(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 547 101**

(51) Int. CI.:

G07C 9/00 (2006.01)
E05B 47/00 (2006.01)
H04B 13/00 (2006.01)
B60R 25/24 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.10.2012 E 12450043 (0)**

(97) Fecha y número de publicación de la concesión europea: **05.08.2015 EP 2584541**

(54) Título: **Procedimiento para el control de acceso**

(30) Prioridad:

18.10.2011 AT 15252011

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.10.2015

(73) Titular/es:

EVVA SICHERHEITSTECHNOLOGIE GMBH (100.0%)
Wienerbergstrasse 59-65
1120 Wien, AT

(72) Inventor/es:

ARTHABER, HOLGER y
PSAIER, STEFAN

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento para el control de acceso

La invención concierne a un procedimiento para el control de acceso, en particular en edificios, en el que tiene lugar una transmisión de datos bidireccional entre una llave electrónica y un dispositivo de control de acceso, comprendiendo la transmisión de datos la transmisión de datos de identificación de la llave electrónica al dispositivo de control de acceso, en donde se evalúan los datos de identificación en el dispositivo de control de acceso para verificar la autorización de acceso y, en dependencia de la autorización de acceso verificada, se activa un miembro de bloqueo para desbloquear o bloquear discrecionalmente el acceso, en donde la transmisión de datos se realiza al menos parcialmente por medio de un acoplamiento capacitivo entre la llave electrónica y el dispositivo de control de acceso.

La invención concierne además a un dispositivo para llevar a cabo este procedimiento, que comprende un dispositivo de control de acceso y una llave electrónica que presentan respectivamente un dispositivo de emisión/recepción para hacer posible una transmisión de datos bidireccional entre la llave electrónica y el dispositivo de control de acceso, en donde la llave electrónica presenta una memoria para los datos de identificación que coopera con el dispositivo de emisión/recepción de la llave para transmitir los datos de identificación al dispositivo de control de acceso, en donde el dispositivo de control de acceso presenta un circuito de evaluación para verificar la autorización de acceso sobre la base de los datos de identificación recibidos y el circuito de evaluación coopera con un miembro de bloqueo para desbloquear o bloquear discrecionalmente el acceso, en donde el dispositivo de emisión/recepción de la llave electrónica y del dispositivo de control de acceso presenta al menos un respetivo módulo de transmisión de datos capacitivo que presenta una capacitancia de acoplamiento, de modo que la transmisión de datos puede realizarse al menos parcialmente por medio de un acoplamiento capacitivo entre la llave electrónica y el dispositivo de control de acceso.

Procedimientos y dispositivos de este tipo se han dado a conocer, por ejemplo, por los documentos WO 2007/128009 A1, EP 1168678 A1 y WO 00/15931 A1. La ventaja de la transmisión de datos capacitiva está en que la transmisión de datos entre la llave electrónica y el dispositivo de control de acceso no puede escucharse o interceptarse con medios sencillos. La transmisión de datos capacitiva funciona de modo que la llave electrónica genera un campo próximo a través del cual se evalúan los datos a transmitir. El campo próximo capacitivo se acopla en este caso a la persona que lleva la llave y se transporta adicionalmente a través de la persona. Además, la unidad de recepción del dispositivo de control de acceso presenta una superficie de acoplamiento capacitiva de modo que, durante el contacto del dispositivo de control de acceso o durante la aproximación al dispositivo de control de acceso por parte de la persona, se cierre un circuito de corriente alterna y se origine un flujo eléctrico por el dispositivo de control de acceso que puede captarse por la unidad de recepción. La transmisión de datos capacitiva tiene como consecuencia que la propia llave electrónica no debe colocarse en la proximidad inmediata del receptor del dispositivo de control de acceso y no es necesaria ninguna activación de la llave controlada por el usuario, por ejemplo por medio de una presión de botón. Por el contrario, es suficiente que la llave electrónica se encuentre en la proximidad del cuerpo del respectivo usuario, por ejemplo en un bolsillo del pantalón, una cartera de mano o similar. Los datos a transmitir pueden modularse en este caso, por ejemplo, sobre una frecuencia portadora generada por la llave electrónica.

Por tanto, se eleva esencialmente la facilidad de manejo del control de acceso y se asegura además que se realice una transmisión de datos solamente cuando la persona que lleva la llave se acerca al dispositivo de control de acceso o contacta con éste, de modo que casi se eliminan las posibilidades de manipulación por terceros. Además, debido a la circunstancia de que se utiliza un campo próximo capacitivo reducidamente energético, el consumo de energía del sistema de control de acceso es extremadamente reducido y, en particular, lo es el consumo de corriente de la llave electrónica.

Por llaves electrónicas se entienden a continuación diferentes configuraciones de medios de identificación que tienen almacenado un código electrónico o datos de identificación, por ejemplo en forma de tarjetas, llaveros y combinaciones de llaves mecánicas y electrónicas.

En la transmisión capacitiva de los datos en el curso de un proceso de bloqueo es desventajoso que las corrientes de desplazamiento que se originan durante el acoplamiento capacitivo puedan propagarse debido a estructuras eléctricamente conductoras, por ejemplo en la zona de una puerta, de modo que la propagación de una señal no puede controlarse siempre con precisión. Por tanto, sin precauciones adicionales, puede suceder el caso de que datos de identificación emitidos desde la llave no sólo se proporcionen al dispositivo de control de acceso de la puerta deseada, sino también al de la puerta próxima, de modo que se active posiblemente un proceso de bloqueo en la puerta falsa.

