

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 883 604**

51 Int. Cl.:

G06F 21/83 (2013.01)

G06F 21/86 (2013.01)

H05K 5/02 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **09.05.2016 PCT/EP2016/060319**

87 Fecha y número de publicación internacional: **17.11.2016 WO16180772**

96 Fecha de presentación y número de la solicitud europea: **09.05.2016 E 16722160 (5)**

97 Fecha y número de publicación de la concesión europea: **30.06.2021 EP 3295365**

54 Título: **Detección de apertura de un dispositivo de entrada de datos**

30 Prioridad:

11.05.2015 FR 1554198

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

09.12.2021

73 Titular/es:

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

72 Inventor/es:

**BARNERON, SYLVAIN y
ROUX, JULIEN**

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 883 604 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Detección de apertura de un dispositivo de entrada de datos

1. Campo de la invención

5 La invención se refiere al campo de los dispositivos de entrada de datos, tales como terminales de pago. Más en particular, la invención se refiere al aumento de la seguridad en tales dispositivos de entrada de datos, por ejemplo por detección de apertura o de intrusión.

2. Técnica anterior

En los terminales de pago que procesan datos sensibles, es necesario protegerse contra intentos de fraude. De este modo, existen medidas de protección, en soporte físico y/o en soporte lógico.

10 Entre las medidas de protección en soporte físico, encontramos, en especial, las técnicas destinadas a detectar la apertura de la cubierta del terminal de pago electrónico, por intermedio, por ejemplo, de la puesta en práctica de "teclas falsas" de elastómero asociadas a "pads de carbono" o "cúpulas de metal", que permiten comprobar que el terminal no sufre un intento de desmontaje.

15 En efecto, un terminal de pago, según es convencional, comprende una semicarcasa superior y una semicarcasa inferior. La semicarcasa superior comprende aberturas que son utilizadas, por ejemplo, para dar paso a las teclas del teclado y la pantalla de presentación del terminal. En correspondencia con el teclado, los dispositivos "teclas falsas" se utilizan para comprobar que, por una parte, la semicarcasa superior del terminal está bien encastrada en la semicarcasa inferior y, por otra, que las teclas falsas descansan sobre al menos una placa de circuito impreso (placa madre) presente dentro del terminal de pago. Esto permite asegurarse de que el terminal de pago no está
20 abierto y, por tanto, que no se produce un intento de introducción de un dispositivo espía en correspondencia con el teclado del terminal de pago, por ejemplo. Las teclas falsas son presionadas, por ejemplo, por mediación de una extensión de plástico (maciza o no) que se extiende por el interior de la semicarcasa superior para venir a emplazarse sobre la tecla falsa de la placa de circuito impreso (placa madre). Esta solución de la técnica anterior es generalmente bastante eficaz. No obstante, esta solución es muy antigua y no necesariamente es apta para los
25 nuevos tipos de terminales de pago.

En efecto, es difícil crear tales teclas falsas cuando las teclas del teclado están dispuestas de manera compacta y apretada, pues la solución de la técnica anterior precisa de espacios relativamente importantes entre las teclas, con el fin de que puedan atravesar el teclado extensiones de plástico que se extienden por el interior de la semicarcasa superior y venir a emplazarse sobre la tecla falsa de la placa madre. Ahora bien, desde una perspectiva de
30 reducción del tamaño de los terminales de pago, no obligatoriamente está presente el espacio disponible para tales extensiones de plástico.

Otro inconveniente se debe a la propia fabricación de la extensión de plástico y, desde una perspectiva más general, a la fabricación de la semicarcasa superior. Esta fabricación es problemática tanto desde el punto de vista estético como desde el punto de vista de la seguridad. Desde el punto de vista estético, en la cara externa, visible, de la semicarcasa superior, la presencia de las extensiones provoca una leve deformación ahuecada, en el lugar donde
35 se sitúa esta extensión. Esto es debido a que la semicarcasa inferior y la semicarcasa superior, como también la mayoría de las demás piezas plásticas necesarias para la fabricación del terminal, se fabrican con el concurso de un procedimiento de inyección consistente en introducir, en un molde, material plástico caliente bajo presión. La inyección plástica provoca deformaciones en ciertos lugares de las piezas, por ejemplo en correspondencia con las extensiones. El problema de la seguridad se deriva de este problema estético. Y es que un atacante sabe justamente donde se sitúan las teclas falsas observando el teclado: las deformaciones que hay presentes entre las teclas, en los lugares donde las extensiones de plástico se prolongan hacia las teclas falsas dispuestas sobre la placa madre del terminal, permiten identificar con facilidad la ubicación de estas teclas falsas y, por consecuencia,
40 dar una indicación al atacante sobre los lugares donde no se sitúan estas teclas falsas. El atacante, entonces, puede tratar de perforar la semicarcasa superior para introducir en ella un dispositivo espía.

