(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 380 382**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08157401 .4**
(96) Fecha de presentación: **02.06.2008**
(97) Número de publicación de la solicitud: **1998292**
(97) Fecha de publicación de la solicitud: **03.12.2008**

(54) Título: **Identificación de tipo móvil para sistemas de seguridad y de gestión de bienes**

(30) Prioridad:
01.06.2007 US 756901

(45) Fecha de publicación de la mención BOPI:
11.05.2012

(45) Fecha de la publicación del folleto de la patente:
11.05.2012

(73) Titular/es:
Honeywell International Inc.
101 Columbia Road
Morristown, NJ 07960, US

(72) Inventor/es:
Jayappa, Mahesh;
Drive, Marine;
Salgar, Mayur y
Subbian, Deepakumar

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Identificación de tipo móvil para sistemas de seguridad y de gestión de bienes

La presente invención se refiere, en general, a sistemas de seguridad y de gestión de bienes. En particular, esta invención se refiere a la utilización de dispositivos de consumo, tales como teléfonos móviles, para identificar y autenticar, así como para localizar y entrar en contacto con usuarios de sistemas de seguridad y de gestión de bienes.

Los sistemas de seguridad y de gestión de bienes se utilizan para vigilar viviendas y empresas con el fin de impedir intrusiones no deseadas así como para servir de protección contra desastres naturales. Dichos sistemas controlan la entrada y salida a estructuras así como a zonas dentro de las estructuras. En los sistemas de seguridad de la técnica anterior, se requerían llaves para la entrada en edificios protegidos. En los sistemas más recientes, sin embargo, el acceso se consigue utilizando dispositivos de identidad, que interaccionan con un dispositivo de control del acceso, tal como un lector, que funciona en conjunción con un panel de control que permite o deniega el acceso a usuarios en función de su identificación o autorización. Estos sistemas suelen emplear un dispositivo pasivo, tal como una tarjeta de proximidad o un dispositivo activo, tal como una etiqueta RFID, para identificar y/o autenticar los usuarios del sistema. Un usuario puede presentar su dispositivo a un dispositivo de control de acceso y el dispositivo del usuario puede iniciar el procedimiento de autenticación. Como alternativa, un dispositivo de control de acceso puede iniciar la verificación de entrada o autorización buscando un dispositivo de usuario válido.

Un dispositivo de control de acceso que busca un dispositivo de usuario válido se da a conocer en la solicitud de patente del Reino Unido, GB 2 417 858, titulada “Dispositivo de control de acceso utilizando teléfonos móviles para acceso inalámbrico automático con códigos de seguridad y datos biométricos”. Esta solicitud da a conocer un dispositivo de control del acceso que utiliza un proceso automático de autenticación basado en códigos encriptados secretos determinados con un algoritmo de encriptación basado en el transcurso del tiempo. En al menos una forma de realización, la búsqueda y detección automática de credenciales de un usuario autorizado que utiliza un teléfono móvil que tiene un código de acceso válido, se realiza por un módulo de identidad de abonado (SIM) dedicado en el controlador de acceso de entrada. En otra forma de realización, las credenciales de usuarios se transmiten desde un teléfono móvil de un usuario como un servicio de mensajes cortos (SMS) a la tarjeta SIM del controlador de acceso de entrada a través de canales de comunicación estándar, tales como Bluetooth®. Este sistema requiere la utilización de una tarjeta SIM dedicada, en el controlador, para poner en práctica el algoritmo de encriptación y para memorizar los códigos encriptados.

La publicación de solicitud de patente de Estados Unidos número 2005/0143051, ‘Sistema de autenticación de móvil/transacción financiera utilizando un código de identificación de móvil único y su método’, da a conocer un sistema de autenticación de móvil y transacción financiera que utiliza un código de identificación de móvil único, en donde el control de la admisión y/o una diversidad de operaciones financieras se realizan sobre la base de la información de llamada transmitida por un terminal de comunicación móvil. El código de identificación único puede ser un “código de identidad móvil peculiar” o una combinación del número de teléfono registrado y un número de serie electrónico. Todas las formas de realización, dadas a conocer en esta solicitud de patente, utilizan la frecuencia para telefonía móvil y el sistema de telecomunicaciones para la comunicación.

La patente de los Estados Unidos número 5.895.436, titulada ‘Sistema de seguimiento de vehículos utilizando una red celular’, da a conocer un sistema de seguimiento de vehículos que utiliza la infraestructura de la red celular existente. Un transceptor celular de localización está instalado en un vehículo y se registra el Número de Serie Electrónico (ESN) del transceptor. Si el vehículo es robado, el número ESN se utiliza para determinar la localización general del vehículo; su localización precisa se establece utilizando un buscador de dirección de radio que se sintoniza para el canal de voz del transceptor celular. De este modo, una red celular de un sistema de telecomunicación o sistema buscapersonas es necesaria para identificar y para efectuar el seguimiento de los vehículos.

