(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 673 187**

(51) Int. CI.:

G07F 7/10 (2006.01)
G07F 7/08 (2006.01)
G06Q 20/34 (2012.01)
G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.02.2009 E 09152319 (1)**

(97) Fecha y número de publicación de la concesión europea: **04.04.2018 EP 2091028**

(54) Título: **Procedimiento de detección de tarjetas no auténticas con microprocesador, tarjeta con microprocesador, terminal lector de tarjetas y programas correspondientes**

(30) Prioridad:

12.02.2008 FR 0850888

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.06.2018

(73) Titular/es:

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

(72) Inventor/es:

NACCACHE, DAVID

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de detección de tarjetas no auténticas con microprocesador, tarjeta con microprocesador, terminal lector de tarjetas y programas correspondientes.

1. Campo de la invención

El campo de la invención es el de la lucha contra la falsificación de objetos con microprocesador seguro, denominado en lo sucesivo chip electrónico.

Más en particular, la invención se refiere a la detección de fraudes, de intentos de fraude o de cualesquiera otros actos ilícitos con el concurso de objetos con chip copiados, falsificados, imitados, o clonados, por personas malintencionadas.

La invención es de especial aplicación en las tarjetas inteligentes.

2. Técnica anterior

Se describe en lo sucesivo, a título de ejemplo, la utilización de estas tarjetas inteligentes como tarjetas de pago que, de manera conocida, son utilizadas, por ejemplo, para abonar compras en el establecimiento de un comerciante o para efectuar un reintegro de billetes en un cajero automático (DAB).

Claro es que otras aplicaciones, tales como el acceso a un sitio o a un servicio, son conocidas también y tratadas de igual manera. Igualmente, se comprende que la noción de “tarjeta inteligente” se puede generalizar o otros tipos de objetos portátiles equipados con un microprocesador seguro.

Las especificaciones de las tarjetas inteligentes que funcionan con un contacto eléctrico están definidas por la norma internacional ISO 7816 de la Organización Internacional de Normalización (“International Organization for Standardization” en inglés). Estas especificaciones son públicas y accesibles a todos y, por tanto, especialmente, a las personas malintencionadas.

En particular, la norma ISO 7816-4 especifica el contenido de los mensajes (comandos, respuestas) entre una tarjeta inteligente y un lector de tarjetas, así como las estructuras de los datos contenidos en estos mensajes (mejora de la seguridad de las comunicaciones). Los comandos base para la lectura, la escritura y la actualización de los datos de una tarjeta inteligente mediante un lector de tarjetas, y que en lo sucesivo se denominarán “comandos estándar y públicos”, son, por ejemplo:

- un comando de seguridad (verificar un número de identificación personal, denominado PIN, por ejemplo);
- un comando de personalización (escribir en la memoria);
- un comando de pago (operar a débito, operar a crédito);
- un comando de criptografía (firmar un bloque de datos, verificar la firma, generar una clave);
- un comando de gestión de los archivos (seleccionar, leer, escribir, crear).

El estándar internacional de seguridad EMV (abreviatura en inglés de Europay, Mastercard y Visa (marcas registradas)), que es específico del ámbito bancario, establece las reglas necesarias para la interoperabilidad internacional entre las tarjetas de pago y los terminales lectores de tarjetas, permitiendo efectuar transacciones de manera segura, cualquiera que sea el emisor de la tarjeta de pago y cualquiera que sea el terminal lector de tarjetas.

Un falsificador (perpetrador de fraude) que ha extraído de una tarjeta legítima o auténtica (es decir, puesta en el mercado por los fabricantes autorizados de tarjetas inteligentes) la información que le permite reproducir su comportamiento lógico puede, a partir de las especificaciones públicas mencionadas anteriormente, programar un circuito electrónico comprado en el comercio para producir una tarjeta clonada o no auténtica (denominada en lo sucesivo “clon”).

Con anterioridad se ha tratado de impedir la clonación de las tarjetas de pago auténticas mediante la utilización de claves criptográficas, asociando a una tarjeta de pago un número de identificación personal (NIP), al que también denominamos PIN (en inglés, “Personal Identification Number”), código confidencial o código secreto, y del que se supone que tan solo lo conoce el titular (usuario autorizado) de la tarjeta de pago.

