(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 483 543**

(51) Int. CI.:

G06F 21/35 (2013.01)
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.10.2006 E 06122983 (7)**

(97) Fecha y número de publicación de la concesión europea: **07.05.2014 EP 1783695**

(54) Título: **Monitorización del desbloqueo de un ordenador**

(30) Prioridad:

03.11.2005 DE 102005052949
23.06.2006 DE 102006029339

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.08.2014

(73) Titular/es:

TERATRON GMBH (100.0%)
BUNSENSTRASSE 10
51647 GUMMERSBACH, DE

(72) Inventor/es:

PETSCHING, WILFRIED;
KONRAD, REIMUND;
SCHMALE, RALF y
DÖHL, ANDREAS

(74) Agente/Representante:

VEIGA SERRANO, Mikel

DESCRIPCIÓN

Monitorización del desbloqueo de un ordenador

Sector de la técnica

La invención se refiere, en general, a la monitorización y al control de una autorización de acceso para un aparato, en el que un módulo de lectura emite un campo de consulta y al menos una llave recibe el campo de consulta.

Estado de la técnica

Los sistemas de control de autorización de acceso para ordenadores se conocen en la técnica. Por ejemplo, por el documento de patente europea EP 1 496 344 B1 se conoce un equipo para el control de la autorización para la manipulación de un aparato con una unidad de activación. En la disposición que se describe, a través de una bobina de emisión se genera un campo alterno electromagnético. Un transpondedor, que penetra en este campo alterno electromagnético, se alimenta mediante la energía de la componente eléctrica del campo electromagnético. Con ayuda de la energía eléctrica del campo alterno, el transpondedor emite a continuación una señal de respuesta. La señal de respuesta la recibe la bobina de emisión, que ya ha emitido el campo alterno electromagnético. Mediante el intercambio de información a través del campo alterno electromagnético puede tener lugar una autenticación del transpondedor. En caso de una autenticación satisfactoria/autorización, el ordenador se desbloquea. En esta disposición es desventajoso que el alcance del campo alterno electromagnético sólo pueda ajustarse con dificultad. Puesto que el transpondedor se alimenta mediante la energía eléctrica del campo alterno electromagnético, su energía de emisión debe ser alta. En la disposición conocida se producen perturbaciones en el intercambio de información de autenticación siempre que el transpondedor no puede obtener suficiente energía del campo alterno electromagnético.

Un sistema similar se conoce por el documento DE 40 15 482 C1. También en este caso la autenticación de un usuario tiene lugar a través de una consulta sin contacto. Tal como se describió también anteriormente, este sistema presenta una única bobina de emisión y de recepción, que genera el campo alterno electromagnético, mediante el cual se alimenta el transpondedor y que recibe al mismo tiempo el campo de respuesta generado por el transpondedor. También en este caso se producen problemas con el ajuste del alcance del campo alterno y perturbaciones en la comunicación entre el transpondedor y la bobina de emisión / recepción.

Por último, por el documento US 5.952.641 también se conoce un sistema, en el que se realiza una consulta sin contacto de una autorización de acceso mediante un campo alterno electromagnético. También en este caso se genera un campo de consulta y se recibe un campo de respuesta a través de una única bobina. En este caso, el transpondedor que contiene el código de autorización de acceso también recibe alimentación con energía mediante la componente eléctrica del campo de consulta, de modo que aparecen problemas con el ajuste del alcance.

El documento DE 101 09 869 se refiere a un sistema para controlar remotamente una función (por ejemplo el acceso a través de una entrada que puede bloquearse, por ejemplo una puerta de vehículo). Un transceptor portátil emite una señal de petición en un gran número de frecuencias. Una unidad base recibe la señal de petición y ejecuta la función solicitada, reaccionando a la recepción. La unidad (24) base comprende componentes que seleccionan una frecuencia, en la que el transceptor portátil emite la señal de petición de función, y que proporcionan la frecuencia seleccionada al transceptor portátil. En un ejemplo, los componentes en la unidad base comprenden componentes de emisión o transmisión, que emiten una señal. Preferiblemente, el transceptor portátil emite su señal a alta frecuencia y la unidad base emite su señal como campo magnético de baja frecuencia. En otro ejemplo, la unidad base y/o el transceptor portátil cambia la frecuencia de las señales emitidas desde el mismo. En otro ejemplo, el transceptor portátil emite la señal con frecuencia diferente, hasta que la unidad base recibe una de las señales.