La patente de Estados Unidos número 6.624.739, ‘Sistema de control del acceso’, da a conocer un transpondedor móvil con un código de autorización para proporcionar acceso al usuario. El sistema proporciona el acceso en función de una comparación de las características biométricas de una persona con los datos biométricos almacenados en su memoria. Sin embargo, no supera el problema de requerir un dispositivo especial, el transpondedor móvil, para las funciones de identificación y/o autorización. Además, el transpondedor no permite la identificación y/o autenticación del usuario para situaciones de emergencia.

La patente de Estados Unidos número 6.069.411, ‘Método antirrobo para un vehículo con la utilización de un teléfono móvil’, da a conocer la utilización de la Identificación de Equipo Móvil Internacional (IMEI) de un teléfono móvil como un elemento de un método antirrobo de vehículos. Para arrancar un vehículo, un usuario pone su teléfono portátil en un elemento de sujeción. El teléfono compara, entonces, su número ESN o número de IMEI con el que está memorizado en una posición en el elemento de sujeción. Si coinciden ambos números, se puede arrancar el vehículo. Sin embargo, todas las funciones de procesamiento o de coincidencia o de autenticación se realizan en el teléfono utilizando el elemento de sujeción solamente como un conducto. Además, el teléfono móvil debe iniciar la identificación o autorización de un usuario y el elemento de sujeción no puede buscar un dispositivo de identificación.

El documento EP–A-1424861 da a conocer un método y aparato para identificar un usuario que emplea un teléfono móvil, en donde el teléfono móvil se inserta en un lector para proteger al teléfono de la red telefónica circundante. El lector puede obtener, entonces, información de identificación del usuario desde el teléfono. El sistema se utiliza, por ejemplo, para identificar un comprador cuando recoge mercancías previamente pedidas.

Los documentos WO-A-00/38119, FR-A-2861943 y US-A-2002/0070273 dan a conocer, cada uno, sistemas de identificación en los que se pueden utilizar teléfonos móviles.

Entre los problemas de los sistemas antes citados están la necesidad de sistemas de telecomunicaciones para comunicación y de dispositivos específicos, tales como tarjetas SIM incorporadas en el aparato de control. Si dispositivos distintos de los teléfonos móviles se utilizan como identificadores de usuario, los dispositivos, tales como etiquetas RFID, tienen limitaciones de alcance y de duración de la batería y además, tienen gastos extraordinarios para su mantenimiento. Además, un usuario del sistema de seguridad debe proporcionar su dispositivo de identidad específico, tal como un aparato que contenga una etiqueta RFID, para identificarse o autenticarse, teniendo la necesidad el usuario de llevar consigo el dispositivo de identidad. Además, estos dispositivos no suelen ser utilizables en caso de una emergencia, para que el sistema identifique y comunique con el usuario o para que el usuario se comunique con el sistema.

La presente invención da a conocer un sistema de seguridad y de gestión de bienes según se establece en la reivindicación 1 o la reivindicación 11 de la presente invención y un método según se define en la reivindicación 12.

La presente invención da a conocer, ventajosamente, un sistema de seguridad y de gestión de bienes accesible utilizando dispositivos de consumo, tales como teléfonos móviles, para identificar, autenticar, localizar y entrar en contacto con los usuarios del sistema de seguridad. Dichos dispositivos de consumo se pueden utilizar no solamente con el sistema de seguridad si no también para otros usos. Un dispositivo se registra inicialmente con el sistema de seguridad no simplemente como un punto de acceso específico. Cuando es necesario, el dispositivo se presenta al sistema para autenticación, permitiendo a una persona acceder a una zona segura. Además, el sistema puede determinar y memorizar la localización de la persona en la zona segura y puede avisar a la persona en caso de emergencia.

El sistema de seguridad y de gestión de bienes incluye un dispositivo utilizable para comunicación móvil, teniendo dicho dispositivo un código de identificación y una interfaz de comunicación de dispositivo utilizable para iniciar la transmisión del código de identificación y para dar respuesta a una demanda de transmisión del código de identificación. El sistema comprende, además, al menos un lector que tiene una interfaz de comunicación de lector utilizable para obtener el código de identificación desde el dispositivo; un panel de control utilizable para comunicarse con dicho al menos un lector y una memoria, accesible a través del panel de control, para memorizar datos de localización y datos de ID que comprende al menos uno o más códigos de identificación, en donde el panel de control valida el código de identificación recibido desde dicho lector y el panel de control memoriza una localización del dispositivo determinada utilizando los datos de localización y una señal recibida desde el dispositivo.

