(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 534 591**

(51) Int. CI.:

G06F 3/0488 (2013.01)
G06F 21/31 (2013.01)
G06F 21/34 (2013.01)
G06F 21/82 (2013.01)
G07F 7/10 (2006.01)
G06F 3/048 (2013.01)
G07F 19/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.11.2011 E 11191060 (0)**

(97) Fecha y número de publicación de la concesión europea: **28.01.2015 EP 2458491**

(54) Título: **Dispositivo para leer tarjetas de banda magnética y/o inteligentes con pantalla táctil para la introducción del PIN**

(30) Prioridad:

29.11.2010 DE 102010060862

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2015

(73) Titular/es:

WINCOR NIXDORF INTERNATIONAL GMBH (100.0%)
Heinz-Nixdorf-Ring 1
33106 Paderborn, DE

(72) Inventor/es:

GOLÜCKE, PETER y
CAROZZI, ANDREA

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Dispositivo para leer tarjetas de banda magnética y/o inteligentes con pantalla táctil para la introducción del PIN

La invención concierne a un dispositivo para leer tarjetas de banda magnética y/o inteligentes, especialmente para leer tarjetas bancarias, tarjetas EC y/o tarjetas de crédito. El dispositivo comprende una unidad de visualización y un módulo táctil dispuesto delante de la unidad de visualización, el cual comprende al menos un sensor para obtener una posición de un toque de una zona de visualización. Asimismo, el dispositivo tiene un módulo de seguridad para controlar la unidad de visualización y el módulo táctil.

El dispositivo consiste especialmente en un cajero automático, un sistema de caja automático, una caja fuerte automática y/o un terminal de pagos que se utiliza, por ejemplo, en empresas del comercio minorista y/o en restaurantes para el pago sin dinero en efectivo del importe de facturas por medio de una tarjeta de banda magnética y/o inteligente, especialmente una tarjeta EC o una tarjeta de crédito. En dispositivos conocidos un usuario introduce una tarjeta de banda magnética y/o inteligente en una ranura prevista para ello. Con ayuda de una unidad de lectura se leen datos de la tarjeta de banda magnética y/o inteligente, a través de la cual se autentifica el usuario. Los dispositivos comprenden una unidad de visualización, a través de la cual se invita al usuario a introducir un número de identificación personal, un llamado PIN, debiendo asegurarse a través de la introducción del PIN que el usuario está también autorizado para sacar dinero y/o pagar con ayuda de la tarjeta de banda magnética y/o inteligente introducidas. El usuario introduce seguidamente el PIN a través de un teclado previsto para ello, especialmente a través de un llamado teclado de Pin encriptado (EPP, acrónimo de Encrypted Pin Pad).

En esta introducción del PIN a través del teclado es problemático el hecho de que se tiene que prever para ello adicionalmente un teclado EPP de adquisición relativamente cara para asegurar que no se pueda interceptar el PIN introducido. Asimismo, tiene que estar previsto para el teclado EPP un espacio de montaje que sea de escasas dimensiones en los dispositivos citados. Además, estos teclados EPP son susceptibles de intentos de clonación (skimming), ya que se pueden aplicar sencillamente sobre ellos unos teclados adicionales a través de los cuales se espía el PIN.

Se conoce por el documento DE 10 2008 014 324 A1 un aparato de autoservicio que comprende una unidad de mando y una superficie de cubierta con escotaduras que rodea a la unidad de mando.

Se conoce por el documento DE 10 2008 021 046 A1 un procedimiento para la puesta en funcionamiento de un teclado de un terminal de autoservicio.

Se conoce por el documento US 6.317.835 B1 un sistema para generar discrecionalmente datos cifrados y no cifrados.

La reivindicación 1 está limitada frente al documento US 6317835 B1.

El problema de la invención consiste en indicar un dispositivo para leer tarjetas de banda magnética y/o inteligentes que haga posible una introducción segura de un número de identificación personal.

Este problema se resuelve por medio de un dispositivo con las características de la reivindicación 1. En las reivindicaciones subordinadas se indican perfeccionamientos ventajosos de la invención.

Mediante el cifrado de los segundos datos, que comprenden informaciones sobre la posición del toque de la zona de visualización, se consigue por medio del módulo táctil y la transmisión cifrada de estos datos al módulo de seguridad que la posición del toque sea cifrada inmediatamente por el módulo táctil, de modo que las informaciones sobre la posición del toque no se transmitan sin cifrar. Por tanto, se evita una interceptación de las informaciones no cifradas y se evita así que se saquen conclusiones sobre la cifra del número de identificación personal señalada por la posición del toque o sobre todo el número de identificación personal. Se hace posible así una introducción segura del PIN. Mediante la transmisión de los primeros datos con informaciones para la representación de un teclado con ayuda de la unidad de visualización desde el módulo de seguridad hasta la unidad de visualización se asegura que no pueda manipularse la información representada con ayuda de la unidad de visualización y que el teclado para la introducción del PIN se visualice solamente cuando esto sea también necesario para el desarrollo del proceso.

El módulo táctil comprende preferiblemente su unidad de procesamiento, especialmente un procesador, que cifra los segundos datos. El módulo táctil presenta preferiblemente un criptoprocesador separado con cuya ayuda se cifran los datos. Por criptoprocesador se entiende especialmente una pastilla electrónica o un microprocesador que reúne en si las funciones básicas para la comunicación segura de datos, tales como la criptografía, la autentificación y la administración de claves de criptología.

El dispositivo consiste especialmente en un dispositivo para la manipulación de efectos de valor, por ejemplo un cajero automático, una caja fuerte automática y/o un sistema de caja automático. Asimismo, el dispositivo puede consistir también en un terminal de pagos, por ejemplo un terminal para el pago sin dinero en efectivo en filiales del

comercio minorista y/o en establecimientos de gastronomía. Además, el dispositivo puede ser también una impresora de extractos de cuentas y/o un terminal de información en una filial bancaria.

El dispositivo comprende especialmente un aparato lector en el que se introduce la tarjeta de banda magnética o inteligente y que lee los datos de la tarjeta de banda magnética o inteligente. Después de la lectura de los datos se invita al usuario del dispositivo, especialmente a través de la unidad de visualización, a que introduzca el PIN para asegurarse así de que el usuario está autorizado para utilizar la tarjeta de banda magnética y/o inteligente.

La zona de visualización sobre la cual se detecta la posición del toque puede estar formada por un cristal de la unidad de visualización y/o un cristal separado del módulo táctil. Asimismo, la unidad de visualización y el módulo táctil pueden estar configurados como integrados en forma de una pantalla táctil. La detección de la posición del toque a través del sensor se efectúa especialmente por vía óptica, resistiva, capacitiva y/o inductiva.

El módulo táctil puede ser especialmente un módulo táctil resistivo en el que el sensor comprende dos capas conductivas dispuestas delante de la unidad de visualización, estando aplicada una tensión a al menos una de estas capas y detectándose las tensiones en los bordes de la al menos una capa. En función de estas tensiones detectadas se detecta la posición del toque, especialmente con ayuda de la unidad de procesamiento del módulo táctil. Una de las dos capas puede estar configurada especialmente por el cristal.

Como alternativa, al módulo táctil puede ser también un módulo táctil capacitivo que comprende un cristal que está revestido con una capa transparente de óxido metálico. En las esquinas del revestimiento está aplicada una tensión eléctrica que genera un campo eléctrico uniforme. Mediante el toque del cristal se originan pequeñas corrientes que se miden en las esquinas. Las corrientes resultantes están en relación directa con la posición en la que el cristal del módulo táctil es tocado por un usuario. El cristal puede ser también un cristal de la unidad de visualización.

En otra forma de realización alternativa puede estar previsto también un módulo táctil que determina la posición del toque con ayuda de luz infrarroja. En este caso, el módulo táctil comprende unos diodos emisores de luz infrarroja que generan una red de rayos infrarrojos a través del cristal. Enfrente de los diodos emisores de luz infrarroja están previstos unos diodos detectores de luz infrarroja que reciben los rayos infrarrojos emitidos sin interrupción de los mismos. Al producirse un toque del cristal se interrumpe al menos una parte de los rayos infrarrojos emitidos, de modo que una parte de los diodos detectores no capta ninguna radiación infrarroja o bien capta una radiación infrarroja sensiblemente más pequeña. En función de esto, se determina la posición el toque, especialmente con ayuda de la unidad de procesamiento.

Los primeros datos y/o los segundos datos pueden transmitirse en forma de señales. Por disposición del módulo táctil delante de la unidad de visualización se entiende especialmente que el módulo táctil está dispuesto delante de una zona de visualización de la unidad de visualización. La zona de captación del módulo táctil para captar el toque está dispuesta preferiblemente entre la unidad de visualización y el usuario. En una forma de realización preferida de la invención el módulo de seguridad cifra los primeros datos y transmite estos datos cifrados a la unidad de visualización. Se consigue de esta manera que se impidan o al menos se dificulten una manipulación de los primeros datos y, por tanto, la manipulación de la información visualizada con ayuda de la unidad de visualización. En particular, se impide con esto que, ante una intención fraudulenta, se visualice en la unidad de visualización un teclado con la invitación a introducir el PIN.