El documento WO 97/39553 se refiere a un sistema de autenticación inalámbrico para el control de un estado operativo de un primer nodo (por ejemplo un ordenador) basándose en la proximidad de un usuario habilitado con respecto al primer nodo. El sistema de autenticación inalámbrico comprende un dispositivo de seguridad implementado en el primer nodo y un testigo para la autenticación de usuario, que se encuentra en posesión del usuario autorizado (por ejemplo lo lleva puesto, lo lleva consigo, etc.). El dispositivo de seguridad genera un mensaje de consulta y lo transmite al testigo. Como reacción al mismo, el testigo genera y transmite un mensaje de respuesta al dispositivo de seguridad, si el testigo se encuentra a menos de una distancia predefinida con respecto al dispositivo de seguridad. Entonces, el usuario autorizado puede acceder al primer nodo, ya que éste se encuentra en un estado operativo.

El documento EP 1 016 947 A2 se refiere a un sistema de seguridad, en particular a un dispositivo electrónico portátil, con tecnología RFID (“identificación por radiofrecuencia”). A este respecto, cuando se presenta un transpondedor ante el equipo electrónico, por ejemplo un ordenador, se lee el código de identificación del transpondedor. Éste se compara con códigos que están depositados en el equipo electrónico y, en caso de resultado positivo, el ordenador se desbloquea.

El documento EP 1 460 508 A se refiere a un sistema para el control del acceso por parte de un usuario a un aparato. El sistema comprende una unidad de control conectada al aparato, para transmitir al aparato al menos una señal de autorización de acceso, y al menos un soporte de identificación móvil, en el que están almacenados datos de solicitud y conjuntos de datos de identificación del usuario y que se comunica de manera inalámbrica con la unidad de control. Según la invención se propone que la unidad de control presente una unidad de lectura, que detecta una característica de identificación personal del usuario. Está presente una unidad de programa que, mediante la característica de identificación, genera un primer conjunto de datos y una unidad lógica en la que el primer conjunto de datos se compara con los conjuntos de datos de identificación almacenados. En caso de una comparación satisfactoria del conjunto de datos con un conjunto de datos de identificación, se emite a la unidad de control una señal de solicitud con los datos de solicitud almacenados en el soporte de identificación. La señal de autorización de acceso se genera mediante los datos de solicitud y se transmite al aparato. Además está previsto un control de presencia del soporte de identificación.

El documento EP 0 295 658 A2 se refiere a un sistema de identificación para el desbloqueo en particular de una caja registradora.

Todos los sistemas descritos anteriormente presentan la desventaja de que, debido a la alimentación con energía del transpondedor mediante el campo de consulta, el ajuste del alcance resulta problemático. Por este motivo, todos estos sistemas proponen poner a disposición las antenas de emisión y recepción con una superficie de antena lo más grande posible. Todos los sistemas deben encontrar un compromiso entre tamaño de antena y tamaño del módulo de lectura, de modo que o bien el tamaño del módulo de lectura o bien la precisión de consulta son insatisfactorios.

Objeto de la invención

Por tanto, la invención se basa en el objetivo de poner a disposición un sistema de control de acceso para un aparato, que posibilite una alta precisión de consulta con al mismo tiempo una construcción pequeña del módulo de lectura.

La invención se describe en las reivindicaciones 1 y 5 independientes.

El aparato es un ordenador. Este ordenador está conectado preferiblemente a una red y el desbloqueo tiene lugar mediante el desbloqueo de un acceso a la red. Un descifrado de un soporte de datos cifrado en el ordenador también es un desbloqueo posible. El aparato también puede ser una caja registradora, y puede posibilitarse un desbloqueo mediante una apertura y/o desbloqueo de un cajetín para el dinero.

Se ha reconocido que el ajuste del alcance siempre es problemático cuando la llave se alimenta con energía mediante el campo de consulta. Por tanto se propone que la llave genere un campo de respuesta de manera autoalimentada. En cuanto la llave detecta el campo de consulta, preferiblemente la componente magnética, el campo B, ésta se activa. Sin embargo, la llave no obtiene su energía a partir del campo de consulta, sino que presenta una fuente de energía propia. El campo de respuesta se genera mediante esta fuente de energía propia. Este campo de respuesta contiene el código de autorización de acceso. En el módulo de lectura se recibe el campo de respuesta y se verifica la autorización de acceso. En caso de verificación positiva, el ordenador se desbloquea. Es preferible que mediante el ordenador se desbloquee un acceso de red a una red informática. Sin embargo, también es posible desbloquear el acceso al propio ordenador, por ejemplo mediante un cifrado del disco duro. También es preferible que el ordenador forme parte de una caja registradora. En este caso, en caso de verificación positiva de la llave puede desbloquearse el acceso a la caja y al cajetín para el dinero. Esto es interesante, por ejemplo, en supermercados ya que las cajas se protegen de este modo frente a accesos de personas ajenas.