En una forma de realización, el lector solicita el código de identificación desde el dispositivo, mientras que en otra forma de realización, el dispositivo transmite su código de identificación sin recibir una demanda del lector. En otra forma de realización, el dispositivo tiene un módulo de seguridad para la encriptación del código de identificación y el lector tiene un módulo de seguridad para desencriptar el código de identificación.

Los anteriores y otros objetos, aspectos, características y ventajas de la invención se harán más evidentes a partir de la siguiente descripción y de las reivindicaciones.

La invención se describe, además, en la forma detallada ilustrada a continuación, haciendo referencia a los dibujos indicados, a modo de formas de realización ilustrativas no limitadoras de la invención, en donde las referencias numéricas similares representan elementos similares en todos los dibujos. Debe entenderse, sin embargo, que la invención no está limitada a las disposiciones e instrumentalidades precisas ilustradas. En los dibujos:

La Figura 1 es un diagrama de bloques de una forma de realización ejemplo de la presente invención;

La Figura 2 es un diagrama de bloques de una zona segura según una forma de realización de la presente invención;

La Figura 3 es un diagrama de flujo que ilustra las etapas para una forma de realización de la presente invención y

La Figura 4 es un diagrama de flujo que ilustra las etapas para otra forma de realización de la presente invención.

Una solución inventiva se presenta para la necesidad de un sistema de seguridad y de gestión de bienes (“sistema de seguridad”) utilizable con un dispositivo que se puede emplear para identificar, autenticar, localizar y entrar en contacto con su usuario, de modo que el dispositivo se puede utilizar no solamente con el sistema de seguridad si no que también tiene funcionalidad separada desde el sistema de seguridad, esto es, un dispositivo tal como un teléfono móvil.

La Figura 1 representa un sistema de seguridad ejemplo 100. El sistema de seguridad 100 puede incluir un dispositivo de autenticación y de identificación 110, un dispositivo de acceso o lector 140, un panel de control 170 y una memoria 180. El dispositivo 110 puede incluir un código de identificación 112, un módulo de seguridad 114 y una interfaz de comunicación 116. El código de identificación 112 se registra inicialmente y se memoriza en los datos de identificación y autorización (ID) del sistema de seguridad 182 que reside en la memoria del sistema 180. El dispositivo 110 puede transmitir también una señal 118 a partir de la cual se puede determinar su localización p.e., localización del dispositivo 119. El dispositivo tiene la capacidad no solamente para transmitir una señal y transmitir su código de identificación, sino que también tiene una funcionalidad para actuar como un dispositivo de comunicación móvil, un dispositivo de cálculo, un procesador, un organizador electrónico y dispositivos similares. Dichos dispositivos pueden incluir, sin limitación, dispositivos móviles tales como teléfonos celulares, teléfonos inteligentes, ordenadores portátiles, PDAs (asistentes digitales personales) y otros dispositivos similares. El módulo de seguridad opcional 114 del dispositivo proporciona una comunicación segura, tal como funciones de encriptación y desencriptación.

El lector 140 puede incluir un módulo de seguridad 142 y una interfaz de comunicación 144 que permite la comunicación entre el lector y el dispositivo 110 así como entre el lector y el panel de control 170 del sistema de seguridad. La interfaz de comunicación del lector 140 y el dispositivo 116 pueden incluir, sin limitación, uno de entre los dispositivos de infrarrojos (IR), Bluetooth®, frecuencia de 2,4 GHz (banda de frecuencia sin licencia), frecuencia de GSM/GPRS/CDMA y frecuencias de RFID/tarjeta inteligente/tarjeta de proximidad. Para evitar la sobrecarga y dependencias operativas, las frecuencias de móviles o redes celulares no se suelen utilizar para una comunicación segura. El módulo de seguridad 142, tal como el módulo de seguridad del dispositivo 114, permite una comunicación segura. El lector 140 puede tener circuitos electrónicos que pueden consultar el teléfono móvil 110 para su código de identificación 112. El teléfono móvil tendrá una interfaz de comunicación 116 para transmitir el código de identificación 112 al lector 140.

El lector 140 se comunica con el panel de control 170 que proporciona acceso a la memoria del sistema de seguridad 180 que contiene información que incluye datos de ID 182, que comprenden los códigos de identificación de múltiples dispositivos y datos de localización 184. Según se ilustra en la Figura 1, los datos de ID 182 se memorizan por separado desde el panel de control 170 y el lector 140, lo que mejora la seguridad del sistema de seguridad y permite al usuario acceder a través de múltiples lectores, según se describe a continuación. Además, los datos de localización 184 que describen y localizan recintos y otras zonas protegidas por el sistema de seguridad 100 se almacenan en la memoria del sistema 180 y se acceden a través del panel de control 170. Los datos de ID 182 pueden residir en la misma memoria que los datos de localización 184 o cada uno pueden residir en una memoria separada (no ilustrada).

