(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 323 213**

(21) Número de solicitud: 200702697

(51) Int. Cl.:
G07C 9/00 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación: **03.10.2007**

(43) Fecha de publicación de la solicitud: **08.07.2009**

Fecha de la concesión: **03.03.2010**

(45) Fecha de anuncio de la concesión: **16.03.2010**

(45) Fecha de publicación del folleto de la patente: **16.03.2010**

(73) Titular/es: **TALLERES DE ESCORIAZA S.A.**
Barrio Ventas, 35
20305 Irún, Guipúzcoa, ES

(72) Inventor/es: **Vila Errandonea, Julia y**
Francés Pedraz, Mercedes

(74) Agente: **Izquierdo Faces, José**

(54) Título: **Sistema electrónico programable de control de accesos.**

(57) Resumen:
Sistema electrónico programable de control de accesos, que comprende una unidad actualizadora (1) en conjunción con una unidad central de control (2), provista de software de gestión de control global de los accesos de instalación con unos elementos de acceso (3) asociados a las vías de entrada / salida y una credencial (4) asociada a cada usuario del sistema, cuya unidad actualizadora (1) tiene medios de transferencia de datos en ambos sentidos tanto con las credenciales de usuario (4), como con la unidad central de control (2); la unidad actualizadora (1) transfiere a las credenciales de usuario (4) exclusivamente la información concerniente a dicho usuario y al plan de cierre de la instalación al tiempo que la unidad actualizadora (1) recibe de cada credencial de usuario (4) la información almacenada relativa a los eventos ocurridos con ella que han sido transferidos en cada uno de los elementos de acceso (3).

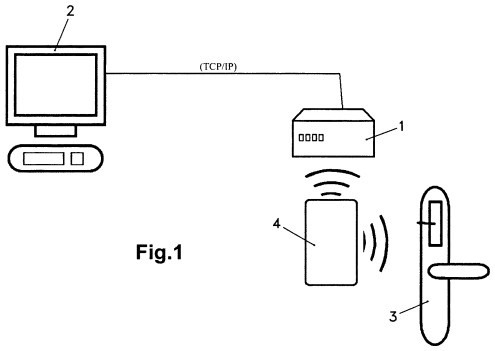

Fig.1

ES 2 323 213 B1

DESCRIPCIÓN

Sistema electrónico programable de control de accesos.

Campo de la invención

Esta invención concierne a un sistema para el control de accesos a una instalación, el cual está basado en tecnología electrónica, admite diversos soportes de acreditación de usuario y está gestionado mediante un programa informático.

Estado de la técnica anterior

Un sistema de control de accesos convencional comprende una unidad central de control, una serie de elementos de acceso y unas credenciales de acceso.

En la unidad central de control está instalada una aplicación de software o programa informático que gestiona el control de accesos global de la instalación, es decir, define los usuarios de la instalación, las diferentes vías de acceso de la instalación, las diferentes zonas horarias e interrelaciona todas estas variables definiendo lo que se denomina el plan de cierre de la instalación.

Los elementos de acceso están asociados a las vías de entrada/salida de la instalación para gestionar el acceso concreto a través de cada una de ellas; estos elementos de acceso pueden ser de distinto tipo, por ejemplo, cerraduras, lectores murales, u otros capaces de asumir tal función.

Las credenciales de acceso están asociadas individualmente a cada usuario y admiten soportes de diversa naturaleza (tarjeta, llave, etc.). La función de estas credenciales es ser presentadas al elemento de acceso para, en el caso de que el usuario portador esté incluido en el plan de cierre permitido, le sea autorizado el acceso a la instalación.

