(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 638 410**

(51) Int. CI.:

G07B 15/00 (2011.01)
G07C 9/00 (2006.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.12.2015 E 15198211 (3)**

(97) Fecha y número de publicación de la concesión europea: **14.06.2017 EP 3040947**

(54) Título: **Métodos para la prevención de abuso de autorizaciones de acceso de un sistema de control de acceso basado en un identificador**

(30) Prioridad:

11.12.2014 DE 102014118388

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.10.2017

(73) Titular/es:

SKIDATA AG (100.0%)
Untersbergstrasse 40
5083 Grödig/Salzburg, AT

(72) Inventor/es:

DR. KERSCHBAUMER, ANDREAS

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Métodos para la prevención de abuso de autorizaciones de acceso de un sistema de control de acceso basado en un identificador

[0001] La presente invención se refiere a un método para la prevención de abuso de autorizaciones de acceso de un sistema de control de acceso basado en un identificador.

[0002] Sistemas de control de acceso basado en un identificador utilizan un soporte de cliente, donde el identificador de un soporte de cliente mediante los dispositivos de control de acceso del sistema de control de acceso es leído y transmitido a un servidor central, que mediante el identificador concede o rehúsa el acceso sobre el dispositivo de control de acceso que transmite el identificador.
El soporte de cliente puede por ejemplo ser realizado como día de identificación por radiofrecuencia, tarjeta de identificación por radiofrecuencia o ticket de papel con informaciones legibles por máquina.

[0003] Sistemas de control de acceso basados en identificador presentan, al contrario de los llamados sistemas de control de acceso basados en soporte, en los que el acceso mediante las informaciones depositadas en un soporte de cliente se conceden o se rehúsan, sin contactar un servidor central, la ventaja de que se garantiza una flexibilidad y escala alta.
Un identificador de un soporte de cliente puede asignar varios tipos de autorizaciones de acceso, por ejemplo para zonas diversas y horarios diversos y gestores diversos, lo que es particularmente ventajoso en estaciones de esquí.

[0004] Los soportes de cliente utilizados pueden sin embargo ser abusados, en cuanto que son por ejemplo copiados y usados.
Esto resulta por un lado en pérdidas de ventas para el gestor de los sistemas de control de acceso y por otra parte, para el caso de un escenario de postpago, en una cuenta demasiado alta para la persona que posee el soporte de cliente conforme a la ley.
Además puede también añadirse en el abuso de un soporte de cliente, que el acceso para el propietario legal del soporte de cliente sea rehusado al utilizar el soporte de cliente original.

[0005] Cuando por ejemplo sean usados como soportes de cliente días de identificación por radiofrecuencia estándar, éstos pueden ser programados libremente, de modo que es posible un abuso sin más.
Además para el caso de tickets de código de barras puede ser copiado un ticket de código de barras sin más.

[0006] La publicación WO 2014/012998 A1, del 23.01.2014, describe un método para la prevención de abuso de autorizaciones de acceso de un sistema de detección de acceso basado en un identificador, particularmente un procedimiento de gestión de tiempo de aparcamiento y pago para vehículos automóviles, incluyendo al menos un dispositivo de detección de acceso y un servidor central, con el que sea conectable al menos un dispositivo de detección de acceso con el objetivo de la comunicación de datos, donde una base de datos del servidor central puede contener un identificador del soporte de cliente, donde cuando el coche es aparcado, o cuando el coche es puesto en marcha, antes de que se marche, se puede enviar un aviso al propietario del soporte de cliente, con el requerimiento para permitir el pago de la tarifa de aparcamiento mediante la introducción del código PIN de su tarjeta de pago, donde hasta que no es enviada ninguna concesión de parte del usuario legal al sistema de detección de acceso, un abandono del campo cubierto por el sistema de detección de acceso puede ser rehusado.
La presente invención tiene el objeto de indicar un método para la prevención de abuso de autorizaciones de acceso en un sistema de control de acceso basado en un identificador.

