(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 793 406**

(51) Int. CI.:

G07F 19/00 (2006.01)
G06Q 20/18 (2012.01)
G06Q 20/20 (2012.01)
G07F 9/02 (2006.01)
G07F 11/00 (2006.01)
G07F 11/72 (2006.01)
G07F 17/24 (2006.01)
G07F 17/42 (2006.01)
G06Q 20/40 (2012.01)
G07F 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.11.2017 E 17204165 (9)**

(97) Fecha y número de publicación de la concesión europea: **26.02.2020 EP 3330934**

(54) Título: **Sistema y procedimiento de refuerzo de la seguridad de al menos un elemento de una terminal de transacciones desatendida**

(30) Prioridad:

01.12.2016 FR 1661799

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.11.2020

(73) Titular/es:

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

(72) Inventor/es:

PAVAGEAU, STÉPHANE y
DEVORNIQUE, ROGER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y procedimiento de refuerzo de la seguridad de al menos un elemento de una terminal de transacciones desatendida

Campo de la invención

La invención se refiere al campo de los terminales de pago, llamados desatendidos (denominados en inglés “unattended”), como por ejemplo terminales de pago para aparcamiento, estacionamiento, para comprar títulos de transporte o plazas de espectáculo, distribuidores de bebidas o golosinas..., y distribuidores de billetes, asimismo desatendidos.

Más en particular, la invención se refiere al refuerzo de la seguridad de los teclados y lectores de tarjetas de tales dispositivos, denominados en lo sucesivo, para una lectura más cómoda, “terminales de transacciones desatendidas”.

Técnica anterior

Actualmente, este tipo de terminales de transacciones desatendidas es objeto de un ataque conocido consistente en depositar, por ejemplo por pegado, encima de un teclado o un lector de tarjetas existente, un teclado/lector de tarjetas simulado que permite espiar el código introducido por un usuario en el teclado, sin que se entere, o los datos de la tarjeta insertada en el lector (datos del chip o de la pista magnética de la tarjeta).

Este tipo de ataque puede no modificar en nada, para el usuario, el desarrollo de la transacción, pues los datos sensibles son espiados de manera electrónica, por intermedio del teclado simulado o el lector de tarjetas pegado(s) por un tercero malintencionado, pero pueden ser procesados “normalmente” para efectuar la transacción. En efecto, en el caso de un teclado simulado, las pulsaciones de teclas efectuadas por el usuario para introducir su código confidencial son interceptadas por el teclado simulado, pero validadas a pesar de todo por el teclado auténtico, permitiendo el teclado simulado transmitir el esfuerzo mecánico al teclado auténtico. Por lo tanto, es difícil, para un usuario (ya sea éste avezado o novato), asegurarse de que la terminal de transacciones desatendida que se dispone a utilizar es o no auténtica.

Se han desarrollado técnicas para tratar de impedir la puesta en práctica de este tipo de ataques, por ejemplo modificando el aspecto exterior del teclado para hacer más difícil el pegado de un teclado simulado encima. Determinados teclados auténticos presentan, pues, por ejemplo, una cara anterior no lisa (por ejemplo, con nervaduras y/u ondulaciones y/o grabaciones en relieve). Para los lectores de tarjetas, asimismo, se pueden utilizar técnicas similares.

Estas técnicas, sin embargo, presentan inconvenientes, como por ejemplo el encarecimiento de los teclados/lectores de tarjetas auténticos para que presenten formas complejas, y el hecho de que, con el surgimiento de las impresoras 3D, estas formas complejas pasan a ser cada vez más fáciles de reproducir.

Existe otra técnica, esta vez para tratar de detectar este tipo de ataque sobre un lector de tarjetas, mediante modificación del color de la cara enrasada con el lector. Por ejemplo, un lector de tarjetas que presenta una embocadura de un verde transparente puede ser identificado como probablemente auténtico. En cambio, al ser conocida esta técnica, los infractores pueden poner en práctica igualmente lectores de tarjetas simulados que presenten un aspecto visual muy similar al de los lectores “convencionales”, haciendo más difícil la detección por parte de un usuario.

El documento KR 20090107693 A da a conocer la utilización de una retroiluminación a color con LED para detectar la presencia de aparatos “espías” en los cajeros automáticos. Se le solicita al usuario que confirme que el color elegido al azar sobre el lector de tarjetas se corresponde realmente con el color presentado en la pantalla del cajero automático. Como alternativa, se pueden utilizar detectores ópticos para efectuar una comparación automática.

El documento JP 2007279877 A da a conocer, asimismo, la utilización de una retroiluminación a color con LED para detectar la presencia de aparatos “espías” en los cajeros automáticos. Se le solicita al usuario que confirme que el color elegido al azar sobre el lector de tarjetas se corresponde con el color presentado en la pantalla del cajero.

Existe, por tanto, una necesidad de una solución que permita dar respuesta a la problemática de refuerzo de la seguridad de los teclados y lectores de tarjetas de las terminales de transacciones desatendidas contra los ataques del tipo pegado de dispositivos simulados encima de los teclados/lectores de tarjetas auténticos, al propio tiempo que se limitan las repercusiones de coste en la fabricación de las terminales de pago de transacciones desatendidas auténticas y no se rebaja la ergonomía para los usuarios.

Sumario

La invención concierne a un sistema de refuerzo de la seguridad de al menos un elemento de una terminal de transacciones desatendida, llamado elemento objeto de seguridad reforzada, comprendiendo el sistema:

• unos medios de refuerzo de la seguridad del o los elementos objeto de seguridad reforzada, que suministran al menos un medio de interacción con al menos un usuario de la terminal de transacciones desatendida;

• unos medios de detección de una anomalía en función del medio de interacción.

De este modo, la invención propone una solución novedosa e inventiva que permite interactuar con un usuario de una terminal de transacciones desatendida (por ejemplo, para pagar un aparcamiento o una plaza de estacionamiento, un billete de transporte o una plaza de espectáculo, una bebida o una golosina...) para detectar una anomalía en al menos un elemento objeto de seguridad reforzada de la terminal de transacciones desatendida, como por ejemplo el teclado o el lector de tarjetas.

Para llevarlo a cabo, la invención, según sus diferentes formas de realización, prevé proporcionar al menos un medio de interacción con un usuario, merced a unos medios de refuerzo de la seguridad puestos en práctica para el elemento objeto de seguridad reforzada, y tener luego en cuenta este medio de interacción para detectar o no una anomalía.

De acuerdo con una primera forma de realización de la invención, los medios de refuerzo de la seguridad comprenden:

• unos medios de gobierno de al menos un parámetro de retroiluminación de al menos una parte del elemento objeto de seguridad reforzada;

• unos medios de emisión de al menos una señal portadora de al menos un mensaje, relativo al parámetro de retroiluminación, destinado a ser presentado en una pantalla de la terminal de transacciones desatendida, correspondiendo el mensaje al medio de interacción,

y los medios de detección de una anomalía suministran una alerta si no se recibe ninguna respuesta al mensaje presentado antes del vencimiento de un tiempo predeterminado o si una respuesta recibida al mensaje presentado es negativa.

De este modo, esta primera forma de realización permite interactuar con un usuario de una terminal de transacciones desatendida en vistas a detectar la presencia de un elemento espía sobre al menos un elemento objeto de seguridad reforzada de la terminal, como por ejemplo el teclado o el lector de tarjetas.

Para llevarlo a cabo, se prevé, de acuerdo con esta forma de realización, gobernar al menos un parámetro de retroiluminación del elemento objeto de seguridad reforzada, por ejemplo el color, y pedir luego al usuario que confirme, o desmienta, que realmente ve el resultado de este mandato.