En este campo existen sistemas de control denominados “off line” debido a que no existe una conexión entre la unidad central de control y el elemento de acceso. En este tipo de sistemas es necesario disponer un elemento externo que ejerce la función de programador portátil para configurar el elemento de acceso según los datos programados en el plan de cierre, así como para recoger los eventos almacenados en dicho elemento de acceso. Esto conlleva que cualquier intercambio de información entre las acciones realizadas en la cerradura (por ejemplo, aperturas de diferentes usuarios realizadas a diferentes horas, o estado de las baterías que equipan dichos productos) necesita ser volcado en la unidad central de control mediante este citado programador portátil que constituye un accesorio de almacenamiento masivo de datos. Esto supone un inconveniente en el caso de grandes instalaciones en las que es necesario recorrer todas las vías de acceso con el programador portátil para mantener la instalación actualizada y monitorizar los eventos; lo que de paso significa que la instalación sólo estará actualizada inmediatamente después de cada ronda de actualización, pero no en los intervalos entre dos rondas sucesivas. Por otro lado, la actualización por rondas viene a requerir que en las credenciales de usuario sea almacenada una gran cantidad de información, ya que ésta no es actualizada en el momento de producirse los distintos eventos resultantes del uso del sistema por los múltiples usuarios.

Otro inconveniente de los sistemas de control “off line” es que la invalidación de una credencial antes de la fecha de caducidad establecida en el momento de su emisión está sujeta a que sea realizada una ronda de actualización; de modo que una credencial extraviada podrá ser usada entretanto, lo que representa un fallo de seguridad importante.

Explicación de la invención y ventajas

El sistema de control de accesos que ahora se propone se deriva de la reflexión sobre las posibilidades de la tecnología actual al respecto. Así, resulta que las tecnologías actuales permiten dotar a las credenciales de usuario cada vez de más información y gestionar ésta con mayor flexibilidad. Sea cual fuera la tecnología empleada de comunicación entre la credencial soporte y el elemento de acceso; como proximidad RFID (identificación por radiofrecuencia), chip de contacto, etc. Resulta posible hoy en día almacenar de una manera segura a través de potentes sistemas de encriptación cierto nivel de información y compartirla con los sistemas periféricos de manera biunívoca mediante comunicación bidireccional.

Aplicado esto a sistemas de control de accesos, resulta que, desarrollando elementos de gestión adecuados y adaptando la gestión de comunicación de los diferentes sistemas, es posible traspasar la información necesaria desde la unidad central de control a la credencial de usuario, almacenar dicha información en la credencial y traspasarla finalmente al elemento de acceso. Del mismo modo, sería posible traspasar también información desde el elemento de acceso a la credencial de usuario, almacenar dicha información en la credencial y enviarla finalmente a la unidad central de control para su procesamiento. En tanto en cuanto la aplicación es para controles de acceso, todo este trasvase y almacenamiento de información ha de hacerse garantizando una total seguridad y fiabilidad.

Pues bien, teniendo en cuenta lo anterior, el sistema que al respecto propugna la presente invención consiste en que comprende una unidad actualizadora que opera en conjunción con una unidad central de control, provista del software de gestión del control global de los accesos de la instalación, y con unos elementos de acceso asociados a las vías de entrada/salida para gestionar el acceso por las mismas, y con una credencial asociada a cada usuario del sistema, cuya

unidad actualizadora tiene medios de transferencia de datos en ambos sentidos tanto con las credenciales de usuario, como con la unidad central de control.

Otra particularidad de la invención consiste en que la unidad actualizadora transfiere a las credenciales de usuario exclusivamente la información concerniente a dicho usuario, al tiempo que la unidad actualizadora recibe de cada credencial de usuario la información almacenada en la misma relativa a los eventos ocurridos con ella en cada uno de los elementos de acceso.

Otra particularidad de la invención es que, además de la información de caducidad asociada a cada credencial de usuario, la unidad actualizadora transfiere a las credenciales de usuario también un parámetro configurable de invalidación temporal comprendida en el período de caducidad de las mismas.

Otra particularidad de la invención es que la unidad actualizadora transfiere a la unidad central de control la información tomada de las credenciales de usuario, a la vez que recibe la información relativa al plan programado de control de cierre de los accesos de la instalación vigente en cada momento.

Otra particularidad de la invención es que una unidad actualizadora estará asociada a, al menos, las vías principales de acceso, en conjunción con un programa de la unidad central de control que exige que las credenciales de usuario sean presentadas en la unidad actualizadora antes que en el elemento de acceso relativo a esa vía de acceso.

De acuerdo con esta constitución del sistema propugnado se cumple lo siguiente.