El documento WO 01/86601 A describe un método que permite a un dispositivo (de tipo terminal) autenticar un objeto portátil, tal como, por ejemplo, una tarjeta inteligente. Para ello, se ha previsto el envío al objeto portátil, por parte del terminal, de una orden de cálculo de firma. En lugar de enviar a la tarjeta una variable aleatoria convencional constituida por un número definido por el servidor, el terminal envía una orden de cálculo en forma de un mensaje.

El documento EP 0427601 A describe un método que permite autenticar una tarjeta con microprocesador utilizada, por ejemplo, en un terminal de televisión de pago, permitiendo tal tarjeta desaleatorizar programas recibidos por el terminal. La autenticación está regida mediante mensajes de autenticación producidos por un centro de gestión y puede comprender, por ejemplo, al menos dos operaciones combinatorias diferentes efectuadas en la tarjeta a partir de un número secreto ("firma") memorizado en la tarjeta.

3. Inconvenientes de la técnica anterior

Sin embargo, tal técnica no ofrece todas las garantías contra la clonación de las tarjetas de pago, ya que un código confidencial asociado a una tarjeta de pago puede ser desvelado, bien en los locales del fabricante de tarjetas inteligentes, con motivo de la personalización de la tarjeta, o bien en los locales del emisor de la tarjeta (el proveedor de servicios, tal como un operador telefónico o un organismo bancario, por ejemplo) con fines malintencionados o a consecuencia de un ataque de un perpetrador de fraude.

Una tarjeta de pago clonada, si ha sido programada eficazmente, es difícilmente diferenciable de una tarjeta de pago auténtica, siendo sus comportamientos lógicos idénticos, aunque no incluyan el mismo circuito electrónico y, a día de hoy, no existe un método de detección eficaz capaz de detectar tarjetas de pago clonadas.

4. Objetivos de la invención

La invención tiene como objetivo principal subsanar estos inconvenientes de la técnica anterior.

Más concretamente, es un objetivo de la invención proporcionar una técnica eficaz de lucha contra la falsificación de tarjetas inteligentes, o de un objeto portátil similar.

Es otro objetivo de la invención detectar las tarjetas no auténticas, denominadas clones, e impedir su utilización.

Asimismo, la invención tiene como objetivo proporcionar una técnica de este tipo que sea relativamente económica, fiable y simple en su puesta en práctica.

5. Explicación de la invención

La invención propone una novedosa solución que no presenta el conjunto de estos inconvenientes de la técnica anterior, en forma de un procedimiento según la reivindicación independiente 1. De este modo, el procedimiento según la invención permite una verificación de la autenticidad de una tarjeta inteligente basándose en el reconocimiento y/o en el tratamiento por la tarjeta inteligente de un comando secreto (distinto, pues, de aquellos normalizados o públicos) transmitido por un terminal lector de tarjetas. Al haber sido insertado con anterioridad el comando secreto en cada tarjeta inteligente auténtica, solo una tarjeta inteligente auténtica puede reconocer y/o tratar de manera correcta tal comando secreto cuando es transmitido por un terminal lector de tarjetas. Por lo tanto, la presencia de un clon se detecta cuando una tarjeta inteligente no puede reconocer y/o tratar de manera correcta tal comando secreto (aun si este clon reacciona correctamente a los comandos públicos).

Tal procedimiento es relativamente económico, fiable y simple en su puesta en práctica. Basta con, en un momento dado en que ello es necesario (por ejemplo, un recrudecimiento de clones), adaptar los equipos lógicos de los terminales para que emitan uno o varios comandos secretos. De acuerdo con otro aspecto, la invención se refiere a una tarjeta con microprocesador según la reivindicación independiente 5. La invención se refiere, de acuerdo con otro aspecto, a un terminal lector de tarjeta con microprocesador, según la reivindicación independiente 7. Se refiere un aspecto más de la invención a un producto de programa de ordenador según la reivindicación independiente 8.

6. Lista de figuras

Otras características y ventajas de la invención se pondrán más claramente de manifiesto con la lectura de la siguiente descripción de dos formas particulares de realización, dadas a título de meros ejemplos ilustrativos y no limitativos, y de los dibujos que se acompañan, de los cuales:

- la figura 1 ilustra esquemáticamente un ejemplo de sistema que lleva a la práctica la invención según una forma particular de realización de la invención;
- la figura 2 presenta las principales etapas del procedimiento de detección de tarjetas con microprocesador no auténticas según una primera forma de realización; y
- la figura 3 presenta las principales etapas del procedimiento de detección de tarjetas con microprocesador no auténticas según una segunda forma de realización.