En una forma de realización preferida representada en la Figura 2, el teléfono móvil 110 es un dispositivo de identificación, autenticación y/o localización de un usuario. En la técnica anterior, cualquier teléfono móvil puede identificarse, de forma única, por su IMEI o su número ESN. De este modo, un teléfono móvil 110 puede convertirse en un dispositivo de identificación, autenticación y/o localización de un usuario utilizando su IMEI como el código de identificación único 112 registrando o inscribiendo el IMEI en un sistema de seguridad existente. Por lo general, el registro del código IMEI con el sistema de seguridad se realiza solamente una vez.

La Figura 2 representa una zona segura 240, cuyo acceso está controlado por un sistema de seguridad y de gestión de bienes. La zona segura 240 puede ser una estructura o un grupo predeterminado de estructuras o edificios. Cuando un usuario de un teléfono móvil 110 desea entrar en la zona segura 240, el usuario deberá identificarse. La entrada se permite solamente si el IMEI del usuario está integrado o registrado por el sistema de seguridad y el usuario está autorizado a entrar por dicho sistema de seguridad. Además, un usuario puede necesitar autorización para desplazarse de un lugar a otro. Por ejemplo, de un edificio a otro, de una planta a otra o de un recinto a otro, dentro de la zona segura. De este modo, según se representa en la Figura 2, los lectores 140 pueden situarse en el interior y en el exterior de la zona segura 240. El lector recibe el IMEI del teléfono móvil del usuario y transmite este IMEI al panel de control que determina si el usuario está autorizado para entrar. Si el panel de control 170, basado en los datos de ID 182 en el sistema de seguridad, determina que el IMEI es válido y auténtico, se autoriza el acceso del usuario y se permite que entre en la zona segura 240. Debido a que todos los lectores pueden obtener acceso a los datos de ID del sistema de seguridad 182 a través del panel de control 170, estos datos se memorizan solamente una vez en una localización segura y no se almacenan en la memoria de cada lector. En una forma de realización de la invención, cuando la persona es autorizada para entrar, el panel de control puede realizar una tarea tal como una apertura de una puerta o compuerta.

El sistema puede ser activo o pasivo. En el sistema pasivo, las funciones de identificación, autenticación y/o localización del teléfono móvil del usuario se pueden realizar, de forma no intrusiva, por los lectores del sistema de seguridad 140. Cada lector 140 explora la zona para obtener el código de identificación 112, por ejemplo, el IMEI, desde el teléfono móvil. El sistema pasivo puede utilizar las interfaces de comunicación de Bluetooth®, frecuencia de 2,4 GHz y frecuencias de GSM/GPRS/CDMA. Las interfaces de comunicaciones de frecuencias de infrarrojos (IR) y de frecuencias de tarjetas de proximidad que requieren, cada una, una línea de mira, que en general no se utilizaría en el sistema pasivo. El protocolo de comunicación entre el lector y el teléfono móvil implicará un método para explorar por el lector cualquier fuente válida (p.e., teléfono móvil) que contenga un IMEI dentro de un margen de distancia particular. Según se describió anteriormente, el lector deberá explorar e identificar automáticamente así como autenticar al usuario en conjunción con el panel de control.

En el sistema activo, el usuario debe interaccionar o iniciar la autorización. El usuario comunica el IMEI al lector bien sea pulsando la tecla (por ejemplo, la tecla de asterisco (*)) en su teléfono móvil o presentando el teléfono móvil cerca del lector. El protocolo de comunicación entre el teléfono móvil y el lector deberá implicar la obtención del IMEI, su validación o autenticación en conjunción con el panel de control y tomar la acción adecuada. El sistema activo soporta todas las interfaces de comunicación antes citadas, incluyendo las de infrarrojos IR y frecuencia de tarjetas de proximidad.

Además, los lectores 140 pueden determinar la dirección y distancia de la señal recibida 118 desde el teléfono móvil del usuario 110 y reenviar esta señal 118 junto con el IMEI al panel de control 170. Uno u otro de los lectores 140 puede entrar en contacto con el teléfono móvil del usuario 110 para obtener su señal 118 o un usuario puede suministrar la señal sin que se la pidan. La localización del usuario 119 dentro de la estructura o zona segura 240, por ejemplo, la planta o recinto ocupado por el usuario, se puede establecer coordinando la señal 118 con los datos de localización 184 del sistema de seguridad disponible para el panel de control 170. El lector podría transmitir un mensaje a través del dispositivo del usuario. El mensaje podría enviarse por el lector si el usuario está autenticado, o no, por el panel de control para el lector particular. Esta función podría utilizarse, por ejemplo, para informar a un usuario de que solamente le está permitido permanecer en la planta principal del edificio y podría utilizarse también en situaciones de emergencia tales como “localizar un médico” o “encontrar una persona en caso de un incendio”, etc.