[0007] Esta tarea es resuelta mediante las características de la reivindicación 1.
Otras configuraciones y ventajas según la invención se deducen de las reivindicaciones secundarias.

[0008] Se propone un método para la prevención de abuso de autorizaciones de acceso de un sistema de control de acceso basado en un identificador, incluyendo al menos un dispositivo de control de acceso y un servidor central, con el que es conectable al menos un dispositivo de control de acceso con el objetivo de la comunicación de datos, en cuyo marco en una base de datos del servidor central se deposita un conjunto de datos por soporte de cliente, que contiene al menos una dirección de contacto del propietario legal del soporte de cliente y al menos un identificador del soporte de cliente.
Al menos una dirección de contacto del propietario legal se puede indicar en la compra de la autorización de acceso, por ejemplo sobre una transacción en línea.

[0009] Según la invención se concede con la primera interacción entre un soporte de cliente y un dispositivo de control de acceso del sistema de control de acceso con autorización de acceso válida del acceso, donde simultáneamente o dentro de un lapsus de tiempo prefijado configurable después de la interacción mediante el conjunto de datos depositado en el servidor central y el identificador leído del soporte de cliente, al que está asociada la autorización de acceso, un aviso es enviado a una dirección de contacto del propietario legal del

soporte de cliente, con el requerimiento de confirmación, que la utilización actual del soporte de cliente está efectuada por él.

[0010] Hasta que no es enviada una confirmación de parte del propietario legal a una dirección de contacto prefijada del sistema de control de acceso, es rehusada otra entrada sobre los dispositivos de control de acceso del sistema de control de acceso, donde para el caso de un escenario de postpago un abandono del campo cubierto por el sistema de control de acceso es rehusado.

[0011] Sistemas de control de acceso con un escenario de postpago de acuerdo a la invención son sistemas de control de acceso, en los que para el abandono del campo cubierto del sistema de control de acceso deben pagarse las tasas correspondientes, para poder abandonar el campo.

[0012] Con la primera interacción entre el soporte de cliente y un dispositivo de control de acceso del sistema de control de acceso el identificador del soporte de cliente, al que está asociada la autorización de acceso, es leído y transmitido al servidor central, donde por un lado la autorización de acceso se comprueba sobre su validez y por otro lado con autorización de acceso válida se envía el aviso al usuario legal mediante el conjunto de datos depositado en la base de datos en el servidor central.

[0013] El tipo del aviso, que se envía del sistema de control de acceso al propietario legal del soporte de cliente, depende del tipo de dirección de contacto, que está depositada en el conjunto de datos correspondiente.
El aviso puede ser por ejemplo un E-Mail, un SMS o una dirección de contacto asignada de una App en un aparato móvil del usuario.

[0014] La confirmación necesaria de parte del usuario es enviada conforme a ello como SMS, E-mail o notificación de App a una dirección de contacto prefijada del sistema de control de acceso.

[0015] Hasta que el propietario legal del soporte de cliente no transmita la confirmación necesaria, se bloquean la autorización de acceso, el identificador del soporte de cliente, al que está asociada la autorización de acceso, todos los identificadores del soporte de cliente, en caso de que existan varios, o todos los identificadores del propietario legal.
Esto se realiza a través de la colocación de un indicador correspondiente en la base de datos del servidor central del sistema de control de acceso.
Cuando el propietario legal transmite la confirmación y ésta se recibe, es suprimido este indicador, donde con cada nueva interacción dentro del sistema de control de acceso entre el soporte de cliente y los dispositivos de control de acceso para un tiempo prefijado o para un número prefijado en interacciones entre el soporte de cliente y uno de los dispositivos de control de acceso del sistema de control de acceso se realiza una comprobación normal sin el envío del aviso con el requerimiento de confirmación.

