(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 166 321**

(21) Número de solicitud: 200000768

(51) Int. Cl.[7]: G07C 9/00
G07F 7/08
G07F 7/10
G08B 3/00
G06K 7/00

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación: **29.03.2000**

(43) Fecha de publicación de la solicitud: **01.04.2002**

(43) Fecha de publicación del folleto de la solicitud: **01.04.2002**

(71) Solicitante/s: **UNIVERSIDAD DE MURCIA**
Avda. Teniente Flomesta,
Ed. La Convalecencia
30003 Murcia, ES

(72) Inventor/es: **Tomás Balibrea, Luis Manuel;**
Roca Nieto, Lucas;
Artero Caballero, José Pascual;
Pizarro Méndez, José Ramón;
López Melero, Carlos Emilio;
Caballero Montesinos, Adolfo;
Gomariz Guillermo, Javier y
Fernández Sánchez, Joaquín

(74) Agente: **No consta**

(54) Título: **Sistema de control de accesos por tarjeta inteligente.**

(57) Resumen:
Sistema de control de accesos por tarjeta inteligente.
El sistema de control de accesos por tarjeta inteligente, de aplicación especial en el control de accesos de personas a edificios o instalaciones mediante el uso de elementos de comunicación por Internet, se constituye a partir de una placa microcontroladora (1) que dispone de medios de gestión y control de los elementos de la propia placa así como de comunicación tanto con los posibles usuarios del sistema como con los elementos de actuación del mismo, incorporando elementos de seguridad física y de comunicaciones, habiéndose previsto, además de su alimentación a red, incorporar un sistema de alimentación ininterrumpida.

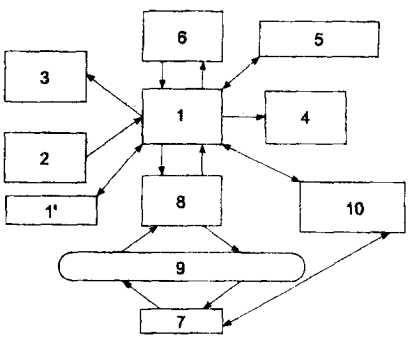

FIG. 1

ES 2 166 321 A1

DESCRIPCION

Sistema de control de accesos por tarjeta inteligente.

Objeto de la invención

La presente invención, tal como se expresa en el enunciado de esta memoria descriptiva, consiste en un sistema de control de accesos por tarjeta inteligente que tiene como objeto el control de acceso de personas a instalaciones, permitiendo de esta forma fijar restricciones de entrada a distintas zonas del edificio o instalaciones y un mayor seguimiento del personal que accede a él. De igual modo posibilita la generación de informes que permitan realizar un seguimiento horario de las entradas y salidas al puesto de trabajo realizadas por los usuarios del servicio.

La invención es principalmente aplicable a todo tipo de actividad donde es necesario limitar los accesos a personas no autorizadas, facilitando un registro y control de acceso de las mismas.

Antecedentes de la invención

Los controles de accesos pueden definirse como elementos diseñados para recoger información de un usuario y discriminar si se le otorga permiso para acceder a diferentes espacios.

Básicamente existen dos tipos de acceso: el acceso a servicios y el acceso a espacios reales. Dentro de los servicios, la extensión de las redes de comunicación ha derivado progresivamente de los controles de accesos a servicios a controles de accesos a espacios virtuales. La contraseña necesaria para acceder, desde un ordenador conectado a la red telefónica, a los datos de una red de estaciones meteorológicas podría ser un ejemplo de control de acceso que únicamente permitiese visualizar información sin excesivos cambios, este sistema podría considerarse en un control de acceso al espacio virtual formado por la imagen virtual de las estaciones reales.

La mayoría de los equipos comerciales de controles de accesos presentan una estructura claramente modular. Son elementos usualmente distinguibles los terminales de acceso, el sistema de decodificación de datos recogidos del usuario, el sistema de comprobación de éstos. El primero, componente visible del sistema, puede estar integrado desde por un simple teclado hasta por complejos sistemas de captura de imágenes. El sistema puede precisar que el usuario se detenga para introducir el código o permitir su paso sin necesidad de ningún tipo de interacción al ser capaz de captar la información del usuario a distancia. La parte que más variación experimenta, dependiendo del sistema e información utilizada, es la de identificación de códigos, siendo la encargada de transformar la información leída por el sistema de lectura procesándola hasta ser capaz de generar un código interpretable de forma simple por el resto del sistema. Dicho sistema puede ser prácticamente inexistente, como en el caso de códigos numéricos, o necesitar de complejos equipos electrónicos o informáticos si la información es muy compleja, como podría ser el caso de utilizar rasgos faciales humanos. En todos los casos, el sistema debe proporcionar al sistema de reconocimiento los datos necesarios para poder juzgar si el usuario debe ser o no aceptado.