Además, según se describió anteriormente, la persona puede proporcionar su posición o localización del dispositivo 119 al lector más cercano 140. De este modo, el usuario puede avisar al lector de una situación de emergencia enviando una señal con una demanda de asistencia, por ejemplo, buscapersonas en caso de emergencia, junto con su número IMEI. El sistema de seguridad 100 identificará la emergencia del usuario e iniciará las acciones adecuadas.

El funcionamiento de los sistemas de seguridad activos y pasivos se describe a continuación con referencia a las Figuras 3 y 4. En el sistema pasivo ilustrado en la Figura 3, en P1 el lector escanea la zona y obtiene el IMEI desde un teléfono móvil. En P2, el lector se comunica con el panel de control para validar el IMEI. Si el IMEI es válido, se realiza la autenticación en P3. Si el IMEI no es válido, el lector escanea de nuevo la zona en P1.

En el sistema activo representado en la Figura 4, en A1 un usuario presenta un teléfono móvil al lector. El lector obtiene el IMEI desde el teléfono móvil en A2. En A3, el lector se comunica con el panel de control para validar el IMEI. Si el IMEI es válido, la autenticación se realiza por el panel de control en A4. Si el IMEI no es válido, el lector espera a que un usuario presente un teléfono móvil en A1.

Las formas de realización descritas anteriormente son ejemplos ilustrativos y no deben interpretarse en el sentido de que la presente invención esté limitada a dichas formas de realización particulares. Por consiguiente, se pueden realizar por los expertos en esta materia varios cambios y modificaciones dentro del alcance de protección de la invención según se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema de seguridad y de gestión de bienes (100) que controla el acceso a una zona o una estructura segura, comprendiendo el sistema:

un teléfono móvil (110) dotado de un código de identificación (112) y de una interfaz de comunicación de dispositivo (116) utilizable para iniciar la transmisión del código de identificación (112) y para dar respuesta a una demanda de transmisión del código de identificación (112);

al menos un lector (140) dotado de una interfaz de comunicación de lector (144) utilizable para obtener el código de identificación (112) a partir del teléfono móvil (110);

un panel (170) de control utilizable para comunicarse con dicho al menos un lector (140) y

una memoria (180) para almacenar datos de localización (184) que describen y localizan zonas protegidas por el sistema (100) y datos de identificación ID (182) que comprende al menos uno o más códigos de identificación (112) incluyendo el código de identificación (112) del teléfono móvil (110), siendo dicha memoria (180) accesible por dicho panel de control (170),

en donde el panel de control (170) está adaptado para validar el código de identificación (112) del teléfono móvil (110) recibido desde dicho lector (140) y el panel de control (170) está adaptado para memorizar una localización de dispositivo (119) determinada utilizando los datos de localización memorizados (184) coordinados con una señal (118) recibida desde el teléfono móvil (110),

caracterizado porque el al menos un lector (140) está separado del panel de control (170) y es utilizable, además, para determinar la dirección y distancia de la señal (118) recibida desde el teléfono móvil (110) y la localización del teléfono móvil dentro de la estructura o zona segura y porque el al menos un lector (140) está adaptado para enviar un mensaje al teléfono móvil (110) que incluye la información con respecto a donde está permitido el acceso dentro de la estructura o zona segura.

2. El sistema según la reivindicación 1, en donde el lector transmite un mensaje a dicho teléfono móvil (110).

3. El sistema según la reivindicación 1 o la reivindicación 2, en donde el lector demanda dicho código de identificación desde dicho teléfono móvil (110).

4. El sistema según la reivindicación 1 o la reivindicación 2, en donde el teléfono móvil (110) inicia la transmisión de dicho código de identificación sin recibir una demanda desde el lector.

5. El sistema según cualquiera de las reivindicaciones precedentes, en donde el teléfono móvil (110) tiene un módulo de seguridad (114) para la encriptación del código de identificación.

6. El sistema según cualquiera de las reivindicaciones precedentes, en donde el lector tiene un módulo de seguridad (142) para la desencriptación del código de identificación.

7. El sistema según cualquiera de las reivindicaciones precedentes, en donde la interfaz de comunicación del teléfono móvil (110) es una de entre las interfaces de IR (infrarrojos), Bluetooth, frecuencia de 2,4 GHz (banda de frecuencia sin licencia) y las frecuencias de RFID/tarjeta inteligente/tarjeta de proximidad.

8. El sistema según cualquiera de las reivindicaciones precedentes, en donde la interfaz de comunicación del lector es una de entre las interfaces de IR (infrarrojos), Bluetooth, frecuencia de 2,4 GHz (banda de frecuencia sin licencia) y las frecuencias de RFID/tarjeta inteligente/tarjeta de proximidad.