En efecto, esta forma de realización se basa en el hecho de que, si ha sido pegado o dispuesto un elemento espía (por un tercero malintencionado) sobre el elemento auténtico objeto de seguridad reforzada, entonces una modificación del aspecto visual del elemento auténtico no puede ser vista, correctamente, por un usuario.

Por ejemplo, si se ha posado un teclado simulado sobre el teclado auténtico de la terminal de transacciones desatendida, una modificación del color de retroiluminación del teclado auténtico no será visible correctamente para el usuario, e incluso no visible en absoluto, por ocultar total o parcialmente el teclado simulado este cambio de color. Igualmente, si se ha posado un lector de tarjetas simulado sobre el lector de tarjetas auténtico, entonces un parpadeo de la retroiluminación del lector de tarjetas auténtico no será visible claramente para el usuario.

El usuario, si no ve en absoluto, o nítidamente, el resultado anunciado por el mensaje presentado en la pantalla de la terminal de transacciones desatendida, puede responder negativamente al mensaje presentado, o no responder y abandonar la transacción en curso. En estos dos casos, se puede generar una alerta, a fin de prevenir (al usuario o a un destinatario a cargo del mantenimiento de la terminal de transacciones desatendida...) de un riesgo de fraude sobre la terminal, o también de impedir la utilización de la terminal bajo sospecha de ser fraudulenta.

De acuerdo con un aspecto particular de la invención, el sistema de refuerzo de la seguridad comprende además unos medios de verificación de una anomalía detectada, que comprenden los siguientes medios:

• unos medios de gobierno de una fuente luminosa externa al sistema de refuerzo de la seguridad;

• unos medios de análisis de una intensidad luminosa, que suministran una decisión de validación de la anomalía detectada si la intensidad luminosa analizada no es conforme a una intensidad luminosa de referencia.

De este modo, de acuerdo con esta variante de la primera forma de realización, cuando se ha detectado una anomalía en una terminal de transacciones desatendida, como consecuencia de una ausencia de respuesta, o una respuesta negativa de un usuario a una modificación del aspecto visual del teclado o del lector de tarjetas, la invención prevé poder verificar que esta anomalía realmente es representativa de un fraude sobre la terminal.

Por ejemplo, esta verificación es efectuada por una persona a cargo del mantenimiento de la terminal de transacciones desatendida.

Para llevarlo a cabo, se ponen en práctica unos medios de soporte físico, como por ejemplo unos medios de detección de una obstrucción por encima del teclado o del lector de tarjetas, mediante detección de una intensidad luminosa no conforme. Por ejemplo, estos medios de detección de una obstrucción alían, por una parte, una fuente de luz, exterior al teclado o al lector de tarjetas (diferenciada, por lo tanto, de las fuentes luminosas internas para la retroiluminación), cuyo encendido puede ser pilotado a distancia y, por otra, un sensor de luminosidad, a fin de detectar que la intensidad luminosa recibida por el sensor no se corresponde con la que debería recibir en una configuración auténtica. Esto permite, pues, detectar que un elemento obstruye el sensor, como por ejemplo un elemento espía posicionado por encima del elemento objeto de seguridad reforzada.

Se entiende que la ubicación del sensor de luminosidad se debe elegir en orden a optimizar la detección de obstrucción, teniendo en cuenta asimismo la luz ambiental, que puede ser diferente según la ubicación de la terminal de transacciones desatendida, o también el momento en que se efectúa la verificación de anomalía, o también la potencia de la fuente de luz exterior.

De acuerdo con una segunda forma de realización de la invención, los medios de refuerzo de la seguridad comprenden:

- unos medios de gobierno de una fuente luminosa externa al sistema de refuerzo de la seguridad, correspondiendo un encendido de la fuente luminosa externa al medio de interacción;

- unos medios de análisis de una intensidad luminosa,

y los medios de detección de una anomalía suministran una alerta si la intensidad luminosa analizada no es conforme a una intensidad luminosa de referencia.

De este modo, de acuerdo con esta segunda forma de realización, la invención prevé interactuar con un usuario, o más exactamente un agente de mantenimiento de la terminal de transacciones desatendida, por intermedio de unos medios de detección de una obstrucción por encima del teclado o del lector de tarjetas, mediante detección de una intensidad luminosa no conforme.

Por ejemplo, estos medios de detección de una obstrucción alían, por una parte, una fuente de luz, exterior al teclado o al lector de tarjetas (diferenciada, por lo tanto, de las fuentes luminosas internas para la retroiluminación), cuyo encendido puede ser pilotado a distancia, por ejemplo por el citado usuario, y, por otra, un sensor de luminosidad, a fin de detectar que la intensidad luminosa recibida por el sensor no se corresponde con la que debería recibir en una configuración auténtica. Esto permite, pues, detectar que un elemento obstruye el sensor, como por ejemplo un elemento espía posicionado por encima del elemento objeto de seguridad reforzada.

Se entiende que la ubicación del sensor de luminosidad se debe elegir en orden a optimizar la detección de obstrucción, teniendo en cuenta asimismo la luz ambiental, que puede ser diferente según la ubicación de la terminal de transacciones desatendida, o también el momento en que se efectúa la verificación de anomalía, o también la potencia de la fuente de luz exterior.

Por ejemplo, un elemento objeto de seguridad reforzada corresponde a un teclado o un lector de tarjetas.

De este modo, el o los elementos objeto de seguridad reforzada de la terminal de transacciones desatendida corresponden a los elementos por intermedio de los cuales transitan datos sensibles y confidenciales, como por ejemplo el teclado en el que un usuario introduce su código confidencial o un lector de tarjetas apto para leer datos sensibles presentes en la tarjeta de pago insertada por el usuario.

En efecto, estos dos elementos objeto de seguridad reforzada son los principales elementos objetivo de ataques por pegado de un elemento simulado por encima del elemento auténtico, de manera casi indetectable por un usuario, incluso receloso.

De acuerdo con una característica particular de la invención, el sistema de refuerzo de la seguridad comprende unos medios de recepción de al menos un mandato de disparo de los medios de refuerzo de la seguridad, con origen en un módulo de refuerzo de la seguridad de la terminal de transacciones desatendida.

De este modo, de acuerdo con esta variante de realización, el sistema de refuerzo de la seguridad comprende, asimismo, unos medios de recepción de un mandato para disparar/activar los medios de refuerzo de la seguridad propiamente dichos, a fin de no poner en práctica la invención sino cuando son susceptibles de ser interceptados datos sensibles por un eventual elemento espía. Por ejemplo, el sistema de refuerzo de la seguridad recibe un mandato de disparo de sus medios cuando un usuario activa el teclado para introducir un código confidencial, o cuando se inserta una tarjeta en el lector de tarjetas, imperativamente antes de que sean leídos los datos de la tarjeta.

De esta manera, la invención no se lleva a la práctica cuando no se detecta ninguna actividad en la terminal de transacciones desatendida, a fin de no modificar inútilmente el comportamiento de la terminal.

Además, esto permite no alertar a la persona maliciosa, con el fin de que no afine su sistema.

Por ejemplo, los medios de recepción de un mandato de disparo y/o los medios de refuerzo de la seguridad son llevados a la práctica en el elemento objeto de seguridad reforzada.

De este modo, la invención no precisa de módulos de soporte físico o lógico específicos, sino que utiliza medios ya presentes en uno de los elementos objeto de seguridad reforzada de la terminal de transacciones desatendida, por ejemplo en el teclado.

En efecto, actualmente es corriente que el teclado comprenda medios de soporte lógico y físico que se corresponden con una “inteligencia”, es decir, que permiten, por ejemplo, transmitir mensajes con destino a la interfaz hombre-máquina de la terminal de transacciones desatendida, procesar mensajes recibidos con origen en la interfaz hombre-máquina, recibir mandatos, por ejemplo para activar componentes del teclado...