Mediante una conexión en red a la unidad central de control en la que se establecen los parámetros y se gestiona el plan de cierre de una instalación, la unidad actualizadora se encarga de manera bidireccional de comunicar la información requerida con la credencial de usuario. La unidad actualizadora identifica la credencial de usuario y almacena en ella la información correspondiente al plan de cierre de dicho usuario. Por su parte, la información previamente almacenada en la credencial de usuario que recoge los eventos ocurridos en cada uno de los elementos de acceso, es transferida desde la credencial al actualizador y desde aquí a la unidad central de control para su procesamiento.

Cada vez que un usuario accede a una vía de acceso y presenta su credencial al elemento de acceso, una vez reconocido el usuario dentro del plan de cierre, traspasa la información de la credencial al elemento de acceso de manera que actualiza su plan de cierre si es necesario. A su vez, la información almacenada en el elemento de acceso (recogida de eventos o acontecimientos) es transferida a la credencial de usuario y almacenada, y además abre o rechaza.

Así, cuando un usuario presenta su credencial en el actualizador la información de la instalación se actualiza (tanto el plan de cierre como el estado de los diferentes elementos de la instalación), liberándose de la memoria de la credencial.

Con objeto de garantizar que la información de la instalación esté permanentemente actualizada, es necesario asegurar que las credenciales de usuario se presenten en el actualizador. Para ello, se asocia al actualizador un control de puerta, generalmente vinculado a las vías de acceso principales, de manera que sea necesario presentar la credencial de usuario en dicho actualizador para poder acceder a la instalación. Así, si el usuario está dentro del plan de cierre de dicha instalación y automáticamente habrá actualizado el sistema.

Hay otra función asociada al actualizador para garantizar que todo usuario presente su credencial y actualice así la información: la revalidación. Además de la información de caducidad asociada a toda credencial, existe un parámetro configurable por el actualizador que obliga a un usuario a presentar su credencial cada cierto tiempo. De no ser así dicha credencial quedaría invalidada dentro de la instalación hasta que se presente en el actualizador.

Esta funcionalidad de la invención conlleva, entre otras, las siguientes ventajas:

En cada una de las credenciales de usuario se almacena únicamente la información asociada a dicho usuario, frente a otras técnicas que necesitan almacenar una mayor cantidad de información para cubrir el control de acceso. Ello implica que el espacio de memoria restante para almacenar eventos o cambios de plan de cierre es más óptimo en la presente invención. Además, para un mismo número de eventos recogidos, tanto el tiempo de transacción como el consumo de baterías es menor en el sistema actual en tanto en cuanto la cantidad de información almacenada es menor para cubrir la misma funcionalidad.

La función de revalidación, además de garantizar que todo usuario presente su credencial en el actualizador y se actualice automáticamente la información de la instalación, garantiza la invalidez de una credencial si ha sido extraviada. En otros sistemas una tarjeta extraviada o robada pudiera seguir utilizándose en una instalación con la consiguiente vulnerabilidad del sistema, mientras que mediante la presente invención, toda vez que una credencial ha sido extraviada, no puede ser utilizada en la instalación mientras no se revalide en el actualizador. En ese momento el sistema de gestión automáticamente anularía la credencial, toda vez que ha sido dada de baja de la instalación.

Respecto a la Patente ES 2,183,739, con el sistema propuesto basta grabar la credencial nueva para que sea factible abrir la cerradura correspondiente a la que se le ha dado acceso en el sistema directamente sin necesidad de recurrir al programador portátil.

Otra ventaja concerniente al sistema propuesto se basa en que en la credencial considerada se puede incluir los datos concernientes a otra credencial cuyo plan de cierre se quiere modificar, borrar o añadir.

Dibujos y referencias

Para comprender mejor la naturaleza del invento, en los dibujos adjuntos se representa una forma de realización que tiene carácter de ejemplo meramente ilustrativo y no limitativo.

La figura 1 es una representación esquemática del sistema de control de accesos, de la invención.