El módulo táctil determina especialmente una primera coordenada y/o una segunda coordenada de la posición del toque de la zona de visualización y determina un primer valor de transmisión por adición de un primer valor de decalaje a la primera coordenada y/o un segundo valor de transmisión por adición de un segundo valor de decalaje a la segunda coordenada. Los segundos datos comprenden informaciones sobre el primer valor de transmisión y/o el segundo valor de transmisión. Mediante la adición de los valores de decalaje se consigue que no se transmita la coordenada real, sino un valor numérico modificado. Por tanto, se consigue que no sea posible deducir la posición del toque de la zona de visualización a partir de los valores de transmisión. En particular, sin los valores de decalaje se tiene que, solamente en base a los valores de transmisión, no se pueden sacar conclusiones sobre la cifra o el PIN introducidos a través del módulo táctil. La determinación de los valores de transmisión se efectúa especialmente con ayuda de la unidad de procesamiento del módulo táctil.

El módulo táctil determina preferiblemente el primer valor de decalaje y/o el segundo valor de decalaje, especialmente con ayuda de un generador de números aleatorios. Se consigue así que las coordenadas de diferentes toques de la zona de visualización, especialmente incluso cada coordenada de toques diferentes de la zona de indicación, sean falseadas con un valor de decalaje diferente, de modo que se consigue un mayor grado de seguridad. El módulo de seguridad transmite al módulo táctil unos terceros datos con informaciones sobre el primer valor de decalaje y/o el segundo valor de decalaje antes del toque de la zona de visualización. La transmisión se efectúa especialmente en forma cifrada, de modo que no se pueden capturar los valores de decalaje. Los valores de decalaje cifrados son descifrados especialmente por la unidad de procesamiento del módulo táctil. Por tanto, se incrementa aún más el grado de seguridad. En particular, cada cifra de un PIN se cifra con valores de decalaje distintos.

El cifrado de los primeros datos, los segundos datos y/o los terceros datos se efectúa preferiblemente con ayuda de un algoritmo de cifrado archivado, especialmente con ayuda de un algoritmo de cifrado del estándar de encriptado de datos (DES). Se incrementa así aún más la seguridad de transmisión de datos. En una forma de realización especialmente preferida de la invención se efectúan tanto el cifrado de los datos por la adición de los valores de decalaje como el cifrado por el algoritmo de cifrado archivado, de modo que se proporciona un cifrado doble de los datos transmitidos. Se consigue así un grado muy alto de seguridad de los datos.

El cifrado de los primeros, los segundos y/o los terceros datos se efectúa preferiblemente con ayuda del mismo algoritmo de cifrado. En una forma de realización alternativa de la invención el módulo de seguridad puede cifrar también los primeros datos y/o los terceros datos con un algoritmo de cifrado distinto del algoritmo de cifrado con el que el módulo táctil cifra los segundos datos.

El módulo de seguridad descifra preferiblemente los segundos datos recibidos del módulo táctil y determina la primera coordenada por resta del primer valor de decalaje respecto del primer valor de transmisión y/o la segunda coordenada por resta del segundo valor de decalaje respecto del segundo valor de transmisión. Se consigue así que en el módulo de seguridad puedan determinarse, a través de las coordenadas, la posición del toque de la zona de visualización y, por tanto, la cifra introducida.

Los primeros datos transmitidos por el módulo de seguridad al módulo táctil comprenden especialmente informaciones sobre la posición en la que se debe visualizar el teclado en la unidad de visualización. Los primeros datos comprenden en este caso especialmente una primera coordenada y una segunda coordenada de un punto preajustado del teclado, especialmente el punto medio del teclado. La posición en la que se visualiza el teclado en la unidad de visualización se fija por el módulo de seguridad especialmente con ayuda de un procedimiento aleatorio. A este fin, se determinan la primera coordenada y la segunda coordenada preferiblemente por un generador de números aleatorios. Se consigue así que, en caso de introducciones diferentes del número PIN, se visualice el teclado en posiciones diferentes de la unidad de visualización. Gracias a esta variación de la posición del teclado en la unidad de visualización se hace imposible que las personas que intenten fraudulentamente espiar el PIN saquen, en base a la posición en la que se toca la zona de visualización, una conclusión sobre la cifra del PIN introducida por el toque. En particular, se impide así que se instale en la zona de visualización con intención fraudulenta una unidad adicional para determinar la posición del toque de la zona de visualización a través de la cual las personas que realizan el fraude intenten llegar al PIN.

El módulo de seguridad controla para ello la unidad de visualización de tal manera que esta unidad de visualización, en una primera introducción de un PIN, visualice el teclado en una primera posición y, en una segunda introducción de un PIN, visualice dicho teclado en una segunda posición diferente de la primera posición.

El módulo táctil y el módulo de seguridad están unidos uno con otro preferiblemente a través de un primer enlace de cable, especialmente con ayuda de un cable USB. La unidad de visualización y el módulo de seguridad están unidos entre ellos preferiblemente a través de un segundo enlace de cable, especialmente con ayuda de un cable USB y/o un cable DVI. Gracias a la unión del módulo de seguridad con el módulo táctil o con la unidad de visualización a través de un enlace por cable se consigue un mayor grado de seguridad en comparación con una transmisión de datos por vía inalámbrica. Asimismo, es ventajoso que estén previstos un primer sensor para detectar una interrupción del primer enlace de cable y/o un segundo sensor para detectar una interrupción del segundo enlace de cable. Se pueden prevenir así intentos de manipulación, especialmente la intercalación de una unidad para leer los datos transmitidos a través del respectivo enlace de cable, y, por tanto, se pueden prevenir tales intentos de manipulación. Si el primer sensor y/o el segundo sensor detectan una interrupción del primero o del segundo enlace de cable, se dispara preferiblemente una alarma, con lo que se advierte a un usuario sobre el intento de manipulación. Asimismo, al detectarse una interrupción del primer enlace de cable y/o del segundo enlace de cable se puede encender un elemento de visualización rojo, por ejemplo un LED, o se puede activar una zona de visualización prevista para ello y/o un elemento de visualización previsto para ello, con lo que se llama la atención de un usuario sobre la manipulación. Como alternativa, es posible que, en caso de una interrupción del primer enlace de cable y/o del segundo enlace de cable, se ponga el dispositivo en un modo de avería en el que no sea posible una introducción de un PIN.

Es ventajoso que el módulo táctil comprenda un elemento de memoria en el que estén almacenados datos para la identificación unívoca del módulo táctil, especialmente un número de serie. El módulo de seguridad lee estos datos a intervalos de tiempo preajustados o bien continuamente y, en función de estos datos leídos, determina la presencia del módulo táctil. En una forma de realización especialmente preferida de la invención el módulo de seguridad compara el número de serie leído con un número de serie nominal preajustado. Cuando no coinciden el número de serie leído y el número de serie nominal y/o cuando el módulo de seguridad ni siquiera puede determinar un número de serie, se detecta con ello la no presencia de la unidad de visualización.

Asimismo, es ventajoso que la unidad de visualización comprenda también un elemento de memoria en el que estén almacenados datos para la identificación unívoca de la unidad de visualización. El módulo de seguridad lee también estos datos a intervalos de tiempo preajustados o bien continuamente y, en función de los datos leídos, determina la

presencia de la unidad de visualización. En el elemento de memoria de la unidad de visualización está almacenado también especialmente un número de serie que es comparado por el módulo de seguridad con un número de serie nominal preajustado.

El elemento de memoria del módulo táctil y/o el elemento de memoria de la unidad de visualización están preferiblemente unidos con el módulo de seguridad a través de un respectivo interbús de circuito integrado (I2C). Se consigue así una unión sencilla y segura contra falsificaciones.

Asimismo, es ventajoso que el módulo táctil y/o la unidad de visualización estén alojados, en una posición de montaje, dentro una carcasa del dispositivo y que estén previstos un primer interruptor de protección contra desmontaje y/o un segundo interruptor de protección contra desmontaje. Mediante el primer interruptor de protección contra desmontaje se puede determinar la retirada del módulo táctil de la posición de montaje y mediante el segundo interruptor de protección contra desmontaje se puede determinar la retirada de la unidad de visualización de la posición de montaje. A este fin, cuando el módulo táctil es retirado de la posición de montaje, el primer interruptor de protección contra desmontaje abre un circuito eléctrico cerrado o cierra un circuito eléctrico abierto. Gracias a la apertura o al cierre del circuito el módulo de seguridad detecta la retirada del módulo táctil de la posición de montaje. De manera correspondiente, el segundo interruptor de protección contra desmontaje abre este circuito eléctrico cerrado u otro circuito eléctrico cerrado o cierra este circuito eléctrico abierto u otro circuito eléctrico abierto cuando la unidad de visualización es retirada de la posición de montaje. En función de la apertura o del cierre del circuito, el módulo de seguridad detecta de manera correspondiente la retirada de la unidad de visualización de la posición de montaje. Por tanto, mediante los interruptores de protección contra desmontaje se puede determinar de manara sencilla cuándo el módulo táctil y/o la unidad de visualización son retirados de la posición de montaje, con lo que se pueden determinar intentos de manipulación de manera sencilla y próxima en el tiempo. En una forma de realización alternativa puede estar previsto también solamente un interruptor de protección contra desmontaje con cuya ayuda se pueda detectar tanto la retirada del módulo táctil de la posición de montaje como la retirada de la unidad de visualización de la posición de montaje.