De acuerdo con un aspecto particular, los medios de gobierno de al menos un parámetro de retroiluminación pertenecen al grupo que comprende:

• unos medios de activación de uno o varios color(es) emitido(s) por al menos una fuente luminosa interna al elemento objeto de seguridad reforzada;

• unos medios de activación intermitente de al menos una fuente luminosa interna al elemento objeto de seguridad reforzada;

• una combinación de los medios de activación.

De este modo, la invención, según sus diferentes variantes de la primera forma de realización, permite gobernar un aspecto visual externo del elemento objeto de seguridad reforzada (el teclado o el lector de tarjetas) a fin de permitir a un usuario reaccionar si el resultado esperado de este mandato no se le manifiesta explícitamente, lo cual significaría que probablemente hay instalado un elemento espía por encima del teclado/lector de tarjetas.

Por ejemplo, el color “de conjunto” del elemento objeto de seguridad reforzada se puede cambiar con respecto al color “convencional”, escogiendo un color diferente para todas las fuentes luminosas (por ejemplo, los leds de retroiluminación del teclado o del lector de tarjetas) o utilizando leds multicolor que permitan elegir el color que va a emitirse, por ejemplo de manera aleatoria para aumentar la complejidad de la reproducción malintencionada del comportamiento del elemento seguro. El mensaje presentado simultáneamente en la pantalla de la terminal de transacciones desatendida puede consistir, por ejemplo, en preguntar al usuario si el teclado / el lector de tarjetas aparece realmente en el color específico elegido.

De acuerdo con otra variante, puede cambiarse solamente el color de una parte del elemento objeto de seguridad reforzada con respecto al color “convencional”, eligiendo un color diferente para una parte solamente de las fuentes luminosas (por ejemplo, los leds de retroiluminación de determinadas teclas del teclado, o únicamente del “perímetro” del teclado, o los leds de retroiluminación de la parte inferior del lector de tarjetas...).

De acuerdo con aún otra variante, el mandato consiste en activar de manera intermitente uno o varios leds de retroiluminación del teclado/lector de tarjetas, para obtener un parpadeo. Esta variante permite, por ejemplo, tener en cuenta una eventual deficiencia de visión del usuario (el daltonismo), quien no vería correctamente los colores, pero podría ver sin problema un parpadeo.

Finalmente, por supuesto es posible combinar estas diferentes formas de realización, a fin de elegir no solo el color, en su conjunto o parcialmente, del elemento objeto de seguridad reforzada, sino también de obtener un parpadeo de este color.

De acuerdo con una característica particular de la invención, el sistema de refuerzo de la seguridad comprende medios de retroiluminación de al menos una parte del elemento objeto seguridad reforzada, perteneciendo los medios de retroiluminación al grupo que comprende:

• una guía de luz alrededor de al menos una parte del elemento objeto de seguridad reforzada;

• una estructura compuesta de una pieza plástica, unida a al menos una fuente luminosa interna al elemento objeto de seguridad reforzada, posada sobre una pieza blanca resistente al choque;

• una estructura compuesta de una pieza difusora de la luz, unida a al menos una fuente luminosa interna al elemento objeto de seguridad reforzada, de una película deslustrada difusora de la luz y de una pieza de protección resistente al choque;

• una fuente luminosa dispuesta bajo al menos una tecla del elemento objeto de seguridad reforzada, cuando este último corresponde a un teclado.

De este modo, la invención, según sus diferentes variantes de la primera forma de realización, comprende unos medios específicos de retroiluminación que permiten la puesta en práctica de los medios de refuerzo de la seguridad y especialmente de los gobiernos de los parámetros de retroiluminación antes descritos.

Se pueden llevar a la práctica varias variantes diferentes de los medios de retroiluminación, y pueden utilizarse especialmente medios existentes, como por ejemplo guías de luz utilizadas convencionalmente para la retroiluminación de un teclado o de un lector de tarjetas. Así, esto permite limitar las modificaciones de estructura que han de efectuarse sobre el dispositivo objeto de seguridad reforzada.

Por otro lado, se pueden utilizar unos medios muy precisos, en orden a fortalecer el refuerzo de la seguridad, como por ejemplo una iluminación diferenciada para cada tecla del teclado, cuyo color, por ejemplo, podrá ser diferente.

Por ejemplo, la alerta pertenece al grupo que comprende:

• un mensaje de alerta presentado, con destino al usuario, en la pantalla de la terminal de pago electrónico;

• un mensaje de alerta transmitido a un destinatario predefinido, por ejemplo un agente de mantenimiento;

• una combinación de las citadas alertas.

Asimismo, la invención concierne a un procedimiento de refuerzo de la seguridad de al menos un elemento de una terminal de transacciones desatendida, llamado elemento objeto de seguridad reforzada, que comprende:

• una etapa de refuerzo de la seguridad del elemento objeto de seguridad reforzada, que suministra al menos un medio de interacción con al menos un usuario de la terminal de transacciones desatendida;

• una etapa de detección de una anomalía en función del medio de interacción.

Asimismo, la invención concierne a un producto programa de ordenador, que comprende instrucciones de código de programa para la puesta en práctica de un procedimiento tal y como se ha descrito anteriormente, cuando el programa se ejecuta en un ordenador.

Asimismo, la invención concierne a un medio de almacenamiento legible por ordenador y no transitorio, que almacena un producto programa de ordenador tal y como se ha descrito anteriormente.

4. Figuras

Otras características y ventajas se pondrán más claramente de manifiesto con la lectura de la siguiente descripción de una forma particular de realización de la divulgación, dada a título de mero ejemplo ilustrativo y no limitativo, y de los dibujos que se acompañan, de los cuales:

- las figuras 1a a 1c ilustran, respectivamente, un ejemplo de sistema de refuerzo de la seguridad según el principio general de la invención y dos formas de realización;

- las figuras 2a a 2d ilustran cuatro variantes de realización de los medios de retroiluminación de un sistema de refuerzo de la seguridad tal como se ilustra en la figura 1; y

- la figura 3 ilustra las etapas principales de un procedimiento de refuerzo de la seguridad según una forma de realización de la invención.

En todas las figuras del presente documento, los elementos y etapas idénticos se designan mediante una misma referencia.

5. Descripción

5.1. Principio general

El principio general de la técnica descrita consiste en modificar un aspecto visual de un elemento objeto de seguridad reforzada de una terminal de transacciones desatendida y en disparar una interacción, en nexo con la modificación efectuada, con un usuario de esta terminal para detectar una eventual anomalía en este elemento objeto de seguridad reforzada, como por ejemplo el teclado o el lector de tarjetas chip.

De este modo, la solución de la invención, según sus diferentes formas de realización, permite detectar un eventual fraude sobre un elemento de una terminal de transacciones desatendida, fraude difícilmente detectable por un usuario (en particular, para un usuario inexperto) sin medios específicos, involucrando directamente al usuario de la terminal por intermedio de unos medios de interacción.

En lo sucesivo, a efectos de una lectura más sencilla, aunque se describirán ejemplos de refuerzo de la seguridad de un elemento objeto de seguridad reforzada de una terminal de transacciones desatendida, se da por supuesto que se puede reforzar la seguridad de varios elementos al mismo tiempo (por ejemplo, el teclado y el lector de tarjetas) en el seno de una misma terminal de transacciones desatendida.

Por ejemplo, y como se ilustra en la figura 1a, un elemento objeto de seguridad reforzada de una terminal de transacciones desatendida corresponde al teclado K (10) o al lector de tarjetas R (11). En efecto, estos dos

elementos acusan con frecuencia intentos de pirateo o de fraude, debido a que permiten transitar datos sensibles para efectuar una transacción bancaria (por ejemplo, un código confidencial introducido en el teclado o datos de la tarjeta chip / de pista insertada en el lector de tarjetas). Como ya se ha indicado en relación con la técnica anterior, uno de los ataques que con más frecuencia se observan sobre estos elementos consiste en pegar un elemento simulado, muy difícilmente detectable por un usuario, a fin de espiar los datos sensibles que transitan, sin impedir el funcionamiento convencional de la terminal de transacciones desatendida y, por tanto, sin alertar al usuario final.