Finalmente, a un atacante le es posible, con facilidad, pegar la tecla falsa, así como el plástico que la sujeta y recortar luego la tapa sobre la que va apoyada. Por lo tanto, un atacante cuenta con un subconjunto constituido a partir del circuito impreso (por ejemplo, una PCB o "Printed Circuit Board" en inglés), de la tecla falsa y de un trozo de cubierta, fácil de manipular. La protección, por lo tanto, es fácil de sortear, aun si le hace perder tiempo al
50 atacante y, con ello, aumenta los riesgos que debe correr.

El documento EP 2924606 A1 describe un elemento de seguridad de un dispositivo de entrada de datos, montado entre dos circuitos impresos al objeto de que sus dos extremos cierren respectivamente unos contactos sobre dichos dos circuitos impresos de dicho dispositivo de entrada de datos cuando dicho dispositivo de entrada de datos se halla en posición cerrada, no estando dichos extremos conectados eléctricamente entre sí.

55

3. Sumario

La invención propone una nueva solución que no presenta el conjunto de estos inconvenientes de la técnica anterior, en forma de un elemento de seguridad de un dispositivo de entrada de datos, presentando el elemento de seguridad una forma adaptada para cerrar unos contactos por intermedio de cada uno de sus dos extremos respectivamente sobre dos circuitos impresos del dispositivo de entrada de datos cuando el dispositivo de entrada de datos se halla en posición cerrada, no estando los extremos conectados eléctricamente entre sí, correspondiendo dicha forma adaptada a un cilindro almenado en al menos una parte de la altura de su superficie externa.

De este modo, la invención propone una solución novedosa e inventiva del aumento de la seguridad en un dispositivo de entrada de datos, que permite crear una zona provista de seguridad en el interior del dispositivo, entre dos circuitos impresos, por mediación de un elemento de seguridad único.

Para hacer esto, la invención prevé la puesta en práctica de una a modo de “tecla falsa de doble cara” que apoya, por intermedio de cada uno de sus extremos, en dos circuitos impresos, no estando unidos eléctricamente entre sí los dos extremos de la tecla falsa. De este modo, los dos circuitos impresos se hacen seguros mutuamente, por intermedio de este elemento de seguridad, pues, si se retira o se deteriora, se detecta una intrusión/fractura, sobre uno u otro de los circuitos impresos.

En efecto, cuando el dispositivo de entrada de datos se halla en posición cerrada, cada uno de los dos extremos del elemento de seguridad cierra respectivamente uno o varios contactos sobre cada uno de los dos circuitos impresos, al objeto de poder detectar una apertura de estos contactos tan pronto como es abierto el dispositivo de entrada de datos. En este caso, en efecto, el elemento de seguridad ya no está en contacto con uno de los circuitos impresos, o los dos, y esta ruptura de los contactos es detectada por los circuitos de detección previstos al efecto sobre cada uno de los dos circuitos impresos.

Es de señalar que los dos extremos del elemento de seguridad no están unidos electrónicamente entre sí, por lo que no permiten conectar eléctricamente los dos circuitos impresos entre ellos. El propósito que se pretende, en efecto, no es detectar una ruptura de conexión entre dos circuitos impresos unidos entre sí por intermedio de un elemento tal como un Zebra, sino, realmente, detectar la apertura del dispositivo de entrada de datos merced a un elemento de seguridad que constituye una “tecla falsa de doble cara”.

De este modo, de acuerdo con la invención, el elemento de seguridad presenta una forma de cilindro almenado, particularmente adaptada para limitar las respectivas presiones sobre los dos circuitos impresos.

De acuerdo con un aspecto particular de la invención, el elemento de seguridad presenta una excrecencia de forma cilíndrica en cada extremo, estando las excrecencias destinadas a encargarse de los contactos con cada uno de los circuitos impresos.