El intercambio del código de autorización de acceso a través del campo de respuesta tiene lugar preferiblemente de manera cifrada. Se conocen algoritmos de cifrado apropiados.

El campo de consulta puede estar codificado por ejemplo con un identificador unívoco. Este identificador unívoco puede referirse por ejemplo al ordenador, para el que se consulta una autorización de acceso. La llave puede determinar el identificador unívoco a partir del campo de consulta recibido, y por ejemplo reaccionar sólo cuando el identificador unívoco coincide con uno de varios identificadores unívocos depositados en la llave. De este modo puede programarse la llave para determinados ordenadores.

El campo de consulta se emite preferiblemente en el modo de difusión. Es decir, que el campo de consulta se genera por el módulo de lectura a intervalos regulares y puede recibirse por todas las llaves que están dentro del alcance del campo de consulta.

Si la llave recibe el campo de consulta, ésta evalúa los datos contenidos en el campo de consulta, por ejemplo el identificador unívoco. Si éste coincide con un identificador unívoco previsto para la llave, la llave establece contacto con el módulo de lectura. Para ello, la llave emite un campo de respuesta electromagnético, que contiene un código de autorización de acceso. Es posible, por ejemplo, que la llave transmita en primer lugar sólo su número de

identificación. Este número de identificación se determina en el módulo de lectura a partir del campo de respuesta. Si el número de identificación coincide con un número de identificación de una lista almacenada en el módulo de lectura o en el ordenador, entonces se efectúa una autenticación de la llave. A este respecto se intercambia información de autenticación, preferiblemente cifrada, a través del campo de respuesta electromagnético entre la llave y el módulo de lectura y, en caso de autenticación satisfactoria, el ordenador se desbloquea mediante el módulo de lectura.

También es posible que varias llaves detecten al mismo tiempo el campo de consulta. Para evitar una perturbación mutua de los campos de respuesta emitidos en cada caso por las llaves, también se propone efectuar, antes de la emisión del campo de respuesta, una verificación anticolisión. Puede emplearse para ello por ejemplo un algoritmo de acceso múltiple por detección de portadora (CSMA). También puede activarse un modo de detección de colisión (CD).

La autenticación de la llave tiene lugar a intervalos regulares. De este modo se consigue que el ordenador se bloquee en caso de que la llave se aleje del módulo de lectura. En este caso, se genera de nuevo el campo de consulta por el módulo de lectura.

El módulo de lectura emite un campo de consulta de baja frecuencia. Este campo de consulta de baja frecuencia es preferiblemente un campo magnético, que se genera con ayuda de una bobina. Debido a que el campo de consulta es de baja frecuencia, su alcance puede ajustarse fácilmente. Son preferibles alcances de entre 30 y 90 cm. En el área cercana, la intensidad del campo del campo magnético es proporcional a $1/r^3$. La antena de emisión en el módulo de lectura y la antena de recepción en la llave para el campo de consulta están diseñadas para un acoplamiento magnético. Las antenas son bobinas cuyo campo emitido tiene una componente magnética considerablemente mayor en comparación con la componente eléctrica. Por tanto, preferiblemente, el campo de consulta es un campo magnético.

Si en la llave se ajusta un umbral de recepción para una determinada intensidad de campo del campo magnético, entonces puede ajustarse con mucha precisión el alcance del campo de consulta.

El módulo de lectura está configurado para emitir un campo de consulta de 125 kHz.

Para conseguir que el tamaño constructivo del módulo de lectura se mantenga pequeño, también se propone que el módulo de lectura presente una bobina de emisión que genera el campo de consulta. Puesto que el campo de consulta sólo debe presentar un alcance reducido y además no sirve para la alimentación con energía de la llave, basta con una bobina de emisión de pequeño tamaño constructivo.

Para posibilitar una buena recepción del campo de respuesta, también se propone que el módulo de lectura presente una antena de recepción separada de la bobina de emisión. El campo de respuesta puede recibirse a través de la antena de recepción. La antena de recepción en el módulo de lectura es una antena HF adaptada para altas frecuencias. La antena HF está adaptada para el circuito de recepción. La antena puede estar formada como lazo (bucle) sobre el hilo conductor. Se ha reconocido que mediante el empleo de una bobina de emisión y una antena de recepción separada de la misma puede aumentarse la calidad de transmisión con una reducción simultánea del tamaño constructivo.