Convencionalmente, una terminal de transacciones desatendida comprende asimismo una interfaz hombre-máquina IHM que permite, por intermedio de una pantalla, interactuar con un usuario (por ejemplo, para presentar consignas de inserción de tarjeta o de introducción de un código, presentar cuantías de reintegro o elecciones de posibles acciones).

Por otro lado, el sistema de refuerzo de la seguridad de la presente invención, según sus diferentes formas de realización, comprende, por una parte, unos medios de refuerzo de la seguridad 12 capaces de modificar, de manera visual, un aspecto de la terminal de transacciones desatendida, y de interactuar con el usuario de la terminal por intermedio de un medio de interacción 120 y, por otra, unos medios de detección 13 de una anomalía, en función de la interacción con el usuario.

Estos diferentes medios quedan descritos seguidamente con mayor detalle, en relación con diferentes formas de realización de la invención.

5.2. Descripción de una primera forma de realización

5.2.1. Refuerzo de la seguridad

Pasamos a presentar, en relación con la figura 1a, un ejemplo de un sistema de refuerzo de la seguridad de al menos un elemento de una terminal de transacciones desatendida, según una primera forma de realización de la invención.

De acuerdo con esta primera forma de realización de la invención, los medios de refuerzo de la seguridad (12) del sistema de refuerzo de la seguridad comprenden:

• por una parte, unos medios de gobierno de al menos un parámetro de retroiluminación del elemento objeto de seguridad reforzada, a fin de modificar el aspecto visual del elemento objeto de seguridad reforzada,

• por otra parte, unos medios de emisión de una señal portadora de un mensaje relacionado con este parámetro de retroiluminación y destinado a ser presentado en una pantalla de la terminal de transacciones desatendida, a fin de proponer al usuario que confirme que realmente ha visualizado la modificación del aspecto visual del elemento objeto de seguridad reforzada.

De este modo, el sistema de refuerzo de la seguridad según esta forma de realización de la invención permite detectar una eventual anomalía, en caso de que la respuesta del usuario no se corresponda con una respuesta esperada en una situación normal. Por ejemplo, si el usuario no confirma que visualiza la modificación, o no responde a la solicitación de interacción, el sistema de refuerzo de la seguridad detecta una eventual anomalía.

Por otro lado, los medios de gobierno que permiten la modificación del aspecto visual del elemento objeto de seguridad reforzada corresponden, por ejemplo, a:

• unos medios de activación de un color emitido por al menos una fuente luminosa interna al elemento objeto de seguridad reforzada, a fin de hacer cambiar de color la totalidad o parte del elemento objeto de seguridad reforzada, según la ubicación de la fuente o de las fuentes luminosa(s) (alrededor del teclado, bajo cada tecla del teclado, alrededor de la ranura de inserción del lector de tarjetas....), y/o

• unos medios de activación intermitente de al menos una fuente luminosa interna a dicho al menos un elemento objeto de seguridad reforzada, a fin de hacer parpadear una o varias fuente(s) luminosa(s) interna(s) al elemento objeto de seguridad reforzada.

Se puede llevar a la práctica una combinación de estos medios de activación, por ejemplo haciendo parpadear una o varias fuentes luminosas al propio tiempo que se cambia el color. Los medios llevados a la práctica con relación a estas fuentes luminosas quedan descritos seguidamente con mayor detalle.

Por otro lado, la interacción puesta en práctica con el usuario corresponde, por ejemplo, a la presentación de un mensaje en la pantalla de la terminal de transacciones desatendida, por intermedio de la IHM, que solicita una respuesta por parte del usuario. Este mensaje, por supuesto, debe estar adaptado a la modificación efectuada sobre el aspecto visual del elemento objeto de seguridad reforzada, a fin de que la respuesta del usuario sea coherente. Este mensaje se presenta de manera simultánea a la modificación efectuada sobre el aspecto visual, con el fin de hacer más difícil la reproducción de este comportamiento por un tercero malintencionado.

De este modo, si la modificación consiste, por ejemplo, en retroiluminar el teclado en azul, mientras que

convencionalmente está retroiluminado en blanco, el mensaje puede formularse como sigue:

«*Por favor, confirme que el teclado aparece ahora en azul, pulsando la tecla OK.*

Si no, pulse la tecla CANCELACIÓN».

Si la modificación consiste en hacer parpadear la retroiluminación de la ranura de inserción del lector de tarjetas, sin modificar su color, el mensaje puede formularse como sigue:

«*Por favor, confirme que la ranura de inserción de tarjetas parpadea, pulsando la tecla OK.*

Si no, pulse la tecla CANCELACIÓN».

Este mensaje puede venir precedido de otro mensaje consistente en un anuncio relativo a la seguridad de la terminal de transacciones desatendida que se está utilizando, que informa al usuario de que seguidamente se va a proceder a una operativa simple y rápida de detección de anomalía con solicitación de una respuesta por su parte.

Por lo tanto, se incita al usuario a introducir una respuesta, por intermedio del teclado. Esta respuesta, o la ausencia de respuesta al vencimiento de un espacio de tiempo predeterminado, es procesada por los medios de detección 13 de una anomalía para inferir o no la presencia de una anomalía.

De acuerdo con los anteriores ejemplos de mensaje, si el usuario pulsa la tecla OK, los medios de detección 13 analizan esta respuesta como una ausencia de anomalía y la transacción se prosigue con normalidad, tranquilizándose además al usuario sobre la autenticidad de los elementos sensibles de la terminal de transacciones desatendida que está utilizando.

En cambio, si el usuario pulsa la tecla *CANCELACIÓN*, los medios de detección 13 analizan esta respuesta como una detección de anomalía y suministran, por ejemplo, una alerta. Igualmente, si el usuario, desconfiando por no visualizar el color y/o el parpadeo anunciado, prefiere no proseguir, no respondiendo al mensaje presentado, los medios de detección 13 procesan esta ausencia de respuesta como una detección de anomalía y suministran, por ejemplo, una alerta. Convencionalmente, una ausencia de respuesta tan solo se considera como confirmada al vencimiento de un plazo predeterminado, dando al usuario el tiempo de interactuar. Durante este plazo, se mantiene el aspecto visual modificado por los medios de refuerzo de la seguridad (por ejemplo, el parpadeo continúa, o sigue presentándose el color modificado).

Tal alerta puede tomar varias formas, que combinan por ejemplo una información con destino al usuario y/o a un administrador (o persona a cargo del mantenimiento) de la terminal de transacciones desatendida y la custodia de la terminal bajo sospecha de ataque.

De este modo, la alerta puede consistir en presentar un nuevo mensaje en la pantalla de la terminal de transacciones desatendida, que informa al usuario de un potencial fraude y le recomienda que deje de utilizar la terminal.

Por otro lado, asimismo puede enviarse una alerta a un destinatario previamente identificado, como por ejemplo un administrador a cargo del mantenimiento de la terminal de transacciones desatendida. Este administrador, a continuación, podrá verificar si la anomalía detectada resulta ser cierta, desplazándose al propio emplazamiento. Esta verificación se puede llevar a la práctica asimismo merced a unos medios de verificación que seguidamente se describen con mayor detalle (apartado 5.2.3), en relación con esta primera forma de realización de la invención.

Por otro lado, la puesta en práctica de tal refuerzo de la seguridad de un elemento de una terminal de transacciones desatendida tan solo es necesaria, *a priori*, cuando se está utilizando la terminal, es decir, cuando por ejemplo se inicia una transacción.

