(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 786 267**

(51) Int. CI.:

G06F 21/44 (2013.01)
G06Q 20/34 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G07F 7/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.11.2015 E 15196381 (6)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 3032450**

(54) Título: **Procedimiento de control de una autenticidad de un terminal de pago y terminal así asegurado**

(30) Prioridad:

09.12.2014 FR 1462139

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.10.2020

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris , FR

(72) Inventor/es:

NACCACHE, DAVID y
SARRADIN, JEAN-LOUIS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de control de una autenticidad de un terminal de pago y terminal así asegurado

1. Dominio

La técnica propuesta se refiere al dominio de los terminales de pago. La técnica propuesta se refiere más particularmente a la seguridad de los terminales de pago.

2. Técnica anterior

Los terminales de pago son objeto de numerosas tentativas de ataques. En efecto, por la naturaleza de la información que contiene y por la sensibilidad de los datos que trata, el terminal de pago es un objeto que posee un gran valor para las personas malintencionadas. Un cierto tipo de fraude se ha extendido recientemente: se trata de sustituir un terminal de pago válido por un terminal de pago falsificado. El terminal de pago válido es sustituido en un comercio e inmediatamente reemplazado por un terminal de pago con un aspecto de validez, pero que en realidad ha sido modificado, por ejemplo para leer y copiar los datos de las tarjetas bancarias de los clientes, ya sea completamente y vaciado de su contenido, que ha sido sustituido por un simple material de lectura y de registro de datos de clientes. El comerciante no advertido puede fácilmente ser engañado y no darse cuenta del fraude hasta pasados varios días.

Una manera para resolver este problema de sustitución puede consistir en la aplicación de una marca en el terminal. Tal marca permite al comerciante darse cuenta de la sustitución de su terminal. Esta técnica es eficaz a partir del momento en el que el estafador no es capaz él mismo de reproducir esta marca. Esta técnica está pues limitada por la capacidad del estafador de reproducir la marca. O, para que una marca sea eficaz, debe ser visible. Si es visible, esta marca es igualmente visible para el estafador, el cual puede fácilmente reproducirla. Así, esta solución simple de aplicación de una marca no es en realidad eficaz.

Otra manera de resolver este problema es no disponer más que de terminales de pago por cable, es decir terminales de pago conectados físicamente a una caja registradora por ejemplo. Esta solución es ciertamente eficaz, pero en realidad está poco adaptada a la práctica actual que consiste en ofrecer una mayor movilidad a los comerciantes. No obstante, esta técnica es utilizada por ejemplo en las grandes superficies o en ciertos tipos de almacenes.

Las técnicas existentes están sin embargo limitadas cuando se trata de prevenir o de impedir la realización del fraude en comercios de menor envergadura. Existe por lo tanto la necesidad de suministrar una técnica que permita al comerciante detectar un fraude por la sustitución de un terminal y que permita prevenirse contra los efectos negativos de tal fraude.

La publicación de la solicitud de patente francesa FR2824659 A1 describe un procedimiento de verificación de la integridad de un terminal durante una transacción utilizando una tarjeta de memoria, comprendiendo el procedimiento las etapas de: suministro al titular de la tarjeta de memoria de un criptograma calculado utilizando unas informaciones legibles en la memoria de la tarjeta; -en una transacción, lectura por el terminal de informaciones en la memoria de la tarjeta y cálculo por el terminal de un criptograma utilizando las informaciones leídas en la memoria de la tarjeta; y -la visualización por el terminal de destino del titular de la tarjeta del criptograma calculado. El titular de la tarjeta de memoria puede así comparar el criptograma suministrado por el terminal al criptograma al que ha sido proporcionado. Esto le permite suponer que el terminal es íntegro, y que no ha sido objeto de manipulaciones fraudulentas.