El documento WO2009/152628 A1 muestra un sistema de control de acceso con acoplamiento capacitivo y de alta frecuencia (AF).

Por tanto, la invención se basa en el problema de mejorar un procedimiento y un dispositivo de control de acceso del tipo citado al principio con respecto a las desventajas anteriormente mencionadas, sin perder las ventajas de la transmisión capacitiva, como, por ejemplo, la eficiencia energética y la falta de propagación en espacios libres.

La solución de este problema se presenta en las reivindicaciones independientes 1 y 14. La invención prevé que una parte de los datos transmitidos entre la llave electrónica y el dispositivo de control de acceso se transmita a través de un acoplamiento capacitivo y una parte de los datos se transmita a través de ondas de radio. Dado que se utilizan de manera alternativa o paralela diferentes procedimientos de transmisión de datos, las características de transmisión de los respectivos procedimientos pueden aprovecharse de manera óptima. En el acoplamiento capacitivo la transmisión de datos se realiza con ayuda de un campo eléctrico, mientras que la transmisión de datos en el caso de ondas de radio se realiza por medio de un campo electromagnético. Los campos mencionados tienen diferentes propiedades de propagación que se aprovechan dependiendo del tipo de los respectivos datos a transmitir y de la cantidad de datos. El campo eléctrico utilizado para la transmisión de datos con ayuda del acoplamiento capacitivo se propaga solamente unos pocos centímetros, mientras que un campo electromagnético que surge durante la transmisión por ondas de radio presenta una propagación sustancialmente mayor. Durante la utilización de radiación de radio dirigida (lo que implica de manera adecuada una longitud de onda corta) se tiene que, como consecuencia de la elevada frecuencia portadora, la tasa de transmisión de datos puede ser también más alta en comparación con la de la transmisión capacitiva.

Según una forma de procedimiento preferida, los datos de identificación se transmiten desde la llave eléctrica hasta el dispositivo de control de acceso por medio de un acoplamiento capacitivo. En la transmisión de datos de identificación importa especialmente la seguridad de transmisión y escucha. Aquí, en el ámbito de la invención, se aprovechan las ventajas del acoplamiento capacitivo, que funciona solamente a través de distancias muy cortas, de modo que apenas sea posible una escucha o interceptación de los datos transmitidos. Por el contrario, otros datos que no sirven para la identificación directa de una llave, pueden transmitirse a través de ondas de radio. Por ejemplo, los datos transmitidos del dispositivo de control de acceso a la llave electrónica a través de un canal de retorno son menos sensibles. Una forma de procedimiento adicional preferida prevé que al menos una parte de los datos transmitidos del dispositivo de control de acceso a la llave electrónica se transmita a través de ondas de radio.

Para algunos casos de aplicación, puede ser completamente suficiente que todos los datos transmitidos de la llave electrónica al dispositivo de control de acceso se transmitan a través de un acoplamiento capacitivo y todos los datos transmitidos del dispositivo de control de acceso a la llave electrónica se transmitan a través de ondas de radio. Esto reduce el coste estructural tanto en el dispositivo de control de acceso como también en la llave electrónica, dado que la llave electrónica necesita solamente un emisor que trabaje de manera capacitiva y un receptor para la transmisión por ondas de radio, y, por el contrario, el dispositivo de control de acceso necesita solamente un receptor que trabaje de manera capacitiva y un emisor para la transmisión por ondas de radio.

Para aumentar la seguridad es ventajoso que la persona que lleva la llave electrónica pueda ser localizada en el curso del proceso de bloqueo. Esto es especialmente con respecto a la problemática anteriormente citada de la esencial propagación de los datos transmitidos de forma capacitiva. No obstante, esto también con respecto a la problemática de “hombre en medio”, en la que la transmisión capacitiva de datos al dispositivo de control de acceso no se realiza solamente a través de la persona que lleva consigo la llave electrónica, sino a través de una persona que está entre la citada persona y el dispositivo de control de acceso. Por tanto, el “hombre en medio” ni siquiera debería llevar consigo una llave autorizada para procurarse un acceso, sino que, con una mano, podría contactar con el dispositivo de control de acceso y, con la otra mano, con la persona que lleva consigo la llave autorizada. La localización de la persona debe asegurar que la persona, de cuya llave electrónica obtiene datos el dispositivo de control de acceso, se encuentre realmente en la proximidad inmediata del dispositivo de control de acceso. La localización se realiza de manera preferida de modo que el dispositivo de control de acceso emita una señal de control de presencia a través de ondas de radio, cuyo alcance asciende a menos de 2 m, preferiblemente menos de 1 m. La señal de control de presencia se recibe en este caso solamente por una llave electrónica que se encuentra dentro del alcance de la señal de radio. Preferiblemente, puede hacerse una delimitación adicional cuidando de que la señal de control de presencia se emita concentrada a través de al menos una antena direccional. Preferiblemente, en el cuso del proceso de localización se transmite adicionalmente un mensaje de la llave electrónica al dispositivo de control de acceso por medio de un acoplamiento capacitivo. Por tanto, durante el proceso de localización se realiza la transmisión de datos o señales en una dirección a través de ondas de radio y en la otra dirección a través de un acoplamiento capacitivo, de modo que la diferente característica de propagación de un campo eléctrico (acoplamiento capacitivo) y de un campo electromagnético (transición por ondas de radio) puede aprovecharse para verificar la posición de la llave electrónica. La llave electrónica se localiza sólo en la zona en la que se superponen los dos campos de propagación.