De este modo, el sistema de refuerzo de la seguridad de la invención, de acuerdo con esta forma de realización, comprende asimismo unos medios de recepción de al menos un mandato de disparo de los medios de refuerzo de la seguridad, con origen en un módulo de refuerzo de la seguridad de dicha terminal de transacciones desatendida.

Por ejemplo, el módulo de refuerzo de la seguridad, que puede situarse dentro del propio elemento objeto de seguridad reforzada, o más generalmente dentro de la terminal de transacciones desatendida, detecta que este elemento objeto de seguridad reforzada está activado (por ejemplo, cuando se inserta una tarjeta en el lector de tarjetas, o cuando es requerido un código confidencial mediante introducción por intermedio del teclado) y entonces transmite un mandato al sistema de refuerzo de la seguridad para disparar los medios de refuerzo de la seguridad.

De este modo, las modificaciones introducidas en el aspecto visual de uno o varios elementos objeto de seguridad reforzada de una terminal de transacciones desatendida tan solo son llevadas efectivamente a la práctica cuando se está utilizando la terminal y es necesario verificar la ausencia de fraude.

De acuerdo con una variante de utilización, este mandato de disparo del refuerzo de la seguridad se puede enviar, asimismo, a petición de un administrador o de un agente de mantenimiento, que deseara efectuar verificaciones de

la autenticidad de una o varias terminales de transacciones desatendidas al mismo tiempo, por ejemplo a la hora de pasar por un sitio donde hay presentes varias terminales. En tal situación, el agente de mantenimiento puede disparar el refuerzo de la seguridad de varias terminales al mismo tiempo, por ejemplo haciendo parpadear, o eligiendo un color no convencional para la retroiluminación de todos los teclados de las terminales a su alrededor (esto puede corresponder, por ejemplo, a una configuración en una estación donde se encuentran varios distribuidores de billetes de tren) y/o todos los lectores de tarjetas de esas terminales. De este modo, el agente de mantenimiento es capaz de tener una visión de conjunto del parque de terminales de transacciones desatendidas y, si una o varias terminales no parpadea(n), o si una o varias permanece(n) retroiluminada(s) con el color convencional, entonces puede desplazarse más cerca para verificar si se confirma un fraude.

5.2.2. Medios de retroiluminación

Pasamos a describir con mayor detalle los medios de retroiluminación puestos en práctica, según esta primera forma de realización de la invención, para modificar el aspecto visual del elemento objeto de seguridad reforzada.

Es de señalar que, cuando ya existen unos medios de retroiluminación, por ejemplo en forma de fuentes de luz (como LED) asociadas a una o varias guías de luz, estos medios pueden ser utilizados para la puesta en práctica de la presente invención, con el fin de optimizar los costes.

No obstante, los medios existentes se pueden adaptar, por ejemplo sustituyendo los LED blancos utilizados convencionalmente por LED de color. Además, asimismo se necesitan adaptaciones para la puesta en práctica de los medios de verificación que seguidamente se describen.

Cuando de entrada no hay presente ningún medio de retroiluminación para el elemento objeto de seguridad reforzada, la invención, según esta forma de realización, prevé añadirlos.

Por lo tanto, estos medios de retroiluminación se pueden llevar a la práctica en formas variadas tales como, por ejemplo:

• una guía de luz alrededor de al menos una parte del elemento objeto de seguridad reforzada: por ejemplo, una guía de luz que enmarca el teclado o el lector de tarjetas y retroilumina el elemento objeto de seguridad reforzada en forma de cuatro trazos luminosos. Las fuentes luminosas que permiten la retroiluminación pueden ser de colores idénticos o diferentes;

• en el caso en que el elemento objeto de seguridad reforzada corresponde al teclado:

  o una estructura compuesta de una pieza plástica, unida a al menos una fuente luminosa interna al teclado, posada sobre una pieza blanca resistente al choque, como se ilustra en la figura 2a. Tal configuración es relativamente convencional y puede ser modificada para la invención sustituyendo los LED blancos por LED de color;

  o una estructura compuesta de una pieza difusora de la luz, unida a al menos una fuente luminosa interna al teclado, de una película deslustrada difusora de la luz y de una pieza de protección resistente al choque (de vidrio, por ejemplo), como se ilustra en la figura 2b. Tal configuración corresponde, en cierto modo, a un teclado de vidrio, iluminado por detrás por una pieza luminosa;

  o una fuente luminosa dispuesta bajo al menos una tecla del teclado, o bajo cada tecla, permitiendo así iluminar individualmente varias teclas del teclado de colores diferentes, como se ilustra en las figuras 2c y 2d. De este modo, de acuerdo con una primera variante ilustrada en la figura 2c, el teclado es muy simple y presenta un led por tecla, pilotables por separado y sin precisar de una guía de luz; al lado de cada tecla, puede ir posicionado un sensor de luminosidad (para la detección de obstrucción ya descrita anteriormente, con la condición de que el led esté apagado en el momento de la detección de obstrucción, a fin de no deslumbrar el sensor). De acuerdo con una segunda variante ilustrada en la figura 2d, se utiliza un reducido número de leds (por ejemplo, 2 ó 4) y la luz es guiada, por intermedio de una guía de luz, en la vertical de las teclas; por lo tanto, se debe posicionar racionalmente un sensor de luminosidad para ser iluminado en modo suficiente por la luz exterior.

De este modo, según la puesta en práctica elegida para los medios de retroiluminación, es posible modificar y/o hacer parpadear el color de una guía de luz que enmarca el teclado y/o el lector de tarjetas, modificar y/o hacer parpadear el color de conjunto de la retroiluminación de un teclado, o también modificar y/o hacer parpadear de manera independiente el color de varias teclas de un teclado.

Los mensajes de interacción con destino al usuario se adaptan entonces a la modificación del aspecto visual puesta en práctica efectivamente.

5.2.3. Verificación

La invención, de acuerdo con esta forma de realización, prevé asimismo unos medios de verificación que permiten verificar si la anomalía detectada resulta ser cierta, detectando una obstrucción sinónimo de la presencia de un

elemento espía pegado encima del elemento objeto de seguridad reforzada (por ejemplo, un teclado simulado).

Para llevarlo a cabo, los medios de verificación de una anomalía detectada comprenden, según esta primera forma de realización, los siguientes medios:

• unos medios de gobierno/pilotaje 14 de una fuente luminosa 140 externa al sistema de refuerzo de la seguridad, que especialmente permiten pilotar a distancia el encendido, el apagado y/o el parpadeo de una fuente luminosa externa, cuya intensidad luminosa es conocida y corresponde a una intensidad luminosa de referencia, cuando está encendida;

• unos medios de análisis 15 de una intensidad luminosa, que suministran una decisión de validación de la anomalía detectada si la intensidad luminosa analizada no es conforme a una intensidad luminosa de referencia. Por ejemplo, se trata de un sensor de luminosidad, colocado racionalmente para detectar la intensidad de referencia de la fuente luminosa externa en funcionamiento normal y para detectar una obstrucción sinónimo de fraude cuando se halla un elemento espía posicionado malintencionadamente por encima del elemento objeto de seguridad reforzada.

Estos medios de verificación pueden ser activados, por ejemplo, por el agente de mantenimiento de la terminal de transacciones desatendida, avisado por la alerta emitida en el momento de la detección de una anomalía. De esta manera, el agente de mantenimiento puede verificar esta anomalía a distancia, sin desplazarse al sitio donde se encuentra la terminal. Así, puede reforzar las acciones de custodia de la terminal de transacciones desatendida eventualmente ya puestas en práctica, poniendo la terminal “fuera de servicio”, antes de desplazarse para confirmar la avería e implantar medidas correctivas (desmontaje del elemento espía, por ejemplo).