De este modo, de acuerdo con esta forma de realización de la invención, el elemento de seguridad presenta dos excrecencias, en cada extremo del cilindro, al objeto de encargarse de los contactos con cada uno de los dos circuitos impresos.

Es de señalar que estas excrecencias pueden ser de diferente tamaño, por ejemplo según el espacio disponible sobre cada uno de los dos circuitos impresos.

De acuerdo con una característica particular de la invención, el elemento de seguridad presenta adicionalmente al menos una aleta de posicionamiento que se extiende lateralmente en una parte de su altura, destinada a encargarse del posicionamiento y la sujeción del elemento de seguridad dentro de al menos un alojamiento previsto en uno de los dos circuitos impresos.

De este modo, de acuerdo con esta forma de realización de la invención, el elemento de seguridad presenta, asimismo, una aleta de posicionamiento, que se extiende lateralmente en una parte de su altura, y que permite su posicionamiento dentro de un alojamiento previsto en al menos uno de los dos circuitos impresos.

En efecto, es preferible que la posición de este elemento de seguridad en el dispositivo de entrada sea evidente a la hora del montaje del dispositivo de entrada, al objeto de evitar todo error de montaje y todo mal funcionamiento ulterior. De este modo, el alojamiento previsto para el elemento de seguridad, en uno de los dos circuitos impresos, prevé un entrante en el que pasa a insertarse la aleta del elemento de seguridad, que se encarga de su posicionamiento y su sujeción correctos.

Asimismo, la invención concierne a un dispositivo de entrada de datos, que comprende al menos un elemento de seguridad tal como se ha descrito anteriormente, emplazándose el elemento de seguridad entre dos circuitos impresos del dispositivo de entrada de datos, en al menos un alojamiento previsto en uno de los circuitos impresos, cerrando el elemento de seguridad unos contactos por intermedio de cada uno de sus dos extremos respectivamente sobre los dos circuitos impresos del dispositivo de entrada de datos cuando el dispositivo de entrada de datos se halla en posición cerrada.

Tal dispositivo de entrada de datos corresponde, por ejemplo, a un terminal de pago electrónico y presenta el conjunto de las características expuestas anteriormente en relación con el elemento de seguridad.

5 También concierne la invención a un procedimiento de detección de una intrusión en un dispositivo de entrada de datos tal como se ha descrito anteriormente, que comprende una etapa de detección de una intrusión cuando es abierto al menos un contacto entre uno de los dos extremos del elemento de seguridad y uno de los dos circuitos impresos.

Tal procedimiento de detección de una intrusión se lleva a la práctica en el dispositivo de entrada de datos, por ejemplo un terminal de pago electrónico, y presenta el conjunto de las características expuestas anteriormente en relación con el dispositivo de entrada de datos y con el elemento de seguridad.

10 **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:

15 la figura 1 es una vista esquemática de una parte de un terminal de pago según una forma de realización de la invención;

la figura 2 ilustra un ejemplo de un elemento de seguridad según una forma de realización de la invención; y

las figuras 3a y 3 ilustran una parte de un circuito impreso de un terminal de pago electrónico que presenta un alojamiento para un elemento de seguridad, respectivamente sin un elemento de seguridad montado y con él, según una forma de realización de la invención.

20 **5. Descripción**

Consiste el principio general de la técnica descrita en hacer seguro un dispositivo de entrada de datos protegiendo dos circuitos impresos del dispositivo con una sola "tecla falsa" que, montada entre los dos circuitos impresos, cierra unos contactos sobre sus dos extremos. Tal "tecla falsa" se denomina en lo sucesivo "tecla falsa de doble cara" o elemento de seguridad.

25 De este modo, la solución según las diferentes formas de realización de la invención permite crear una zona provista de seguridad entre dos circuitos impresos de un dispositivo de entrada de datos, por ejemplo entre una PCB (o FPC, por "Flexible Printed Circuit") y otra PCB (o FPC), cada uno de los cuales comprende una malla, por mediación de un elemento de seguridad montado entre los dos circuitos impresos. Estos dos circuitos impresos se hacen seguros uno al otro en cierto modo, pues, si se retira la "tecla falsa de doble cara", ya sea por un lado como por el otro (es decir, sobre uno u otro de los circuitos impresos), se detectará una fractura.