Asimismo, es ventajoso que el módulo de seguridad determine si el dispositivo se hace funcionar en un modo de funcionamiento seguro o en un modo de funcionamiento inseguro. El dispositivo se hace funcionar en un modo de funcionamiento seguro especialmente cuando se transmiten datos en forma cifrada entre el módulo de seguridad y el módulo táctil, se transmiten cifrados los datos entre el módulo de seguridad y la unidad de visualización, el primer enlace de cable no está interrumpido, el segundo enlace de cable no está interrumpido, la unidad de visualización está dispuesta en la posición de montaje y/o el módulo táctil está dispuesto en la posición de montaje.

El modo de funcionamiento seguro es especialmente el módulo de funcionamiento que está previsto para la introducción del PIN. En una forma de realización especialmente preferida de la invención la introducción del PIN es posible solamente cuando el dispositivo se hace funcionar también realmente en el modo de funcionamiento seguro.

El módulo de seguridad controla la unidad de visualización especialmente de tal manera que se visualice a través de la unidad de visualización en qué estado de funcionamiento se hace funcionar el dispositivo. Se consigue así que un usuario del dispositivo pueda reconocer el modo de funcionamiento y, ante la visualización del modo de funcionamiento inseguro, pueda omitir la introducción del PIN. Por tanto, se incrementa la protección contra el espiado del PIN. La unidad de visualización visualiza especialmente una superficie roja y una superficie verde, con lo que, cuando el dispositivo se hace funcionar en el modo de funcionamiento seguro, la superficie verde está representada en un verde claro y la superficie roja está representada en un rojo oscuro, mientras que la superficie verde está representada en un verde oscuro y la superficie roja está representada en un rojo claro cuando el dispositivo se hace funcionar en el modo inseguro. En una forma de realización alternativa de la invención pueden estar previstas también unas lámparas dispuestas fuera de la unidad de visualización, especialmente unos LEDs, a través de las cuales se visualiza el modo de funcionamiento. Adicionalmente o como alternativa, es posible también la emisión del modo de funcionamiento por medio de un tono de aviso, especialmente la activación del tono de aviso en caso de un modo de funcionamiento inseguro.

Asimismo, es ventajoso que el módulo de seguridad active la unidad de visualización de tal manera que ésta visualice informaciones que inviten a un usuario del dispositivo a introducir el PIN solamente en el modo de funcionamiento securizado. Se impide así que el usuario no tenga en cuenta por descuido en qué modo de funcionamiento se hace funcionar el dispositivo, y se impide por ello que el usuario introduzca por descuido el PIN en el módulo de funcionamiento inseguro.

Asimismo, es ventajoso que en al menos una zona parcial de la unidad de visualización esté dispuesta una película de protección antivisión por medio de la cual las informaciones visualizadas con ayuda de la unidad de visualización puedan ser leídas solamente desde un rango de distancia de observación preajustado y/o un rango de ángulo de observación preajustado. El rango de distancia de observación y el rango de ángulo de observación se preajustan especialmente de tal manera que solamente un usuario situado inmediatamente delante de la unidad de visualización pueda leer las informaciones visualizadas. Se dificulta así el espiado del PIN, ya que la persona espía puede ciertamente reconocer qué sitio de la zona de visualización toca el usuario que ingresa el PIN, pero no puede

reconocer qué cifra es visualizada en este sitio por la unidad de visualización. La película de protección antivisión forma especialmente un filtro de polarización.

Asimismo, es ventajoso que en al menos un lado de la unidad de visualización esté dispuesto al menos un elemento mecánico de protección antivisión para impedir el espiado de la introducción del PIN. En particular, en al menos tres lados de la unidad de visualización esta previsto un elemento mecánico de protección antivisión de esta clase. El elemento de protección antivisión impide o dificulta que una persona que esté espiando pueda reconocer en qué posición el usuario toca la zona de visualización.

El dispositivo puede comprender especialmente una unidad de control para controlar el módulo de seguridad, estando la unidad de control unida con el módulo de seguridad a través de al menos un enlace de transmisión de datos, preferiblemente un enlace de transmisión de datos por cable. La unidad de control sirve también especialmente para controlar otras unidades del dispositivo, por ejemplo para controlar una unidad de lectura para leer la tarjeta de banda magnética y/o inteligente. Mediante la intercalación del módulo de seguridad entre la unidad de control y el módulo táctil se consigue que la unidad de seguridad no tenga acceso directo a la unidad de visualización y al módulo táctil, de modo que, aún cuando una persona logre ganar acceso a la unidad de control, no sea posible por ello un acceso al PIN introducido y no puedan tampoco manipularse la unidad de visualización y el módulo táctil de tal manera que pueda adquirirse el PIN. Por tanto, se incrementa la seguridad.

En el modo de funcionamiento inseguro el módulo de seguridad retransmite inalterados a la unidad de visualización los datos generados por la unidad de control para controlar la unidad de visualización, de modo que se minimiza el coste de cálculo del módulo de seguridad para el caso de introducciones de datos que no sean relevantes para la seguridad. Por el contrario, en el módulo de funcionamiento seguro el módulo de seguridad retransmite a la unidad de visualización exclusivamente datos autogenerados. Se asegura así que en el modo de funcionamiento seguro las eventuales manipulaciones de la unidad de control no tengan influencia alguna sobre la visualización de la unidad de visualización. El módulo de seguridad comprende especialmente un interruptor DVI a través del cual el enlace de transmisión de datos de la unidad de control al módulo de seguridad en el modo de funcionamiento inseguro está unido directamente con un enlace de transmisión de datos del módulo de seguridad a la unidad de visualización, especialmente con el segundo enlace de cable. En el modo de funcionamiento seguro está interrumpido por el interruptor DVI el enlace de transmisión de datos anteriormente descrito entre la unidad de control y la unidad de visualización.

La unidad de control ejecuta especialmente datos de programa de un primer sistema operativo y el módulo de seguridad ejecuta datos de programa de un segundo sistema operativo diferente del primer sistema operativo. Los sistemas operativos están configurados especialmente de tal manera que no existe ninguna dependencia entre ellos. Por tanto, se incrementa aún más el grado de seguridad. El primer sistema operativo es especialmente un sistema operativo usual en el mercado, mientras que el segundo sistema operativo es un sistema operativo programado especialmente para las tareas del módulo de seguridad. Por tanto, se consigue que las lagunas de seguridad del sistema operativo usual en el mercado no tengan, al menos en el modo de funcionamiento seguro, repercusiones de ninguna clase para la seguridad de la introducción del PIN. Otras características y ventajas de la invención se desprenden de la descripción siguiente, que explica con más detalle la invención en unión de las figuras adjuntas referidas a ejemplos de realización.

Muestran:

La figura 1, un diagrama de bloques de un dispositivo para leer tarjetas de banda magnética y/o inteligentes;

La figura 2, una representación esquemática de un fragmento del dispositivo de la figura 1 según una primera forma de realización de la invención;

La figura 3, una representación esquemática de un fragmento del dispositivo de la figura 1 de acuerdo con una segunda forma de realización de la invención;

La figura 4, una representación esquemática de un fragmento del dispositivo de la figura 1 según una tercera forma de realización de la invención; y

La figura 5, una representación superpuesta de varias visualizaciones de una unidad de visualización del dispositivo de la figura 1 según la tercera forma de realización.

En la figura 1 se ofrece una representación esquemática fuertemente simplificada de un dispositivo 10 para leer una tarjeta de banda metálica y/o inteligente en forma de un diagrama de bloques. El dispositivo 10 comprende una unidad de lectura 12 para leer la tarjeta de banda magnética y/o inteligente, una unidad de visualización 14, un módulo táctil 16 dispuesto delante de la unidad de visualización 14, un módulo de seguridad 18 para controlar el módulo de visualización 14 y el módulo táctil 16, y una unidad de control 20 para controlar la unidad de lectura 12 y el módulo de seguridad 18.

El dispositivo 10 consiste especialmente en un cajero automático, una caja fuerte automática, un sistema de caja automático, un terminal de pagos, una impresora de extractos de cuentas y un terminal de información. La tarjeta de banda magnética y/o inteligente consiste especialmente en una tarjeta bancaria, una tarjeta EC y/o una tarjeta de crédito. Por disposición del módulo táctil 16 delante de la unidad de visualización 14 se entiende especialmente que el módulo táctil 16 está dispuesto delante de la unidad de visualización 14 con cuya ayuda se pueden visualizar las informaciones. El módulo táctil 16 está dispuesto especialmente entre un usuario que maneja el dispositivo 10 y la unidad de visualización 14. La unidad de visualización 14 consiste especialmente en un monitor. En este caso, el módulo táctil 16 está dispuesto delante del monitor.