Descripción de una forma de realización de la invención

6.1 Principio general

El principio general de la invención se basa en la memorización, junto a un juego de comandos estándar y público, de un juego de al menos un comando secreto, que no puede ser conocido por un falsificador, en una memoria de una tarjeta con microprocesador. Más concretamente, el procedimiento de la invención permite la detección de la autenticidad de una tarjeta basándose en el reconocimiento y/o en el tratamiento por esta tarjeta de un comando secreto llamado (emitido) por un terminal lector de tarjetas.

6.2 Ejemplo de sistema que lleva a la práctica la invención

Nos ponemos en lo que sigue en el contexto de una forma particular de realización de la invención, en relación con la figura 1, según la cual una tarjeta inteligente 2 (tarjeta con microprocesador) es una tarjeta de pago emitida por un organismo bancario. La tarjeta inteligente 2 es auténtica, es decir, no clonada, y es capaz de comunicarse con un terminal de pago 4 (terminal lector de tarjetas inteligentes) cuando se inserta en un lector de tarjetas 6 del terminal de pago 4.

Se asume en este punto que el portador de la tarjeta inteligente 2 desea acceder a un servicio bancario que precisa que previamente se autentique por mediación del terminal de pago 4.

La tarjeta inteligente 2 comprende convencionalmente un microprocesador y diferentes memorias RAM, ROM y/o EEPROM (no representados).

El terminal de pago 4 generalmente comprende una pantalla de presentación, un teclado numérico o alfanumérico, una impresora (no representados), un lector de tarjetas 6 y una unidad central de proceso (microprocesador) 7.

Asimismo, el terminal de pago 4 comprende un programa de control PC que puede ser llevado a la práctica por el microprocesador 7.

Por lo tanto, la invención propone insertar en una tarjeta auténtica (tal como la tarjeta inteligente 2), junto a un primer juego de comandos estándar y público CST, un segundo juego de al menos un comando secreto CSE, siendo el primer juego de comandos CST distinto del segundo juego de comandos CSE. Los juegos de comandos primero y segundo CST y CSE se pueden memorizar en una memoria de almacenamiento de comandos 3 de la tarjeta inteligente 2 durante su fabricación, por ejemplo en los locales del fabricante de tarjetas inteligentes. El segundo juego de comandos CSE, al menos, se puede almacenar en una parte segura de la memoria 3.

En la figura 1 se ha representado una tarjeta inteligente clonada 2' que comprende un juego de comandos estándar y público CST' (obtenido, por ejemplo, en Internet), pero que, claro está, no comprende comandos secretos, a diferencia de la tarjeta inteligente 2 auténtica.

En caso de que resultara haber en circulación tarjetas clonadas (del mismo tipo que la tarjeta inteligente 2'), la invención propone, pues, detectar estos clones modificando el programa de control PC de los terminales de pago (o al menos algunos de ellos), tal como el terminal de pago 4, para que utilicen los comandos secretos.

Así, de acuerdo con la invención, el terminal de pago 4 comprende medios de recepción de un programa de control modificado y medios de ejecución del programa de control modificado. Este programa de control modificado puede comprender una llamada (o una puesta en práctica) de al menos un comando secreto del juego de al menos un comando secreto CSE que con anterioridad se ha insertado en cada tarjeta auténtica, como anteriormente se ha destacado.

La llamada a los comandos secretos efectúa al menos una de las operaciones pertenecientes al grupo que comprende:

- lectura y/o escritura en una memoria;
- operaciones matemáticas y lógicas.

Por ejemplo, la llamada a un comando secreto puede consistir en uno o varios accesos, de lectura o de escritura, a una memoria de la tarjeta. De este modo, una llamada a un comando puede requerir, en primera instancia, la escritura en memoria de un dato predeterminado, y luego, en segundo instancia, la lectura de este dato escrito anteriormente.

De manera más compleja, una llamada a un comando secreto puede consistir en una sucesión de operaciones matemáticas o lógicas. Por ejemplo, tal comando secreto puede recuperar dos datos de dos ubicaciones de memoria diferentes, efectuar su suma o su producto, y comparar el resultado con un resultado esperado.

Estos comandos secretos, *a priori*, no modifican el funcionamiento “útil” del terminal (por ejemplo, las operaciones convencionales de dispensación de billetes), sino que permiten añadir tratamientos de control, que van a permitir distinguir las tarjetas auténticas y los clones.