30 Por ejemplo, uno de los dos circuitos impresos corresponde a la placa madre, y el otro puede corresponder a una PCB o un FPC destinado a proteger una función (por ejemplo, un lector de tarjetas inteligentes) o a crear una zona provista de seguridad en la que se podrán ubicar componentes sensibles y/o hacer que transite información sensible.

35 En lo sucesivo, se describen más en particular unas formas de realización en las cuales el dispositivo de entrada de datos corresponde a un terminal de pago electrónico, aunque la invención es de aplicación en todo dispositivo de entrada de datos que responda a las mismas problemáticas de aumento de la seguridad.

40 Se describe a continuación, en relación con la figura 1, un ejemplo de puesta en práctica de la invención en un terminal de pago electrónico que presenta especialmente un primer circuito impreso 10 que corresponde, por ejemplo, a un FPC, y un segundo circuito impreso 11, que corresponde, por ejemplo, a la placa madre. De acuerdo con esta forma de realización, el terminal de pago electrónico presenta, asimismo, un lector de tarjetas inteligentes 13 con una ranura de inserción 14 para la tarjeta.

45 Finalmente, se monta un elemento de seguridad 12 al objeto de establecer contacto, por intermedio de cada uno de sus extremos, con los dos circuitos impresos 10 y 11, en unas ubicaciones específicas, cuando el terminal de pago electrónico se halla en posición cerrada para su utilización (es decir, cuando todos los elementos están montados y efectuado el cierre de las dos partes de la cubierta).

De acuerdo con esta forma de realización de la invención, el elemento de seguridad 12 va montado en la parte posterior del lector de tarjetas, pero se pueden escoger ubicaciones diferentes, según la implantación de los demás elementos del terminal de pago electrónico, por ejemplo.

50 Es de señalar, además, que los dos extremos del elemento de seguridad 12 no están conectados eléctricamente, al objeto de no conectar los dos circuitos impresos cuando queda posicionado el elemento de seguridad. En efecto, el propósito que se pretende mediante la solución según las diferentes formas de realización de la invención no es el

5 de encargarse de un contacto entre dos circuitos impresos por intermedio de un elemento de aumento de seguridad (como, por ejemplo, elementos de aumento de la seguridad conocidos, tales como Zebras previstos para hacer segura una zona por detección de ruptura de contacto desempeñado por el propio Zebra), sino detectar una fractura/intrusión en un dispositivo de entrada de datos merced a un elemento de seguridad que actúa por dos lados para hacer contacto con dos circuitos impresos distintos.

10 De este modo, al contrario que las soluciones de la técnica anterior, aun si un atacante pega la "tecla falsa de doble cara" y su soporte, estará obligado a manipular el conjunto constituido por la "tecla falsa de doble cara", su soporte, así como los dos circuitos impresos. Se conserva, pues, el recinto provisto de seguridad constituido y, si el atacante quiere acceder a esta zona segura y a sus componentes, está obligado a intentar cortocircuitar la malla o los contactos, lo cual precisa de mucho más tiempo y aumenta considerablemente el riesgo de originar una fractura.

15 Además, al utilizarse una sola "tecla falsa de doble cara" para hacer seguros dos circuitos, el esfuerzo (debido a la compresión de las teclas falsas) originado sobre las tapas del dispositivo de entrada de datos es dos veces menor que si se utilizaran dos teclas falsas para hacer seguros respectivamente cada uno de los circuitos impresos. Por lo tanto, la solución de la invención, según sus diferentes formas de realización, no incide en la fiabilidad del dispositivo seguro, e incluso la refuerza, ya que se divide por dos el riesgo de que una de las teclas falsas funcione mal.

Se describe a continuación, con mayor detalle, la estructura de un elemento de seguridad 12, en relación con la figura 2, según una forma de realización de la invención.

20 De acuerdo con esta forma particular de realización de la invención ilustrada en la figura 2, el elemento de seguridad 12 presenta una forma cilíndrica dentellada/almenada 121, en casi toda su altura, que especialmente permite reducir la presión sobre los circuitos impresos.