5.3. Descripción de una segunda forma de realización

Esta segunda forma de realización, en realidad, pone en práctica un refuerzo de la seguridad correspondiente a la verificación antes descrita, consistiendo, por tanto, el refuerzo de la seguridad en detectar una obstrucción sinónimo de la presencia de un elemento espía pegado encima del elemento objeto de seguridad reforzada (por ejemplo, un teclado simulado).

Más exactamente, de acuerdo con esta segunda forma de realización, ilustrada en la figura 1c, los medios de refuerzo de la seguridad 12 comprenden:

• unos medios de gobierno/pilotaje 121 de una fuente luminosa 140 externa al sistema de refuerzo de la seguridad, correspondiendo un encendido de la fuente luminosa externa al medio de interacción. De este modo, la interacción con el usuario consiste en encender la fuente exterior de luz (y no en responder a un mensaje presentado en la pantalla de la terminal de transacciones desatendida, como en la primera forma de realización);

• unos medios de análisis 131 de una intensidad luminosa. Por ejemplo, se trata de un sensor de luminosidad, colocado racionalmente para detectar la intensidad de referencia de la fuente luminosa externa en funcionamiento normal y para detectar una obstrucción sinónimo de fraude cuando se halla un elemento espía posicionado malintencionadamente por encima del elemento objeto de seguridad reforzada.

Además, de acuerdo con esta segunda forma de realización, los medios de detección de una anomalía suministran una alerta si la intensidad luminosa analizada no es conforme a una intensidad luminosa de referencia.

De este modo, esta segunda forma de realización está adaptada más particularmente al caso del mantenimiento de una terminal de transacciones desatendida, o de un parque de terminales de transacciones desatendidas, cuando el agente de mantenimiento desea, antes de desplazarse al propio emplazamiento, efectuar una primera verificación de la autenticidad de las terminales del parque. En efecto, en tal contexto, el agente de mantenimiento puede pilotar a distancia el encendido de cada fuente luminosa externa prevista en cada terminal de transacciones desatendida y detectar una eventual obstrucción por intermedio del sensor de luminosidad colocado en el interior de cada elemento objeto de seguridad reforzada de cada terminal.

5.4. Procedimiento de refuerzo de la seguridad

Asimismo, la invención concierne a un procedimiento de refuerzo de la seguridad de al menos un elemento de una terminal de transacciones desatendida, llamado elemento objeto de seguridad reforzada, tal y como se ilustra en la figura 3.

De acuerdo con esta forma de realización, el procedimiento comprende una etapa de refuerzo de la seguridad 30 de al menos un elemento objeto de seguridad reforzada (el teclado y/o el lector de tarjetas), que suministra al menos un medio de interacción 120 con el usuario de la terminal de transacciones desatendida.

Como ya se ha descrito anteriormente en relación con las dos formas de realización de la invención, el medio de interacción puede consistir en un mensaje presentado en la pantalla de la terminal (primera forma de realización), al que debe responder el usuario según su observación del comportamiento de la terminal, o puede consistir en encender la fuente exterior de luz (segunda forma de realización).

Se lleva a la práctica, a continuación, una etapa de detección 31 de una anomalía, en función del medio de interacción, como anteriormente se ha descrito en relación con las dos formas de realización de la invención.

El procedimiento de refuerzo de la seguridad, según las diferentes formas de realización de la invención, puede ser llevado a la práctica en la terminal de transacciones desatendida, y más en particular en el propio elemento objeto de seguridad reforzada (por ejemplo, el teclado o el lector de tarjetas).

REIVINDICACIONES

1. Sistema de refuerzo de la seguridad de al menos un elemento (10, 11) de una terminal de transacciones desatendida, llamado elemento objeto de seguridad reforzada, comprendiendo dicho sistema:

• unos medios de refuerzo de la seguridad (12) de dicho al menos un elemento objeto de seguridad reforzada, que suministran al menos un medio de interacción (120) con al menos un usuario de dicha terminal de transacciones desatendida, comprendiendo dichos medios de refuerzo de la seguridad:

o unos medios de gobierno de al menos un parámetro de retroiluminación de al menos una parte de dicho al menos un elemento objeto de seguridad reforzada;

o unos medios de emisión de al menos una señal portadora de al menos un mensaje, relativo a dicho parámetro de retroiluminación, destinado a ser presentado en una pantalla de dicha terminal de transacciones desatendida, correspondiendo dicho al menos un mensaje a dicho al menos un medio de interacción;

• unos medios de detección (13) de una anomalía en función de dicho al menos un medio de interacción, suministrando dichos medios de detección de una anomalía una alerta si no se recibe ninguna respuesta a dicho mensaje presentado antes del vencimiento de un tiempo predeterminado o si una respuesta recibida a dicho mensaje presentado es negativa;

• estando caracterizado dicho sistema por comprender unos medios de verificación de una anomalía detectada, que comprenden los siguientes medios:

o unos medios de gobierno de una fuente luminosa externa a dicho sistema de refuerzo de la seguridad;

o unos medios de análisis de una intensidad luminosa, que suministran una decisión de validación de dicha anomalía detectada si dicha intensidad luminosa analizada no es conforme a una intensidad luminosa de referencia.

2. Sistema de refuerzo de la seguridad según la reivindicación 1, caracterizado por que dichos medios de refuerzo de la seguridad comprenden:

• unos medios de gobierno de una fuente luminosa externa a dicho sistema de refuerzo de la seguridad, correspondiendo un encendido de dicha fuente luminosa externa a dicho medio de interacción;

• unos medios de análisis de una intensidad luminosa,

y por que dichos medios de detección de una anomalía suministran una alerta si dicha intensidad luminosa analizada no es conforme a una intensidad luminosa de referencia.

3. Sistema de refuerzo de la seguridad según la reivindicación 1, caracterizado por que dicho al menos un elemento objeto de seguridad reforzada corresponde a un teclado o un lector de tarjetas.

4. Sistema de refuerzo de la seguridad según una cualquiera de las reivindicaciones 1 a 3, caracterizado por comprender unos medios de recepción de al menos un mandato de disparo de dichos medios de refuerzo de la seguridad, con origen en un módulo de refuerzo de la seguridad de dicha terminal de transacciones desatendida.

5. Sistema de refuerzo de la seguridad según la reivindicación 4, caracterizado por que dichos medios de recepción de un mandato de disparo y/o dichos medios de refuerzo de la seguridad son llevados a la práctica en dicho al menos un elemento objeto de seguridad reforzada.

6. Sistema de refuerzo de la seguridad según la reivindicación 1, caracterizado por que dichos medios de gobierno de al menos un parámetro de retroiluminación pertenecen al grupo que comprende:

• unos medios de activación de uno o varios color(es) emitido(s) por al menos una fuente luminosa interna a dicho al menos un elemento objeto de seguridad reforzada;

• unos medios de activación intermitente de al menos una fuente luminosa interna a dicho al menos un elemento objeto de seguridad reforzada;

• una combinación de dichos medios de activación.

7. Sistema de refuerzo de la seguridad según la reivindicación 1, caracterizado por comprender unos medios de retroiluminación de al menos una parte de dicho al menos un elemento objeto de seguridad reforzada, perteneciendo dichos medios de retroiluminación al grupo que comprende:

• una guía de luz alrededor de al menos una parte de dicho elemento objeto de seguridad reforzada;

• una estructura compuesta de una pieza plástica, unida a al menos una fuente luminosa interna a dicho al menos

un elemento objeto de seguridad reforzada, posada sobre una pieza blanca resistente al choque;

• una estructura compuesta de una pieza difusora de la luz, unida a al menos una fuente luminosa interna a dicho al menos un elemento objeto de seguridad reforzada, de una película deslustrada difusora de la luz y de una pieza de protección resistente al choque;

• una fuente luminosa dispuesta bajo al menos una tecla de dicho elemento objeto de seguridad reforzada, cuando este último corresponde a un teclado.

