

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 720 474**

51 Int. Cl.:

**G07C 9/00** (2006.01)

**H04L 29/08** (2006.01)

**H04L 29/06** (2006.01)

12

## TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **02.04.2015** **E 15248002 (6)**

97 Fecha y número de publicación de la concesión europea: **20.02.2019** **EP 2933783**

54 Título: **Sistema y método para acceder a un sistema de seguridad para usuarios temporales mediante el uso de una aplicación móvil**

30 Prioridad:

**18.04.2014 US 201414256010**

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

**22.07.2019**

73 Titular/es:

**HONEYWELL INTERNATIONAL INC. (100.0%)  
115 Tabor Road  
Morris Plains, NJ 07950, US**

72 Inventor/es:

**KURUBA, SUHASINI;  
M, SHANMUGA PRABHU y  
PV, HEMANTH**

74 Agente/Representante:

**LEHMANN NOVO, María Isabel**

ES 2 720 474 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Sistema y método para acceder a un sistema de seguridad para usuarios temporales mediante el uso de una aplicación móvil.

Campo

- 5 La presente solicitud se refiere a sistemas de seguridad y, más concretamente, a métodos de acceso a sistemas de seguridad.

Antecedentes

- 10 Se conocen sistemas para la protección de áreas aseguradas. Dichos sistemas normalmente incluyen uno o más sensores que detectan amenazas dentro del área asegurada. Una alarma audible local puede también proveerse para notificar a los ocupantes presentes dentro del área asegurada sobre amenazas detectadas.

Las amenazas detectadas por dichos sistemas pueden incluir cualquier episodio que amenace la salud y/o seguridad de ocupantes humanos o bienes. Un ejemplo de una amenaza a ocupantes humanos puede incluir gas tóxico. Otras amenazas a la seguridad de ocupantes y/o bienes pueden incluir fuego, explosión o intrusos no autorizados.

- 15 En general, un sistema de seguridad puede incluir un panel de control que monitorea cada uno de los sensores dentro del área asegurada. Donde el sistema de seguridad se usa dentro de un hogar, el panel de control puede incluir un número de estados operacionales incluidos activado en modo ausente, desactivado, activado en modo presente, etc. Una interfaz de usuario puede ubicarse dentro del área asegurada y usarse por un ocupante del área asegurada para seleccionar, de manera individual, cada uno de los estados operacionales.

- 20 En cada uno de los estados, un procesador del panel de control puede monitorear un conjunto respectivo de sensores para la activación. Después de la activación de cualquiera de los sensores, el procesador puede enviar un mensaje de alarma a una estación de monitoreo central.

- 25 Mientras dichos sistemas funcionan bien, estos no son muy flexibles. Por ejemplo, si una persona que realiza reparaciones debe entrar en el hogar de una persona, entonces la persona debe desactivar la alarma y dejar el hogar sin protección durante una visita. De manera alternativa, la persona debe dar a la persona que realiza reparaciones su código de acceso. Sin embargo, ello deja a la persona vulnerable si la persona que realiza reparaciones provee, más tarde, el código de acceso a un delincuente. Por consiguiente, existe la necesidad de métodos más flexibles y seguros para controlar los sistemas de seguridad.

- 30 La Solicitud de Patente de Estados Unidos 2012/0077431 A1, 29 de marzo de 2012, FYKE y otros, describe un sistema de seguridad que puede incluir un dispositivo de comunicación inalámbrica móvil configurado para recibir un código de seguridad de un sensor NFC o receptor inalámbrico.

La Patente de Estados Unidos 4532507, 30 de julio de 1985, Edson y otros, describe un sistema de seguridad con una memoria borrrable que puede programarse con un código de acceso temporal después de la entrada de un código de acceso de orden más alto por la persona que establece el código de acceso temporal.

- 35 La Solicitud de Patente Europea 1154365A1 provee un método para la entrega de bienes encargados a una ubicación segura, mediante la generación de un código de seguridad en el momento de encargar los bienes. El código de seguridad se comunica al encargado de la entrega de los bienes y puede ser válido para una entrega solamente.