25 En efecto, en esta forma de realización, el alojamiento previsto para la "tecla falsa de doble cara" debe presentar un diámetro lo suficientemente grande con el fin de poder alojar en él el circuito FPC. Un elemento de seguridad correspondiente a un simple cilindro que ocupe todo el espacio dentro del alojamiento originaría un gran volumen de material que comprimir y, por tanto, grandes esfuerzos sobre la tapa. Por lo tanto, la forma específica del cilindro con estas nervaduras permite reducir el volumen de material que comprimir y, por tanto, los esfuerzos sobre las tapas, al propio tiempo que conserva un buen guiado dentro del alojamiento.

30 Además, el elemento de seguridad 12 presenta una excrecencia 122 en cada uno de sus extremos, para encargarse de los respectivos contactos con cada uno de los dos circuitos impresos. De acuerdo con la variante ilustrada en la figura 2, las dos excrecencias presentan tamaños diferentes, al objeto de adaptarse a la configuración de los circuitos impresos y, en especial, del espacio disponible. Sin embargo, estas excrecencias pueden ser idénticas. Estas partes específicas del elemento de seguridad 12, los extremos 122, son los que hacen presión sobre cada uno de los circuitos impresos cuando el dispositivo de entrada de datos se halla en posición cerrada, al objeto de cerrar uno o varios contactos. Por otro lado, la apertura de este o estos contactos es detectada por uno o varios circuitos de detección de cada uno de los circuitos impresos en caso, especialmente, de un intento de fractura por remoción de la "tecla falsa de doble cara" o alejamiento de uno de los dos circuitos de uno de los extremos de esta "tecla falsa de doble cara".

40 Finalmente, de acuerdo con esta forma de realización de la invención, el elemento de seguridad 12 presenta asimismo una a modo de aleta lateral que permite asegurar, en el montaje, su correcto posicionamiento, y prevista especialmente para coincidir con un entrante dentro del alojamiento destinado al elemento de seguridad, en uno u otro de los circuitos impresos. En efecto, en virtud de su forma simétrica, sin esta aleta, el elemento de seguridad 12 podría quedar mal posicionado dentro del dispositivo de entrada de datos (es decir, su posicionamiento podría ser ambiguo) y, potencialmente, dar origen a un mal funcionamiento. La presencia de la aleta permite obviar este inconveniente, limitando las posibilidades de posicionamiento a una sola posibilidad, en virtud, asimismo, de la forma del soporte/alojamiento presente en uno u otro de los circuitos impresos.

45 Este posicionamiento del elemento de seguridad 12 se ilustra especialmente en la figura 3b, la cual ilustra una parte del circuito impreso que presenta un alojamiento previsto para recibir el elemento de seguridad.

50 La figura 3a ilustra esta misma parte del circuito impreso 10 (por ejemplo, un FPC o una placa hija) sin el elemento de seguridad 12. Por lo tanto, este circuito impreso 10 presenta un alojamiento 30 asimismo de forma cilíndrica, destinado a recibir el elemento de seguridad 12, y que presenta un entrante 301 destinado a recibir la aleta 123 del elemento de seguridad 12, para un posicionamiento correcto y preciso del elemento de seguridad.

Una vez posicionado dentro del alojamiento 30 (como se ilustra en la figura 3b), el elemento de seguridad 12 queda sujeto sobre el circuito impreso 10, por lo que puede desempeñar su función de aumento de la seguridad en el dispositivo de entrada de datos, cuando se hace llegar el segundo circuito impreso 11 (no ilustrado en la figura 3b) a contactar, por presión, con el otro extremo del elemento de seguridad.

55 Estos diferentes elementos (elemento de seguridad 12, alojamiento 30 dentro del circuito impreso...) están asociados a uno o varios circuitos de detección de intrusión, basados en la detección de apertura de contacto. Así, el

procedimiento de detección de una intrusión en tal dispositivo de entrada de datos seguro lleva a la práctica una etapa de detección de una intrusión cuando son abiertos uno o varios contactos, entre al menos uno de los extremos del elemento de seguridad 12 y el circuito impreso. Esta detección es llevada a la práctica especialmente por el o los circuitos de detección de intrusión, en sí conocidos y no descritos en el presente documento.

- 5 De acuerdo con una forma de realización de la invención, los dos extremos del elemento de seguridad son, por ejemplo, pastillas con carga de carbono y, por tanto, conductoras, mientras que la parte central de forma cilíndrica dentellada y la aleta son de silicona, por lo que constituyen un aislante. Por supuesto, se pueden utilizar cualesquiera otros materiales que permitan, por una parte, conferir un carácter conductor a los dos extremos del elemento de seguridad y un carácter aislante a su parte central y su aleta.