El módulo táctil 16 comprende al menos un sensor no representado para detectar la posición del toque de una zona de visualización. La zona de visualización puede ser especialmente un cristal de la unidad de visualización 14 o un cristal separado del módulo táctil 16 previsto para proteger la unidad de visualización 14. La unidad de visualización 14 y el módulo táctil 16 pueden estar realizados preferiblemente como una sola pieza en forma de una pantalla táctil.

El módulo de seguridad 18 está unido con el módulo táctil 16 para la transmisión de datos a través de un primer enlace de cable 22, especialmente a través de un cable USB. Asimismo, el módulo de seguridad 18 está unido con la unidad de visualización 14 a través de un segundo enlace de cable 24, especialmente un cable USB y/o un cable DVI. Además, el módulo de seguridad 18 está unido con la unidad de control 20 a través de un enlace 26 de transmisión de datos. El enlace 26 de transmisión de datos se efectúa especialmente a través de un cable USB o un cable DVI. En una forma de realización alternativa de la invención la unidad de control 20 puede estar unida también con el módulo de seguridad 18 a través de dos enlaces de transmisión de datos, especialmente a través de un cable USB y a través de un cable DVI.

El módulo de seguridad 18 comprende un interruptor DVI 28 a través del cual, en un modo de funcionamiento inseguro, se hace que unos datos transmitidos de la unidad de control 20 al módulo de seguridad 18 a través del enlace 26 de transmisión de datos sean retransmitidos inalterados a la unidad de visualización 14 por medio del segundo enlace de cable 24. Por el contrario, en un módulo de funcionamiento seguro el interruptor DVI interrumpe el enlace directo entre la unidad de control 20 y la unidad de visualización 14, de modo que, a través del segundo enlace de cable 24, se pueden transmitir a la unidad de visualización 14 únicamente datos generados por el módulo de seguridad 18.

La unidad de control 20 es hecha funcionar especialmente con un primer sistema operativo y el módulo de seguridad 18 lo es con un segundo sistema operativo diferente del primer sistema operativo. El primer sistema operativo es especialmente un sistema operativo usual en el mercado, por ejemplo Windows de Microsoft, mientras que el segundo sistema operativo del módulo de seguridad 18 es un sistema operativo programado especialmente para el módulo de seguridad 18. Por tanto, el segundo sistema operativo está exactamente adaptado a las tareas del módulo de seguridad 18. Gracias a la separación del enlace de datos directo entre la unidad de control 20 y la unidad de visualización 14 en el modo de funcionamiento seguro se consigue que las lagunas de seguridad eventualmente existentes del primer sistema operativo comercial de la unidad de control 20 no puedan aprovecharse, al menos en el modo de funcionamiento seguro, para la manipulación de la visualización de la unidad de visualización 14. Se logra así un alto grado de seguridad.

La unidad de visualización 14 y el módulo táctil 16 están unidos en una posición de montaje con al menos una parte de carcasa no representada del dispositivo 10. El dispositivo 10 comprende cuatro interruptores 30 a 36 de protección contra desmontaje que se denominan también interruptores de retirada. Si se retiran la unidad de visualización 14 y/o el módulo táctil 16 sacándolos de la posición de montaje, uno de los interruptores 30 a 36 de protección contra desmontaje o varios de estos interruptores 30 a 36 abren entonces un circuito eléctrico previamente cerrado. Debido a la apertura del circuito cerrado el módulo de seguridad 18 detecta la retirada de la unidad de visualización 14 y/o del módulo táctil 16 hacia fuera de la posición de montaje. En una forma de realización alternativa de la invención puede ocurrir también que, al retirar la unidad de visualización 14 y/o el módulo táctil 16 hacia fuera de la posición de montaje, se cierre un circuito previamente abierto por uno o varios de los interruptores 30 a 36 de protección contra desmontaje y el módulo de seguridad 18, en función de la apertura del circuito, detecte la retirada de la unidad de visualización 14 y/o del módulo táctil 16 hacia fuera de la posición de montaje. Se consigue así que puedan detectarse de manera sencilla manipulaciones en la unidad de visualización 14 y/o el módulo táctil 16 y, por tanto, se incrementa la seguridad.

Asimismo, la unidad de visualización 14 comprende un elemento de memoria 38 en el que están almacenados datos para la identificación unívoca de la unidad de visualización 14. Estos datos comprenden especialmente un número de serie unívoco. El módulo de seguridad 18 lee a intervalos de tiempo preajustados o continuamente los datos almacenados en el elemento de memoria 38 y, en función de los datos leídos, determina si está presente o no la unidad de visualización 14. Esto se efectúa especialmente mediante una comparación del número de serie leído en el elemento de memoria 38 con un módulo de serie nominal preajustado almacenado en un elemento de memoria del módulo de seguridad 18 o bien analiza y comprueba de otra manera la validez el módulo de serie leído. Si los dos números se desvían uno de otro o bien el módulo de seguridad 18 no puede leer un número de serie en el elemento de memoria 38, se deduce entonces de esto que la unidad de visualización 14 ha sido retirada de la

posición de montaje, se ha cortado el segundo enlace de cable 24, se ha manipulado la unidad de visualización 14 y/o se ha manipulado el segundo enlace de cable 24.

Asimismo, el módulo táctil 16 comprende un elemento de memoria 40 en el que están almacenados datos para la identificación unívoca del módulo táctil 16. El módulo de seguridad 18 lee a intervalos de tiempo preajustados o continuamente los datos del elemento de memoria 40 y, en función de los datos leídos, determina la presencia del módulo táctil 16. Los datos almacenados en el elemento de memoria 40 comprenden especialmente un número de serie del módulo táctil 16. El módulo de seguridad 18 compara este número de serie con un número de serie nominal preajustado almacenado en un elemento de memoria del módulo de seguridad 18. Si la comparación arroja el resultado de que el número de serie y el número de serie nominal no coinciden o bien el módulo de seguridad 18 ni siquiera ha podido leer un número de serie, se deduce entonces de esto que el módulo táctil 16 ha sido retirado de la posición de montaje, se ha manipulado el módulo táctil 16, se ha cortado el primer enlace de cable 22 y/o se ha manipulado el primer enlace de cable 22.

Los elementos de memoria 38, 40 comprenden preferiblemente sendas pastillas electrónicas de número de serie de la firma Maxim Integrated Products Inc. del tipo "DS2401". Los elementos de memoria 38, 40 están unidos con el módulo de seguridad preferiblemente a través de sendos buses de circuito integrado (I2C). Por retirada del módulo táctil 16 o de la unidad de visualización 14 hacia fuera de la posición de montaje se entiende especialmente que se desmonta el módulo táctil 16 o la unidad de visualización 14 o que se varía la posición y/o la orientación dentro del dispositivo 10. Como alternativa o adicionalmente, se puede detectar también con ayuda de sensores de aceleración una retirada de la unidad de visualización 14 y/o del módulo táctil 16 hacia fuera de la posición de montaje.

Si se introduce por un usuario del dispositivo 10 una tarjeta de banda magnética y/o inteligente en la unidad de lectura 12, el módulo de seguridad 18 genera entonces unos primeros datos para representar un teclado de introducción de un número de identificación personal (PIN) del usuario en la unidad de visualización 14. El módulo de seguridad 18 cifra los primeros datos con ayuda de un algoritmo de cifrado preajustado, especialmente con ayuda de un algoritmo de cifrado del estándar de encriptación de datos (DES), y transmite los primeros datos cifrados a la unidad de visualización 14 a través del segundo enlace de cable 24. En la unidad de visualización 14 se representa seguidamente un teclado a través del cual el usuario del dispositivo 10 puede introducir un PIN.

En la figura 2 se ofrece una representación esquemática de un fragmento del dispositivo 10 de la figura 1 según una primera forma de realización de la invención. En esta primera forma de realización el teclado para la introducción del PIN está representado en el centro de la unidad de visualización 14. En la primera forma de realización mostrada en la figura 2 el módulo táctil 16 está configurado de tal manera que toda la pantalla de la unidad de visualización 14 es abarcada por éste, con lo que se puede determinar la posición de un toque en toda la pantalla. Por tanto, en la vista en planta esquemática mostrada en la figura 2 coinciden la unidad de visualización 14 y el módulo táctil 16, por lo que estos se designan por los mismos símbolos de referencia 14, 16. El teclado representado en la unidad de visualización 14 se ha designado con el símbolo de referencia 42.