Así, el terminal de pago 4 comprende medios de detección de la autenticidad de una tarjeta inteligente insertada en el lector de tarjetas 6 si el comando secreto es reconocido y/o tratado de manera correcta por la tarjeta inteligente, o de la presencia de un clon, si el comando secreto no es reconocido y/o tratado de manera errónea por la tarjeta.

6.3 Primer ejemplo de puesta en práctica

A continuación se presentan, en relación con la figura 2, las principales etapas de un procedimiento de detección de tarjetas con microprocesador no auténticas según una primera forma particular de realización de la invención.

Nos ponemos en lo que sigue en una configuración en la que está insertada una tarjeta inteligente (ya sea auténtica 2 o clonada 2’) en el lector de tarjetas 6 del terminal de pago 4 y en la que se ha modificado el programa de control PC del terminal de pago 4 como respuesta, por ejemplo, a una información según la cual hay circulando tarjetas clonadas.

Como se ilustra en la figura 2, el procedimiento de detección según la invención da comienzo con una etapa de llamada 20 a al menos un comando, llamado secreto, en el programa de control PC modificado del terminal de pago 4.

Se determina a continuación, en la etapa 22, si el comando secreto es reconocido y/o tratado de manera correcta por la tarjeta inteligente.

La salida “sí” 24 permite, por ejemplo, un paso a una etapa de autenticación 30 convencional que consiste en comparar una firma introducida en el teclado del terminal de pago 4 con los datos presentes en la tarjeta inteligente 2. Este tratamiento, en sí conocido y aplicado en todas las tarjetas inteligentes, no se describe en este punto con mayor detalle.

La salida “no” 26 indica la detección de la presencia de un clon, que puede llevar consigo, en la etapa 28, la generación de una alarma y/o la desactivación o el bloqueo del clon por parte del terminal de pago 4.

6.4 Segundo ejemplo de puesta en práctica

A continuación se presentan, en relación con la figura 3, las principales etapas de un procedimiento de detección de tarjetas con microprocesador no auténticas según una segunda forma particular de realización de la invención.

Nos ponemos en lo que sigue en una configuración en la que está insertada una tarjeta inteligente (ya sea auténtica 2 o clonada 2’) en el lector de tarjetas 6 del terminal de pago 4 y en la que se ha modificado el programa de control PC del terminal de pago 4 como respuesta, por ejemplo, a una información según la cual hay circulando tarjetas clonadas.

Como se ilustra en la figura 3, el procedimiento de detección según la invención da comienzo con una etapa de llamada 40 a al menos un primer comando, llamado secreto, en el programa de control PC modificado del terminal de pago 4.

Este primer comando secreto es tratado por la tarjeta inteligente y, a continuación, se transmite (comunica) el resultado del tratamiento (primera información) al terminal de pago 4, en la etapa 42.

Le sigue una etapa de llamada 44 a al menos un segundo comando, llamado secreto, en el programa de control PC modificado del terminal de pago 4.

Este segundo comando secreto es tratado por la tarjeta inteligente y, a continuación, se transmite el resultado del tratamiento (segunda información) al terminal de pago 4, en la etapa 46.

A continuación, se comparan o combinan en el terminal de pago 4, en la etapa 48, las informaciones primera y segunda, con el fin de proporcionar un resultado de detección de la autenticidad de la tarjeta inteligente.

Por ejemplo, la llamada a los primeros y segundos comandos secretos permite, en primer lugar, recuperar respectivamente una primera y una segunda información de dos diferentes ubicaciones de memoria de la tarjeta y, luego, efectuar su suma o su producto, y comparar el resultado con un resultado esperado, con el fin de proporcionar un resultado de detección (52 o 56).

De igual manera que en la primera forma de realización en relación con la figura 2, la salida “sí” 52 permite, por ejemplo, un paso a una etapa de autenticación 54 convencional que consiste en comparar una firma introducida en el teclado del terminal de pago 4 con los datos presentes en la tarjeta inteligente 2. La salida “no” 56 indica la detección de la presencia de un clon, que puede llevar consigo, en la etapa 58, la generación de una alarma y/o la desactivación o el bloqueo del clon por parte del terminal de pago 4.

Así, el envío simultáneo o secuencial de dos comandos secretos en esta segunda forma de realización permite detectar de manera aún más fiable una tarjeta inteligente clonada.

El procedimiento de la invención es relativamente económico, fiable y simple en su puesta en práctica. Permite luchar contra la falsificación de tarjetas inteligentes, o de un objeto portátil similar, detectar las tarjetas no auténticas (clones) e impedir su utilización.