Básicamente, la señal de control de presencia puede ser la respuesta a un mensaje de consulta de la llave o la señal de control de presencia puede activar el reenvío de un mensaje de confirmación de recepción. Son imaginables también ambas posibilidades.

En este caso, preferiblemente, se procede de modo que el dispositivo de control de acceso emita la señal de control de presencia después de haber recibido un mensaje de consulta por medio de un acoplamiento capacitivo.

Se prevé preferiblemente que la llave electrónica, al recibir la señal de control de presencia, retransmita un mensaje de confirmación de recepción y el dispositivo de control de acceso desbloquee la transmisión adicional de datos entre el dispositivo de control de acceso y la llave electrónica solamente al recibir el mensaje de aprobación de recepción. El mensaje de confirmación de recepción se retransmite en este caso, en particular, a través de un acoplamiento capacitivo.

Para poder asociar uno a otro los mensajes transmitidos en el curso del proceso de localización, se prevé preferiblemente que se transmita con el mensaje de consulta o la señal de control de presencia un indicativo que se devuelva con el mensaje retransmitido.

Una forma de procedimiento especialmente ventajosa para la localización de la llave electrónica durante la transmisión de los datos de identificación especialmente sensibles consiste en que la transmisión de datos bidireccional entre la llave electrónica y el dispositivo de control de acceso comprenda los siguientes pasos:

- Transmitir los datos de identificación de la llave electrónica al dispositivo de control de acceso por medio de un acoplamiento capacitivo,

- Comprobar si la llave electrónica está presente en una zona local predeterminada en la proximidad del dispositivo de control de acceso para lo cual se emite una señal de control de presencia por el dispositivo de control de acceso a través de ondas de radio dirigidas y débiles, y, en caso de la recepción de la señal de control de presencia por la llave electrónica, se transmite un mensaje de confirmación de recepción de la llave electrónica al dispositivo de control de acceso.

Una localización especialmente precisa de la llave electrónica se realiza en este caso haciendo que la señal de control de presencia se emita a través de ondas de radio cuyo alcance asciende a menos de 2 m, preferiblemente menos de 1 m.

Para delimitar lo mejor posible la zona de superposición antes comentada de los campos de propagación del campo eléctrico y del campo electromagnético, se procede preferiblemente de modo que el dispositivo de control de acceso esté asociado a una puerta y que la señal de control de presencia se emita y/o se reciba a través de ondas de radio dirigidas en sentido sustancialmente perpendicular a la puerta. En esta forma de procedimiento se captan solamente las llaves electrónicas que están presentes en la zona de las ondas de radio dirigidas de manera sustancialmente perpendicular a la puerta. De esta manera, se consigue una localización selectiva en una zona circundante predeterminada.

El principio en el que se basa la invención para transmitir los datos parcialmente a través de un acoplamiento capacitivo y parcialmente a través de ondas de radio, puede utilizarse también en caso de la transmisión cifrada de datos. Una forma de procedimiento preferida prevé en este contexto que los datos de identificación se transmitan por un enlace seguro mediante un acoplamiento capacitivo y que el intercambio de datos entre la llave electrónica y el dispositivo de control de acceso, necesario para establecer el enlace seguro, se realice al menos parcialmente por medio de ondas de radio.

La transmisión de datos por medio de un acoplamiento capacitivo tiene la ventaja, como se ha mencionado al principio, de que la propia llave electrónica no debe colocarse en la proximidad inmediata del dispositivo de control de acceso para provocar la transmisión de datos. Por el contrario, es suficiente que la llave electrónica se lleve en el cuerpo o en la proximidad del cuerpo de la persona en cuestión, dado que el cuerpo humano puede utilizarse como medio de transmisión. Una forma de procedimiento preferida prevé en este contexto que los datos transmitidos de la llave electrónica al dispositivo de control de acceso a través de un acoplamiento capacitivo se acoplen a la persona que lleva la llave electrónica y se acoplen en el dispositivo de control de acceso por una parte corporal de la persona que se aproxima a un electrodo de acoplamiento del dispositivo de control de acceso o contacta con éste.

Según un aspecto adicional de la presente invención, se perfecciona un dispositivo del tipo citado al principio de tal modo que el dispositivo de emisión/recepción de la llave electrónica y del dispositivo de control de acceso presente además un respectivo módulo de transmisión por radio, para que los datos transmitidos entre la llave electrónica y el dispositivo de control de acceso puedan transmitirse discrecionalmente a través de un acoplamiento capacitivo y/o a través de ondas de radio. Perfeccionamientos preferidos del dispositivo según la invención se desprenden de las reivindicaciones subordinadas.

La invención se explica con más detalle a continuación con ayuda de ejemplos de realización representados en el dibujo. En éste muestran la figura 1, una representación esquemática del funcionamiento de un dispositivo de control de acceso que trabaja con acoplamiento capacitivo, la figura 2, un esquema eléctrico equivalente simplificado de la configuración según la figura 1, la figura 3, un ejemplo de realización en el que la transmisión de datos entre la llave electrónica y el dispositivo de control de acceso se realiza tanto de forma capacitiva como también por medio de ondas de radio, y la figura 4, un esquema del desarrollo de la transmisión de datos.