Para la recepción del campo de consulta, la llave presenta preferiblemente una bobina de recepción. Esta bobina de recepción puede presentar por ejemplo una característica de recepción independiente del sentido. Esto es posible, por ejemplo, con ayuda de una bobina de ferrita 3-D. En una bobina de ferrita 3-D de este tipo están dispuestas tres bobinas, que están orientadas en tres planos perpendiculares entre sí. La bobina de recepción está diseñada para la recepción de un campo magnético.

Según un ejemplo de realización ventajoso es preferible que la llave, para la generación del campo de respuesta, presente un circuito de excitación. El circuito de excitación aplica una señal de desbloqueo que presenta el código de autorización de acceso a una antena de emisión. La antena de emisión está diseñada preferiblemente para emitir campos de alta frecuencia. El campo de respuesta se genera a través de la antena de emisión. Éste presenta el código de autorización de acceso. El código de autorización de acceso se aplica a la antena de emisión por medio de una señal de desbloqueo. La señal de desbloqueo junto con el código de autorización de acceso se genera en un circuito de excitación.

El circuito de excitación está alimentado por batería. En este caso, la fuente de energía para el campo de respuesta se posibilita mediante una batería. Ya no es necesario que el circuito de excitación obtenga su energía a través del campo de consulta. Más bien una configuración de este tipo posibilita una generación autoalimentada del campo de respuesta.

El campo de respuesta es un campo electromagnético de alta frecuencia. Se ha demostrado que es ventajosa una frecuencia en el intervalo de los megahercios de entre 400 y 950 Mhz, por ejemplo 433 MHz, 868 MHz, 915 MHz, 916 MHz, para el campo de respuesta. Esta banda de frecuencia es una banda ISM que puede utilizarse libremente

y por tanto no está sujeta a tasas. El campo de respuesta es un campo eléctrico con una componente de campo eléctrica, que es considerablemente mayor que la componente magnética.

Tal como ya se mencionó anteriormente, es especialmente preferible que el módulo de lectura presente una antena de recepción para intercambiar información de autenticación con la llave tras la recepción de un código de autorización de acceso. La antena de recepción está formada de manera que está optimizada para la recepción de campos de alta frecuencia. A través de la antena de recepción, el módulo de lectura puede intercambiar con la llave información a través de un campo de alta frecuencia. Debido a que la llave genera el campo de alta frecuencia de manera autoalimentada, éste puede presentar una intensidad de campo E alta, de modo que la antena de recepción puede diseñarse con una construcción pequeña.

Un objeto adicional es un procedimiento para el control de una autorización de acceso para un aparato con la emisión de un campo de consulta por un módulo de lectura y la recepción del campo de consulta por una llave. Este procedimiento se caracteriza por una emisión autoalimentada, por la llave, de un campo de respuesta electromagnético con un código de autorización de acceso al recibir el campo de consulta y un desbloqueo del aparato al recibir el módulo de lectura el código de autorización de acceso.

Para garantizar que una llave en el área de recepción del módulo de lectura se reconozca rápidamente se propone que el campo de consulta se genere a intervalos de tiempo y, tras la emisión del campo de consulta, se monitoriza una recepción del código de autorización de acceso. En el módulo de lectura, en un denominado modo de difusión, se genera el campo de consulta a intervalos de tiempo y se monitoriza si en respuesta al campo de consulta se recibe un campo de respuesta con un código de autorización de acceso.

En la llave se genera de manera autoalimentada una señal de desbloqueo que presenta el código de autorización de acceso para la generación del campo de respuesta al recibir el campo de consulta. Para ello la llave, mediante una alimentación por batería, genera una señal de desbloqueo, que contiene el código de autorización de acceso. La señal de desbloqueo se aplica a la antena de emisión de la llave y genera un campo de alta frecuencia.

Después de que la llave haya transmitido a través del campo de respuesta de alta frecuencia el código de autorización de acceso o al menos su número de identificación al módulo de lectura, entre el módulo de lectura y la llave, a través del campo de respuesta de alta frecuencia, se efectúa una autenticación de la llave y el ordenador sólo se desbloquea en caso de autenticación satisfactoria.