9. El sistema según una cualquiera de las reivindicaciones precedentes, en donde si el código de identificación es válido, el panel de control realiza una actividad.

10. Un método para identificar un dispositivo en un sistema de seguridad y de gestión de bienes (100) que controla el acceso a una estructura o zona segura, que comprende:

la transmisión de una señal (118) que comprende un código de identificación (112) desde un teléfono móvil (110);

la recepción del código de identificación (112) en un lector (140);

la transmisión del código de identificación (112), desde el lector (140), a un panel de control (170) y

la localización del teléfono móvil (110) en una zona segura (240) coordinando la señal (118) transmitida desde el teléfono móvil (110) al lector (140) con los datos de localización memorizados (184) que describen y localizan zonas protegidas

por el sistema, en donde los datos de localización memorizados (184) son accesibles desde el panel de control (170) y el panel de control (170) valida el código de identificación (112) utilizando datos de identificación ID (182) y si el código de identificación (112) es válido, se autoriza el teléfono móvil (110),

caracterizado porque el lector (140) está separado del panel de control (170) y la determinación de la dirección y distancia de la señal (118) recibida desde el teléfono móvil (110) y la localización del teléfono móvil dentro de la zona o estructura segura y por el lector que transmite un mensaje al teléfono móvil (110) que incluye información en cuanto a dónde está permitido el acceso dentro de la estructura o zona segura.

11. El método según la reivindicación 10, en donde el lector transmite un mensaje al teléfono móvil (110).

12. El método según la reivindicación 10 o la reivindicación 11, en donde el código de identificación (112) se transmite en respuesta a una demanda desde el lector.

13. El método según cualquiera de las reivindicaciones 10 a 12, en donde el lector demanda dicho código de identificación (112).

14. El método según cualquiera de las reivindicaciones 10 a 13, en donde el teléfono móvil (110) tiene un módulo de seguridad (114) para la encriptación del código de identificación.

15. El método según cualquiera de las reivindicaciones 10 a 14, en donde el lector tiene un módulo de seguridad (142) para la desencriptación del código de identificación.

16. El método según cualquiera de las reivindicaciones 10 a 15, en donde el teléfono móvil (110) comprende una interfaz de comunicación seleccionada de entre el grupo constituido por las interfaces de IR (infrarrojos), Bluetooth, frecuencia de 2,4 GHz (banda de frecuencia sin licencia) y las frecuencias de RFID/tarjeta inteligente/tarjeta de proximidad.

17. El método según cualquiera de las reivindicaciones 10 a 16, en donde el lector comprende una interfaz de comunicación de lector seleccionada de entre el grupo constituido por las interfaces de IR (infrarrojos), Bluetooth, frecuencia de 2,4 GHz (banda de frecuencia sin licencia) y las frecuencias de RFID/tarjeta inteligente/tarjeta de proximidad.

18. El método según una cualquiera de las reivindicaciones 10 a 17 que comprende, además, el panel de control que realiza una actividad cuando el dispositivo está autorizado.

