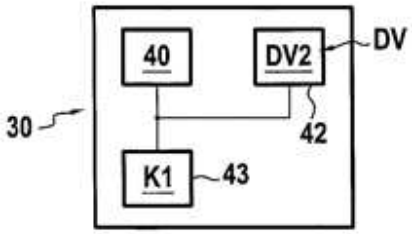

FIG.6

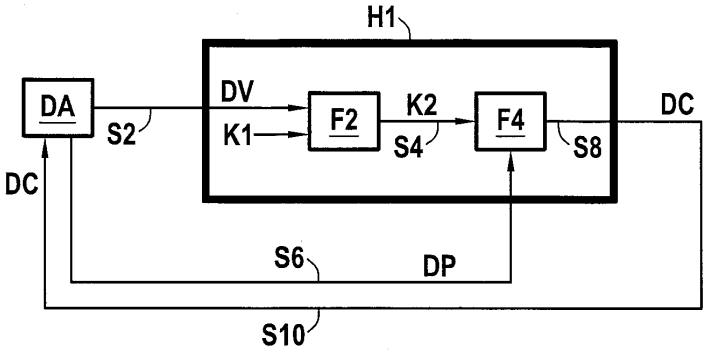

FIG.7

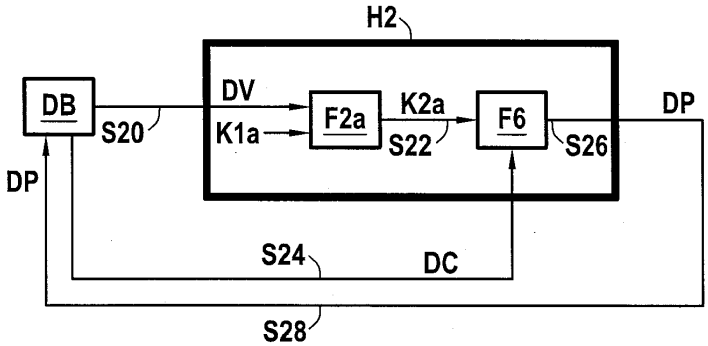

FIG.8

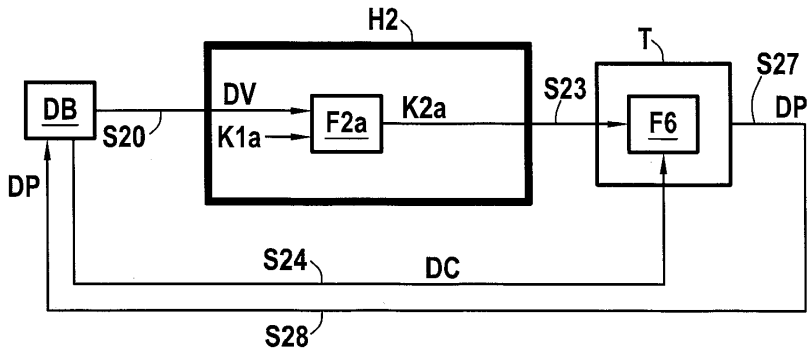

FIG.9