Para monitorizar si la llave permanece dentro del área de recepción del módulo de lectura, o se aleja del área de recepción del módulo de lectura, se propone que la información de autenticación se intercambie a intervalos de tiempo entre el módulo de lectura y la llave y que el ordenador sólo permanezca desbloqueado en caso de autenticación satisfactoria. Esto significa que, durante el periodo en el que la llave permanece en el área de recepción del módulo de lectura, el ordenador permanece desbloqueado. Esto se garantiza mediante una consulta regular de la llave.

Si la llave se aleja del área de recepción del módulo de lectura, el ordenador se bloquea. Si el usuario se aleja del ordenador, el ordenador se bloquea automáticamente.

Mediante el desbloqueo y el bloqueo automático del ordenador, ya no tiene que pedirse a los usuarios que introduzcan sus contraseñas para acceder al ordenador y, al abandonar el ordenador, éste ya no tiene que protegerse frente a accesos por personas ajenas. La seguridad de las redes informáticas aumenta considerablemente, ya que el acceso al ordenador se bloquea automáticamente cuando un usuario autorizado, o la llave asociada al usuario, se aleja del área de recepción del módulo de lectura.

Mediante un acoplamiento magnético entre el módulo de lectura y la llave por medio del campo de consulta magnético puede conseguirse un ajuste del alcance preciso. Por tanto el ordenador sólo se desbloquea cuando una llave autorizada se encuentra en un determinado perímetro alrededor del aparato de lectura. Se evita que llaves que se encuentren por ejemplo a más de 1,50 m del módulo de lectura provoquen un desbloqueo accidental del ordenador.

Es preferible la protección de un ordenador a través de un cifrado de soporte de datos. En este caso, mediante el desbloqueo del ordenador puede tener lugar un descifrado del soporte de datos. Los soportes de datos pueden ser discos duros, disquetes, soportes de datos ópticos, soportes de datos USB u otros.

Estas y otras ventajas se desprenden también de las reivindicaciones dependientes. A continuación se explicará más detalladamente la invención por medio de un dibujo que muestra un ejemplo de realización.

Descripción de la figura

En el dibujo, la única figura muestra un sistema para el control de una autorización de desbloqueo.

Descripción detallada de la invención

En dicha figura se muestra un ordenador (2), que está conectado a un módulo (4) de lectura. El módulo (4) de lectura presenta un control (6), una primera unidad (8) de emisión/recepción, una bobina (10), un módulo (12) de memoria, una segunda unidad (14) de emisión/recepción y una antena (16) de alta frecuencia. Se representa además una llave (18). La llave (18) presenta un control (20), una unidad (22) de emisión/recepción, una bobina (24) de ferrita 3-D, un circuito (26) de excitación, una antena (28) de alta frecuencia, una unidad (30) de memoria así como una fuente (32) de energía.

Las bobinas (10) y (24) están diseñadas para emitir y recibir campos magnéticos de baja frecuencia de entre 100 kHz y 150 kHz. Las unidades (8) y (22) de emisión/recepción están adaptadas para la emisión y recepción de estos campos de baja frecuencia.

La unidad (14) de emisión/recepción está adaptada para emitir y recibir campos de alta frecuencia a través de la antena (16) de alta frecuencia. Preferiblemente se aplican en este caso señales portadoras con 868 MHz a la antena (16) HF. El circuito (26) de excitación está diseñado también para recibir y emitir campos de alta frecuencia a 868 MHz. El circuito (26) de excitación aplica a la antena (28) HF una señal portadora correspondiente.

La unidad (12) de memoria almacena, entre otras cosas, un identificador unívoco para el módulo (4) de lectura, o respectivamente el ordenador (2). Además, la unidad (12) de memoria puede almacenar códigos de autorización de acceso de llaves. Además, en la unidad (12) de memoria pueden estar almacenadas claves para una comunicación cifrada.

La unidad (30) de memoria almacena un número de identificación de la llave (18). Además, la unidad (30) de memoria puede almacenar una lista de identificadores unívocos de módulos de recepción así como diferentes claves para una comunicación cifrada.

La fuente (32) de energía se garantiza mediante una batería.