Es ésta precisamente la función fundamental del sistema del nivel jerárquico más elevado de los que conforman el acceso: determinar a qué espacios tiene acceso el usuario y a qué nivel. El sistema podrá ofrecer a su vez información a otros sistemas de nivel jerárquico superior para que actúen consecuentemente según la información.

Debido al importante peso que tiene sobre el sistema los captadores o decodificadores, la principal clasificación entre diferentes tipos de acceso suele realizarse dependiendo del tipo de información que se capta en el lector.

Una tipología muy usada es la de los sistemas basados en claves o contraseñas memorizadas por el usuario, contraseñas que deberán ser introducidas en el terminal de entrada, normalmente constituido por un simple teclado. En la actualidad estos sistemas basados en contraseñas no constituyen por sí solos el único elemento de captación en prácticamente ningún sistema de control de accesos. Es común encontrarlos combinados junto con otros sistemas, como los basados en tarjetas magnéticas o de reconocimiento de voz, aumentándose, de esta manera la seguridad del sistema con un coste incremental relativamente bajo.

La mayoría de los sistemas captan la información a través de algún tipo de llave física; un dispositivo simple, pero de demostrada utilidad, lo constituyen las tradicionales llaves mecánicas de cerraduras. En este caso el decodificador es el sistema mecánico de la cerradura. Algunos de los inconvenientes de estos sistemas son, por una parte, la gran cantidad de llaves que el usuario se ve obligado a transportar, su incapacidad de comunicarse con otros sistemas y la posibilidad de que, en caso de pérdida otro usuario pueda suplantarle accediendo al sistema.

Sin embargo, son también llaves físicas aquellas llaves que contiene una información que deberá ser interpretada por un sistema electrónico de control. La solución clásica en lo que a formato de llave electrónica se refiere es la clásica tarjeta. Existen muchas modalidades, desde las tarjetas con código óptico hasta tarjetas de proximidad, pasando por las conocidas tarjetas con banda magnética o con circuitos integrados.

Para causar mayor sensación de confianza en el usuario existen formatos mixtos entre la llave tradicional y los diversos tipos de tarjetas. En éstos, un formato de cerradura clásico es modificado para poder transmitir la información de la llave clásica en un formato interpretable de mayor nivel.

Únicamente características que fueran propias e intransferibles del usuario permitirían realizar un control de accesos sin posibilidad de robo del código. Este hecho ha provocado un importante crecimiento de las aplicaciones biométricas en seguridad. Son aplicaciones biométricas las basadas en el análisis de características humanas únicas de cada persona.

Descripción de la invención

Todos los sistemas presentan una serie de problemas operativos solventados con esta nueva invención.

El primer inconveniente que presenta es la actualización del software que requiere un desplaza-

miento de personal autorizado a los equipos instalados. En el nuevo sistema no es necesario dicho desplazamiento, ya que el sistema incorpora la actualización del software mediante comunicación Ethernet o radiofrecuencia. Este procedimiento permite la distribución de equipos con total hermeticidad, aumentando así la seguridad de manipulación contra terceros.

Para el aumento de la seguridad y comodidad de los usuarios se incorporan distintos sistemas de identificación. El sistema primario de identificación es la lectura de una tarjeta inteligente, según estándar ISO 7816, haciendo necesario la introducción del número de identificación personal, mediante un teclado, siendo susceptible de complementariedad con otros dispositivos como los de identificación por huella digital o de reconocimiento por cámara.

Normalmente los sistemas ya existentes consideran que la seguridad de los dispositivos de identificación es suficiente con evitar la duplicación, asegurando así la identificación, o como la incorporación en su software de ANTI-PASS BACK, asegurando, de esta forma, que un usuario no puede acceder a las instalaciones si previamente no las ha abandonado. En el nuevo sistema inventado, lo anteriormente mencionado, es una prestación más de seguridad, no basándose el control de acceso sólo en esta posibilidad. Para lo cual el invento incorpora comunicaciones con otros terminales de acceso dónde, dependiendo de la jerarquía de autorización, se indica la presencia del usuario en las instalaciones interiores. Esta incorporación a la seguridad de las instalaciones permite un control en tiempo real de cualquier violación no accidental de la seguridad producida tras un intento de introducir la tarjeta inteligente en un terminal no autorizado para el usuario.