Para la introducción del PIN el usuario toca el cristal en el sitio en el que está representada la cifra del PIN que debe ser introducida. La posición del toque del cristal es detectada con ayuda del sensor del módulo táctil 16. En particular, el sensor detecta una primera coordenada y una segunda coordenada de la posición del toque del cristal. Una unidad de procesamiento del módulo táctil 16 determina a partir de ello un primer valor de transmisión y un segundo valor de transmisión añadiendo para ello un primer valor de decalaje a la primera coordenada y un segundo valor de decalaje a la segunda coordenada. Los dos valores de decalaje se han transmitido previamente cifrados al módulo táctil 16 por el módulo de seguridad 18 y se han descifrado por la unidad de procesamiento. A continuación, la unidad de procesamiento del módulo táctil 16 genera unos segundos datos con informaciones sobre el primer valor de transmisión y el segundo valor de transmisión, cifra estos segundos datos con un algoritmo de cifrado preajustado, especialmente con ayuda de un algoritmo de cifrado del estándar de encriptación de datos (DES), y transmite los segundos datos cifrados al módulo de seguridad 18 a través del primer enlace de cable 22. El algoritmo de cifrado con el que la unidad de procesamiento cifra los segundos datos es especialmente el mismo algoritmo de cifrado con el que el módulo de seguridad 18 cifra los primeros datos.

Gracias a la transmisión de los valores de transmisión y no de las coordenadas reales del toque se consigue que, si un tercero determinara y descifrara los valores de transmisión, sea imposible con las informaciones obtenidas sacar conclusiones sobre la posición del toque del cristal y, por tanto, sobre la cifra del PIN introducida a través de la posición. Se hace así posible una introducción segura del PIN.

Especialmente, con cada toque del cristal se falsean las coordenadas de este toque por medio de otros valores de decalaje, de modo que mediante la sola comparación de los valores de transmisión con las coordenadas reales no pueden sacarse conclusiones sobre los valores de decalaje para otros toques. Los valores de decalaje se determinan por el módulo de seguridad 18 especialmente con ayuda de un procedimiento aleatorio. En particular, se utiliza para ello un generador de números aleatorios.

El módulo de seguridad 18 descifra los segundos datos cifrados y establece la primera coordenada y la segunda

coordenada de la posición del toque del cristal por resta del primer valor de decalaje respecto del primer valor de transmisión y por resta del segundo valor de decalaje respecto del segundo valor de transmisión. Mediante la comparación de la posición del toque del cristal y la posición en la que se visualiza el teclado 42, el módulo de seguridad 18 determina la cifra del PIN introducida por el toque. En una forma de realización alternativa de la invención no puede tampoco transmitirse individualmente cada cifra del PIN del módulo táctil 16 al módulo de seguridad 18, sino que se transmiten datos con informaciones sobre las coordenadas de varios toques que dan como resultado conjuntamente el PIN.

Gracias al cifrado de los segundos datos por el módulo táctil 16 se consigue que estos datos no se transmitan nunca en forma no cifrada, con lo que, aun cuando se capturen los datos no es posible sacar de ellos ninguna conclusión sobre el PIN introducido. Por tanto, se consigue un alto grado de seguridad.

Como se ha descrito anteriormente, el módulo de seguridad 18 puede hacerse funcionar en un modo de funcionamiento inseguro y un modo de funcionamiento seguro. En la unidad de visualización 14 se visualizan especialmente dos elementos de visualización, preferiblemente en forma de lámparas virtuales 44, 46, con cuya ayuda se visualiza en qué modo de funcionamiento se hace que funcione actualmente el dispositivo 10. A este fin, especialmente en el modo de funcionamiento seguro se visualiza la primera lámpara virtual 44 en un tono verde claro y la segunda lámpara virtual 46 en un tono rojo oscuro, y en el modo de funcionamiento inseguro se visualiza la primera lámpara virtual 44 en un tono verde oscuro y la segunda lámpara virtual 46 en un tono rojo claro. Por tanto, se señala la iluminación de una lámpara verde o una lámpara roja, de modo que el usuario sabe que, cuando se ilumina la lámpara verde, el dispositivo 10 se hace funcionar en el modo de funcionamiento seguro y, cuando se ilumina la lámpara roja, se le hace funcionar en el modo de funcionamiento inseguro. Por tanto, el usuario puede cuidar de que introduzca su PIN solamente en el modo de funcionamiento seguro, con lo que queda garantizado el mantenimiento en secreto de su PIN. En una forma de realización especialmente preferida de la invención se invita al usuario, a través de una indicación correspondiente de la unidad de visualización 14, a que introduzca su PIN únicamente cuando el dispositivo se haga funcionar en el modo de funcionamiento seguro.

Adicionalmente o como alternativa, el módulo de seguridad 18 puede activar la unidad de visualización 14 y/o el módulo táctil 16 de tal manera que sea posible una introducción de un PIN únicamente cuando el dispositivo 10 se hace funcionar en el módulo de funcionamiento seguro. A este fin, el módulo de seguridad 18 activa la unidad de visualización 14 especialmente de tal manera que dicha unidad de visualización 14 visualice un teclado solamente cuando el dispositivo 10 se haga funcionar en el modo de funcionamiento seguro.

En una forma de realización alternativa de la invención el modo de funcionamiento puede visualizarse también, como alternativa a las lámparas virtuales 44, 46, por medio de unas lámparas especialmente LEDs, previstas fuera de la unidad de visualización 14. Asimismo, es posible la visualización del modo de funcionamiento en forma de texto sobre la unidad de visualización 14 y/o es también posible la emisión de un tono de aviso cuando el dispositivo 10 se haga funcionar en el modo de funcionamiento inseguro.

Si se determina a través de los interruptores 30 a 36 de protección contra desmontaje y/o los elementos de memoria 38, 40, la inexistencia de la unidad de visualización 14, la inexistencia del módulo táctil 16, una manipulación de la unidad de visualización 14, una manipulación del módulo táctil 16, un corte del primer enlace de cable 22, un corte del segundo enlace de cable 24 y/o un intento de manipulación de otra naturaleza, el módulo de seguridad 18 activa la unidad de visualización 14 de tal manera que se indique a través de ella que el dispositivo 10 se hace funcionar en el módulo de funcionamiento seguro. En particular, en este caso no es posible tampoco la introducción de un PIN.

Asimismo, el dispositivo 10 comprende un elemento 48 de protección antivisión que impida que se espíe la introducción del PIN. El elemento 48 de protección antivisión está configurado especialmente de tal manera que al menos tres lados de la unidad de visualización 14 están rodeados por el elemento 48 de protección antivisión para que otra persona que esté al lado del usuario no tenga visión de la unidad de visualización 14. Se impide así que esta otra persona pueda ver la posición en la que el usuario toca el cristal.

En la figura 3 se muestra una representación esquemática de un fragmento del dispositivo 10 de acuerdo con una segunda forma de realización de la invención. En esta segunda forma de realización de la invención se ha aplicado sobre el cristal una película 50 de protección antivisión mediante la cual se deberá impedir también que se espíe el PIN. La película 50 de protección antivisión está configurada de tal manera que solamente el usuario situado inmediatamente delante del dispositivo 10 puede leer la indicación de la unidad de visualización 14. Por el contrario, una persona situada más lejos o bien una persona situada al lado del usuario no pude leer la indicación de la unidad de visualización 14. Se consigue así que, aun cuando esta otra persona pueda reconocer en qué posición el usuario toca el cristal, esta otra persona no pueda reconocer que tecla se visualiza en ese lugar. Por tanto, esta otra persona no puede espiar el PIN del usuario.

En la figura 4 se muestra una representación esquemática de un fragmento del dispositivo 10 según una tercera forma de realización de la invención. En esta tercera forma de realización de la invención el módulo de seguridad 18 transmite, antes de la introducción del PIN por el usuario, unos terceros datos con informaciones sobre la posición

en la que se debe visualizar el teclado 42 sobre la unidad de visualización 14. En particular, estos terceros datos comprenden una primera coordenada y una segunda coordenada de un punto preajustado del teclado 42, especialmente el punto medio del teclado 42.

Adicionalmente o como alternativa, se pueden variar también el tamaño del teclado representado, el tamaño de una o varias teclas del teclado representado y/o las distancias entre las teclas.

El módulo de seguridad 18 determina la posición en la que se debe representar el teclado 42, especialmente con ayuda de un procedimiento aleatorio, de modo que, en el caso de diferentes introducciones del PIN, el teclado se representa en diferentes posiciones de la unidad de visualización 14. Esta representación del teclado 42 en posiciones diferentes de la unidad de visualización 14 se representa en la figura 5. El módulo de seguridad 18 comprende especialmente un generador de números aleatorios que fija las coordenadas y/o el tamaño del teclado 42.

Mediante la visualización del teclado en posiciones diferentes de la unidad de visualización 14 para diferentes introducciones del PIN se incrementa la seguridad de la introducción del PIN. En particular se evita así que una persona que espíe el PIN instale con pretensiones fraudulentas una unidad de determinación de la posición del toque del cristal para determinar así la posición del cristal con independencia del propio módulo táctil 16. Dado que el teclado 42 se visualiza siempre en una posición distinta de la unidad de visualización 14, se tiene que, ni siquiera a partir del conocimiento de las coordenadas reales del toque del cristal, la persona espía puede sacar conclusiones sobre la cifra introducida por el toque y, por tanto, sobre el PIN.