10

REIVINDICACIONES

- 5 1. Elemento de seguridad (12) de un dispositivo de entrada de datos, que presenta una forma adaptada para cerrar unos contactos por intermedio de cada uno de sus dos extremos respectivamente sobre dos circuitos impresos (10, 11) de dicho dispositivo de entrada de datos cuando dicho dispositivo de entrada de datos se halla en posición cerrada, no estando dichos extremos conectados eléctricamente entre sí, caracterizado por que dicha forma adaptada corresponde a un cilindro almenado (121) en al menos una parte de la altura de su superficie externa.
2. Elemento de seguridad según la reivindicación 1, caracterizado por que presenta una excrecencia (122) de forma cilíndrica en cada extremo, estando dichas excrecencias destinadas a encargarse de los contactos con cada uno de los circuitos impresos.
- 10 3. Elemento de seguridad según una cualquiera de las reivindicaciones 1 y 2, caracterizado por que presenta adicionalmente al menos una aleta de posicionamiento (123) que se extiende lateralmente en una parte de su altura, destinada a encargarse del posicionamiento y la sujeción de dicho elemento de seguridad dentro de al menos un alojamiento previsto en uno de los dos circuitos impresos.
- 15 4. Dispositivo de entrada de datos, caracterizado por que comprende al menos un elemento de seguridad según una de las reivindicaciones 1 a 3, emplazándose dicho elemento de seguridad entre dos circuitos impresos de dicho dispositivo de entrada de datos, en al menos un alojamiento previsto en uno de dichos circuitos impresos, cerrando el elemento de seguridad unos contactos por intermedio de cada uno de sus dos extremos respectivamente sobre dichos dos circuitos impresos de dicho dispositivo de entrada de datos cuando dicho dispositivo de entrada de datos se halla en posición cerrada.
- 20 5. Procedimiento de detección de una intrusión en un dispositivo de entrada de datos según la reivindicación 4, caracterizado por que comprende una etapa de detección de una intrusión cuando es abierto al menos un contacto entre uno de los dos extremos de dicho elemento de seguridad y uno de dichos dos circuitos impresos.