El nuevo sistema de invención, aparte de tener como utilidad principal el control de accesos, servirá también para el control de presencia en las instalaciones o edificios. El software respecto a sistemas ya existentes, no sólo delimita el acceso teniendo en cuenta restricciones horarias, calendario o acceso libre, sino incorporando, además una búsqueda de restricciones jerárquica en función de grupos de usuarios con distintas prioridades de acceso. Gracias a esta característica, permite generar informes de control horario para supervisar las incidencias de incorporación al puesto de trabajo realizadas durante la jornada laboral.

Contra posibles coacciones por parte de terceros, que pretendan obligar al propietario de la tarjeta a permitir la apertura de la puerta, se incorpora un segundo PIN, denominado código de pánico, diferente a la clave de usuario personal, que permite el ingreso al área controlada pero que, inmediatamente comunica con el servidor, el cual advierte al personal de seguridad de dicha situación.

Todo ello se realiza mediante una placa microcontroladora que gestiona y controla los siguientes dispositivos:

- Módulo de inserción de tarjeta inteligente ISO 7816
- Módulo radiofrecuencia conectado a la placa microcontroladora para transmisión de datos a largo alcance en situaciones de difícil acceso por red, fallo por caída de la misma o transmisión de bases de datos placa microcontroladora-servidor.
- Dispositivos de comunicación para corto alcance, compuesto de “Dispositivos de comunicación por infrarrojos”, “Dispositivos de comunicación por RF” y “Dispositivos de comunicación por protocolos RS-232 y RS-485”, conectados a la placa microcontroladora para la transmisión de datos a corto alcance.
- La propia placa microcontroladora, que incorpora diversos puestos, reloj interno y alimentación estabilizada.
- Sistemas de interacción con el usuario, compuestos por un LCD 4x20 retroiluminado, “Teclado alfanumérico retroiluminado” y “Dispositivo acústico de señalización y alarma”.
- Cerradura electrónica de seguridad, accionada eléctricamente, con la posibilidad de acceso por llave física.
- Dispositivos de conexión a red, mediante un conector RJ-45 y coaxial.
- Sistema de alimentación ininterrumpida, compuesta por una lamentación de 220 V AC, junto a un dispositivo de alimentación propio autónomo.
- Sistema informático del control de acceso, consta de un servidor que administra y registra toda la información generada por cada acceso realizado, quedando registradas todas las incidencias.
- Control de periféricos auxiliares.
  - Control de alarmas ya sean locales o propias de las instalaciones.
  - Control de iluminación de las instalaciones o edificio.
  - Control de cámaras televisivas o fotográficas.
  - Control de dispositivos de identificación, distintos a módulos de inserción de tarjetas inteligentes, como pueden ser reconocimiento de huellas dactilares, reconocimiento de iris, etc.
- Seguridad física antiapertura de los dispositivos mediante circuito tamper.
- Seguridad física antivandálica por alarma local o remota.
- Seguridad de la información enviada/recibida por medios criptográficos.

La comunicación queda estructurada de tal forma que no sea posible una manipulación del sistema desde el exterior por personas no autorizadas, para lo cual las comunicaciones quedan divididas en:

- Comunicaciones placa microcontroladora-periféricos. Se establecen los protocolos de comunicación entre el microcontrolador y los periféricos para su control sobre éstos.

- Comunicaciones placa microcontroladora-servidor. Mediante protocolos propios de comunicación se regulan todas las comunicaciones de actualización de bases de datos, tanto de usuarios, por parte del servidor, como incidencias y registros almacenados en la placa microcontroladora.
- Comunicaciones servidor-terminal externo a las instalaciones. Se permiten consultas desde el exterior o interior de la instalación al servidor a las bases de datos por personas autorizadas desde terminales ajenos a la instalación del sistema de control de acceso.
- Comunicaciones Terminal de acceso-Terminal de acceso. Estas comunicaciones tienen como última finalidad evitar cualquier acceso por parte de un usuario a un terminal no autorizado, para lo cual el terminal último avisa previamente al usuario mediante señalización acústica o luminosa de su intento de violación del sistema de seguridad, para su posterior almacenaje y aviso a todos los terminales y al servidor, bloqueando de esta forma la tarjeta.