En estas figuras están indicadas las siguientes referencias:

1.- Unidad actualizadora

2.- Unidad central de control

3.- Elemento de acceso

4.- Credencial de usuario

Exposición de una realización preferente

Con relación a los dibujos y referencias arriba enumerados, se ilustra en los planos adjuntos un modo de ejecución preferente del objeto de la invención, referida a un sistema electrónico programable de control de accesos que comprende una unidad actualizadora (1) que opera en conjunción con una unidad central de control (2), provista del software de gestión del control global de los accesos de la instalación, y con unos elementos de acceso (3) asociados a las vías de entrada/salida para gestionar el acceso por las mismas, y con una credencial (4) asociada a cada usuario del sistema, cuya unidad actualizadora (1) tiene medios de transferencia de datos en ambos sentidos tanto con las credenciales de usuario (4), como con la unidad central de control (2). Los elementos de acceso (3) y la credenciales de usuario (4) pueden ser de tecnologías diversas; en el primer caso, puede tratarse de cerraduras, lectores murales, etc.; en el segundo caso, de tarjetas, llaves, etc..

El esquema de la figura 1 es ilustrativo de esta constitución del sistema preconizado, se cumplen también las particularidades siguientes: que la unidad actualizadora (1) transfiere a las credenciales de usuario (4) exclusivamente la información concerniente a dicho usuario, al tiempo que la unidad actualizadora (1) recibe de cada credencial de usuario (4) la información almacenada en la misma relativa a los eventos ocurridos con ella en cada uno de los elementos de acceso (3); que, además de la información de caducidad asociada a cada credencial de usuario (4), la unidad actualizadora (1) transfiere a las credenciales de usuario (4) también un parámetro configurable de invalidación temporal comprendida en el período de caducidad de las mismas; que la unidad actualizadora (1) transfiere a la unidad central de control (2) la información tomada de las credenciales de usuario (4), a la vez que recibe la información relativa al plan programado de control de cierre de los accesos de la instalación vigente en cada momento; y que una unidad actualizadora (1) estará asociada a, al menos, las vías principales de acceso, en conjunción con un programa de la unidad central de control (2) que exige que las credenciales de usuario (4) sean presentadas en la unidad actualizadora (1) antes que en el elemento de acceso (3) relativo a esa vía de acceso.

En definitiva, a través del esquema de la figura 1, se ilustra el funcionamiento antes expuesto, con las ventajas también dichas de él desprendidas Mediante una conexión en red a la unidad central de control (2) en la que se establecen los parámetros y se gestiona el plan de cierre de una instalación, la unidad actualizadora (1) se encarga de modo bidireccional de comunicar la información requerida con la credencial de usuario (4); de modo que la unidad actualizadora (1) identifica la credencial de usuario (4) y almacena en ella la información correspondiente al plan de cierre de dicho usuario, al tiempo que recibe la información previamente almacenada en la credencial de usuario (4), donde han ido siendo recogidos los eventos ocurridos en cada uno de los elementos de acceso (3), información ésta que es transferida desde la credencial de usuario (4) a la unidad actualizadora (1) y desde aquí a la unidad central de control (2) para ser procesada.

Cuando un usuario accede a una vía de acceso y presenta su credencial de usuario (4) al elemento de acceso (3), una vez reconocido el usuario dentro del plan de cierre, la información de la credencial de usuario (4) es traspasada al elemento de acceso (3), de manera que, si es necesario, en ésta es actualizado su plan de cierre. A su vez, la información almacenada en el elemento de acceso (3) (recogida de aperturas o estados internos del elemento de acceso) es transferida a la credencial de usuario (4) y almacenada en la misma.

Cuando una credencial de usuario (4) es presentada en la unidad actualizadora (1), la información relativa a la instalación se actualiza (tanto el plan de cierre como el estado de los diferentes elementos de la instalación), liberándose de la memoria de la credencial de usuario (4).

Para garantizar que la información de la instalación esté permanentemente actualizada, es necesario asegurar que las credenciales de usuario (4) sean presentadas en la unidad actualizadora (1). Para ello, a la unidad actualizadora (1) se le asocia un control de puerta, generalmente vinculado a las vías de acceso principales, de manera que sea

necesario presentar la credencial de usuario (4) en dicha unidad actualizadora (1) para poder acceder a la instalación. Así, si el usuario está dentro del plan de cierre de dicha instalación, tendrá acceso permitido y automáticamente habrá actualizado el sistema.