[0016] En el marco de un perfeccionamiento de la invención se puede dividir el campo cubierto del sistema de control de acceso en campos parciales, donde el método según la invención con cada primera interacción entre un dispositivo de control de acceso y un soporte de cliente es llevado a cabo en los campos parciales respectivos.
Por ejemplo puede ser evitado así un abuso de un soporte de cliente para el acceso a los ascensores, para la entrada a un aparcamiento y para el acceso a una zona de wellness de una estación de esquí.

[0017] En el marco de un perfeccionamiento de la invención se puede prever, que para el caso de un sistema de control de acceso de un aparcamiento una confirmación es necesaria con cada entrada, independientemente de si una entrada previamente realizada por el propietario legal del soporte de cliente ha sido confirmada.

[0018] Según la invención para el caso de un sistema de control de acceso con un escenario de postpago puede producir la recepción de la confirmación del usuario legal opcional un proceso de pago correspondiente sobre datos de tarjeta de crédito o de cuenta archivados en el servidor central o que debe introducir el usuario, por lo cual de una manera ventajosa se puede implementar un sistema de pago por uso.
Por ejemplo un esquiador no necesita comprar ningún pase de esquí para un día de antemano, sino que puede comprar éste después de la primera interacción con un dispositivo de control de acceso de la estación de esquí.

[0019] Preferiblemente los avisos del sistema de control de acceso son enviados a aparatos móviles, por ejemplo a teléfonos móviles del usuario legal.

[0020] La invención se explica a continuación más en detalle a modo de ejemplo mediante la figura incluida.

[0021] Al principio del procedimiento según la invención con la primera interacción entre un soporte de cliente y un dispositivo de control de acceso 1 se lee el identificador del soporte de cliente y se transmite al servidor central 2 (pasos 1,2), donde en el servidor central 2 se comprueba la validez de la autorización de acceso y con autorización de acceso válida se memorizan los datos de transacción (paso 3) y en el dispositivo de control de acceso 1 se transmite la información "conceder acceso", donde a continuación un órgano de retención del

dispositivo de control de acceso se acciona en la dirección de apertura (paso 5).

[0022] Simultáneamente o dentro de un lapsus de tiempo prefijado configurable en el ejemplo mostrado en una base de datos del servidor central 2 se bloquea el identificador del soporte de cliente, al que está asociada la autorización de acceso, lo que se realiza a través de la colocación de un indicador correspondiente (paso 6) y es enviado un aviso del servidor central 2 a un teléfono móvil 3 del propietario legal, por ejemplo por SMS, con el requerimiento de confirmación, que se realiza a través de él la utilización actual del soporte de cliente (paso 7).

[0023] Hasta que no es enviada ninguna confirmación de parte del usuario legal al sistema de control de acceso, es rehusada otra entrada sobre un dispositivo de control de acceso 1' del sistema de control de acceso (pasos 8, 9, 10,11).
Con esta interacción se lee el identificador del soporte de cliente y se transmite al servidor central 2 (pasos 8,9), a lo cual en el servidor central 2 se determina, si el identificador del soporte de cliente, al que está asociada la autorización de acceso, debido a una confirmación todavía pendiente es bloqueado (paso 10).
Si éste es el caso, entonces la información "conceder acceso" es transmitida al dispositivo de control de acceso (paso 11).

[0024] Cuando la confirmación necesaria del propietario legal del soporte de cliente ha sido recibida por el sistema de control de acceso (paso 12), es revocado el bloqueo del identificador en el servidor central 2 mediante la cancelación del indicador (paso 13), de modo que con una próxima interacción entre el soporte del cliente y un dispositivo de control de acceso 1' del sistema de control de acceso (pasos 14,15) y evaluación correspondiente del identificador en el servidor central 2 (paso 16) se transmite la información "conceder acceso" al dispositivo de control de acceso 1' (paso 17).