Las comunicaciones disponen de distintos módulos para asegurar las comunicaciones anteriormente descritas. Estos módulos son:

Módulo de comunicación para corto alcance:

Dispositivos de comunicación por infrarrojos.

Dispositivos de comunicación por PF.

Dispositivos de comunicación por protocolos RS-232 o RS-485.

Módulo de comunicación para largo alcance:

Dispositivos de comunicación por radiofrecuencia.

Dispositivos de conexión a red con conector RJ-45 y coaxial.

Para aumentar la seguridad de las comunicaciones, toda la información es enviada por medios criptográficos.

Las posibilidades básicas de control de periféricos accionados por la placa base son:

- Control de la cerradura electrónica de seguridad, accionada eléctricamente, con posibilidad de acceso por llave física.
- Dispositivo de seguida física antivandálica por alarma local (sonora y luminosa) y remota.
- Dispositivo de seguridad física antiapertura del dispositivo mediante circuito tamper.
- Módulo de inserción de tarjeta.
- LCD 4x20 retroiluminado.
- Teclado alfanumérico retroiluminado.
- Dispositivo acústico de señalización y alarma.
- Alarmas remotas.
- Iluminación del edificio o instalación.

Todo el sistema de control de accesos está gestionado por un software que permite el control del análisis de la información registrada por el control de acceso, así como la gestión de las bases de datos del tiempo real, para lo cual la placa microcontroladora, compuesta por un microcontrolador con diversos puertos de comunicación, reloj interno y alimentación estabilizada, se comunica con el servidor.

El software que incorpora el servidor tiene capacidad de crear una base de datos en la que queda registrado el personal autorizado, el código personal, las horas y/o días permitidos para el acceso, permitiendo además las siguientes parametrizaciones del acceso:

- Zonas de tiempo: Se trata de la definición de horarios que se le asignan a cada usuario al objeto de permitir el ingreso a las diferentes áreas, especificando horas y fechas en que puede acceder.
- Por terminal: A cada usuario se le asigna el terminal o los terminales a través de los cuales tendrá posibilidades de acceso permitido.
- Base de datos interna del Servidor: Cada alta, baja o bloqueo de usuario, así como cada consulta que se realiza al servidor, queda registrada, previa identificación del usuario autorizado, para gestión del servidor y posterior emisión de informes relacionados con el control de accesos y horarios.

Descripción de los dibujos

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características del invento, de acuerdo con un ejemplo de realización práctica del mismo, se acompaña como parte integrante de dicha descripción, una hoja única de planos en la que con carácter ilustrativo y no limitativo y en su única figura, se ha representado el diagrama de bloques funcional del sistema de control de acceso.

Realización preferente de la invención

A continuación se realiza una descripción de la invención basada en la figura anteriormente comentada.

Tal y como fue expresado en apartados anteriores, la invención consiste en un sistema de control de acceso, que es de especial aplicación en el control de acceso en edificios o instalaciones, para lo cual consta de una arquitectura integrada por placa microcontroladora (1), teclado (2), LCD (3), cerradura electrónica (4) y módulos (5) para control de periféricos adicionales.

La placa microcontroladora (1), gestiona todos los dispositivos y las comunicaciones; por ejemplo, la inserción de una tarjeta inteligente en un dispositivo de lectura o tarjetero (6) o reconocimiento de otro dispositivo de identificación establece comunicación con el microcontrolador, a través de los puertos de la placa microcontroladora estableciéndose posteriormente comunicaciones con el teclado (2) y el display (3) para confirmación del usuario.

El microcontrolador (1) examina todas las bases de datos existentes y prioridades para confirmar la identificación y registrar el acceso. Dependiendo de la confirmación de identificación el

microcontrolador (1) actuará sobre los distintos dispositivos periféricos, luminosos, sonoros, alarmas, y cerradura electrónica.

A partir de este momento se establece comunicación con otros terminales de control de acceso, indicando la presencia del usuario en las instalaciones. Quedando de esta forma delimitado el acceso. Además si en el día y hora en que se intenta realizar el acceso, el usuario está autorizado para acceder en esa banda diaria y horaria, el control de acceso conectará la iluminación, si se requiriese, desconectando las alarmas si las hubiera, de aquellas zonas donde el acceso del usuario no fuera restringido y se tuviera constancia de su presencia.