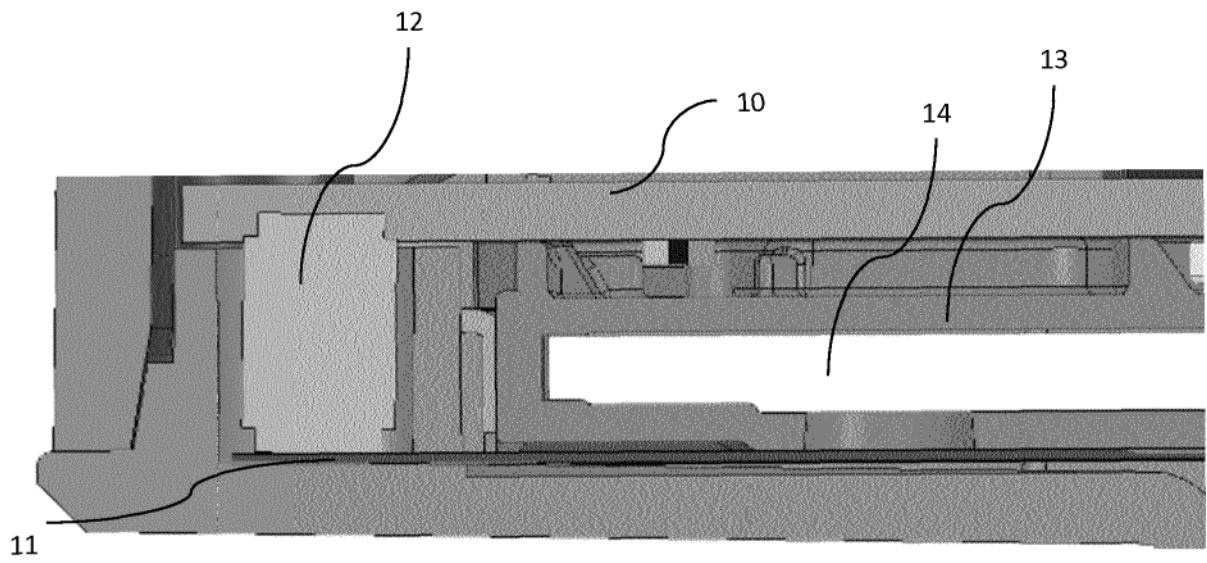


Figura 1

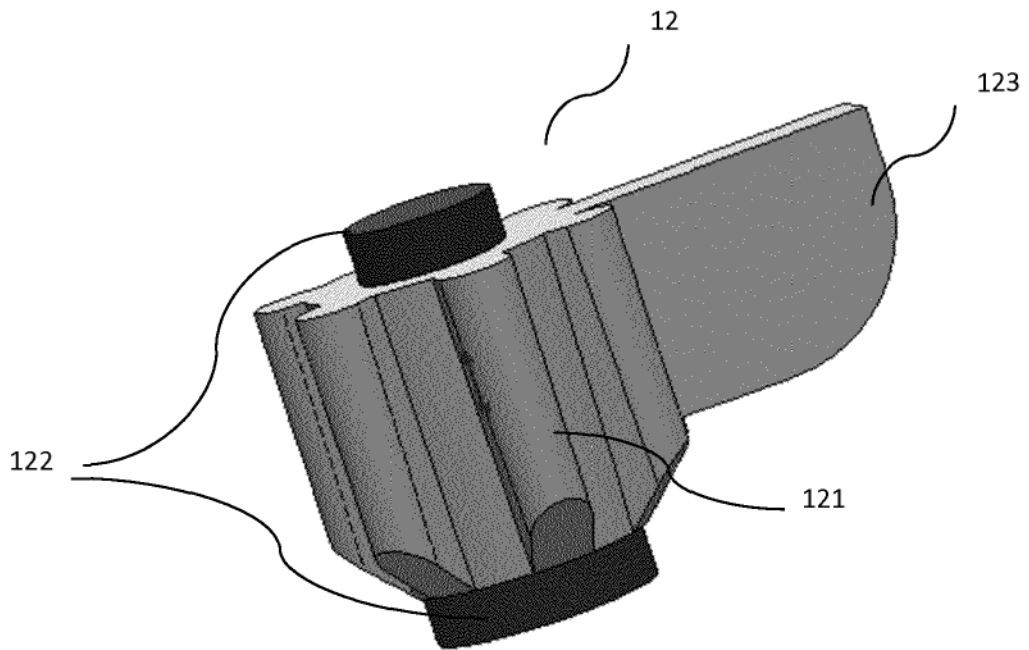


Figura 2