3. Resumen

La técnica propuesta no presenta estos inconvenientes de la técnica anterior. Más particularmente, la técnica propuesta se refiere a un método de verificación de una autenticidad de un terminal de pago que comprende una etapa de obtención de al menos una información externa a dicho terminal de pago y al menos una etapa de tratamiento de dicha información externa, proporcionando dicha etapa de tratamiento una información cifrada y una etapa de comparación de la información cifrada obtenida con al menos una información correspondiente, inaccesible para el terminal de pago.

Así, la comparación entre la información cifrada obtenida a partir del terminal de pago y el dato de referencia correspondiente a esta información cifrada permite verificar si el terminal de pago es un terminal auténtico o si se trata de un terminal comprometido. No se trata en esta divulgación de verificar una identidad del terminal de pago (por ejemplo un número de serie cifrado u otro dato de este tipo), sino hacer un desafío al terminal de pago y verificar si el terminal de pago es capaz de producir una respuesta correcta a este desafío. Si el terminal no está a la altura de advertir el desafío o bien si el resultado de este desafío es malo, se detecta entonces simplemente que el terminal es una “falsedad”, es decir que el terminal está modificado.

Más específicamente, la técnica descrita se refiere a un Procedimiento de tratamiento de un dato inicial tal como reivindicado en la reivindicación 1.

Así, de una manera simple, el usuario está preparado para conocer dos aspectos de seguridad importantes que son por una parte la capacidad del terminal de responder al reto que se le ha propuesto: si el terminal no es capaz de obtener la información externa, entonces se deduce inmediatamente que el terminal está comprometido. Por otra parte, si el terminal es capaz de comprender que se le ha propuesto un reto, entonces se obtiene una restitución del resultado del reto.

Según una característica particular, posteriormente a dicha etapa de restitución de dicho dato tratado, una etapa de verificación de una concordancia entre dicho dato tratado y un dato de referencia.

Así la restitución del reto (propuesto al terminal) es comparada con una información de referencia en posesión del comerciante (por ejemplo una tarjeta específica que comprende el resultado del reto). Si el resultado suministrado por el terminal es diferente de este dato de referencia, se puede concluir que el terminal está comprometido.

Según una característica particular, dicha etapa de obtención pone en práctica un lector de tarjetas con chip.

Con respecto a otras técnicas (como por ejemplo una entrada al teclado), existen dos ventajas: por una parte el comerciante no conoce él mismo el reto propuesto al terminal; por otra parte, el lector de la tarjeta con chip, teniendo en cuenta la naturaleza del terminal, está extremadamente bien asegurado: es por tanto muy difícil para un atacante intentar obtener este dato inicial antes de robar el terminal al comerciante para modificarlo y comprometerle.

Según una característica particular, dicha etapa de tratamiento de dicho dato inicial comprende una etapa de cifrado de dicho dato inicial.

Así, a diferencia de las técnicas anteriores que se conforman con descifrar una identidad (como un número de serie) que está cifrado dentro del terminal, la presente técnica cifra la información transmitida. A partir de entonces el terminal no tiene necesidad de conocer una información complementaria: utiliza una información que ya posee (una clave de cifrado) para transformar, al menos en parte, el dato inicial.

Según una característica particular dicha etapa de cifrado es una etapa de desmenuzamiento de dicho dato inicial con la ayuda de una clave privada registrada en una memoria asegurada del terminal de pago.

Así, la obtención del dato tratado es simple y rápida.

Según una característica particular, dicha etapa de restitución comprende una etapa de impresión del dato tratado, con la ayuda de una impresora de dicho terminal de pago.

Según otro aspecto, la técnica descrita se refiere igualmente a un terminal de pago tal como está reivindicado en la reivindicación 7.

La invención se refiere igualmente a un dispositivo de control tal como está reivindicado en la reivindicación 9.