En la figura 1 se representan esquemáticamente una puerta con una persona que abre la puerta, así como las capacitancias de dispersión, pérdida y acoplamiento individuales. La puerta está designada con 1 y presenta un dispositivo de control de acceso 2 con un miembro de accionamiento 3 configurado como un pomo. La persona 4

lleva una llave electrónica 5 que puede introducirse, por ejemplo, en un bolsillo de pantalón. La llave electrónica 5 genera en este caso un campo próximo capacitivo con una frecuencia portadora sobre la cual se modulan datos de identificación. El campo próximo capacitivo se acopla a la superficie del cuerpo de la persona 4 y, a continuación, se retransmite a un receptor del dispositivo de control de acceso 2. En este caso, la llave electrónica 5 presenta una capacitancia de dispersión Cst frente al suelo 6. En la transición entre la llave electrónica 5 y la persona 4 puede observarse una capacitancia de acoplamiento Ck. Además, aparece una capacitancia de pérdida Cv entre la persona 4 y el suelo 6. Finalmente, el dispositivo de control de acceso 2 o su cilindro de cierre presentan una capacitancia de cilindro Cz frente al suelo.

El esquema eléctrico equivalente simplificado correspondiente está representado en la figura 2, en la que se indican de nuevo las capacitancias descritas. En este caso, Cv representa todas las capacitancias que tienen como consecuencia flujos eléctricos que no se cierran por el emisor a través del condensador de recepción del receptor, sino que se pasan por delante de éste y, por tanto, no aportan nada al acoplamiento entre el receptor y el emisor. Cst representa las capacitancias que están disponibles como suma para el acoplamiento capacitivo del electrodo de emisión frente al suelo. Ck representa las capacitancias que están disponibles como suma para el acoplamiento capacitivo de la persona 4 al segundo electrodo. Cz representa las capacitancias que están disponibles como suma para el acoplamiento capacitivo del dispositivo de control de acceso o su cilindro de cierre al suelo. En este caso, en la figura 2, el dispositivo de control de acceso está designado de nuevo con 2 y presenta un condensador de recepción 7. El diseño del condensador de recepción 7 debe elegirse de modo que, por un lado, se cierre un flujo eléctrico suficiente a través del condensador de recepción y que, por otro lado, la tensión en el condensador no se haga demasiado pequeña. Si la capacitancia del condensador de recepción es demasiado pequeña, entonces se cierra demasiado poco flujo eléctrico a través del mismo. No obstante, una capacitancia demasiado grande del condensador de recepción es también molesta en el sentido de que la tensión en el condensador U=Q/C se hace desfavorablemente pequeña.

En la figura 3, el dispositivo de control de acceso está designado de nuevo con 2 y la llave electrónica con 5. El dispositivo de control de acceso 2 comprende un dispositivo de emisión/recepción 8 con un circuito de control 9 que es responsable de conducir los datos a transmitir al módulo de transmisión por radio 10 o al módulo de transmisión de datos capacitivo 11, que transmite los datos a través de ondas de radio o a través de un acoplamiento capacitivo. El módulo de transmisión por radio 10 y el módulo de transmisión de datos capacitivo 11 comprenden una respectiva antena no representada. La antena del módulo de transmisión por radio 10 está configurada, por ejemplo, como una antena direccional. La antena del módulo de transmisión de datos capacitivo comprende una capacitancia de acoplamiento, por ejemplo en forma de un condensador con al menos un electrodo de acoplamiento. Los datos obtenidos por el dispositivo de emisión/recepción a través de un acoplamiento capacitivo con la llave 5 o a través de un enlace de radio con la llave 5 se suministran a unos medios de procesamiento en forma de un microcontrolador 12 en el que se procesan los datos. En el microcontrolador 12 se materializa un circuito de evaluación 13 con el que se verifica si los datos de identificación recibidos de la llave 5 se traducen una autorización de acceso. En caso de una comprobación positiva de la autorización de acceso, el microcontrolador 12 activa un elemento de desbloqueo 14, de modo que se desbloquea un miembro de bloqueo de un dispositivo de cierre (no representado).

En el curso de un deseo de acceso se realiza una transmisión bidireccional de datos entre la llave 5 y el dispositivo de control de acceso 2. Es necesario un enlace bidireccional, por ejemplo, para el intercambio de datos de autentificación durante el establecimiento de un enlace seguro entre la llave 5 y el dispositivo de control de acceso 2 y para el intercambio de datos de estado y datos de comprobación o similares. Los datos previstos para su envío del dispositivo de control de acceso 2 a la llave 2 se generan y se elaboran en el microcontrolador 12 y se suministran al dispositivo de emisión/recepción 8. Un circuito de adaptación 15 configurado en el microcontrolador 12 es responsable en este caso de que se adapten los datos para su envío a través del módulo de transmisión por radio 10 o el módulo de transmisión de datos capacitivo 11, lo que puede hacerse necesario, por ejemplo, debido a los diferentes protocolos de transmisión según el módulo. Se puede adaptar también la intensidad de la señal, pudiendo preverse el circuito de adaptación básicamente también en el dispositivo de emisión/recepción 8.

La llave electrónica 5 presenta también unos medios de procesamiento en forma de un microcontrolador 16 y un dispositivo de emisión/recepción 17 unido con el microcontrolador 16 y dotado de un módulo de transmisión por radio 18 y un módulo de transmisión de datos capacitivo 19. El circuito de control 20 es responsable de que los datos a enviar se suministren, según las especificaciones, al módulo de transmisión por radio 18 o al módulo de transmisión de datos capacitivo 19. El microcontrolador comprende una memoria 21 para los datos de identificación.