Compendio de la invención

- 40 La presente invención provee un método según se define en la reivindicación 1. El método puede incluir las características de una o más de las reivindicaciones dependientes 2 a 10.

La presente invención también provee un sistema según se define en la reivindicación 11. El sistema puede incluir las características de una o más de las reivindicaciones dependientes 12 a 15.

Breve descripción de los dibujos

- 45 La Figura 1 ilustra un diagrama de bloques de un sistema de seguridad según la presente memoria;  
la Figura 2 representa un conjunto de etapas del proceso que pueden usarse por el sistema de la Figura 1;  
la Figura 3 representa una pantalla que el sistema de la Figura 1 puede mostrar en un dispositivo móvil; y

la Figura 4 representa un mensaje que puede mostrarse en el dispositivo móvil de un receptor de una contraseña temporal.

#### Descripción detallada

5 Mientras las realizaciones descritas pueden tomar muchas formas diferentes, realizaciones específicas de aquellas se muestran en los dibujos y se describirán en la presente memoria en detalle en el entendimiento de que la presente descripción se considerará una ejemplificación de los principios de aquellas, así como del mejor modo de practicarlas, y no pretende limitar la aplicación o reivindicaciones a la realización específica ilustrada.

10 La Figura 1 es un diagrama de bloques simplificado de un sistema de seguridad 10 que se muestra, en general, según una realización ilustrada. El sistema de seguridad puede incluir un número de sensores 12, 14 que detectan amenazas dentro de un área asegurada (p.ej., un hogar, un negocio, etc.) 16.

Los sensores pueden basarse en cualquiera de un número de diferentes técnicas de detección. Por ejemplo, al menos algunos de los sensores pueden ser interruptores de final de carrera colocados en las puertas y ventanas que proveen acceso a y salen del área asegurada. Otros sensores pueden ser detectores de fuego y/o humo que detectan amenazas ambientales.

15 Los sensores pueden monitorearse por un panel de control de alarma 18. El panel de control puede ubicarse dentro del área asegurada, como se muestra en la Figura 1, o puede ubicarse remotamente del área asegurada. Tras detectar la activación de uno de los sensores, el panel de control puede componer y enviar un mensaje de alarma a una estación de monitoreo central 20. El mensaje de alarma puede incluir un identificador del sistema de alarma (p.ej., número de cuenta, dirección, etc.), un identificador del sensor, el tipo de sensor y un tiempo). La estación de monitoreo central puede decodificar el mensaje de alarma y responder mediante la convocatoria de la ayuda apropiada (p.ej., policía, departamento de bomberos, etc.).

El sistema de alarma puede también incluir una interfaz de usuario 32. La interfaz de usuario puede usarse por un usuario autorizado para activar y desactivar el sistema de seguridad.

25 La interfaz de usuario puede incluir una visualización 34 y un teclado 36. De manera alternativa, la interfaz de usuario puede usar una pantalla táctil que combina las funciones de visualización y teclado.

El sistema de alarma puede también adaptarse para aceptar instrucciones de un número de dispositivos inalámbricos portátiles 38, 40. Los dispositivos inalámbricos portátiles pueden interactuar con el panel de control mediante Internet 42.

30 Ubicados dentro del panel de alarma y dispositivos portátiles puede haber uno o más aparatos de procesador (procesadores) 22, 24, cada uno operando bajo control de uno o más programas de ordenador 26, 28, cargados desde un medio legible por ordenador no transitorio (memoria) 30. Según su uso en la presente memoria, la referencia a una etapa llevada a cabo por un programa de ordenador también es una referencia al procesador que ha ejecutado dicha etapa.

35 Durante la operación normal, un procesador de estado del panel de alarma puede monitorear la interfaz de usuario para instrucciones de control. Por ejemplo, un usuario autorizado puede ingresar un número de identificación personal (PIN, por sus siglas en inglés) seguido de la activación de una tecla de función para cambiar un estado de monitoreo del sistema de alarma. Mediante el ingreso de un número PIN seguido por la activación de una alarma en modo ausente, el usuario puede activar el sistema de alarma durante períodos mientras el usuario está lejos del hogar. En respuesta, un procesador de alarma puede monitorear cada uno de los sensores para la activación e

40 informar episodios a la estación de monitoreo central. Después de regresar al hogar, el usuario puede ingresar su PIN seguido por la activación de la tecla de desactivación para desactivar el sistema.