Según una puesta en práctica preferida, las diferentes etapas de los procedimientos según la técnica propuesta son aplicadas por uno o varios soportes lógicos o programas de ordenador, que comprenden unas instrucciones de soporte lógico destinadas a ser ejecutadas por un procesador de datos de un módulo de relé según la técnica propuesta y estando concebido para dirigir la ejecución de las diferentes etapas de los procedimientos.

En consecuencia, la técnica propuesta apunta también a un programa susceptible de ser ejecutado por un ordenador o por un procesador de datos, teniendo este programa las instrucciones para dirigir la ejecución de las etapas de un procedimiento tal como se ha mencionado anteriormente.

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

La técnica propuesta apunta también a un soporte de información legible por un procesador de datos, y que tiene las instrucciones de un programa tal como el anteriormente mencionado.

El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, tal como un ROM, por ejemplo un CD ROM o un ROM de circuito microelectrónico, o incluso un medio de registro magnético, por ejemplo un disquete (floppy disc) o un disco duro.

Por otra parte, el soporte de información puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede ser encaminada por medio de un cable eléctrico u óptico, por radio o por otros medios. El programa según la técnica propuesta puede ser en particular telecargado en una red de tipo Internet.

Alternativamente, el soporte de informaciones puede ser un circuito integrado en el que está incorporado el programa, estando el circuito adaptado para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

Según un modo de realización la técnica propuesta es puesta en práctica por medio de componentes de soporte lógico y/o de soporte físico. En esta óptica el término “módulo” puede corresponder en este documento también a un componente de soporte lógico, como a un componente de soporte físico o a un conjunto de componentes de soportes materiales y de soportes lógicos.

Un componente de soporte lógico corresponde a uno o varios programas de ordenador, uno o varios subprogramas de un programa, o de una manera más general a cualquier elemento de un programa o de un soporte lógico apto para poner en práctica una función o un conjunto de funciones, según lo que se describe más adelante para el módulo en cuestión. Tal componente de soporte lógico es ejecutado por un procesador de datos de una entidad física (terminal, servidor, pasarela, enrutador, etc) y es susceptible de acceder a los recursos materiales de esta entidad física (memorias, soportes de registro, bus de comunicación, tarjetas electrónicas de entradas/salidas, interfaces de usuario, etc.).

De la misma manera, un componente material corresponde a cualquier elemento de un conjunto de soporte físico (o hardware) apto para aplicar una función o un conjunto de funciones según lo que se describe más adelante para el módulo en cuestión. Se puede tratar de un componente material programable o con un procesador integrado para la ejecución del soporte lógico, por ejemplo un circuito integrado, una tarjeta con chip, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microsoporte lógico (firmware), etc.

Cada componente del sistema antes descrito pone en marcha bien entendido sus propios módulos de soporte lógico.

Los diferentes modos de realización antes mencionados son combinables entre sí para la puesta en práctica de la técnica propuesta.

4. Figuras

Otras características y ventajas de la técnica propuesta aparecerán más claramente por la lectura de la siguiente descripción de un modo de realización preferencial, dado a título de simple ejemplo ilustrativo y no limitativo, y de los dibujos anejos, entre los cuales:

- la figura 1 presenta un cuadro sinóptico de la técnica propuesta;
- la figura 2 explica la fase de tratamiento de la información inicial;
- la figura 3 describe un dispositivo de control y de verificación de autenticidad;
- la figura 4 describe un terminal de pago que integra un elemento de verificación de autenticidad.

5. Descripción

5.1 Recordatorio del principio

El comerciante confrontado al vuelo y a la modificación de uno o varios terminales de pago sufre a menudo una pérdida financiera importante. Desde entonces es necesario suministrar a este comerciante un medio simple y eficaz de verificación de la autenticidad del terminal que él posee. Para hacer esto, la técnica actualmente divulgada propone comparar el resultado de una operación interna realizada por el terminal de pago con un resultado esperado (dato de referencia), previamente conocido por el comerciante. Si el dato de referencia es idéntico a la operación interna efectuada por el terminal se considera que el terminal no está comprometido. El resultado esperado (dato de referencia) puede adoptar diversas formas, siendo la más simple desde el punto de vista del tratamiento que realizar, un conjunto de caracteres numéricos o alfanuméricos. Otras formas de resultados esperados pueden igualmente ser puestos en práctica, como imágenes, sonidos. El principio general de la técnica propuesta está descrito en relación con la figura 1.