6.5 Variantes

La presente invención puede ser asimismo de aplicación en cualquier situación que precise de una restricción del acceso a un lugar o a un local, a un vehículo perteneciente a una o varias personas, a un sitio Internet o una base de datos, por ejemplo.

El enlace entre el terminal lector de tarjetas y la tarjeta inteligente se puede efectuar mediante contactos o a distancia (RFID, por ejemplo).

REIVINDICACIONES

1. Procedimiento de autenticación de tarjetas con microprocesador, encaminado a determinar si una tarjeta es una tarjeta auténtica, suministrada por un distribuidor autorizado, o una tarjeta no auténtica, denominada clon, suministrada por un tercero no autorizado, con el concurso de un programa de control de al menos un terminal lector de tarjetas, enviando dicho programa a cada tarjeta unos comandos pertenecientes a un juego de comandos estándar y público,

caracterizado por que, almacenando, en su fabricación, cada tarjeta auténtica, en una memoria de almacenamiento de comandos, dicho juego de comandos estándar y público, y un juego de al menos un comando suplementario, llamado secreto, comprende:

- durante un primer período, una etapa de puesta en práctica de dicho programa de control en al menos un terminal lector de tarjetas, utilizando dicho juego de comandos estándar y público, para cada transacción; y
- previa detección de tarjetas clonadas en circulación:
    - una etapa de recepción, por parte de dicho o dichos terminales lectores de tarjetas, de un programa de control modificado, que envía a cada tarjeta que ha de autenticarse al menos un comando secreto perteneciente a dicho juego de al menos un comando suplementario memorizado en dicha o dichas tarjetas auténticas y ausente en las tarjetas clonadas;
    - una etapa de puesta en práctica de dicho programa de control modificado en dicho o dichos terminales lectores de tarjetas, para cada transacción;
    - una etapa de detección, en una transacción, de la autenticidad de dicha tarjeta, si dicho al menos un comando secreto es reconocido y/o tratado de manera correcta por dicha tarjeta, o de la presencia de un clon, si dicho al menos un comando secreto no es reconocido y/o es tratado de manera errónea por dicha tarjeta.

2. Procedimiento según la reivindicación 1, **caracterizado por que** la detección de la presencia de un clon lleva consigo la generación de una alarma y/o la desactivación o el bloqueo de dicho clon.

3. Procedimiento según una cualquiera de las reivindicaciones 1 y 2, **caracterizado por que** el envío de dicho al menos un comando secreto a dicha tarjeta provoca un tratamiento por parte de dicha tarjeta que comprende al menos una de las operaciones pertenecientes al grupo que comprende:

- lectura y/o escritura en una memoria;
- operaciones matemáticas y lógicas.

4. Procedimiento según una cualquiera de las reivindicaciones 1 a 3, **caracterizado por que** dicha etapa de detección de la autenticidad de dicha tarjeta comprende las siguientes sub-etapas:

- envío de al menos dos comandos secretos a dicha tarjeta, a fin de obtener al menos dos informaciones;
- comparación o combinación de dichas informaciones, para proporcionar el resultado de la detección.

5. Tarjeta con microprocesador para la puesta en práctica del procedimiento de autenticación según una cualquiera de las reivindicaciones 1 a 4, caracterizada por que comprende una memoria de almacenamiento de comandos, que comprende:

- un primer juego de comandos estándar y público; y
- un segundo juego de al menos un comando suplementario, llamado secreto, insertado en la fabricación de una tarjeta auténtica.

6. Tarjeta según la reivindicación 5, caracterizada por que al menos dicho segundo juego está almacenado en una parte segura de dicha memoria.

7. Terminal lector de tarjetas con microprocesador, para la puesta en práctica del procedimiento de autenticación según una cualquiera de las reivindicaciones 1 a 4, **caracterizado por que** comprende:

- medios de recepción y de ejecución de un programa de control modificado, que envían a cada tarjeta que ha de autenticarse al menos un comando suplementario, llamado secreto, de un juego de al menos un comando suplementario, llamado secreto, insertado en la fabricación de cada tarjeta auténtica, junto a dicho juego de comandos estándar y público, en una memoria de almacenamiento de comandos de cada tarjeta auténtica, y ausente en las tarjetas clonadas;
- medios de detección de la autenticidad de dicha tarjeta, si dicho comando secreto es reconocido y/o

tratado de manera correcta por dicha tarjeta, o de la presencia de un clon, si dicho comando secreto no es reconocido y/o es tratado de manera errónea por dicha tarjeta.