8. Procedimiento de refuerzo de la seguridad de al menos un elemento de una terminal de transacciones desatendida, llamado elemento objeto de seguridad reforzada, comprendiendo dicho procedimiento:

• una etapa de refuerzo de la seguridad (30) de dicho al menos un elemento objeto de seguridad reforzada, que suministra al menos un medio de interacción (120) con al menos un usuario de dicha terminal de transacciones desatendida, comprendiendo dicha etapa de refuerzo de la seguridad (12):

  o el gobierno de al menos un parámetro de retroiluminación de al menos una parte de dicho al menos un elemento objeto de seguridad reforzada;

  o la emisión de al menos una señal portadora de al menos un mensaje, relativo a dicho parámetro de retroiluminación, destinado a ser presentado en una pantalla de dicha terminal de transacciones desatendida, correspondiendo dicho al menos un mensaje a dicho al menos un medio de interacción;

• una etapa de detección (31) de una anomalía en función de dicho al menos un medio de interacción, suministrando dicha etapa de detección de una anomalía una alerta si no se recibe ninguna respuesta a dicho mensaje presentado antes del vencimiento de un tiempo predeterminado o si una respuesta recibida a dicho mensaje presentado es negativa;

• estando caracterizado dicho procedimiento por comprender una etapa de verificación de una anomalía detectada, comprendiendo dicha etapa de verificación:

  o el gobierno de una fuente luminosa externa a dicho sistema de refuerzo de la seguridad;

  o el análisis de una intensidad luminosa, que suministra una decisión de validación de dicha anomalía detectada si dicha intensidad luminosa analizada no es conforme a una intensidad luminosa de referencia.

9. Producto programa de ordenador, que comprende instrucciones de código de programa para la puesta en práctica de un procedimiento según la reivindicación 8, cuando dicho programa se ejecuta en un ordenador.

10. Medio de almacenamiento legible por ordenador y no transitorio, que almacena un producto programa de ordenador según la reivindicación 9.