En todo momento se establecen comunicaciones con un ordenador (7), el cual sirve de apoyo para la gestión de las bases de datos y comunicación con otros equipos de acceso, siendo el modo de comunicación on-line u off-line, dependiendo de la fiabilidad de la comunicación escogida por el microcontrolador (1) o en su defecto por el ordenador (6).

En caso de fallo de comunicación con el servidor (8), por caída de la red interna o externa de acceso a INTERNET (9), el microcontrolador (1) intentará realizar la comunicación a través de módulos de comunicación de corto alcance. Tras ésto, si la comunicación no fuera reestablecida, el control cambia de modo de comunicación on-line a off-line. Sí bien el sistema de gestión del control sería trasparente a los usuarios, el almacenaje de los datos registrados en las bases de datos gestionadas por el microcontrolador (1) se realizaría en modo local. Una vez superada la capacidad de almacenaje de las bases de datos, gestionadas en el terminal, el sistema comenzaría a eliminar registros de usuarios por prioridades, comenzando con la eliminación de mayor a menor, siempre y cuando no exista registro de una incidencia de violación de la seguridad por parte de un usuario, ya que, en dichos casos éstos registros no podrán ser eliminados hasta que no hubieran sido descargados al servidor (7).

Por último, el microcontrolador (1) admite la interconexión con el microcontrolador (1') de un nuevo terminal.

En caso de fallo eléctrico el funcionamiento queda limitado solo a al control de accesos y a la gestión de las alarmas. Inmediatamente después del fallo eléctrico la corriente es suministrada por una batería o un SAI asegurando con ello la autonomía necesaria hasta la restauración del suministro energético.

REIVINDICACIONES

1. Sistema de control de accesos por tarjeta inteligente, de aplicación especial en el control de accesos de personas a edificios o instalaciones mediante el uso de elementos de comunicación por Internet, **caracterizado** por estar constituido por una placa microcontroladora (1) que dispone de medios de gestión y control de los elementos de la propia placa así como de comunicación tanto con los posibles usuarios del sistema como con los elementos de actuación del mismo, incorporando elementos de seguridad física y de comunicaciones, habiéndose previsto, además de su alimentación a red, incorporar un sistema de alimentación ininterrumpida.

2. Sistema de control de accesos por tarjeta inteligente, según reivindicación primera, **caracterizado** porque la propia placa microcontroladora (1) incorpora un módulo de inserción de tarjeta inteligente ISO 7816 y un módulo de radiofrecuencia para transmisión de datos de largo alcance en situaciones de difícil acceso por red, fallo de la misma o transmisión de bases de datos placa microcontroladora (1) y el servidor (8).

3. Sistema de control de accesos por tarjeta inteligente, según reivindicación primera, **caracterizado** porque la placa microcontroladora (1) está conectada a dispositivos de comunicación de corto alcance (10), como pueden ser por infrarrojos, radiofrecuencia o de comunicación por protocolos RS-232 y RS-485, para transmisión de datos a corto alcance, dispositivos de conexión a la red, mediante un conector RJ-45 y coaxial y una cerradura electrónica de seguridad, accionada eléctricamente, con la posibilidad de acceso por llave física.

4. Sistema de control de accesos por tarjeta inteligente, según reivindicación primera, **caracterizado** porque la placa microcontroladora (1) mediante conexión a los mismos realiza el control tanto de los sistemas de interacción con el usuario compuestos por un LCD (3), un teclado (2) y un dispositivo acústico de señalización y alarma, como del sistema informático de control de acceso y horario, constituido por un servidor (8) que administra y registra toda la información generada por cada acceso realizado, quedando registradas las incidencias, incluyendo la generación del informe de control de accesos, horario y partes de trabajo del personal que accede al puesto.

5. Sistema de control de accesos por tarjeta inteligente, según reivindicación primera, **caracterizado** porque la placa microcontroladora (1) dispone de medios para realizar el control de periféricos auxiliares como, control de alarmas ya sean locales o propias de las instalaciones, control de iluminación de las instalaciones o edificio, control de cámaras televisivas o fotográficas y control de dispositivos de identificación.

6. Sistema de control de accesos por tarjeta inteligente, según reivindicaciones anteriores, **caracterizado** porque incorpora elementos de seguridad física antiapertura de los dispositivos, de seguridad física antivandálica por alarma local o remota y de seguridad de la información enviada/recibida por medios criptográficos.