De manera alternativa, el usuario puede activar la tecla de alarma en modo presente mientras el usuario está en el hogar. En el modo activado en modo presente, el procesador de alarma puede activar sensores de fuego y sensores de intrusión solamente a lo largo de una periferia del hogar.

45 En este aspecto, un procesador de interfaz gráfica de usuario (GUI, por sus siglas en inglés) puede proveer una interfaz entre la interfaz de usuario y el panel de alarma. Por ejemplo, el procesador GUI puede presentar un icono que representa cada uno de los aspectos funcionales del sistema de alarma (p.ej., activar, desactivar, alarma en modo ausente, etc.) en la interfaz de usuario. Tras activar una de las teclas de función, dicho procesador GUI puede mostrar una ventana que solicita el ingreso de un PIN. Después de ingresar la información de identificación correcta,

50 el procesador GUI puede activar o desactivar el procesador de alarma.

El procesador GUI puede también presentar uno o más iconos que activan y desactivan, de manera selectiva, porciones del área asegurada. Por ejemplo, el área asegurada puede incluir un número de porciones o subáreas diferentes 42, 44, 46. Dichas áreas pueden protegerse, de manera separada, mediante la activación del icono apropiado.

El procesador GUI puede también proveer una interfaz entre el panel de alarma y un dispositivo portátil (p.ej., dispositivo 38) de un usuario autorizado. En este aspecto, un procesador GUI correspondiente dentro del dispositivo portátil puede proveer una interfaz de una visualización del dispositivo portátil que emula la visualización en la interfaz de usuario dentro del área asegurada.

- 5 Bajo una realización ilustrada, el dispositivo inalámbrico portátil de usuario autorizado puede también incluir una función de contraseña temporal que permite al usuario autorizado otorgar contraseñas temporales para su uso por otras personas a quienes, de lo contrario, no se les otorgaría acceso al área asegurada sin activar una alarma. Por ejemplo, si el usuario autorizado es el propietario de la casa, entonces será conveniente si el usuario pudiera otorgar contraseñas temporales que puedan usarse por un fontanero para llevar a cabo reparaciones de emergencia dentro del hogar del propietario. También será conveniente si las contraseñas pueden transmitirse de forma automática a la otra persona en una manera segura con un número de restricciones de uso.

La Figura 2 representa un ejemplo del uso de la función de contraseña temporal bajo una realización ilustrada. Según se muestra, un invitado puede llegar al umbral de la puerta de un propietario y el propietario puede no querer compartir su código de uso. En respuesta, el usuario puede activar una función de contraseña temporal en su dispositivo portátil (p.ej., teléfono inteligente) que automáticamente genera una contraseña temporal. La contraseña se transfiere automáticamente al panel de alarma y al dispositivo portátil (p.ej., dispositivo 40) del invitado.

En este aspecto, el usuario puede activar un icono de contraseña temporal en su dispositivo portátil. En respuesta, un procesador de contraseñas puede confirmar la identidad del usuario y operar para crear una contraseña temporal para su uso por otra persona con un conjunto apropiado de restricciones al uso.

- 20 La Figura 3 representa una ventana interactiva 100 que el procesador de contraseñas puede presentar en la visualización del dispositivo portátil. En este aspecto, el usuario puede ingresar el nombre de la otra persona en una primera ventana 102 y un número telefónico del otro dispositivo portátil en una segunda ventana 104.

Si el intento es un primer intento para un usuario, entonces se pedirá al usuario que provea la dirección del área asegurada en una ventana de dirección 108. De lo contrario, la dirección del hogar puede recuperarse de un archivo de información por defecto 48 dentro del panel de alarma o dentro del dispositivo portátil.