De una manera general, el método propuesto, puesto en práctica por un terminal de pago (POS), comprende:

- una etapa de obtención (10) de al menos una información externa a dicho terminal de pago, denominado dato inicial (DI);
- una etapa de tratamiento (20) de dicho dato inicial (DI), que entrega un dato tratado (DT);
- una etapa de restitución visual y/o sonora (30) de dicho dato tratado (DT).

Posteriormente, a la restitución por el terminal de pago del dato tratado, el comerciante (COM) efectúa una comparación (40) de este dato tratado (DT) con un datos de referencia (DR) correspondiente en su posesión. Cuando el dato de referencia difiere del dato tratado restituido por el terminal de pago, el comerciante puede deducir que el terminal de pago está comprometido (es decir, que el terminal de pago ha experimentado una modificación no autorizada). Cuando el dato de referencia es igual al dato tratado, el compromiso del terminal de pago no está probado y el comerciante puede utilizarlo con un grado de confianza razonable.

En al menos un modo de realización, para ser más eficaz, posteriormente a la restitución del dato tratado por el terminal, éste espera, por parte del comerciante, la confirmación de que el dato tratado es idéntico al dato de referencia. Esta confirmación puede adoptar la forma de una presión sobre una tecla del terminal de pago. El terminal de pago puede entonces funcionar normalmente.

En al menos un modo de realización de la técnica propuesta, el terminal de pago no puede realizar la transacción cuando la verificación de la autenticidad del terminal no ha sido efectuada. Se sabe que durante su puesta en marcha (por ejemplo diariamente), el terminal de pago efectúa las verificaciones de rutina necesarias para su funcionamiento. En este modo de realización se propone añadir la verificación divulgada en la presente técnica. Esta verificación se convierte entonces en obligatoria. Sin esta verificación el terminal no puede funcionar. Consiste en requerir al principio el suministro de la información externa. Si el comerciante es capaz de suministrar esta información externa, entonces el terminal aplica la técnica de verificación antes descrita.

Si el comerciante (o cualquier otra persona) no es capaz de suministrar el dato inicial o que no confirme que el dato tratado es idéntico al dato de referencia (véase el modo de realización anterior), el terminal no se inicia.

En un segundo modo de realización de la técnica propuesta el terminal de pago dispone, a elección, de al menos dos métodos de obtención de la información externa. En este modo de realización, el terminal de pago está solo para decidir la manera en la que la información externa debe ser obtenida. En este modo de realización, el primer modo de obtención de la información externa es por ejemplo la inserción de una tarjeta de verificación (tarjeta con chip o tarjeta de tira) específicamente prevista a este efecto. El segundo modo de obtención de la información externa es por ejemplo, con la ayuda del teclado del terminal de pago, la incautación de una serie de datos numéricos o alfanuméricos. De manera complementaria, esta serie de datos numéricos o alfanuméricos es imprimida en la tarjeta de verificación. Un tercer modo de obtención puede por ejemplo consistir en una captura (con la ayuda de un lector de código de barras), de un código de barras en dos dimensiones que contiene la información externa. El terminal de pago decide, alternativamente y al azar, utilizar uno u otro de los métodos de obtención a su disposición. Así, el comerciante puede constatar visualmente la discontinuidad de las solicitudes de obtención del terminal de pago y tener inmediatamente, antes mismamente de la incautación, una información susceptible de informar al comerciante sobre el buen funcionamiento del terminal: no es en efecto muy poco probable que el terminal requiera la obtención de la información externa de una manera idéntica a cada verificación. Desde entonces, con este modo de realización se aumenta todavía el nivel de seguridad. Sin embargo, tal modo de aplicación de la técnica descrita debería ser reservado a ciertos tipos de entornos particularmente difíciles, susceptibles de hacer frente a numerosos ataques por parte de estafadores.