Gracias a las medidas de seguridad anteriormente descritas se consigue, individualmente y, en particular, en su combinación, un alto grado de introducción segura de un PIN a través de una pantalla táctil. Por tanto, las pantallas táctiles que están previstas en cajeros automáticos, cajas fuertes automáticas, sistemas de caja automáticos, terminales de pagos, impresoras de extractos de cuentas y/o terminales de información y que se utilizan hasta ahora únicamente para el manejo y la introducción de informaciones no relevantes para la seguridad, pueden utilizarse ya también para la introducción del PIN. Por tanto, se puede prescindir de la previsión de un teclado mecánico separado, especialmente un teclado EPP, con lo que se consigue una construcción sencilla y barata del dispositivo 10. Se incrementa así también la facilidad de manejo para el usuario y se reduce el gasto de mantenimiento.

Lista de símbolos de referencia

10	Dispositivo
12	Unidad de lectura
14	Unidad de visualización
16	Módulo táctil
18	Módulo de seguridad
20	Unidad de control
22,24	Enlace de cable
26	Enlace de transmisión de datos
28	Interruptor DVI
30 a 36	Interruptor de protección contra desmontaje
38,40	Elemento de memoria
42	Teclado
44,46	Lámpara virtual
48	Elemento de protección antivisión
50	Película de protección antivisión

REIVINDICACIONES

1. Dispositivo para leer tarjetas de banda magnética y/o inteligentes, especialmente tarjetas bancarias, tarjetas EC y/o tarjetas de crédito, que comprende

una unidad de visualización (14),

un módulo táctil (16) que está dispuesto delante de la unidad de visualización (14) y que comprende al menos un sensor para detectar una posición de un toque de una zona de visualización,

y un módulo de seguridad (18) para controlar la unidad de visualización (14) y el módulo táctil (16), transmitiendo el módulo de seguridad (18) a la unidad de visualización (14) unos primeros datos para representar un teclado (42) con ayuda de la unidad de visualización (14) para introducir un número de identificación personal (PIN),

generando el módulo táctil (16), en respuesta al toque de la unidad de visualización, unos segundos datos con informaciones sobre la posición del toque y

cifrando el módulo táctil (16) los segundos datos y transmitiendo estos segundos datos cifrados al módulo de seguridad (18),

caracterizado por que

el módulo de seguridad (18) determina si el dispositivo (10) se hace funcionar en un modo de funcionamiento seguro o en un modo de funcionamiento inseguro, y

por que el módulo de seguridad (18) activa la unidad de visualización (14) de tal manera que está unidad de visualización (14) indique en qué estado de funcionamiento se hace funcionar el dispositivo (10), o por que se indica el modo de funcionamiento a través de una lámpara dispuesta fuera de la unidad de visualización, o por que se efectúa la emisión del modo de funcionamiento a través de un tono de aviso.

2. Dispositivo (10) según la reivindicación 1, **caracterizado** por que el módulo de seguridad (18) cifra los primeros datos y los transmite en forma cifrada a la unidad de visualización (14).

3. Dispositivo (10) según cualquiera de las reivindicaciones anteriores, **caracterizado** por que el módulo táctil (16) determina una primera coordenada y/o una segunda coordenada de la posición del toque de la zona de visualización, por que el módulo táctil (16) determina un primer valor de transmisión por adición de un primer valor de decalaje a la primera coordenada y/o un segundo valor de transmisión por adición de un segundo valor de decalaje a la segunda coordenada, y por que los segundos datos comprenden informaciones sobre el primer valor de transmisión y/o el segundo valor de transmisión.

4. Dispositivo (10) según la reivindicación 3, **caracterizado** por que el módulo de seguridad (18) determina el primer valor de decalaje y/o el segundo valor de decalaje, especialmente con ayuda de un generador de números aleatorios, y por que el módulo de seguridad (18) transmite al módulo táctil (16), preferiblemente en forma cifrada, antes del toque de la zona de visualización, unos terceros datos con informaciones sobre el primer valor de decalaje y/o el segundo valor de decalaje.

5. Dispositivo (10) según cualquiera de las reivindicaciones anteriores, **caracterizado** por que el módulo de seguridad (18) cifra los primeros datos y/o los terceros datos con ayuda de una algoritmo de cifrado archivado, especialmente con ayuda de un algoritmo de cifrado del estándar de encriptación de datos (DES), y/o por que el módulo táctil (16) cifra los segundos datos con ayuda de un algoritmo de cifrado archivado, especialmente con ayuda de un algoritmo de cifrado del estándar de encriptación de datos (DES).

6. Dispositivo (10) según cualquiera de las reivindicaciones 3 a 5, **caracterizado** por que el módulo de seguridad (18) descifra los segundos datos y determina la primera coordenada por resta del primer valor de decalaje respecto del primer valor de transmisión y/o la segunda coordenada por resta del segundo valor de decalaje respecto del segundo valor de transmisión.

7. Dispositivo (10) según cualquiera de las reivindicaciones anteriores, **caracterizado** por que los primeros datos comprenden informaciones sobre la posición en la que debe visualizarse el teclado (42) sobre la unidad de visualización (14), especialmente una primera coordenada y una segunda coordenada de un punto medio del teclado (42).

8. Dispositivo (10) según la reivindicación 7, **caracterizado** por que el módulo de seguridad (18) fija la posición del teclado (42) con ayuda de un procedimiento aleatorio.

9. Dispositivo (10) según la reivindicación 7 u 8, **caracterizado** por que el módulo de seguridad (18) activa la unidad de visualización (14) de tal manera que esta unidad de visualización (14), al producirse una primera introducción de

un número de identificación personal (PIN), visualice el teclado (42) en una primera posición y, al producirse una segunda introducción del número de identificación personal (PIN), visualice dicho teclado en una segunda posición diferente de la primer aposición.

10. Dispositivo (10) según cualquiera de las reivindicaciones anteriores, **caracterizado** por que el módulo táctil (16) y el módulo de seguridad (18) están unidos uno con otro a través de un primer enlace de cable (22), especialmente con ayuda de un cable USB, y/o la unidad de visualización (14) y el módulo de seguridad (18) están unidos entre ellos a través de un segundo enlace de cable (24), especialmente con ayuda de un cable USB y/o un cable DVI, y por que están previstos un primer sensor para detectar una interrupción del primer enlace de cable (22) y/o un segundo sensor para detectar una interrupción del segundo enlace de cable (24).

11. Dispositivo (10) según cualquiera de las reivindicaciones anteriores, **caracterizado** por que el módulo táctil (16) y/o la unidad de visualización (14) comprenden un respectivo elemento de memoria (38, 40) en el que están almacenados datos para la identificación unívoca del módulo táctil (16) o de la unidad de visualización (14), y por que el módulo de seguridad (18) lee estos datos a intervalos de tiempo preajustados o continuamente y, en función de los datos leídos, determina la presencia del módulo táctil (16) o de la unidad de visualización (14).

12. Dispositivo (10) según cualquiera de las reivindicaciones anteriores, **caracterizado** por que el módulo táctil (16) y/o la unidad de visualización (14) están montados en una posición de montaje dentro una parte de carcasa del dispositivo (10), por que están previstos al menos un primer interruptor (30 a 36) de protección contra desmontaje y/o un segundo interruptor (30 a 36) de protección contra desmontaje, por que el primer interruptor (30 a 36) de protección contra desmontaje, cuando se retira el módulo táctil (16) de la posición de montaje, cierra un circuito eléctrico abierto en la posición de montaje o abre un circuito eléctrico cerrado en la posición de montaje, y por que el módulo de seguridad (18) detecta, por el cierre o la apertura del circuito, la retirada del módulo táctil (16) hacia fuera de la posición de montaje, por que el segundo interruptor (30 a 36) de protección contra desmontaje, cuando se retira la unidad de visualización (14) de la posición de montaje, cierra un circuito eléctrico abierto en la posición de montaje o abre un circuito eléctrico cerrado en la posición de montaje, y por que el módulo de seguridad (18) detecta, por el cierre o la apertura del circuito, la retirada de la unidad de visualización (14) desde la posición de montaje.

13. Dispositivo (10) según cualquiera de las reivindicaciones anteriores, **caracterizado** por que el dispositivo (10) comprende una unidad de control (20) para controlar el módulo de seguridad (18) y por que la unidad de control (20) está unida con el módulo de seguridad (18) a través de al menos un enlace (26) de transmisión de datos.