La unidad actualizadora (1) dispone de una función para garantizar que todo usuario presente su credencial de usuario (4) y actualice así la información: es la función llamada revalidación. Además de la información de caducidad asociada a toda credencial de usuario (4), existe un parámetro configurable por la unidad actualizadora(1) que obliga a un usuario a presentar su credencial de usuario (4) cada cierto tiempo. De no ser así, dicha credencial de usuario (4) quedaría invalidada dentro de la instalación hasta que sea presentada en la unidad actualizadora (1).

Esta funcionalidad de la invención conlleva, entre otras, las siguientes ventajas:

En cada una de las credenciales de usuario se almacena únicamente la información asociada a dicho usuario, frente a otras técnicas que necesitan almacenar una mayor cantidad de información para cubrir el control de acceso.

El espacio de memoria restante para almacenar eventos o cambios de plan de cierre es mayor en la presente invención.

Para un mismo número de eventos recogidos, tanto el tiempo de transacción como el consumo de baterías es menor en el sistema actual en tanto en cuanto la cantidad de información almacenada es menor para cubrir la misma funcionalidad.

La función de revalidación, además de garantizar que todo usuario presente su credencial en el actualizador y se actualice automáticamente la información de la instalación, garantiza la invalidez de una credencial si ha sido extraviada; de modo que, una credencial extraviada no puede ser utilizada en la instalación mientras no se revalide en el actualizador, es decir que el sistema de gestión automáticamente anularía la credencial, toda vez que ha sido dada de baja de la instalación.

Una unidad actualizadora (1) o un editor general de credenciales valida una nueva credencial (4) de uso temporal de forma que al ser interrelacionada con los elementos de acceso (3) validados en el sistema central (2), le permite el acceso a la misma sin necesidad de ser usado el programador portátil.

Asimismo una unidad actualizadora (1) o un editor general de credenciales permite la inserción de información relativa a la anulación de otra credencial (4) dentro del sistema al paso de su actualización por la unidad de control (2).

También una unidad actualizadora (1) o un editor general de credenciales permite la modificación de información relativa a otra credencial diferente correspondiente a los datos del plan de cierre.

REIVINDICACIONES

1. Sistema electrónico programable de control de accesos, **caracterizado** porque comprende una unidad actualizadora (1) que opera en conjunción con una unidad central de control (2), provista del software de gestión del control global de los accesos de la instalación, y con unos elementos de acceso (3) asociados a las vías de entrada/salida para gestionar el acceso por las mismas, y con una credencial (4) asociada a cada usuario del sistema, cuya unidad actualizadora (1) tiene medios de transferencia de datos en ambos sentidos tanto con las credenciales de usuario (4), como con la unidad central de control (2); la unidad actualizadora (1) transfiere a las credenciales de usuario (4) exclusivamente la información concerniente a dicho usuario y al plan de cierre de la instalación al tiempo que la unidad actualizadora (1) recibe de cada credencial de usuario (4) la información almacenada en la misma relativa a los eventos ocurridos con ella que han sido transferidos en cada uno de los elementos de acceso (3).

2. Sistema electrónico programable de control de accesos, de acuerdo con las anteriores reivindicaciones, **caracterizado** porque, además de la información de caducidad asociada a cada credencial de usuario (4), la unidad actualizadora (1) transfiere a las credenciales de usuario (4) también un parámetro configurable de invalidación temporal comprendida en el período de caducidad de las mismas.

3. Sistema electrónico programable de control de accesos, de acuerdo con las anteriores reivindicaciones, **caracterizado** porque la unidad actualizadora (1) transfiere a la unidad central de control (2) la información tomada de las credenciales de usuario (4), a la vez que recibe la información relativa al plan programado de control de cierre de los accesos de la instalación vigente en cada momento.

4. Sistema electrónico programable de control de accesos, de acuerdo con las anteriores reivindicaciones, **caracterizado** porque una unidad actualizadora (1) estará asociada a, al menos, las vías principales de acceso, en conjunción con un programa de la unidad central de control (2) que exige que las credenciales de usuario (4) sean presentadas en la unidad actualizadora (1) para validar su acceso correspondiente.