5.2 Descripción de un modo de realización

Como previamente se ha indicado, la técnica propuesta consiste en ofrecer la posibilidad, por ejemplo al comerciante o a cualquier otra persona a cargo de la gestión de los terminales de pago, de verificar si el terminal de pago es un terminal auténtico o si es un terminal comprometido (es decir, que por ejemplo ha sido subtitulado y modificado).

En este modo de realización (simple) de la técnica propuesta, el comerciante dispone de una tarjeta, preferiblemente una tarjeta con chip, de verificación de la autenticidad. El tratamiento en este modo de realización está presentado en relación con la figura 2.

La tarjeta de verificación se utiliza en dos momentos: en la obtención de la información externa, la tarjeta (Crd) es insertada (E10) en el terminal (POS); más específicamente la información externa está codificada en la tarjeta (bien en el chip de la tarjeta, o bien en la banda magnética de ésta); el segundo momento en el curso del cual la tarjeta (Crd) es utilizada durante la verificación (E40) por el comerciante: el dato de referencia (DR) es imprimido en la tarjeta (Cdr). A partir de entonces es fácil para el comerciante comparar el dato de referencia con el dato restituido por el terminal de pago.

En este modo de realización, para más facilidad para el comerciante, la restitución (E30) del dato tratado (DT) es efectuada realizando una impresión (E31) de esta información (DT) en un recibo. Este recibo, denominado recibo de verificación, es imprimido por la impresora del terminal de pago. Alternativamente, si el terminal no posee una impresora, el dato tratado es mostrado en la pantalla del terminal de pago. La ventaja de disponer de un recibo impreso reside en la ausencia de la necesidad de conservar el terminal en mano para efectuar una verificación y por tanto una ausencia de necesidad de verificar que se ha efectuado un control del terminal.

En este modo de realización, la información externa (dato inicial) suministrada al terminal por la tarjeta es el ATR (del inglés *"Answer to Reset"*). El ATR es la respuesta a la reinicialización. Una respuesta a una reinicialización (ATR) es un mensaje de salida por un contacto de la tarjeta con chip conforme a la norma ISO 7816 / CEI, tras la reinicialización eléctrica del chip de la tarjeta por el terminal de pago. El ATR transmite unas informaciones sobre los parámetros de comunicación propuestos por la tarjeta, y la naturaleza y el estado de la tarjeta. Un ejemplo de ATR es "3B 02 14 50". Esta información externa no está disponible para el terminal. Depende de la tarjeta. Así, la ventaja de la utilización del ATR con respecto a otras informaciones es que se forma un par "tarjeta/terminal". Así, una característica interesante en el marco de la presente técnica es disponer de un dato inicial relativamente único, del

que se puede asegurar que el conocimiento y la reproducción por un atacante es muy difícil de obtener sin robar la tarjeta.

Cuando el terminal está en posesión de este dato inicial, aplica sobre éste un tratamiento informático. Este tratamiento tiene como objeto transformar el dato inicial (DI) que es el ATR en un dato que puede ser comparado (DR). El interés es hacer esta transformación propia al terminal de pago que la efectúa: esto significa que un terminal que está comprometido no suministrará el mismo resultado que un terminal auténtico.

Varias posibilidades de transformación pueden ser utilizadas. Una posibilidad interesante es aplicar (E20) una función de desmenuzamiento en el ATR con la ayuda de una clave privada (CC) del terminal de pago. La ventaja obtenida por esta solución es que la clave privada del terminal de pago no puede ser comprometida, incluso si este terminal debiera ser robado y modificado: existen en efecto unos mecanismos de protección internos del terminal que implican un borrado de la memoria asegurada del terminal cuando se ha detectado una tentativa de apertura o de modificación del terminal.