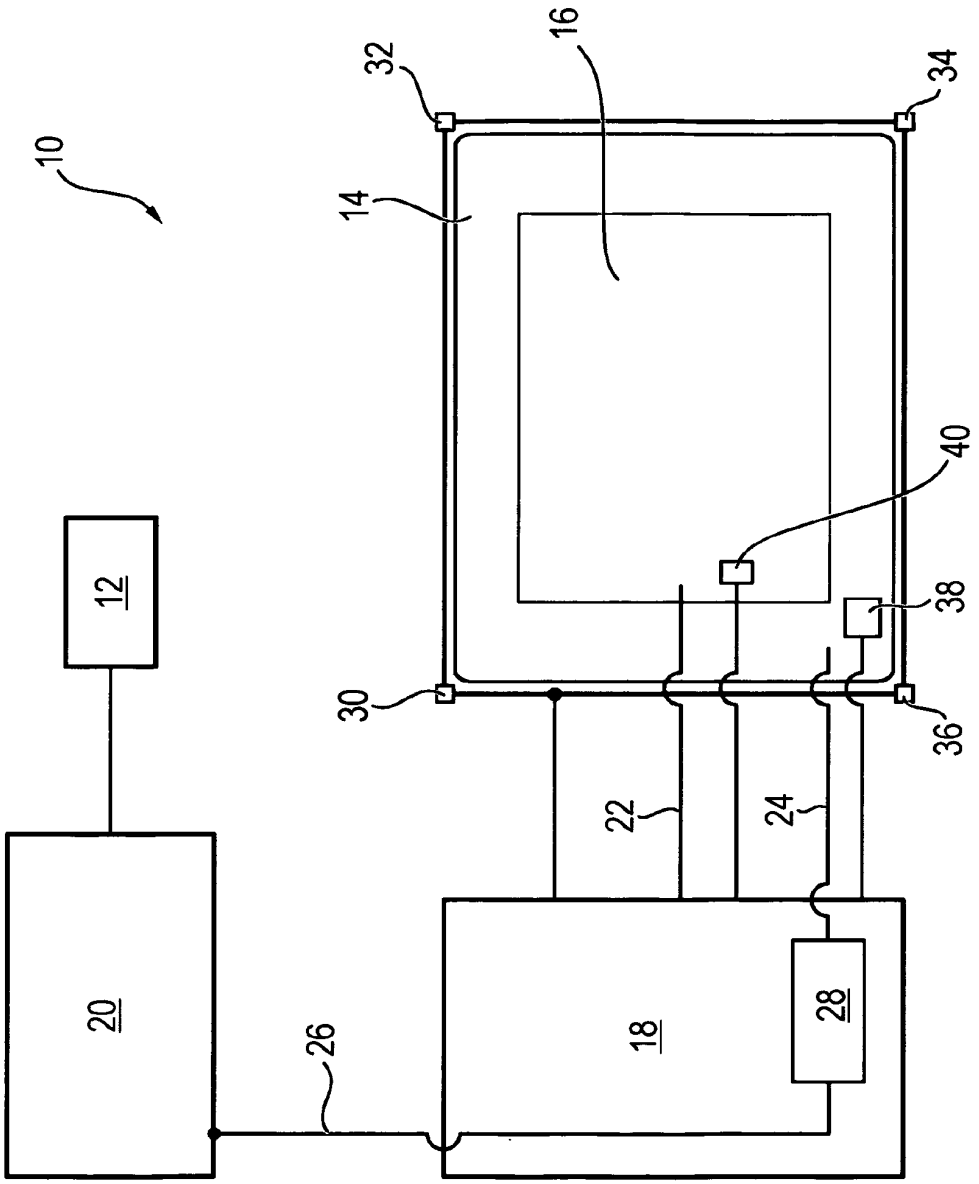

FIG. 1

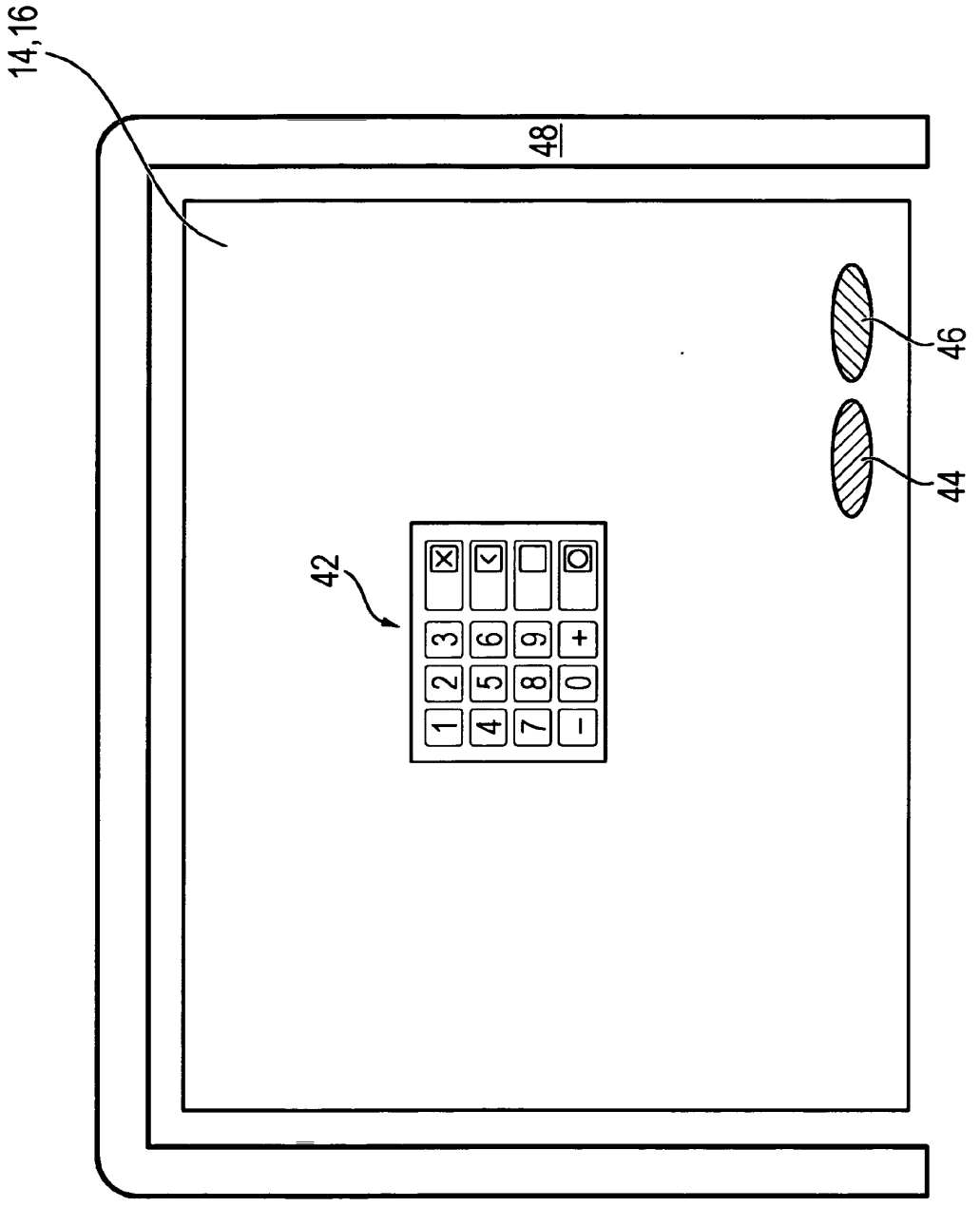

FIG. 2

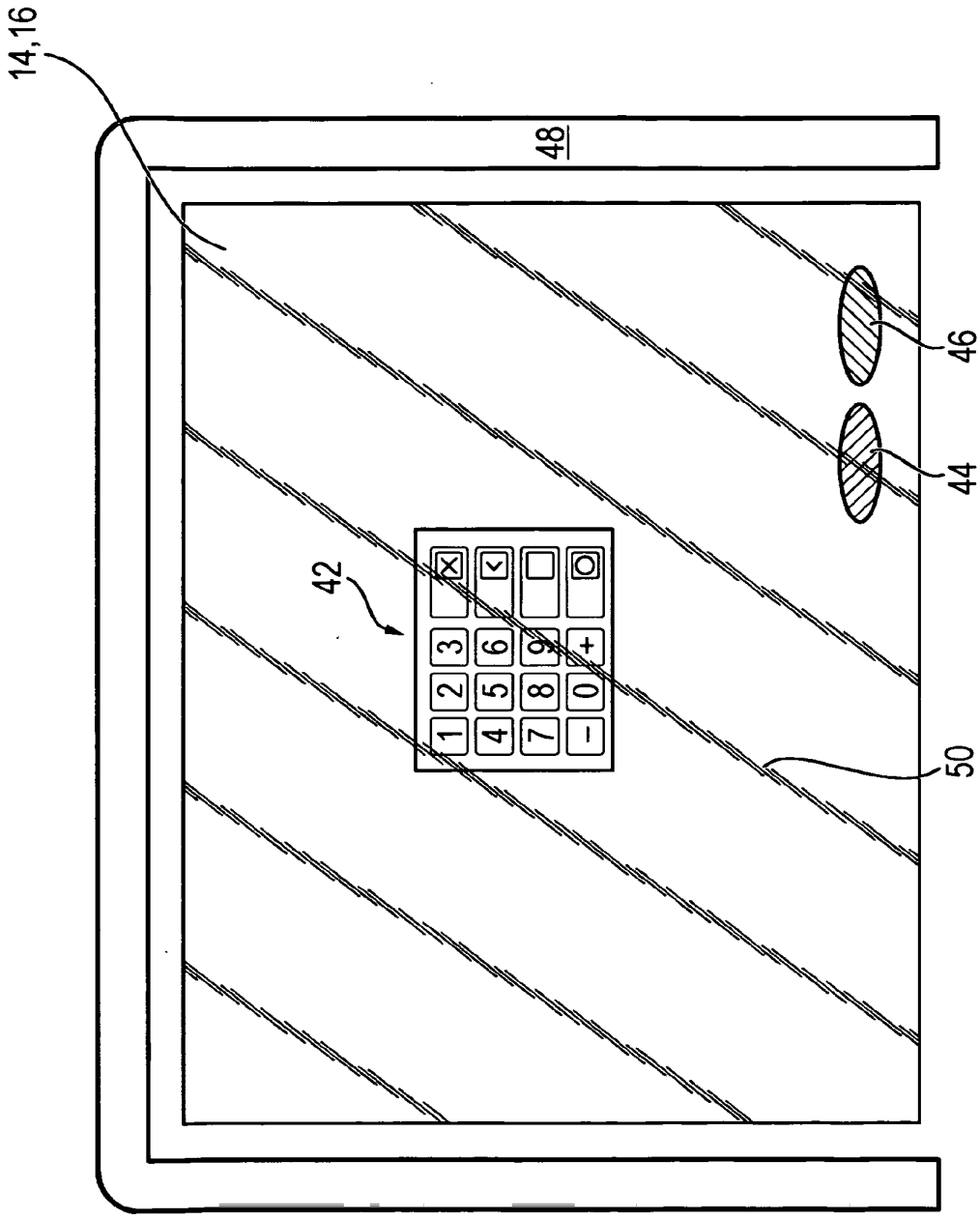