REIVINDICACIONES

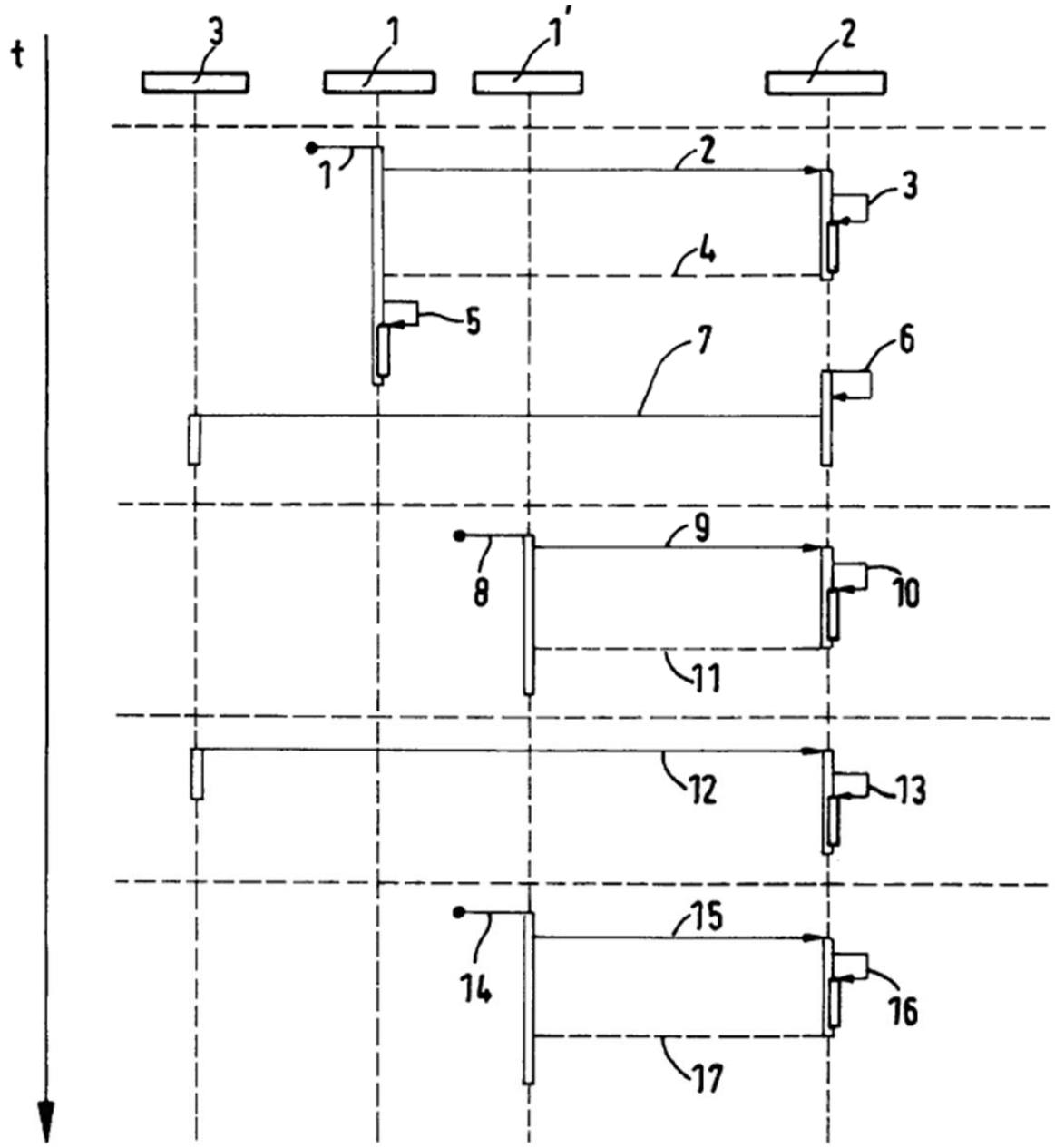
1. Método para la prevención de abuso de autorizaciones de acceso de un sistema de control de acceso basado en un identificador, incluyendo al menos un dispositivo de control de acceso (1,1') y un servidor central (2), con el que al menos un dispositivo de control de acceso (1,1') es conectable para el objetivo de la comunicación de datos, **caracterizado por el hecho de que** se deposita en una base de datos del servidor central (2) un conjunto de datos por soporte de cliente, que contiene al menos una dirección de contacto del propietario legal del soporte de cliente y al menos un identificador del soporte de cliente, donde con la primera interacción entre un soporte de cliente y un dispositivo de control de acceso (1,1') del sistema de control de acceso con autorización de acceso válida se concede el acceso y simultáneamente o dentro de un lapsus de tiempo prefijado configurable después de la interacción mediante el conjunto de datos depositado en el servidor central (2) y el identificador leído del soporte de cliente, al que está asociada la autorización de acceso, se envía un aviso a una dirección de contacto del propietario legal del soporte de cliente, con el requerimiento de confirmación que es realizada por él la utilización actual del soporte de cliente, donde hasta que no es enviada ninguna confirmación de parte del usuario legal a una dirección de contacto prefijada del sistema de control de acceso, otra entrada sobre los dispositivos de control de acceso (1,1') del sistema de control de acceso y para el caso de unos escenarios de postpago un abandono del campo cubierto por el sistema de control de acceso es rehusado.