8. Producto de programa de ordenador descargable desde una red de comunicaciones y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, **caracterizado por que** comprende instrucciones de código de programa para la puesta en práctica del procedimiento de autenticación según una al menos de las reivindicaciones 1 a 4 en un terminal lector de tarjetas.

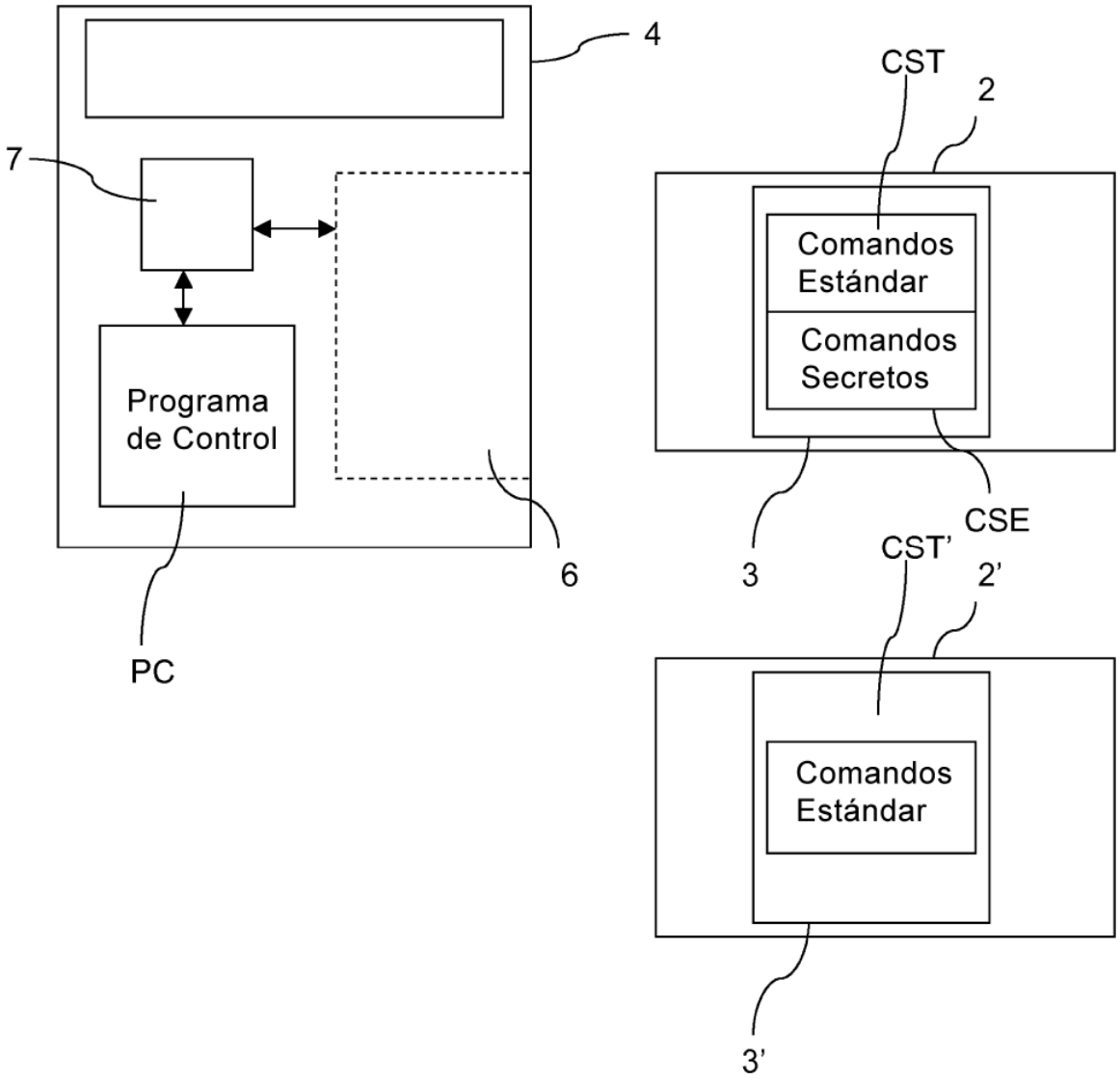
4
7
Programa
de Control
6
PC
CST
2
Comandos
Estándar
Comandos
Secretos
3
CSE
CST'
2'
Comandos
Estándar
3'