También puede solicitarse al usuario que provea un tiempo inicial para la contraseña temporal en una ventana de tiempo inicial 110 y un tiempo final para la contraseña en una ventana de tiempo final 112. Si el usuario no ingresa un tiempo en la ventana de tiempo inicial, entonces el procesador puede usar un tiempo y fecha actuales como un valor por defecto.

- 30 También puede solicitarse al usuario que ingrese un número máximo de desactivaciones que se permitirán para la contraseña temporal. Si el invitado solo tiene motivos para entrar en las instalaciones una vez por día, entonces el número máximo de desactivaciones puede ser igual al número de días antes de la fecha de expiración.

Si solo se permite que el invitado entre en parte del área asegurada, entonces el usuario activará una tecla multifunción de acceso de partición 118. En respuesta, un conjunto de identificadores de porciones del área asegurada se presentará en un menú. Ello puede ser importante en el caso donde el invitado es un contratista a quien solo se le permitirá trabajar en la cocina de una casa. En el presente caso, solo la puerta frontal de la casa puede desactivarse mientras los detectores de movimiento en las áreas de habitaciones o un sótano permanecerán activos.

- 40 De manera similar, el acceso remoto no se permitirá normalmente mediante otro botón de casilla de verificación (botón pulsador) 116. Este el caso debido a que no se permitirá que un invitado desactive, de manera remota, el sistema de seguridad mediante el uso de una aplicación web o una aplicación móvil. Nuevamente, depende del usuario autorizado permitir o no permitir esta opción.

En general, uno o más procesadores dentro del dispositivo portátil del usuario autorizado proveerán la función de contraseña temporal. Bajo una realización, el procesador de contraseñas puede ubicarse dentro del panel de alarma y el acceso puede proveerse a través del procesador GUI. De manera alternativa, los procesadores de la función de contraseña temporal pueden compartirse entre el panel de alarma y el dispositivo portátil del usuario autorizado. Por ejemplo, la contraseña temporal puede generarse dentro del procesador de alarma por un procesador de generador de número aleatorio y transferirse al dispositivo portátil. De lo contrario, la contraseña temporal puede generarse dentro del dispositivo portátil y transferirse al panel de alarma.

- 50 En cualquier caso, una vez que la contraseña temporal y las limitaciones de uso se hayan provisto, el usuario autorizado puede activar un botón de guardar y enviar 120. En respuesta, el procesador de contraseñas puede componer un mensaje que incorpora la información en un formato apropiado (p.ej., SMS) y enviar el mensaje al dispositivo portátil del otro usuario y al panel de alarma en el caso donde la contraseña se genera, de manera independiente, dentro del dispositivo portátil.

La Figura 4 es un ejemplo del mensaje de contraseña temporal que puede entregarse al otro usuario bajo la realización. Según se muestra, el mensaje puede incluir el nombre de la otra persona, la contraseña, la dirección del área asegurada, el tiempo de inicio y expiración de la contraseña temporal y el número máximo de veces que el sistema puede desactivarse.

- 5 En general, el sistema de contraseña temporal ofrece un número de ventajas. En primer lugar, el sistema genera automáticamente un código de usuario válido (contraseña) con una fecha y hora de expiración válidas. En segundo lugar, el usuario autorizado tiene la opción de otorgar o denegar el permiso de acceso remoto. Normalmente, el usuario no otorgará permiso para el acceso remoto.

- 10 En tercer lugar, el usuario puede colocar una restricción en el número de desactivaciones. Ello puede ser importante para un contratista que promete llevar a cabo cierto proyecto particular pero no sabe cuándo podrá hacerlo. Si el contratista indica que puede realizar el proyecto en un solo día, entonces el usuario puede establecer el número máximo de desactivaciones en 1. Dado que el procesador de estado del sistema de alarma guarda la hora y fecha de cada uso de la contraseña temporal, el sistema de alarma provee evidencias de cuándo se ha llevado a cabo el trabajo.