2. Método para la prevención de abuso de autorizaciones de acceso de un sistema de control de acceso basado en un identificador, según la reivindicación 1, **caracterizado por el hecho de que** con la primera interacción entre el soporte de cliente y un dispositivo de control de acceso (1,1') del sistema de control de acceso el identificador del soporte de cliente, al que está asociada la autorización de acceso, es leído y enviado al servidor central (2), donde por un lado la validez de la autorización de acceso se comprueba y, por otro, con autorización de acceso válida se envía el aviso al usuario legal mediante el conjunto de datos depositado en la base de datos en el servidor central (2), donde hasta que el propietario legal del soporte de cliente no transmite la confirmación necesaria, se bloquean la autorización de acceso, el identificador del soporte de cliente, al que está asociada la autorización de acceso, todos los identificadores del soporte de cliente, en caso de que existan varios, o todos los identificadores del propietario legal, lo que se realiza a través de la colocación de un indicador correspondiente en la base de datos del servidor central (2), donde cuando el propietario legal envía la confirmación y ésta es recibida, el indicador es suprimido y donde con cada nueva interacción dentro del sistema de control de acceso entre el soporte de cliente y los dispositivos de control de acceso (1,1') para un tiempo prefijado o para un número prefijado en interacciones se realiza una comprobación normal de la autorización de acceso sin el envío del aviso con el requerimiento de confirmación.

3. Método para la prevención de abuso de autorizaciones de acceso de un sistema de control de acceso basado en un identificador, según la reivindicación 1 o 2, **caracterizado por el hecho de que** el campo cubierto por el sistema de control de acceso se divide en campos parciales, donde el método con cada primera interacción entre un dispositivo de control de acceso (1,1') y un soporte de cliente es llevado a cabo en los campos parciales respectivos.

4. Método para la prevención de abuso de autorizaciones de acceso de un sistema de control de acceso basado en un identificador, según una de las reivindicaciones precedentes, **caracterizado por el hecho de que** para el caso de un sistema de control de acceso de un aparcamiento una confirmación es necesaria con cada entrada, independientemente de si una entrada previamente realizada por el propietario legal del soporte de cliente ha sido confirmada.

5. Método para la prevención de abuso de autorizaciones de acceso de un sistema de control de acceso basado en un identificador, según una de las reivindicaciones precedentes, **caracterizado por el hecho de que** para el caso de un sistema de control de acceso con un escenario de postpago la recepción de la confirmación del usuario legal origina un proceso de pago correspondiente sobre datos de tarjeta de crédito o de cuenta archivados en el servidor central (2) o que debe introducir el usuario.



Figura