Figura 1

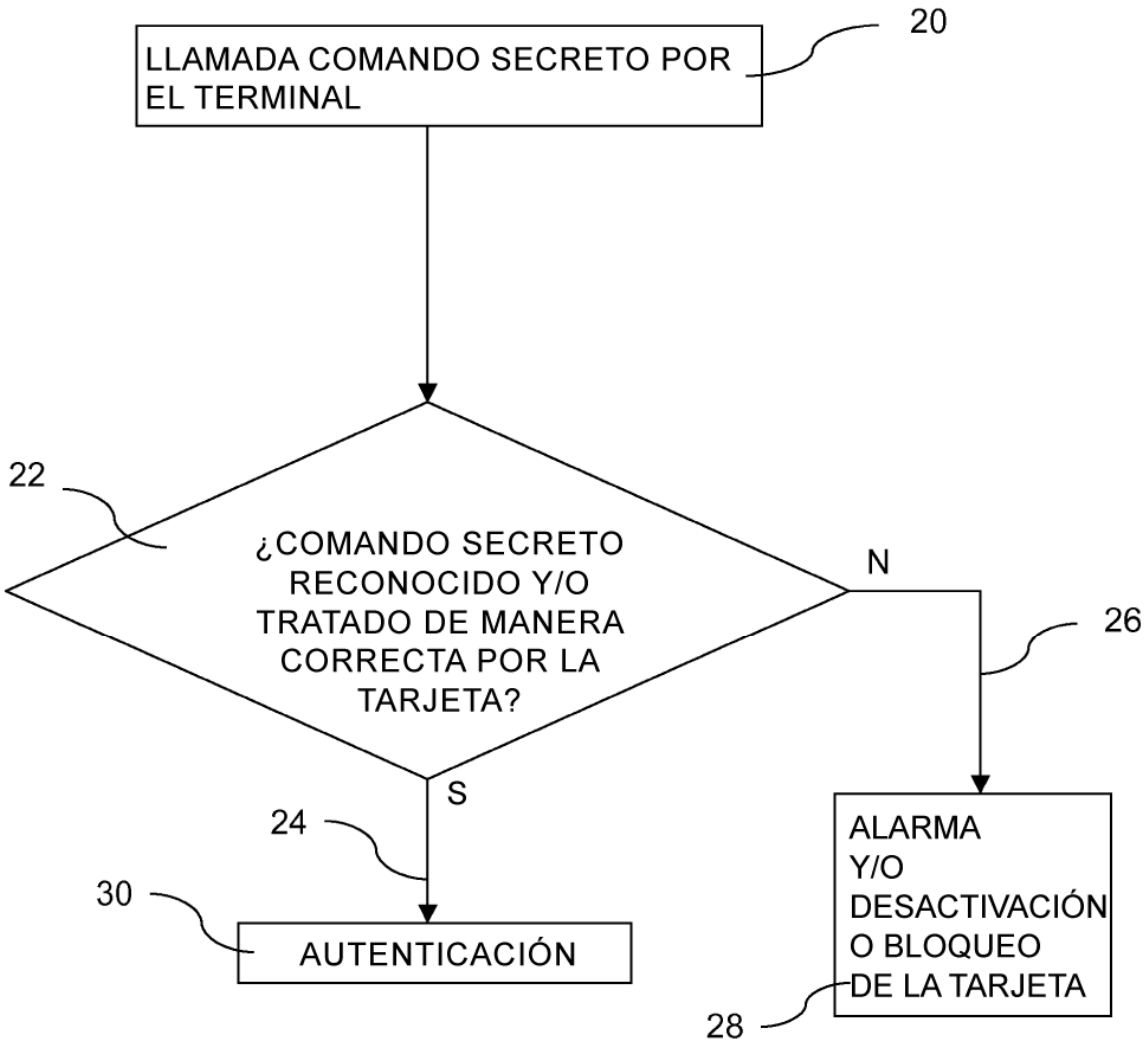
LLAMADA COMANDO SECRETO POR EL TERMINAL
20
22
¿COMANDO SECRETO RECONOCIDO Y/O TRATADO DE MANERA CORRECTA POR LA TARJETA?
N
26
S
24
30
AUTENTICACIÓN
ALARMA Y/O DESACTIVACIÓN O BLOQUEO DE LA TARJETA
28