Desde entonces, incluso si el terminal es sustituido, modificado y devuelto al comerciante sin que éste no se aperciba de la desaparición momentánea del terminal, la modificación efectuada habrá necesariamente implicado un borrado de la memoria asegurada del terminal. Como esta memoria es la que contiene las claves públicas y privadas del terminal, se ha asegurado que el terminal comprometido que es devuelto al comerciante no disponga más que de las mismas claves que cuando ha sido robado. Así, el resultado de la función de desmenuzamiento efectuada en el ATR de la tarjeta será necesariamente diferente del resultado no comprometido. El comerciante puede así apercibirse rápidamente de que su terminal ha sido comprometido.

De manera complementaria una rotación binaria del dato inicial es efectuada antes de la operación de cifrado. Esta rotación binaria es efectuada según un parámetro de rotación binaria predeterminado, que es propio del terminal. El parámetro de rotación binaria es inyectado en la memoria asegurada del terminal, de manera aleatoria, en el momento de su fabricación y/o de su configuración a la salida de la cadena de fabricación. Así, el parámetro de rotación binaria es potencialmente diferente de un terminal a otro, lo que hace todavía más difícil una falsificación del terminal pues además de la obtención de las claves de cifrado, el atacante debe igualmente procurarse el parámetro de rotación binaria.

5.3 Otras características y ventajas

Según otro aspecto, la técnica descrita se refiere igualmente a un dispositivo de verificación de la autenticidad del terminal presentado en relación con la figura 3. Más particularmente, la divulgación se refiere también a un dispositivo de verificación externa (30) que comprende por una parte el dato inicial (DI) y por otra parte el dato de referencia (DR).

En la invención, el dispositivo externo se presenta bajo la forma de una tarjeta con chip, que comprende por una parte el dato de referencia, en relieve sobre la tarjeta y que comprende por otra parte un chip cuya única función es disponer de un dato específico, denominado dato inicial, obtenido tras una reinicialización de la tarjeta por el terminal de pago. En este caso, este dato comprendido en la tarjeta con chip es una respuesta a una reinicialización (ATR). En la invención el método presentado propuesto comprende, en la parte del terminal, una etapa de reinicialización de la tarjeta con chip insertada en el lector de la tarjeta con chip del terminal de pago.

Se describe, en relación con la figura 4, un terminal de pago que comprende unos medios que permiten la ejecución del procedimiento antes descrito.

Por ejemplo, el terminal de pago comprende una memoria 41 constituida por una memoria tampón, una unidad de tratamiento 42, equipada por ejemplo por un microprocesador, y pilotada por el programa de ordenador 43, poniendo en práctica lo necesario para la puesta en práctica de las funciones de pago.

En la inicialización, las instrucciones del código del programa de ordenador 43 son por ejemplo cargadas en una memoria antes de ser ejecutadas por el procesador de la unidad de tratamiento 42. La unidad de tratamiento 42 recibe como entrada por ejemplo un dato externo al terminal, denominado dato inicial. El microprocesador de la unidad de tratamiento 42 pone en práctica las etapas del procedimiento de verificación de la autenticidad, según las instrucciones del programa de ordenador 43 para permitir al comerciante verificar la autenticidad del terminal.