- 15 En cuarto lugar, el sistema tiene la capacidad de añadir automáticamente detalles de usuario existentes como, por ejemplo, el nombre o número de teléfono móvil de un vendedor frecuentemente usado de la lista de contactos del móvil. El usuario puede acceder a la lista de contactos mediante la activación de un botón de lista de contactos 122 en la visualización y seleccionar uno de los contactos.

- 20 En quinto lugar, la dirección para el uso de la contraseña temporal puede ser un valor por defecto. El usuario puede cambiar la dirección por defecto si tiene otro hogar (vacacional) con un sistema de seguridad y desea otorgar acceso al segundo hogar.

En sexto lugar, la contraseña temporal se envía automáticamente al otro usuario. Ello evita errores en la transcripción.

- 25 Finalmente, el panel de alarma y sistema pueden activarse automáticamente según el uso de la contraseña temporal y al final de la fecha y hora de expiración. Ello puede ser importante donde solo se permite al invitado acceder durante horas diurnas. Ello permite al sistema de seguridad activarse automáticamente al anochecer después de la expiración de la contraseña para el día.

- 30 En general, el sistema incluye un dispositivo inalámbrico móvil de una persona autorizada que recibe un identificador de otra persona a quien se le otorgará acceso temporal a un área geográfica asegurada de la persona autorizada por un sistema de seguridad de la persona autorizada, un procesador del dispositivo móvil o sistema de seguridad que genera un código de acceso temporal que se usará por la otra persona para poder entrar en el área asegurada y el dispositivo móvil de la persona autorizada que transfiere la contraseña temporal a un dispositivo inalámbrico móvil de la otra persona.

- 35 El sistema puede también incluir un dispositivo inalámbrico móvil de una persona autorizada con una interfaz de usuario que recibe un identificador de otra persona a quien se le otorgará acceso temporal a un área geográfica asegurada de la persona autorizada por un sistema de seguridad de la persona autorizada, un procesador del dispositivo móvil o sistema de seguridad que genera un código de acceso temporal que se usará por la otra persona para poder entrar en el área asegurada y el dispositivo móvil de la persona autorizada que transfiere la contraseña temporal a un dispositivo inalámbrico móvil de la otra persona.

- 40 El sistema puede también incluir un sistema de seguridad que protege un área geográfica segura, un dispositivo inalámbrico móvil de una persona autorizada que se acopla al sistema de seguridad, el dispositivo móvil recibe un identificador de otra persona a través de una interfaz de usuario del dispositivo inalámbrico a quien se le otorgará acceso temporal al área geográfica asegurada de la persona autorizada por un sistema de seguridad de la persona autorizada, un procesador del dispositivo móvil o sistema de seguridad que genera un código de acceso temporal que se usará por la otra persona para poder entrar en el área asegurada y un procesador del dispositivo móvil de la persona autorizada que transfiere la contraseña temporal a un dispositivo inalámbrico móvil de la otra persona junto con un conjunto de limitaciones donde el conjunto de limitaciones además incluye uno o más de una fecha y hora de inicio, una fecha y hora de fin y un número máximo de episodios de desactivación.

- 50 A partir de lo anterior, se observará que numerosas variaciones y modificaciones pueden llevarse a cabo sin apartarse del espíritu y alcance de la presente memoria. Se comprenderá que ninguna limitación con respecto al aparato específico ilustrado en la presente memoria se pretende o debe inferirse. Por supuesto, se pretende cubrir por las reivindicaciones anexas todas las modificaciones que caigan dentro del alcance de las reivindicaciones. Además, los flujos lógicos representados en las figuras no requieren el orden particular, u orden secuencial, que se muestra para lograr resultados deseables. Otras etapas pueden proveerse, o etapas pueden eliminarse, de los flujos descritos, y otros componentes pueden añadirse a, o eliminarse de, las realizaciones descritas.