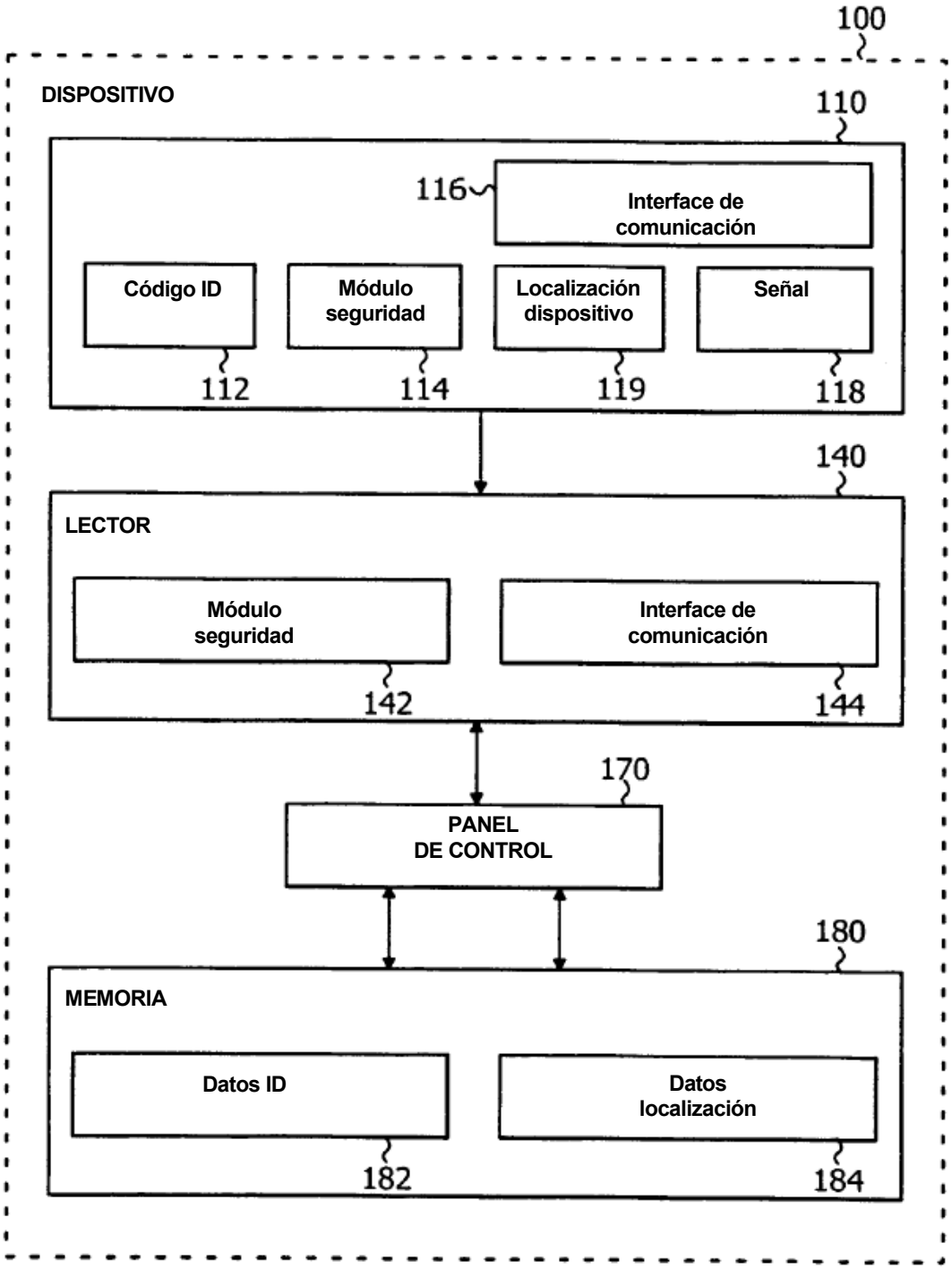
100
DISPOSITIVO
110
116
Interface de comunicación
Código ID
Módulo seguridad
Localización dispositivo
Señal
112
114
119
118
140
LECTOR
Módulo seguridad
Interface de comunicación
142
144
170
PANEL DE CONTROL
180
MEMORIA
Datos ID
Datos localización
182
184

Figura 1

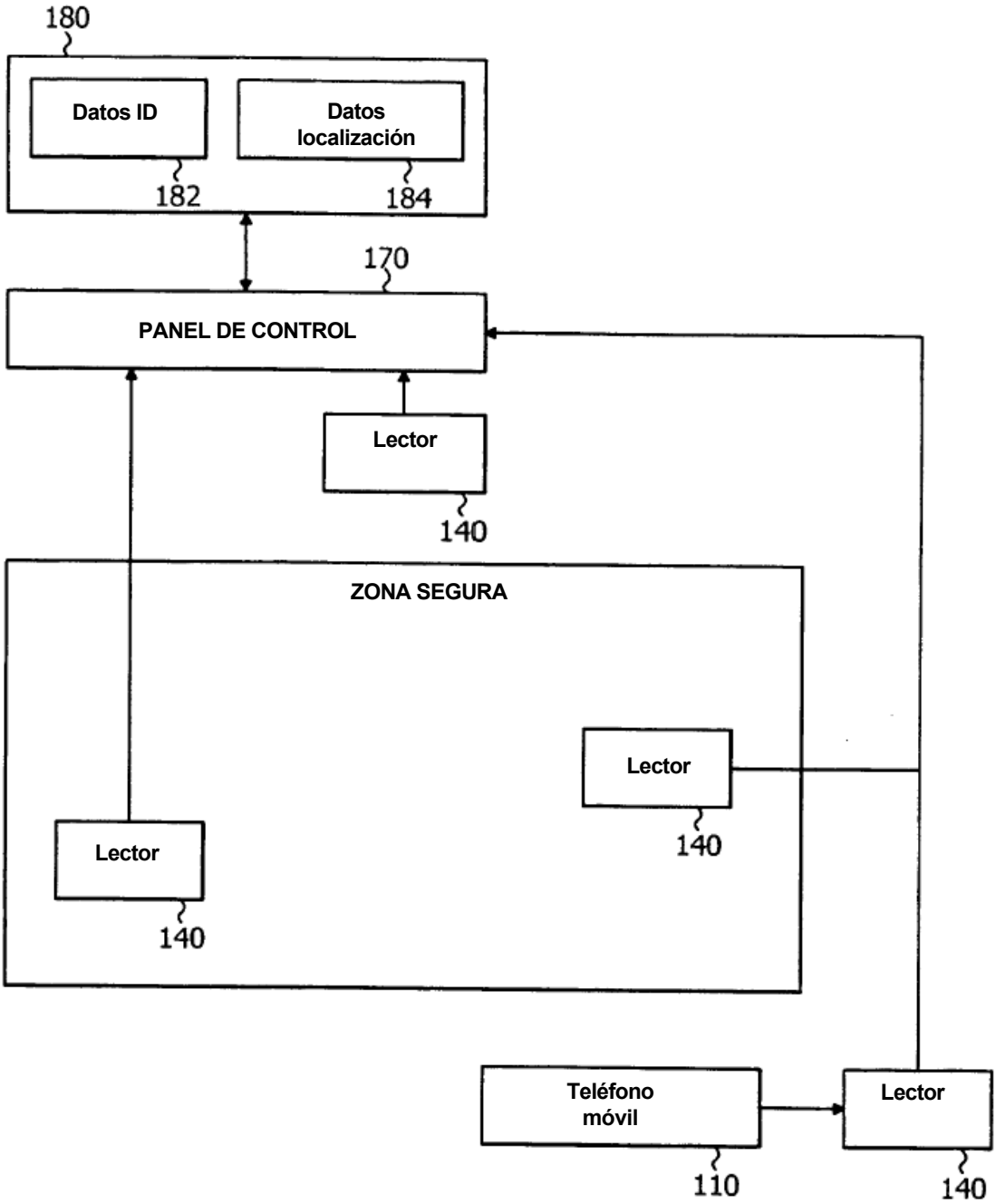
180
Datos ID
Datos localización
182
184
170
PANEL DE CONTROL
Lector
140
ZONA SEGURA
Lector
140
Lector
140
Teléfono móvil
110
Lector
140