En el curso de un deseo de acceso puede tener lugar la comunicación de datos indicada en el ejemplo siguiente. Tan pronto como el dispositivo de control de acceso (por ejemplo, integrado en el herraje) ha reconocido con éxito una llave electrónica (por ejemplo, un medio de identificación) en su entorno, se establece activamente una comunicación por ambos lados. Si la transmisión es puramente capacitiva, no es obligatoriamente necesario utilizar una frecuencia de una banda de frecuencia ISM, dado que en este tipo de transmisión no tiene lugar ninguna radiación electromagnética hacia el espacio. La figura 4 muestra el desarrollo de una transmisión de datos. El herraje emite al comienzo un mensaje de consulta para verificar si el medio de identificación se encuentra en la proximidad y está operativo. Tan pronto como el medio de identificación reconoce con éxito esta señal, devuelve una señal de acuse de recibo (ACK) al herraje. Se realiza seguidamente una autentificación “reto-respuesta”:

Herraje		Medio de identificación
El herraje envía una orden de autentificación al medio de identificación	--> 1 byte	
	<-- SI(RndNrI) 8 bytes	El medio de identificación genera un número aleatorio (RndNrI) de 8 bytes, lo cifra con su clave SI y lo envía al herraje.
El herraje descifra los datos de 8 bytes recibidos con su clave (SB) y genera además un número aleatorio de 8 bytes adicional (RndNrB). Los datos RndNrI y RndNrB se cifran y se envían al medio de identificación.	--> SB (RndNrI+RndNrB) 16 Bytes	
	<-- SI (RndNrB) 8 Bytes o error	El medio de identificación descifra todos los bytes recibidos y controla el RndNrI. Si estos datos se han modificado, entonces SI y SB son diferentes y el medio de identificación envía un aviso de error al herraje. Si el bloque RndNrI es correcto, se devuelve encriptado el RndNrB al herraje.
El herraje descifra los datos recibidos y los controla. Si los datos recibidos son iguales al número aleatorio generado RndNrB, la autentificación está completa.		

Al final tanto el herraje como también el medio de identificación han reconocido con éxito que el correspondiente interlocutor es auténtico o válido. Los datos incompletos, un tiempo de espera demasiado largo en la respuesta y datos inválidos llevan inmediatamente a una interrupción de la comunicación.

A continuación, se puede generar también una clave de sesión de 8 bytes (SK) en ambos lados. Ésta se genera por medio de un algoritmo de cálculo definido a base de RndNrI y RndNrB. Empleando los números aleatorios generados se asegura que en cada autentificación se use una clave diferente, lo que elimina ataques de reproducción y hace que resulten muy complicados los intentos de hackeo para calcular las claves secretas SI y SB. La clave de sesión sirve para intercambiar seguidamente también datos encriptados (véase la figura 4 “Sesión”). Estos son necesarios para leer o escribir informaciones como, por ejemplo, estado de la batería, llave, etc., y son opcionalmente ampliables. Una sesión se termina por medio de una señal de final de sesión (EOS). Una interrupción del enlace, tiempos de cálculo demasiado largos y un número demasiado grande de repeticiones de intentos llevan automáticamente a una finalización de la sesión. Después de una finalización de la sesión, tanto a través de una señal EOS como también a través de un error, se genera de nuevo la clave de sesión.

El canal de comunicación del herraje a la llave utiliza en este ejemplo ondas de radio como medio portador, mientras que el canal de comunicación de la llave al herraje utiliza el campo próximo capacitivo.

Las ventajas de la invención se hacen evidentes también en los siguientes ejemplos de transmisión de datos.

Ejemplo 1:

La comunicación del herraje a la llave se realiza por medio de ondas de radio y la comunicación de la llave al herraje se realiza por medio de un acoplamiento capacitivo.

Caso 1:

El medio de identificación, durante la aproximación y/o contacto, envía los datos de identificación al herraje en un paquete. Después de la obtención de los datos el herraje comprueba la corrección del paquete de datos con la suma de prueba también enviada y calculada. Si los datos están bien (ningún error de transmisión), el herraje envía sus datos de respuesta (estado de la batería, listas de incidencias, ...) por radio al medio de identificación. El medio de identificación responde de forma capacitiva con un OK cuando se han recibido correctamente los datos. De lo contrario, el medio de identificación puede requerir al herraje el nuevo envío de los datos.

Caso 2:

Como en el caso 1, el medio de identificación envía sus datos al herraje, pero en varios paquetes cortos consecutivos asegurados por una suma de prueba o CRC. Si ahora uno de datos paquetes cortos está corrompido, el herraje requiere su nuevo envío. Por tanto, el tiempo de transmisión total se prolonga en caso de perturbaciones individuales en sólo aproximadamente la duración de la repetición del paquete corto perturbado, es decir, en grado insignificante, lo que es más eficiente con respecto al ejemplo-caso 1 (todos los datos de la llave deben enviarse de nuevo).

No resultan limitaciones para la localización de la persona, dado que la persona se debe encontrar en la intersección local del alcance de la comunicación capacitiva y de la comunicación por radio.

Ejemplo 2:

La comunicación de la llave al herraje se realiza por medio de un acoplamiento capacitivo, mientras que la comunicación del herraje a la llave puede realizase tanto a través de ondas de radio como también a través de un acoplamiento capacitivo.

En este caso, los datos se envían y se reciben de manera similar a los casos 1 y 2 anteriormente descritos. No obstante, con la particularidad de que todos los datos se intercambien a través de la señal de radio rápida. En este caso, el medio de identificación recibe del herraje un corto identificador temporalmente válido que se retransmite al herraje de manera capacitiva tan sólo muy poco antes del contacto o únicamente durante el contacto. Dado que la intensidad de la señal aumenta fuertemente en la transmisión capacitiva al establecer un contacto rápido y también muy especialmente durante el contacto, puede reconocerse qué persona contacta con el herraje. Todos los datos se transmiten cifrados a pesar del alcance reducido. En una forma de realización adicional pueden seleccionarse previamente por radio varios medios de identificación (en la zona de emisión/recepción) y se verifica entonces durante el contacto quien acciona la puerta.