Para esto, el terminal de pago comprende, además de la memoria tampón 41, los medios de obtención de una información externa a dicho terminal de pago, denominado dato inicial; presentándose estos medios bajo la forma de un lector de tarjeta con chip. El terminal comprende igualmente los medios de tratamiento, especialmente criptográfico del dato inicial para entregar un dato tratado; comprendiendo estos medios de tratamiento por ejemplo un procesador de seguridad o un procesador de cifrado; comprendiendo el terminal igualmente uno o varios juegos de claves de cifrados a fin de realizar el tratamiento del dato inicial y suministrar un dato tratado que pueda ser comparado con un dato de referencia. Para que el dato tratado pueda ser comparado, el terminal comprende igualmente unos medios de restitución de este dato tratado. Estos medios de restitución se presentan por ejemplo bajo la forma de una impresora de papel, que puede imprimir sobre un recibo el dato tratado. Estos medios de

restitución se presentan igualmente por ejemplo bajo la forma de una interfaz hombre-máquina específica, mostrada en la pantalla del terminal, que muestra el dato tratado.

Estos medios pueden ser pilotados por el procesador de la unidad de tratamiento 42 en función del programa de ordenador 43.

REIVINDICACIONES

1. Procedimiento de tratamiento de un dato inicial para autorizar un control de la autenticidad de un terminal de pago con la ayuda de dicho dato inicial, realizando el procedimiento en dicho terminal de pago:

- una etapa de obtención (10) de al menos una información externa a dicho terminal de pago, dicho dato inicial (DI), siendo dicho dato inicial (DI) una respuesta a la reinicialización (ATR) transmitida por una tarjeta con chip posteriormente a su inserción en dicho terminal de pago;

- una etapa de tratamiento criptográfico (20) de dicho dato inicial (DI), que entrega un dato tratado (DT);

- una etapa de restitución visual y/o sonora (30) de dicho dato tratado (DT).

2. Procedimiento de tratamiento según la reivindicación 1, el cual comprende además, posteriormente a dicha etapa de restitución (30) de dicho dato tratado (DT), una etapa de verificación (40), por un usuario de dicho terminal de pago, de una concordancia entre dicho dato tratado (DT) y un dato de referencia (DR).

3. Procedimiento de tratamiento según la reivindicación 1, en el cual dicha etapa de obtención (10) pone en práctica un lector de tarjeta con chip.

4. Procedimiento de tratamiento según la reivindicación 1, en el que dicha etapa de tratamiento (20) de dicho dato inicial (DI) comprende una etapa de cifrado de dicho dato inicial.

5. Procedimiento de tratamiento según la reivindicación 4, en el que dicha etapa de cifrado es una etapa de desmenuzamiento de dicho dato inicial con la ayuda de una clave privada registrada en una memoria del terminal de pago.

6. Procedimiento de tratamiento según la reivindicación 1, en el que dicha etapa de restitución comprende una etapa de impresión de dicho dato tratado con la ayuda de una impresora de dicho terminal de pago.

7. Terminal de pago configurado para verificar su autenticidad con la ayuda de un dato inicial, comprendiendo el terminal de pago:

- un módulo configurado para obtener al menos una información externa a dicho terminal de pago, denominado dato inicial (DI), siendo dicho dato inicial (DI) una respuesta a la reinicialización (ATR) transmitida por una tarjeta con chip posteriormente a su inserción en dicho terminal de pago;

- un módulo configurado para tratar criptográficamente dicho dato inicial (DI) y entregar un dato tratado (DT);

- un módulo configurado para restituir de manera visual y/o sonora dicho dato tratado (DT).

8. Producto de programa de ordenador telecargable desde una red de comunicación y/o almacenado sobre un soporte legible por ordenador y/o ejecutable por un microprocesador, caracterizado porque comprende instrucciones de código de programa para la ejecución de un procedimiento de tratamiento según la reivindicación 1, cuando es ejecutado en un procesador.

9. Dispositivo de control configurado para efectuar un control de autenticidad de un terminal de pago, siendo el dispositivo de control una tarjeta con chip que comprende:

- una información externa a dicho terminal de pago, denominada dato inicial (DI), siendo dicho dato inicial apto para ser transmitido a dicho terminal de pago por medio de una interfaz de comunicación, siendo dicho dato inicial (DI) una respuesta a la reinicialización (ATR) transmitida por dicho dispositivo de control posteriormente a su inserción en dicho terminal de pago;

- un dato de referencia (DR), inscrito sobre una cara visible de dicho dispositivo de control, destinado a ser utilizado para efectuar una verificación de una concordancia entre un dato tratado (DT), obtenido por el terminal de pago a partir de un tratamiento criptográfico de dicho dato inicial (DI), y dicho dato de referencia (DR).