Los controles (6) y (20) controlan la interacción entre los módulos dentro del módulo (4) de lecturas, o respectivamente de la llave (18). Los controles (6, 20) presentan para ello circuitos integrados y microprocesadores, que están programados de manera correspondiente. El funcionamiento de los sistemas representados es el siguiente:

El ordenador (2) está configurado y conectado al módulo (4) de lectura de tal manera que éste obtiene información de desbloqueo a través del módulo (4) de lectura y sólo permite un acceso cuando el módulo (4) de lectura ha transmitido información correspondiente al ordenador (2). Inicialmente, el ordenador (2) está bloqueado. El módulo (4) de lectura, a través de su control (6), enciende la unidad (8) de emisión/recepción. La unidad (8) de emisión/recepción determina a partir de la unidad (12) de memoria su identificador unívoco. El identificador unívoco se modula a una señal portadora de 125 kHz. La señal portadora se emite a través de la bobina (10). La intensidad del campo magnético de la señal (10) portadora puede ajustarse a través de la unidad (8) de emisión/recepción. Es preferible que la intensidad del campo magnético sea tal que el campo de consulta generado por la bobina (10) tenga un alcance de entre 0,3 y 1,2 m. El campo magnético de baja frecuencia emitido por la bobina (10) se recibe en la bobina (24) de ferrita 3-D. La señal de baja frecuencia recibida por la bobina (24) se demodula en la unidad (22) de emisión/recepción. Se determina el identificador unívoco del módulo (4) de recepción, contenido en la señal y lo transfiere al control (20). En el control (20), mediante los identificadores unívocos almacenados en la unidad (30) de memoria, se verifica si el identificador unívoco recibido coincide con un identificador unívoco asociado a la llave (18). En este caso, la llave (18) se activa.

A este respecto, el control (20) determina a partir de la unidad (30) de memoria un número de identificación de la llave (18). Este número de identificación de la llave (18) se transfiere al circuito (26) de excitación. El circuito (26) de excitación obtiene su energía de la fuente (32) de energía. El circuito (26) de excitación genera con la energía obtenida de la fuente (32) de energía una señal portadora a 868 MHz, que contiene el número de identificación de la llave (18). Esta señal portadora se aplica a la antena (28) HF y se emite un campo HF eléctrico.

La señal portadora emitida por la antena (28) HF se recibe por la antena (16) HF del módulo (4) de lectura. La señal recibida se evalúa en la unidad (14) de emisión/recepción y se extrae el número de identificación de la llave (18). El número de identificación de la llave (18) se transfiere al control (6). El control (6) verifica si en la unidad (12) de memoria está almacenado un número de identificación correspondiente. En la unidad (12) de memoria están almacenados, por ejemplo, todos los números de identificación de todas las llaves (18) que están programadas para el desbloqueo del ordenador (2).

Si el número de identificación de la llave (18) está almacenado en la unidad (12) de memoria, el control (6) ordena a la unidad (14) de emisión/recepción que efectúe una autenticación con la llave. Para ello se intercambia de manera bidireccional a través de las antenas (16, 28) HF información de autenticación entre el módulo (4) de lectura y la llave (18). A este respecto se intercambian claves almacenadas en las unidades (12, 30) de memoria y se codifican

de manera correspondiente. Para ello son adecuados, por ejemplo, procedimientos de cifrado asimétrico. Una vez efectuada satisfactoriamente la autenticación, el módulo (4) de lectura comunica al ordenador (2) que éste debe desbloquearse. El ordenador (2) está disponible para el usuario a partir de entonces. Por ejemplo, este desbloqueo puede incluir un desbloqueo en una red.

Para garantizar que la llave (18) permanece dentro del área de recepción del módulo (4) de lectura y por tanto que el ordenador puede permanecer desbloqueado, el módulo (4) de lectura emite a intervalos regulares a través de la antena (16) HF señales de consulta para consultar si la llave (18) sigue estando en el área de recepción. El ordenador (2) sólo permanece desbloqueado en caso de una respuesta correspondiente de la llave (18) a través de la antena (28) HF. Si a una consulta a través de la antena (16) no se obtiene ninguna respuesta correspondiente de la llave (18) a través de la antena (28), entonces el control (6) del módulo (4) de lectura comunica al ordenador (2) que éste debe bloquearse. El ordenador (2) activa a continuación su bloqueo de acceso y ya no es posible acceder al ordenador (2), o respectivamente a la red conectada al ordenador (2).

Para verificar si una llave (18) está de nuevo cerca del módulo (4) de lectura, el módulo (4) de lectura envía señales de consulta a intervalos regulares a través de la bobina (10). Si ninguna llave (18) se encuentra dentro del campo magnético de la bobina (10), entonces el ordenador (2) permanece bloqueado. Si una llave (18) se mueve al interior del campo magnético de la bobina (10), entonces tiene lugar una verificación, descrita anteriormente, de la llave (18) y, en caso de verificación positiva, el ordenador (2) vuelve a desbloquearse.