REIVINDICACIONES

1. Procedimiento para el control de acceso, en particular en edificios, en el que tiene lugar una transmisión de datos bidireccional entre una llave electrónica y un dispositivo de control de acceso, en donde la transmisión de datos comprende la trasmisión de datos de identificación de la llave electrónica al dispositivo de control de acceso, en donde los datos de identificación se evalúan en el dispositivo de control de acceso para verificar la autorización de acceso y, en función de la autorización de acceso verificada, se activa un elemento de bloqueo para desbloquear o bloquear discrecionalmente el acceso, en donde la transmisión de datos se efectúa al menos parcialmente por medio de un acoplamiento capacitivo entre la llave electrónica y el dispositivo de control de acceso, y en donde una parte de los datos transmitidos entre la llave electrónica (5) y el dispositivo de control de acceso (2) se transmite por medio de un acoplamiento capacitivo y una parte de los datos se trasmite a través de ondas de radio, **caracterizado** por que la transmisión de datos bidireccional comprende la emisión de una señal de control de presencia por medio del dispositivo de control de acceso (2), emitiéndose la señal de control de presencia por medio de ondas de radio, cuyo alcance asciende a menos de 2 m, preferiblemente menos de 1 m.

2. Procedimiento según la reivindicación 1, **caracterizado** por que los datos de identificación se transmiten de la llave electrónica (5) al dispositivo de control de acceso (2) por medio de un acoplamiento capacitivo.

3. Procedimiento según la reivindicación 1 o 2, **caracterizado** por que al menos una parte de los datos transmitidos del dispositivo de control de acceso (2) a la llave electrónica (5) se transmite a través de ondas de radio.

4. Procedimiento según la reivindicación 1, 2 o 3, **caracterizado** por que todos los datos transmitidos de la llave electrónica (5) al dispositivo de control de acceso (2) se transmiten por medio de un acoplamiento capacitivo y todos los datos transmitidos del dispositivo de control de acceso (2) a la llave electrónica (5) se transmiten a través de ondas de radio.

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado** por que la señal de control de presencia se emite de manera concentrada a través de al menos una antena direccional.

6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado** por que el dispositivo de control de acceso (2) emite la señal de control de presencia después de haber recibido un mensaje de consulta por medio de un acoplamiento capacitivo.

7. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado** por que la llave electrónica (5) retransmite un mensaje de confirmación de recepción al recibir la señal de control de presencia y el dispositivo de control de acceso (2) desbloquea la transmisión de datos adicional entre el dispositivo de control de acceso (2) y la llave electrónica (5) solamente al recibir el mensaje de confirmación de recepción.

8. Procedimiento según la reivindicación 7, **caracterizado** por que el mensaje de confirmación de recepción se retransmite por medio de un acoplamiento capacitivo.

9. Procedimiento según una de las reivindicaciones 1 a 8, **caracterizado** por que se transmite con el mensaje de consulta o la señal de control de presencia un indicativo que se devuelve con el mensaje retransmitido.

10. Procedimiento según una de las reivindicaciones 1 a 9, **caracterizado** por que la transmisión de datos bidireccional entre la llave electrónica (5) y el dispositivo de control de acceso (2) comprende los siguientes pasos:

- transmitir los datos de identificación de la llave electrónica (5) al dispositivo de control de acceso (2) por medio de un acoplamiento capacitivo,

- comprobar si la llave electrónica (5) está presente en una zona local predeterminada en la proximidad del dispositivo de control de acceso (2), para lo cual se emite una señal de control de presencia procedente del dispositivo de control de acceso (2) por medio de ondas de radio dirigidas y, en caso de la recepción de la señal de control de presencia por medio de la llave electrónica (5), se transmite una señal de confirmación de recepción de la llave electrónica (5) al dispositivo de control de acceso (2).

11. Procedimiento según una de las reivindicaciones 1 a 10, **caracterizado** por que el dispositivo de control de acceso (2) está asociado a una puerta (1) y por que la señal de control de presencia se emite y/o se recibe por medio de ondas de radio dirigidas sustancialmente en sentido perpendicular a la puerta (1).

12. Procedimiento según una de las reivindicaciones 1 a 11, **caracterizado** por que los datos de identificación se trasmiten por un enlace seguro mediante un acoplamiento capacitivo y por que el intercambio de datos necesario para establecer el enlace seguro entre la llave electrónica (5) y el dispositivo de control de acceso (2) se realiza al menos parcialmente por medio de ondas de radio.

13. Procedimiento según una de las reivindicaciones 1 a 12, **caracterizado** por que los datos transmitidos de la llave electrónica (5) al dispositivo de control de acceso (2) por medio de un acoplamiento capacitivo se acoplan por la llave electrónica (5) a la persona (4) que lleva la llave electrónica (5), y se acoplan al dispositivo de control de acceso

(2) por una parte corporal de la persona (4) que se aproxima a un electrodo de acoplamiento del dispositivo de control de acceso (2) o que toca este electrodo.