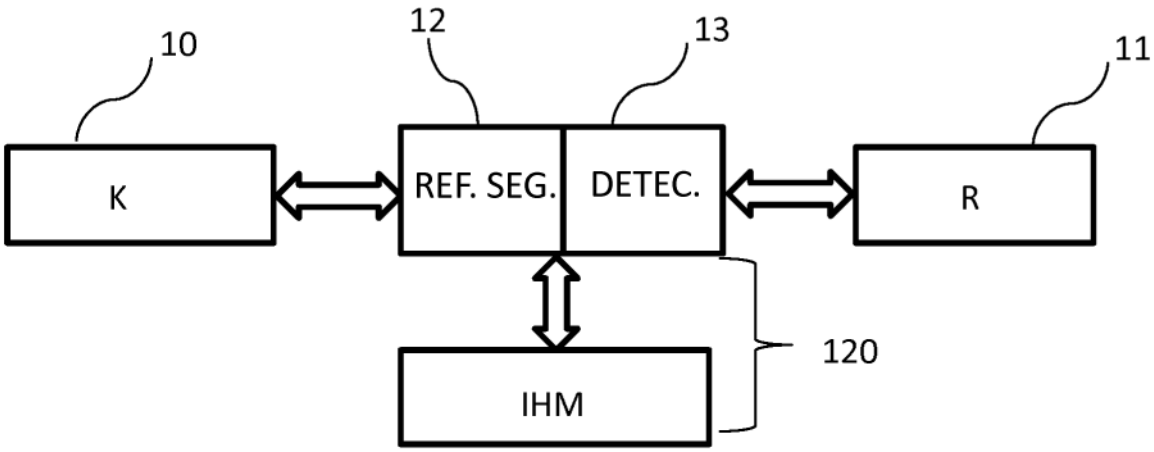

Figura 1a

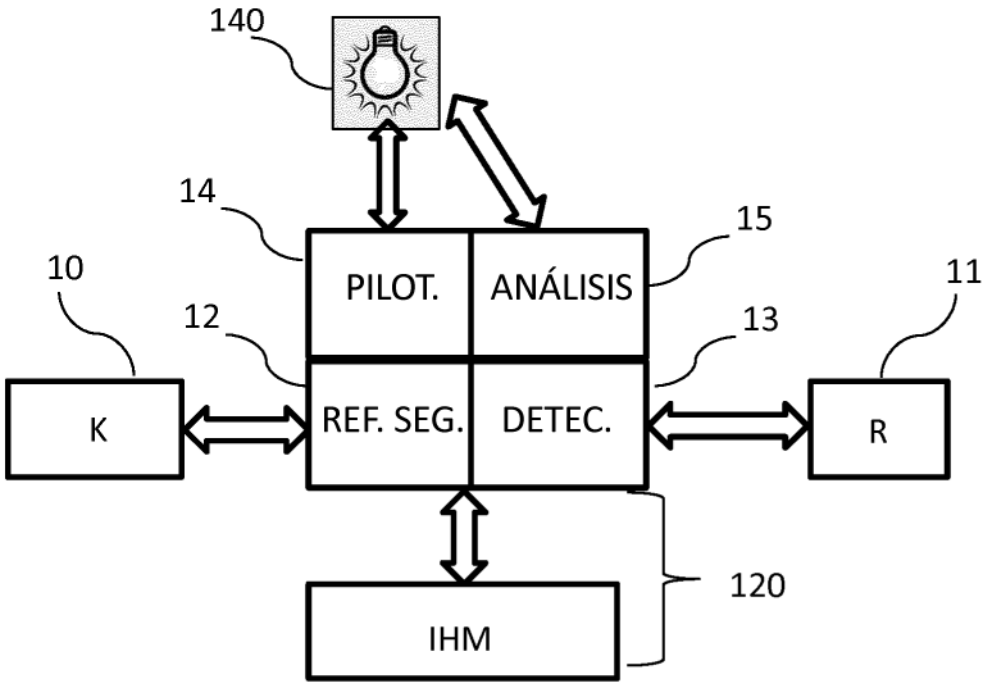

Figura 1b

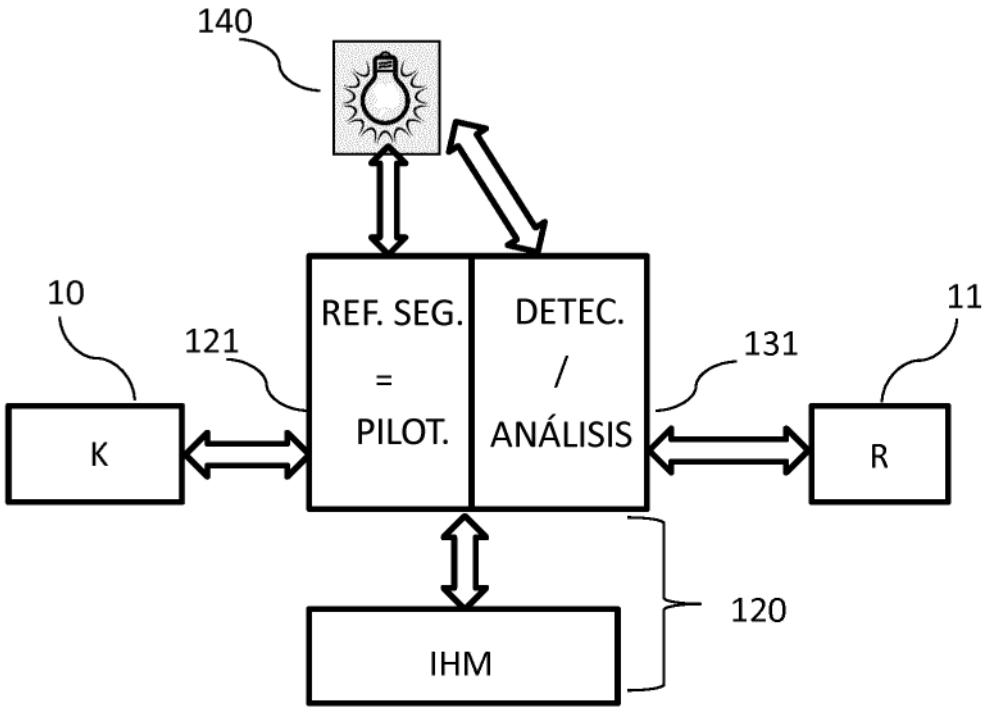

Figura 1c

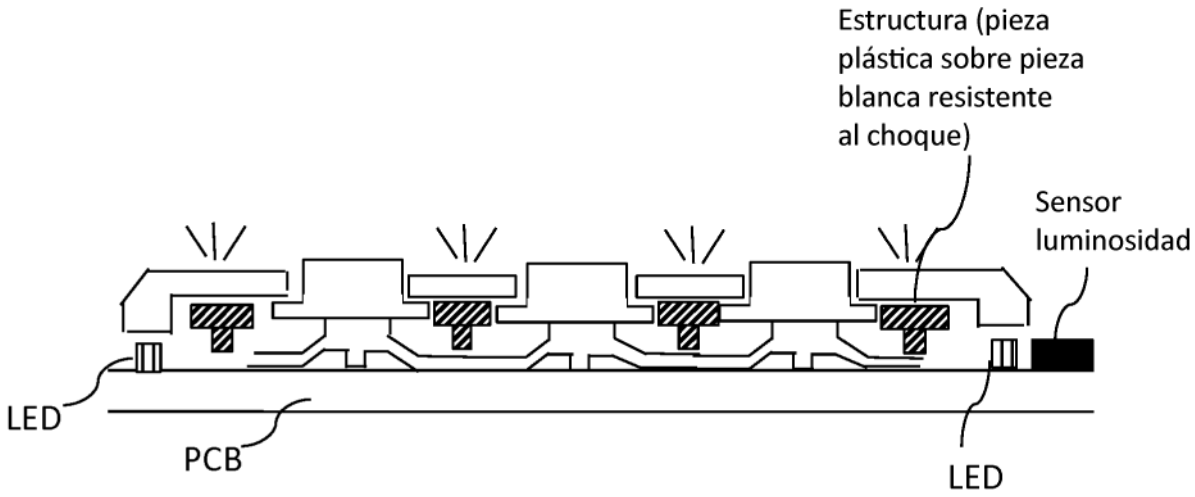

Figura 2a

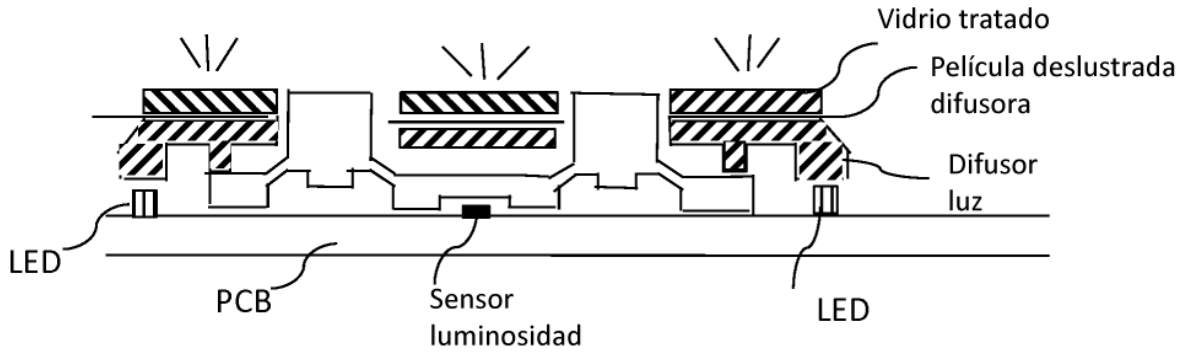

Figura 2b

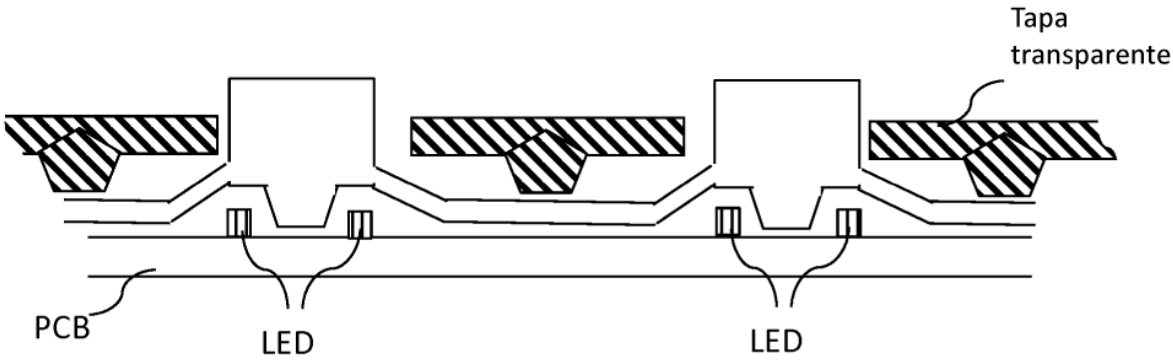

Figura 2c

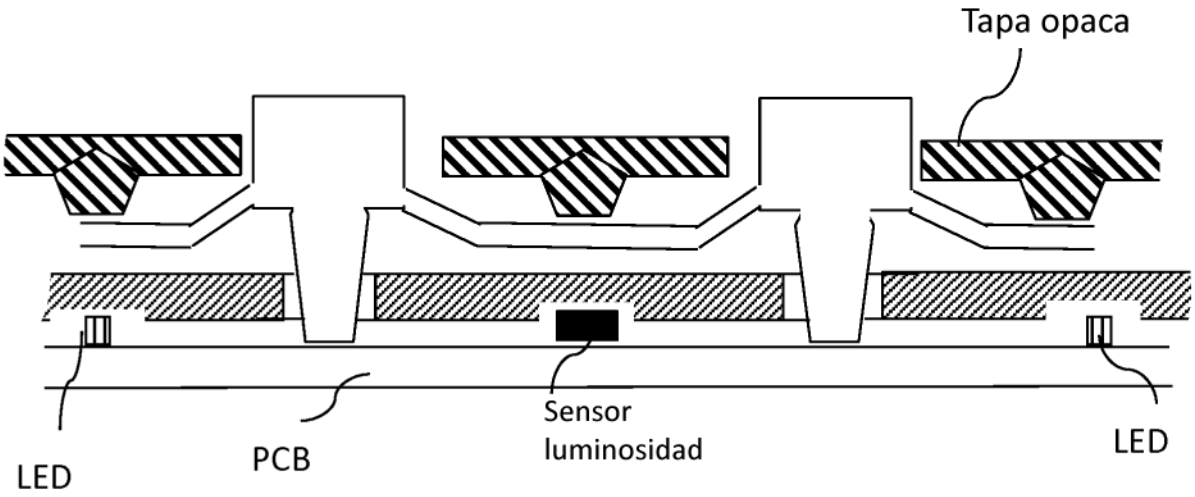

Figura 2d

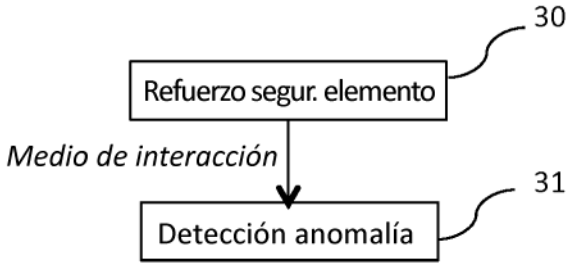

Figura 3