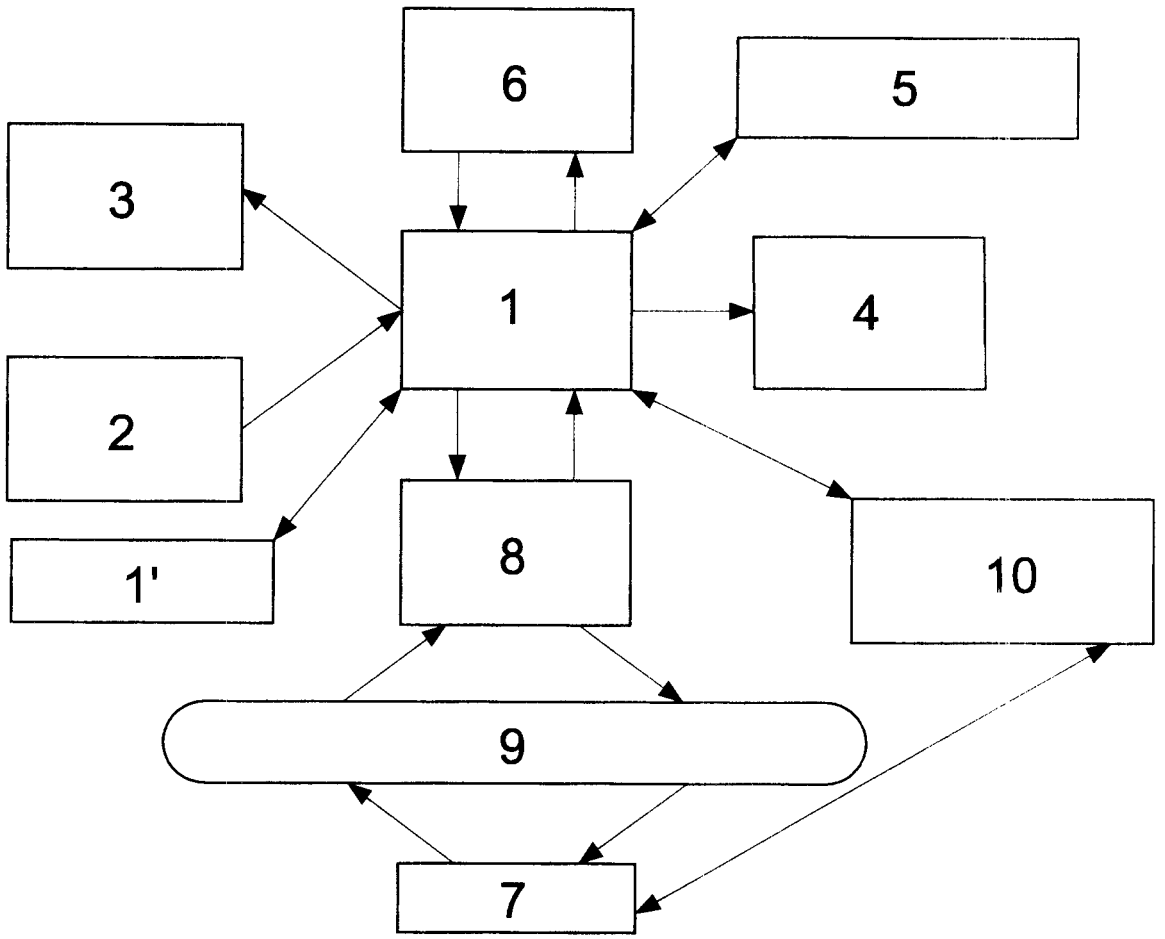

FIG. 1

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 166 321

(21) N.° solicitud: 200000768

(22) Fecha de presentación de la solicitud: **29.03.2000**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl.**[7]**:** G07C 9/00, G07F 7/08, 7/10, G08B 3/00, G06K 7/00

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
X	WO 9410804 A (OAKLEIGH SYSTEMS, INC) 11.05.1994, página 3, línea 29 - página 5, línea 31; figuras.	1
A		2-5
X	EP 0965951 A (AXS TECHNOLOGIES INC) 22.12.1999, página 2, línea 5 - página 4, línea 28; página 5, línea 3 - página 6, línea 54; figuras 1-4.	1
A		2-5
A	US 5204663 A (LEE) 20.04.1993, columna 1, línea 64 - columna 9, línea 52; figuras 1-4.	1-3
A	US 5613159 A (COLNOT) 18.03.1997, todo el documento.	1-3

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 n°:

Fecha de realización del informe	Examinador	Página
04.03.2002	P. Pérez Fernández	1/1