El procedimiento según la invención y el dispositivo según la invención posibilitan una autenticación sin contacto de usuarios de ordenador. Mediante el empleo de bobinas de emisión y de recepción diferentes tanto en el módulo (4) de lectura como en la llave (18) se garantiza que, con un ajuste del alcance preciso, se posibilita una alta seguridad de transmisión. El módulo (4) de lectura y la llave (18) pueden estar formados con una construcción pequeña, ya que los campos de consulta sólo tienen que irradiarse con baja energía y la llave (18) está autoalimentada.

REIVINDICACIONES

1. Dispositivo para el control de una autorización de acceso para un ordenador (2) con un módulo (4) de lectura que emite un campo de consulta electromagnético de entre 100 kHz y 150 kHz, y

al menos una llave (18) que recibe el campo de consulta,

en el que el campo de consulta está codificado con un identificador que identifica unívocamente el ordenador,

en el que la llave determina el identificador unívoco a partir del campo de consulta,

en el que la llave sólo reacciona cuando el identificador unívoco coincide con uno de varios identificadores unívocos depositados en la llave,

en el que la llave (18) está configurada para la emisión autoalimentada de al menos su número de identificación al recibir el campo de consulta a través de un campo de respuesta de alta frecuencia de entre 400 MHz y 950 MHz, y presentando la llave (18) una batería,

en el que el módulo (4) de lectura está configurado para intercambiar información de autenticación con la llave (18) a través del campo de respuesta de alta frecuencia tras una coincidencia del número de identificación con un número de identificación de una lista almacenada en el módulo de lectura o en el ordenador,

en el que la información de autenticación se intercambia de manera bidireccional a través de antenas (16, 28) de alta frecuencia a través del campo de respuesta de alta frecuencia entre el módulo (4) de lectura y la llave (18),

en el que el módulo (4) de lectura está configurado para desbloquear el ordenador (2) tras una autenticación satisfactoria de la llave (18),

en el que la información de autenticación se intercambia a intervalos de tiempo regulares entre el módulo (4) de lectura y la llave (18) a través del campo de respuesta de alta frecuencia, y

en el que el ordenador (2) permanece desbloqueado sólo en caso de autenticación satisfactoria.

2. Dispositivo según la reivindicación 1, caracterizado porque la llave (18) presenta una bobina (24) de recepción que recibe el campo de consulta.

3. Dispositivo según una de las reivindicaciones anteriores, caracterizado porque una bobina (24) de recepción tiene una característica de recepción esencialmente independiente del sentido.

4. Dispositivo según una de las reivindicaciones anteriores, caracterizado porque un circuito (26) de excitación está alimentado por batería.

5. Procedimiento para el control de una autorización de acceso para un ordenador con la emisión de un campo de consulta electromagnético entre 100 kHz y 150 kHz por un módulo (4) de lectura y la recepción del campo de consulta por una llave (18),

en el que el campo de consulta se codifica con un identificador que identifica unívocamente el ordenador,

en el que la llave determina el identificador unívoco a partir del campo de consulta,

en el que la llave sólo reacciona cuando el identificador unívoco coincide con uno de varios identificadores unívocos depositados en la llave, y

en el que la llave (18) está configurada para la emisión autoalimentada al menos de su número de identificación al recibir el campo de consulta a través de un campo de respuesta de alta frecuencia de entre 400 MHz y 950 MHz, en el que la llave (18) presenta una batería, en el que el módulo (4) de lectura intercambia información de autenticación con la llave (18) a través del campo de respuesta de alta frecuencia tras una coincidencia del número de identificación con un número de identificación de una lista almacenada en el módulo de lectura o en el ordenador,

en el que la información de autenticación se intercambia de manera bidireccional a través de antenas (16, 28) de alta frecuencia a través del campo de respuesta de alta frecuencia entre el módulo (4) de lectura y la llave (18),

en el que el ordenador (2) se desbloquea tras una autenticación satisfactoria de la llave (18) por el módulo (4) de lectura,

en el que la información de autenticación se intercambia a intervalos de tiempo regulares entre el módulo (4) de lectura y la llave (18) a través del campo de respuesta de alta frecuencia, y