FIG. 3

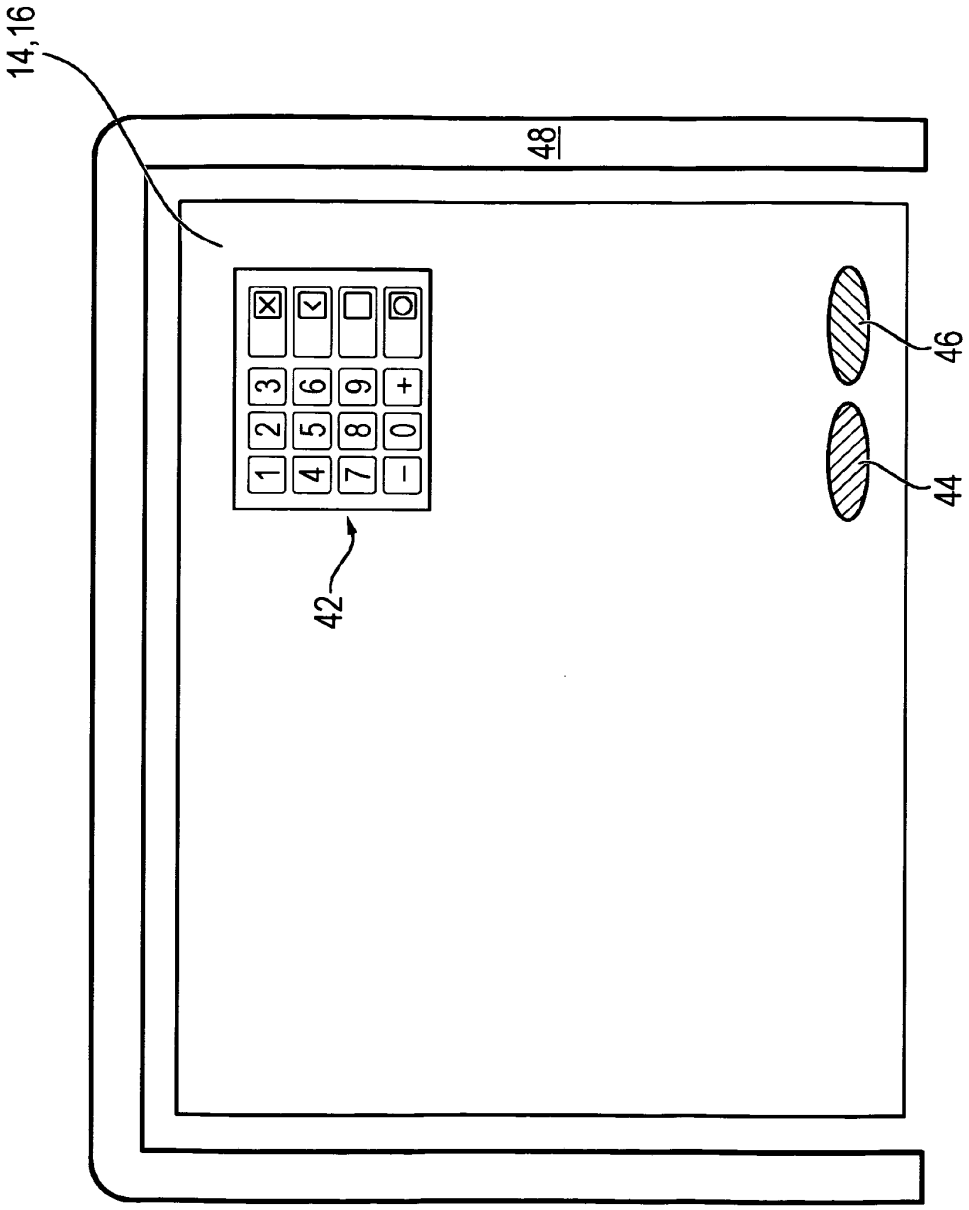

FIG. 4

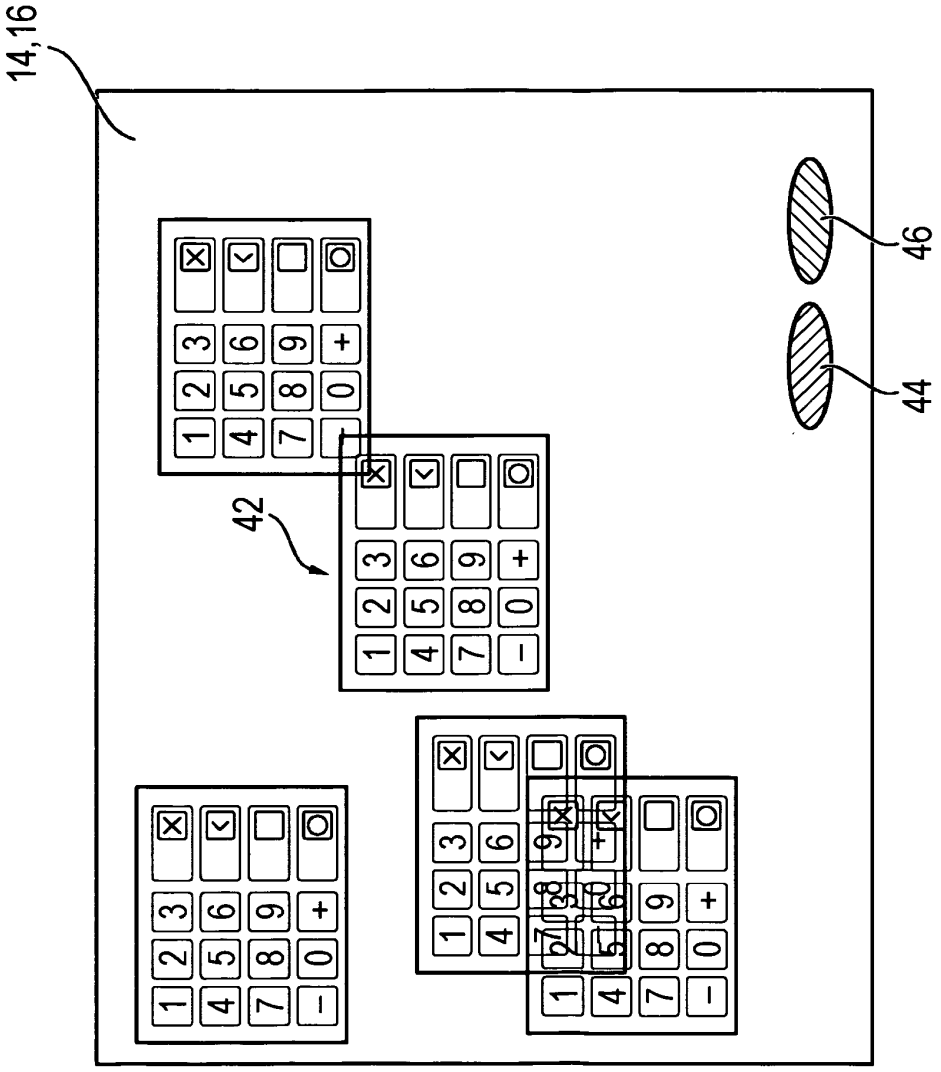

FIG. 5