Figura 2

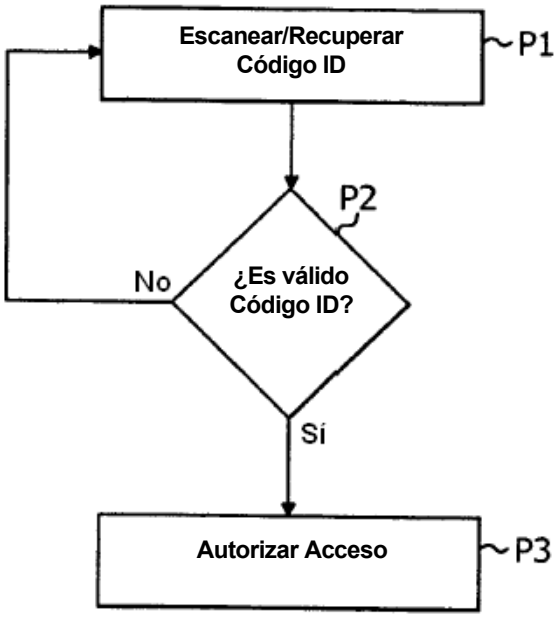
Escanear/Recuperar
Código ID
P1
P2
No
¿Es válido
Código ID?
Sí
Autorizar Acceso
P3

Figura 3

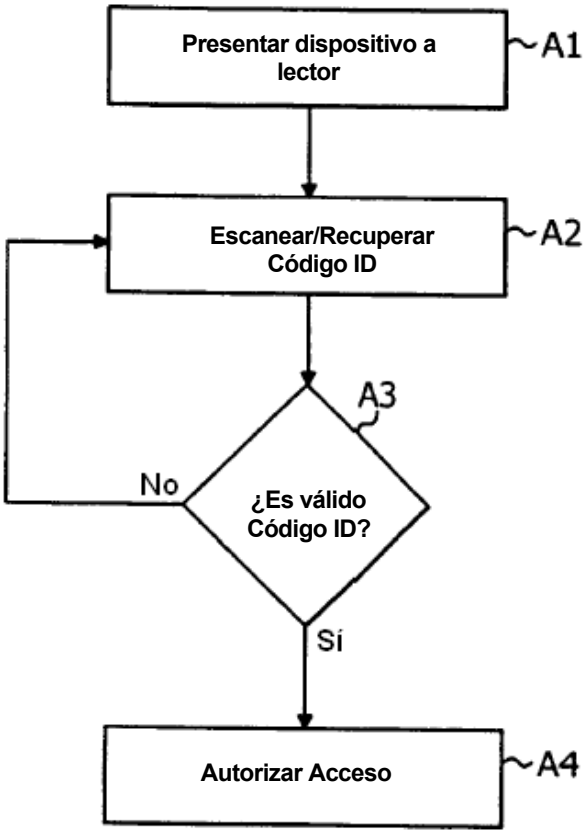
Presentar dispositivo a lector
A1
Escanear/Recuperar Código ID
A2
A3
No
¿Es válido Código ID?
Sí
Autorizar Acceso
A4

Figura 4