14. Dispositivo para la realización del procedimiento según una de las reivindicaciones 1 a 13, que comprende un dispositivo de control de acceso (2) y una llave electrónica (5) que presentan un respectivo dispositivo de emisión/recepción (8) para hacer posible una transmisión de datos bidireccional entre la llave electrónica (5) y el dispositivo de control de acceso (2), en donde la llave electrónica (5) presenta una memoria (21) para datos de identificación que coopera con el dispositivo de emisión/recepción (8) de la llave (5) para transmitir los datos de identificación al dispositivo de control de acceso (2), en donde el dispositivo de control de acceso (2) presenta un circuito de evaluación (13) para verificar la autorización de acceso en base a los datos de identificación recibidos y el circuito de evaluación (13) coopera con un miembro de bloqueo para desbloquear o bloquear discrecionalmente el acceso, en donde el dispositivo de emisión/recepción (8) de la llave electrónica (5) y del dispositivo de control de acceso (2) presenta al menos un respectivo módulo de transmisión de datos (11) capacitivo que presenta una capacitancia de acoplamiento, de modo que la transmisión de datos puede realizarse al menos parcialmente por medio de un acoplamiento capacitivo entre la llave electrónica (5) y el dispositivo de control de acceso (2), y en donde el dispositivo de emisión/recepción (8) de la llave electrónica (5) y del dispositivo de control de acceso (2) presenta además un respectivo módulo de transmisión por radio (10), de modo que los datos transmitidos entre la llave electrónica (5) y el dispositivo de control de acceso (2) pueden transmitirse discrecionalmente por medio de un acoplamiento capacitivo y/o por medio de ondas de radio, **caracterizado** por que el circuito de control (20) del dispositivo de control de acceso (2) está preparado de tal manera que una señal de control de presencia procedente del dispositivo de control de acceso (2) se emite a través de ondas de radio cuyo alcance asciende a menos de 2 m, preferiblemente menos de 1 m.

15. Dispositivo según la reivindicación 14, **caracterizado** por que el dispositivo de emisión/recepción (8) de la llave electrónica (5) y del dispositivo de control de acceso (2) presenta un respectivo circuito de control que está preparado para recibir o emitir los datos, en función de informaciones de control, ya sea a través del módulo de transmisión de radio (10) o a través del módulo de transmisión de datos capacitivo (11), o bien a través de ambos módulos.

16. Dispositivo según la reivindicación 15, **caracterizado** por que el circuito de control (20) está preparado para que los datos de identificación se transmitan de la llave electrónica (5) al dispositivo de control de acceso (2) por medio del módulo de transmisión de datos capacitivo (11).

17. Dispositivo según la reivindicación 15 o 16, **caracterizado** por que el circuito de control (20) está preparado para que al menos una parte de los datos transmitidos del dispositivo de control de acceso (2) a la llave electrónica (5) se transmitan por medio del módulo de transmisión por radio (10).

18. Dispositivo según la reivindicación 15, 16 o 17, **caracterizado** por que el circuito de control (20) está preparado para que todos los datos transmitidos del dispositivo de control de acceso (2) a la llave electrónica (5) se transmitan por medio del módulo de transmisión por radio (10) y todos los datos transmitidos de la llave electrónica (5) al dispositivo de control de acceso (2) se transmitan por medio del módulo de transmisión de datos capacitivo (11).

19. Dispositivo según una de las reivindicaciones 14 a 18, **caracterizado** por que el módulo de transmisión por radio (10) comprende unos medios de ajuste para ajustar la potencia de emisión.

20. Dispositivo según una de las reivindicaciones 14 a 19, **caracterizado** por que el módulo de transmisión por radio (10) presenta una potencia de emisión, de modo que el alcance de las ondas de radio emitidas asciende a menos de 2 m, preferiblemente menos de 1 m.

21. Dispositivo según una de las reivindicaciones 14 a 20, **caracterizado** por que el módulo de transmisión por radio (10) está configurado como un emisor direccional.

22. Dispositivo según la reivindicación 21, **caracterizado** por que el dispositivo de control de acceso (2) está asociado a una puerta (1) y por que la antena direccional del emisor direccional está dispuesta para emitir y/o recibir las ondas de radio dirigidas de manera sustancialmente perpendicular a la puerta (1).

23. Dispositivo según una de las reivindicaciones 14 a 22, **caracterizado** por que están previstos unos medios para establecer un enlace seguro entre la llave electrónica (5) y el dispositivo de control de acceso (2) y por que los circuitos de control de la llave electrónica (5) y del dispositivo de control de acceso (2) están preparados para que los datos de identificación se transmitan por el enlace seguro mediante el módulo de transmisión de datos capacitivo (11, 19), y por que el intercambio de datos entre la llave electrónica (5) y el dispositivo de control de acceso (2), necesario para establecer el enlace seguro, se realiza por medio de los módulos de transmisión por radio (10, 18).

24. Dispositivo según una de las reivindicaciones 14 a 23, **caracterizado** por que los dispositivos de emisión/recepción (8) presentan un respectivo circuito de adaptación de señal para adaptar la señal a transmitir, según sea necesario, para la transmisión por ondas de radio o la transmisión capacitiva.