5. Sistema electrónico programable de control de accesos de acuerdo con las reivindicaciones anteriores, **caracterizado** porque una unidad actualizadora (1) o un editor general de credenciales valida una nueva credencial (4) de uso temporal de forma que al ser interrelacionada con los elementos de acceso (3) validados en el sistema central (2), le permite el acceso a la misma sin necesidad de ser usado el programador portátil.

6. Sistema electrónico programable de control de accesos de acuerdo con las reivindicaciones anteriores, **caracterizado** porque una unidad actualizadora (1) o un editor general de credenciales permite la inserción de información relativa a la anulación de otra credencial (4) dentro del sistema al paso de su actualización por la unidad de control (2).

7. Sistema electrónico programable de control de accesos de acuerdo con las reivindicaciones anteriores, **caracterizado** porque una unidad actualizadora (1) o un editor general de credenciales permite la modificación de información relativa a otra credencial diferente correspondiente a los datos del plan de cierre.

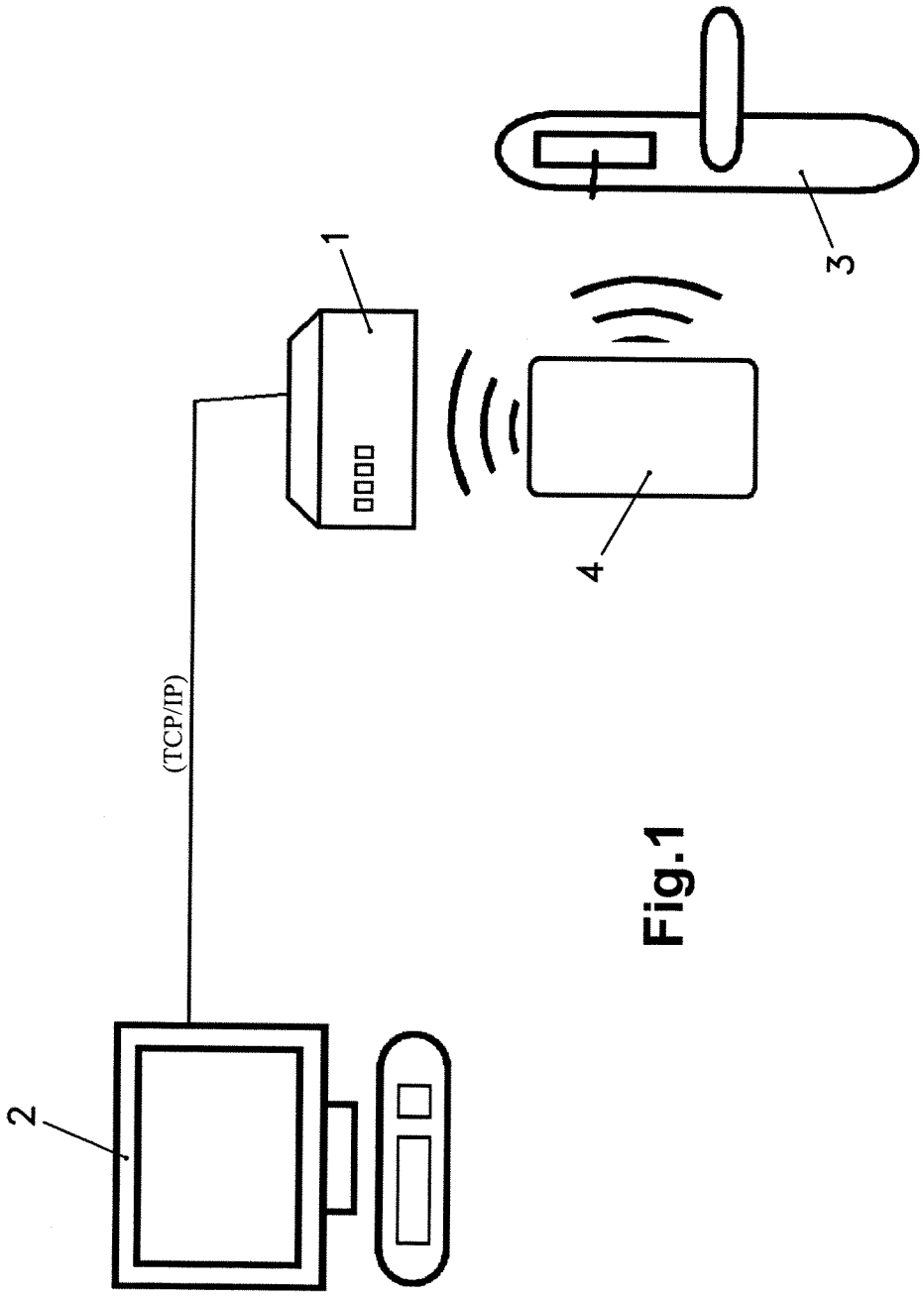

Fig.1

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 323 213

(21) Nº de solicitud: 200702697

(22) Fecha de presentación de la solicitud: **03.10.2007**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.:** ***G07C 9/00*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
X	ES 2253971 B1 (SALTO SYSTEMS) 01.06.2006, columna 2, línea 52 - columna 4, línea 56; columna 5, líneas 7-39; columna 6, líneas 15-35; columna 7, línea 22 - columna 8, línea 25; figura 1.	1-7

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
23.06.2009	M. Alvarez Moreno	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G07C

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

OPINIÓN ESCRITA

Nº de solicitud: 200702697

Fecha de Realización de la Opinión Escrita: 23.06.2009

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-7	**SÍ**
	Reivindicaciones		**NO**
Actividad inventiva	Reivindicaciones		**SÍ**
(Art. 8.1 LP 11/1986)	Reivindicaciones	1-7	**NO**

Se considera que la solicitud cumple con el requisito de **aplicación industrial.** Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión:

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como ha sido publicada.

1. Documentos considerados:

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	ES 2253971 B1	01.06.2006

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

El documento D01 muestra un sistema de control de acceso que, según puede verse en la descripción [col. 2, lin. 52 - col. 4, lin. 56; col.5, lin. 7-39; col. 6, lin. 15- 35; col. 7, lin. 22 - col. 8, lin. 25] dispone de:

1. Elementos de acceso con lectores de llave o tarjeta de usuario, los cuales incluyen capacidad de almacenamiento y un código de identificación. Estos lectores no se encuentran conectados al centro de control. La actualización de su información se realiza a través de la lectura de las distintas llaves.

2. Centro de control que almacena y gestiona, mediante un software apropiado de gestión, todos los datos de funcionamiento del sistema.

3. Llave o tarjeta de usuario: Las identificaciones de llave y de usuario son introducidas por medio del centro de control. En las diferentes áreas de memoria almacena:

- Operaciones permitidas de apertura (proporcionada por el centro de control)

- Histórico de aperturas realizadas (proporcionada por los elementos de acceso).- Esta información es transferida al centro de control y eliminada de la llave cada vez que se realiza una lectura desde el centro de control. - Listas negras de llaves o tarjetas (llaves invalidadas por algún motivo).- proporcionado a través del centro de control, permite que los elementos de acceso adquieran esta información cada vez que un usuario utiliza su llave.

- Identificación por código único de una pluralidad de elementos de acceso - Informaciones de horario y calendario de aperturas de los elementos de acceso.

4. Medio lector particular, denominado actualizador: tiene medios de comunicación con el centro de control y con las llaves; controla el acceso a una puerta y además puede actualizar los datos de las llaves. Vacía la memoria de las llaves y envía la información adquirida al centro de control.

Comparando con el sistema en estudio puede verse que, la reivindicación 1 identifica el sistema en función de sus elementos funcionales (unidad central de control, unidad actualizadora, elementos de acceso y credencial) y por la capacidad de comunicación de la unidad actualizadora con el centro de control y con las credenciales. El documento D01 muestra elementos funcionalmente equivalentes con las mismas capacidades, pudiendo derivarse de su lectura los elementos identificados en la reivindicación 1.

Respectos a las reivindicaciones dependientes 2 a 7, identifican características adicionales de la unidad actualizadora relacionadas con su capacidad de comunicación, como son transferir información de cualquier tipo a cada credencial (ej, caducidad o validez, anulación de otras credenciales...), transferir información hacia/desde la unidad de control, ubicación de dicha unidad en un elemento de acceso, validación de credenciales nuevas. Todas las anteriores características pueden derivarse directamente del documento D01.

Las reivindicaciones 1 a 7 carecen de actividad inventiva.