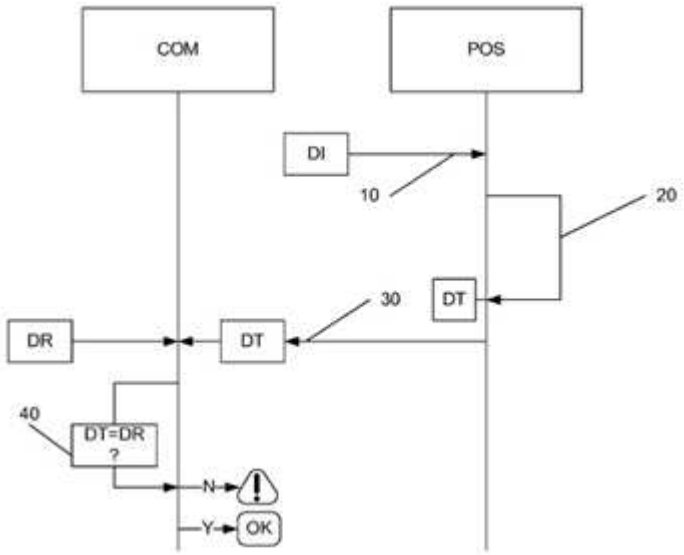

Figura 1

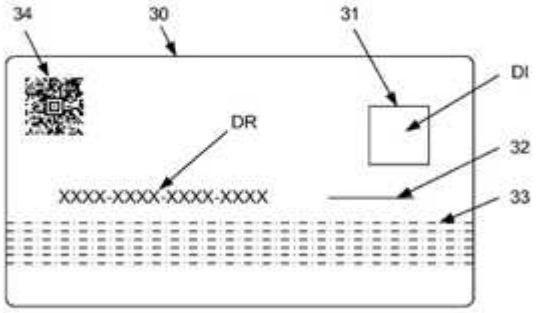

Figura 3

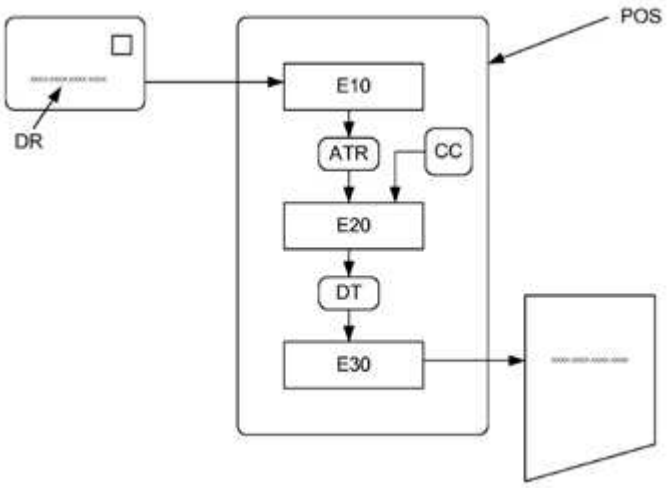

Figura 2

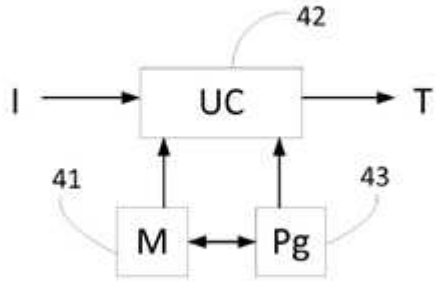

Figura 4