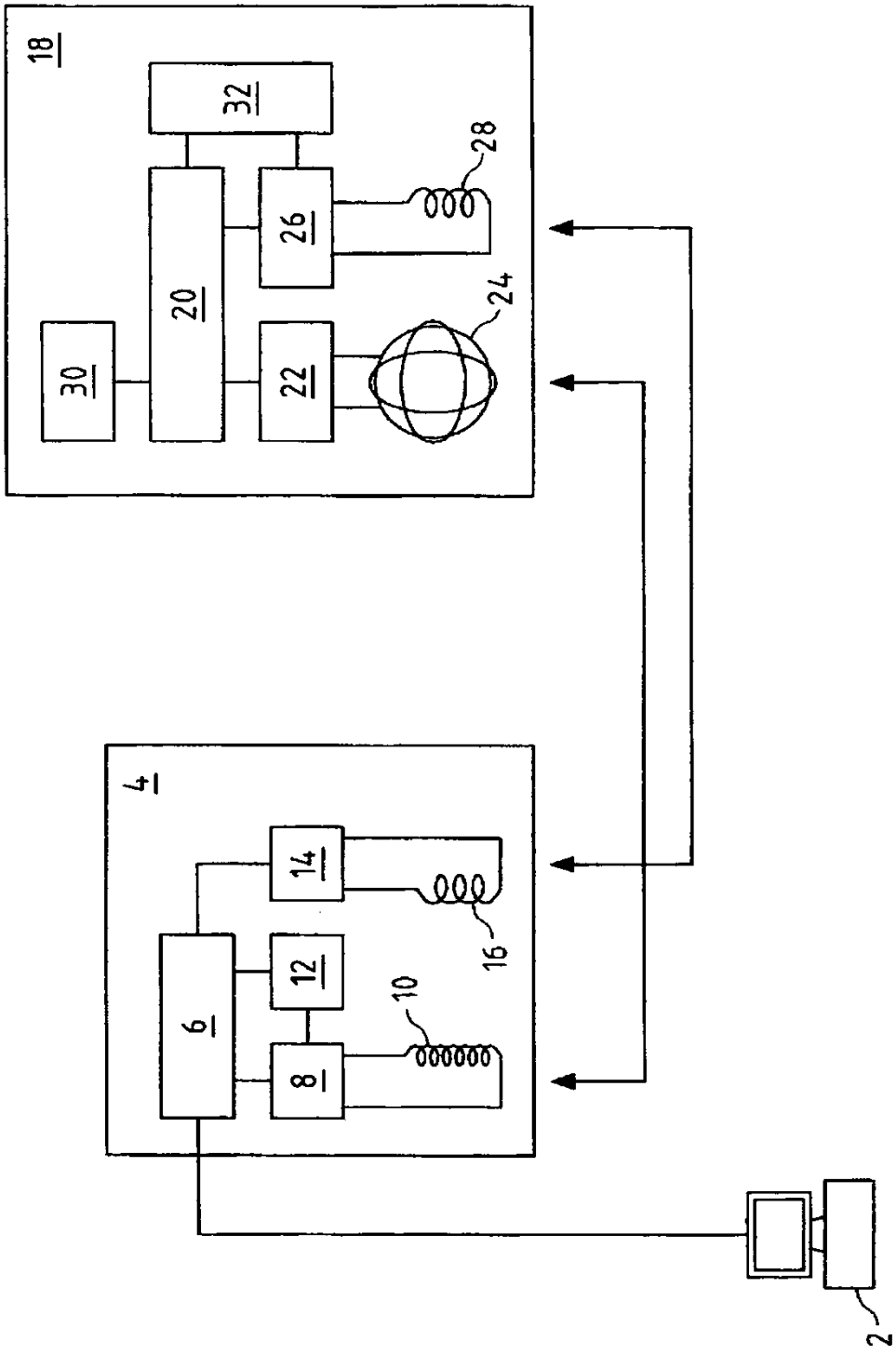
en el que el ordenador (2) permanece desbloqueado sólo en caso de autenticación satisfactoria.

6. Sistema para el control de una autorización de acceso con un ordenador (2) y un dispositivo según una de las reivindicaciones anteriores 1 a 4.

7. Sistema según la reivindicación 6, caracterizado porque el desbloqueo del ordenador se realiza mediante un descifrado de un soporte de datos en el ordenador.

8. Sistema según la reivindicación 6, caracterizado porque el ordenador (2) forma parte de una caja registradora.

9. Sistema según la reivindicación 8, caracterizado porque el desbloqueo de la caja registradora se realiza mediante un desbloqueo de un cajetín para el dinero en la caja registradora.


18
32
28
26
20
24
30
22
4
14
16
12
10
6
8
2