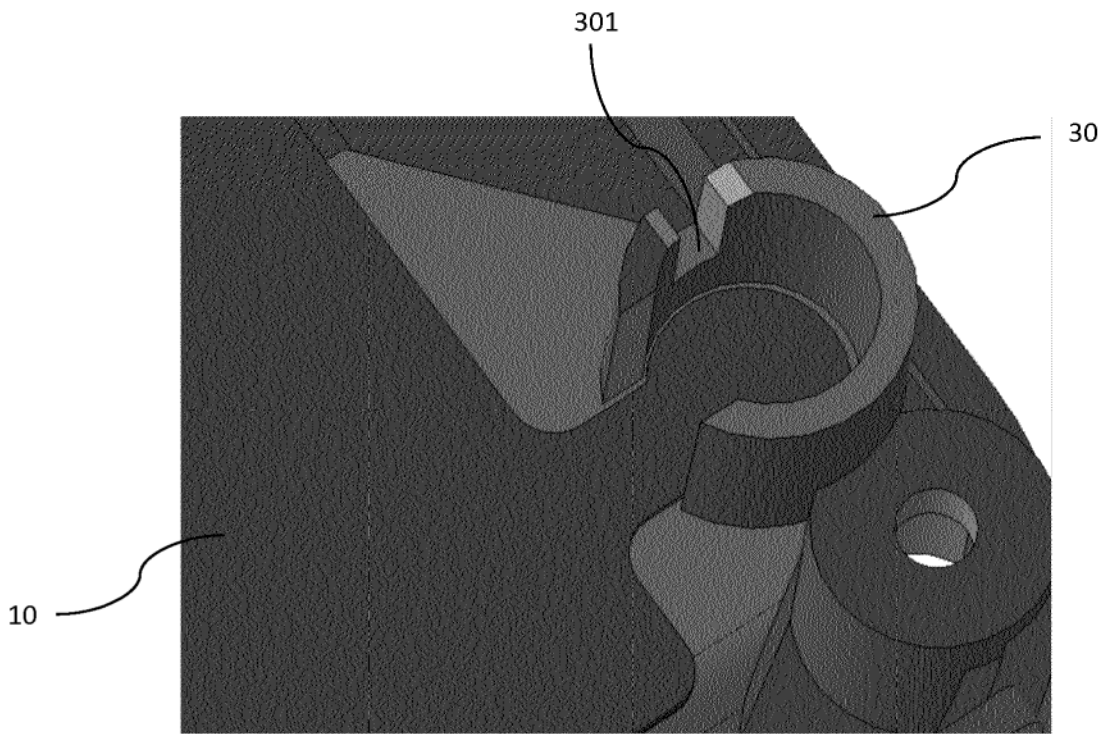


Figura 3a

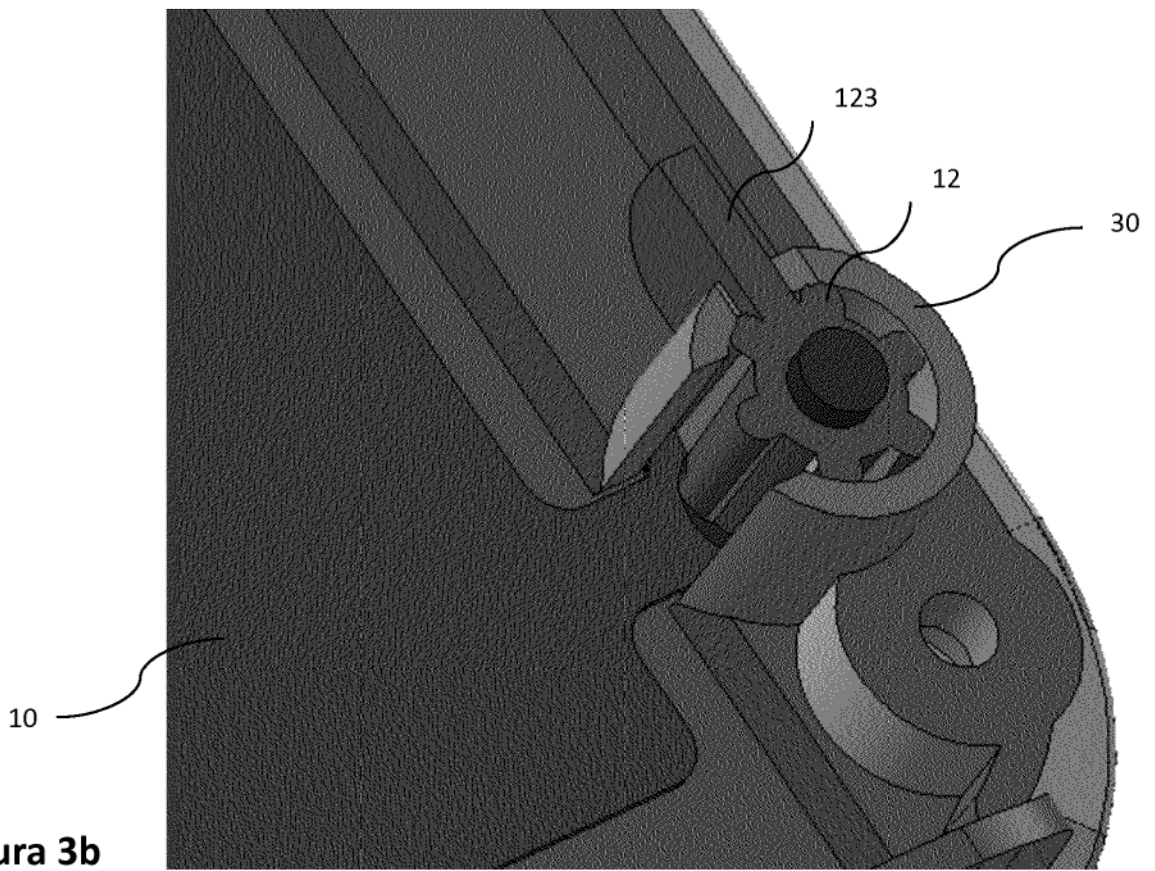


Figura 3b