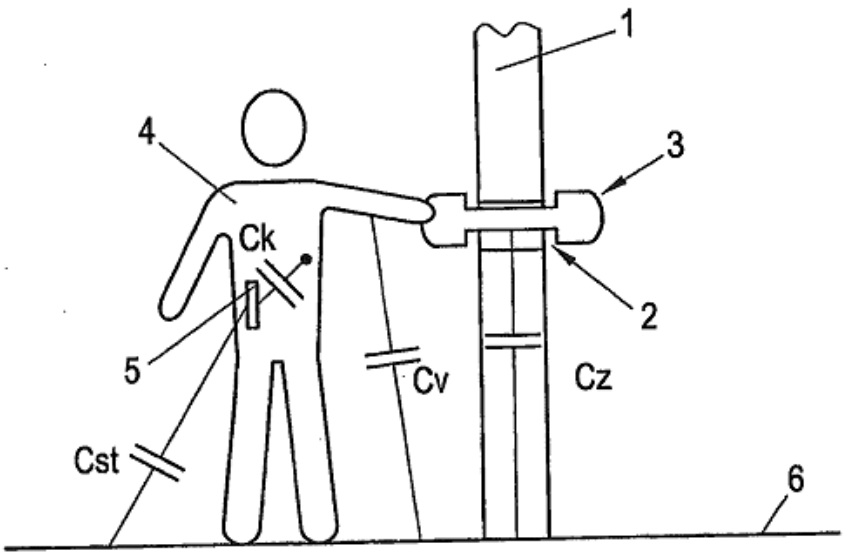

Fig. 1

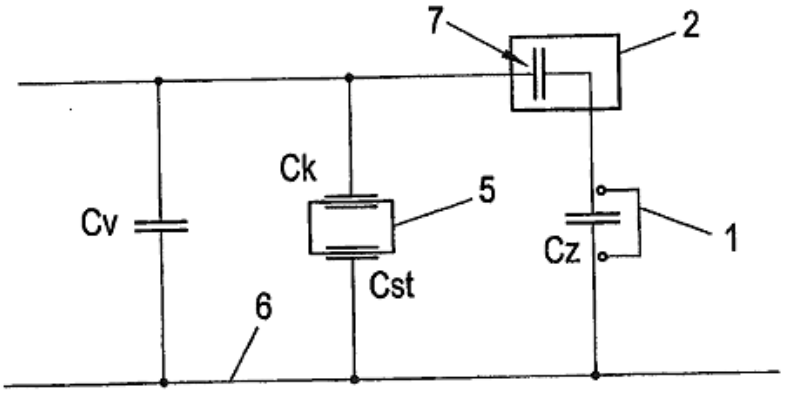

Fig. 2

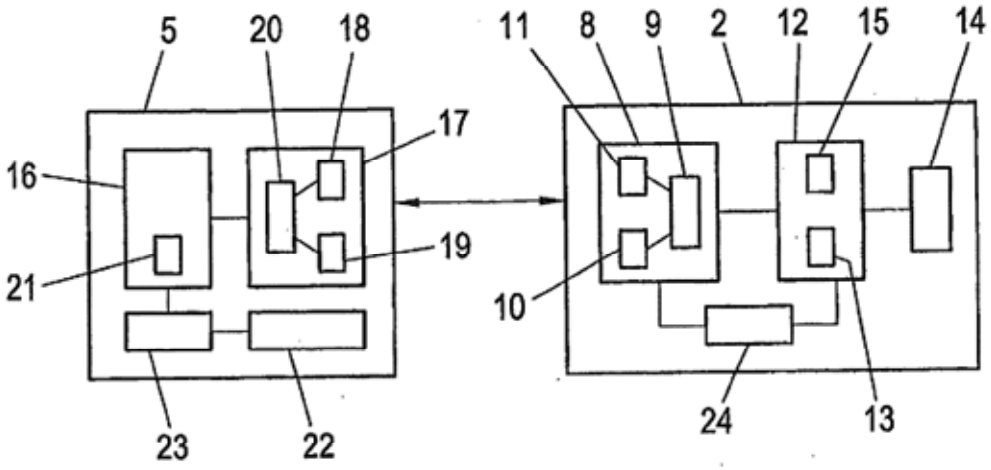
5
20
18
11
8
9
2
12
15
14
17
16
19
21
10
24
13
23
22

Fig. 3

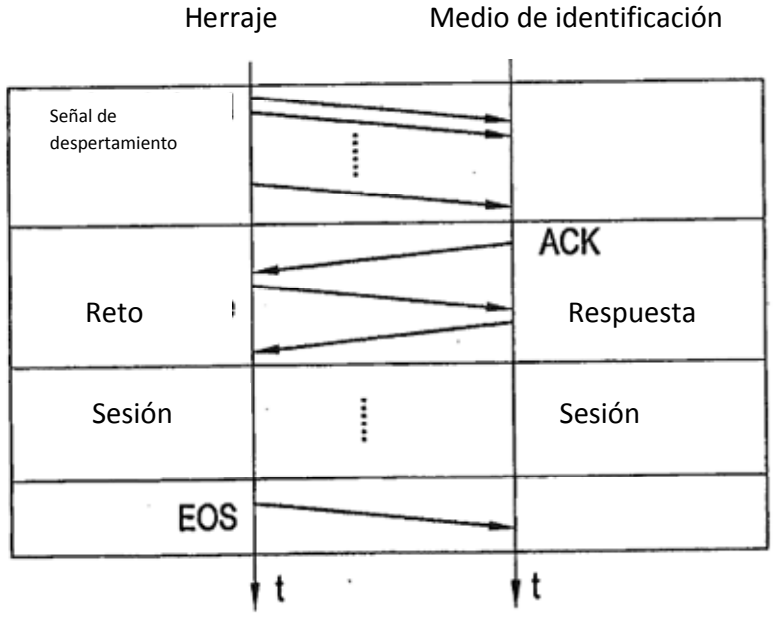
Herraje
Medio de identificación
Señal de despertamiento
ACK
Reto
Respuesta
Sesión
Sesión
EOS
t
t

Fig. 4