Figura 2

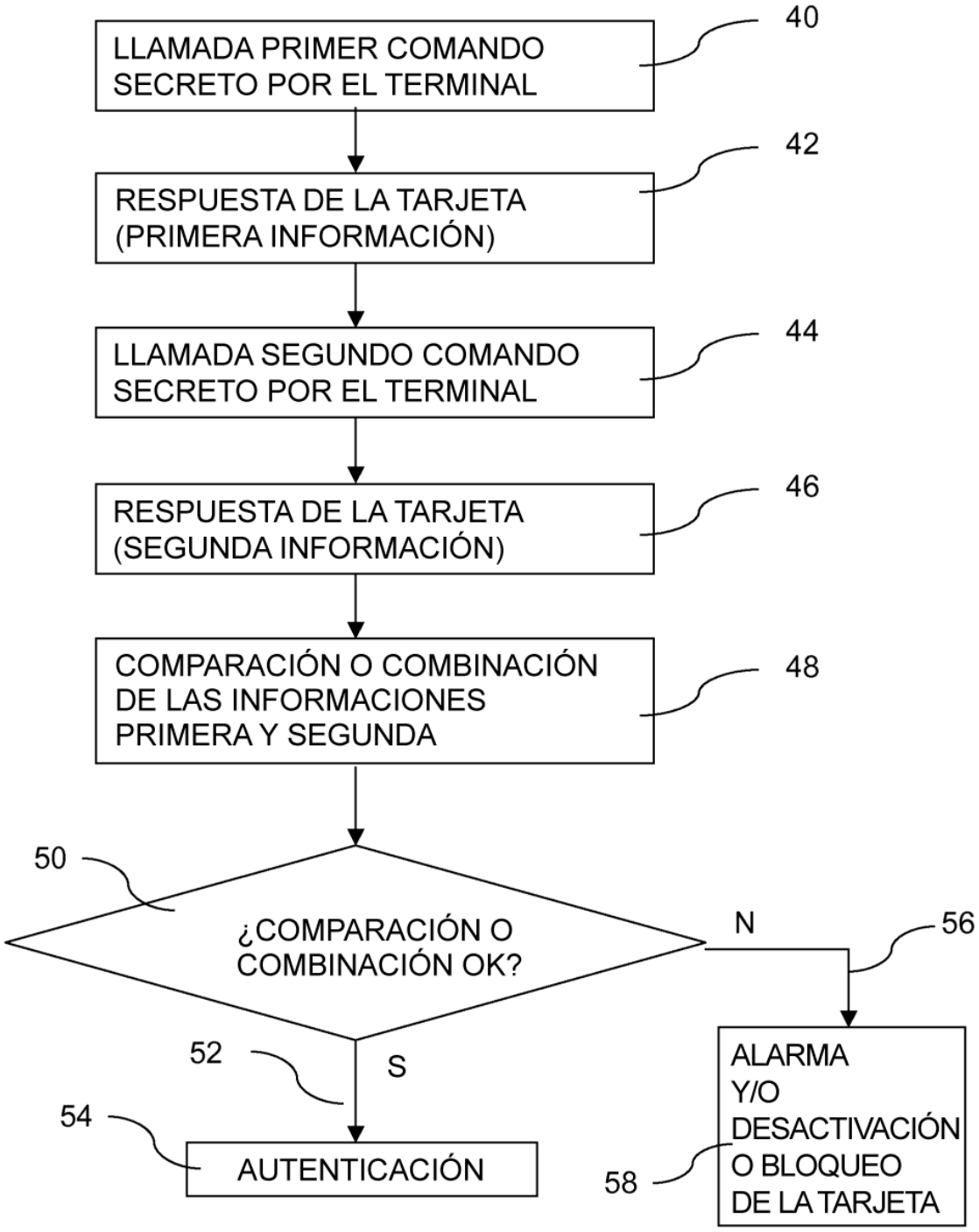
LLAMADA PRIMER COMANDO SECRETO POR EL TERMINAL
40
RESPUESTA DE LA TARJETA (PRIMERA INFORMACIÓN)
42
LLAMADA SEGUNDO COMANDO SECRETO POR EL TERMINAL
44
RESPUESTA DE LA TARJETA (SEGUNDA INFORMACIÓN)
46
COMPARACIÓN O COMBINACIÓN DE LAS INFORMACIONES PRIMERA Y SEGUNDA
48
50
¿COMPARACIÓN O COMBINACIÓN OK?
N
56
ALARMA Y/O DESACTIVACIÓN O BLOQUEO DE LA TARJETA
58
52
S
54
AUTENTICACIÓN

Figura 3