- 55

## REIVINDICACIONES

1. Un método que comprende:

un primer dispositivo inalámbrico portátil (38) de una persona autorizada que recibe un identificador de una persona a quien se le otorgará acceso temporal a un área asegurada (16) por un sistema de seguridad (10);

5 con capacidad de respuesta a la recepción del identificador y activación de un icono de contraseña temporal que se muestra en una visualización de interfaz del primer dispositivo inalámbrico portátil (38), el primer dispositivo inalámbrico portátil (38) generando un código de acceso temporal que se usará para poder entrar en el área asegurada;

10 el primer dispositivo inalámbrico portátil (38) transfiriendo el código de acceso temporal a un segundo dispositivo inalámbrico portátil (40) asociado a la persona a quien se le otorgará el acceso temporal y transfiriendo el código de acceso temporal a un panel de alarma del sistema de seguridad (10).

2. El método según la reivindicación 1 que además comprende el primer dispositivo inalámbrico portátil (38) que transfiere una dirección de hogar del área asegurada al segundo dispositivo inalámbrico portátil (40).

15 3. El método según la reivindicación 1 que además comprende el primer dispositivo inalámbrico portátil (38) que transfiere un conjunto de limitaciones de uso asociadas al uso del código de acceso temporal al panel de alarma.

4. El método según la reivindicación 1 que además comprende un procesador del sistema de seguridad que limita el uso del código de acceso temporal según un parámetro predeterminado.

5. El método según la reivindicación 4 que además comprende recibir una entrada de usuario indicativa del parámetro predeterminado en el primer dispositivo inalámbrico portátil (38).

20 6. El método según la reivindicación 4 que además comprende recuperar un valor por defecto del parámetro predeterminado de una memoria.

7. El método según la reivindicación 4 en donde el parámetro predeterminado incluye una fecha y hora de inicio y una fecha y hora de fin que limitan el uso del código de acceso temporal.

25 8. El método según la reivindicación 4 en donde el parámetro predeterminado incluye un número máximo de desactivaciones permitidas para el uso del código de acceso temporal.

9. El método según la reivindicación 1 que además comprende limitar el uso del código de acceso temporal a una porción predeterminada del área asegurada mediante la desactivación, de manera selectiva, de un subconjunto de sensores acoplados al sistema de seguridad.

30 10. El método según la reivindicación 1 que además comprende el primer dispositivo inalámbrico portátil (38) que transfiere un conjunto de limitaciones de uso al segundo dispositivo inalámbrico portátil (40), en donde el conjunto de limitaciones de uso incluye uno o más de una fecha y hora de inicio, una fecha y hora de fin, y un número máximo de episodios de desactivación.

11. Un aparato que comprende:

35 un primer dispositivo inalámbrico portátil (38) de un usuario autorizado configurado para recibir un identificador de una persona a quien se le otorgará acceso temporal a un área asegurada (16) por un sistema de seguridad (10),

en donde, con capacidad de respuesta a la recepción del identificador y activación de un icono de contraseña temporal que se muestra en una visualización de interfaz del primer dispositivo inalámbrico portátil (38), el primer dispositivo inalámbrico portátil se configura para generar un código de acceso temporal que se usará para poder entrar en el área asegurada, y

40 en donde el primer dispositivo inalámbrico portátil se configura para transferir el código de acceso temporal a un segundo dispositivo inalámbrico portátil (40) asociado a la persona a quien se le otorgará el acceso temporal y transfiere el código de acceso temporal a un panel de alarma del sistema de seguridad (10).

45 12. El aparato según la reivindicación 11, en donde el primer dispositivo inalámbrico portátil (38) se configura para transferir una dirección del hogar del área asegurada y un conjunto de limitaciones de uso del código de acceso temporal al segundo dispositivo inalámbrico portátil.

13. El aparato según la reivindicación 11, en donde el primer dispositivo inalámbrico portátil (38) se configura para transferir un conjunto de limitaciones de uso del código de acceso temporal al panel de alarma.

14. El aparato según la reivindicación 13, en donde el primer dispositivo inalámbrico portátil (38) se configura para recibir el conjunto de limitaciones de un usuario.

15. El aparato según la reivindicación 13, en donde el primer dispositivo inalámbrico portátil (38) se configura para recuperar valores por defecto para el conjunto de limitaciones de un archivo dentro de una memoria (30).

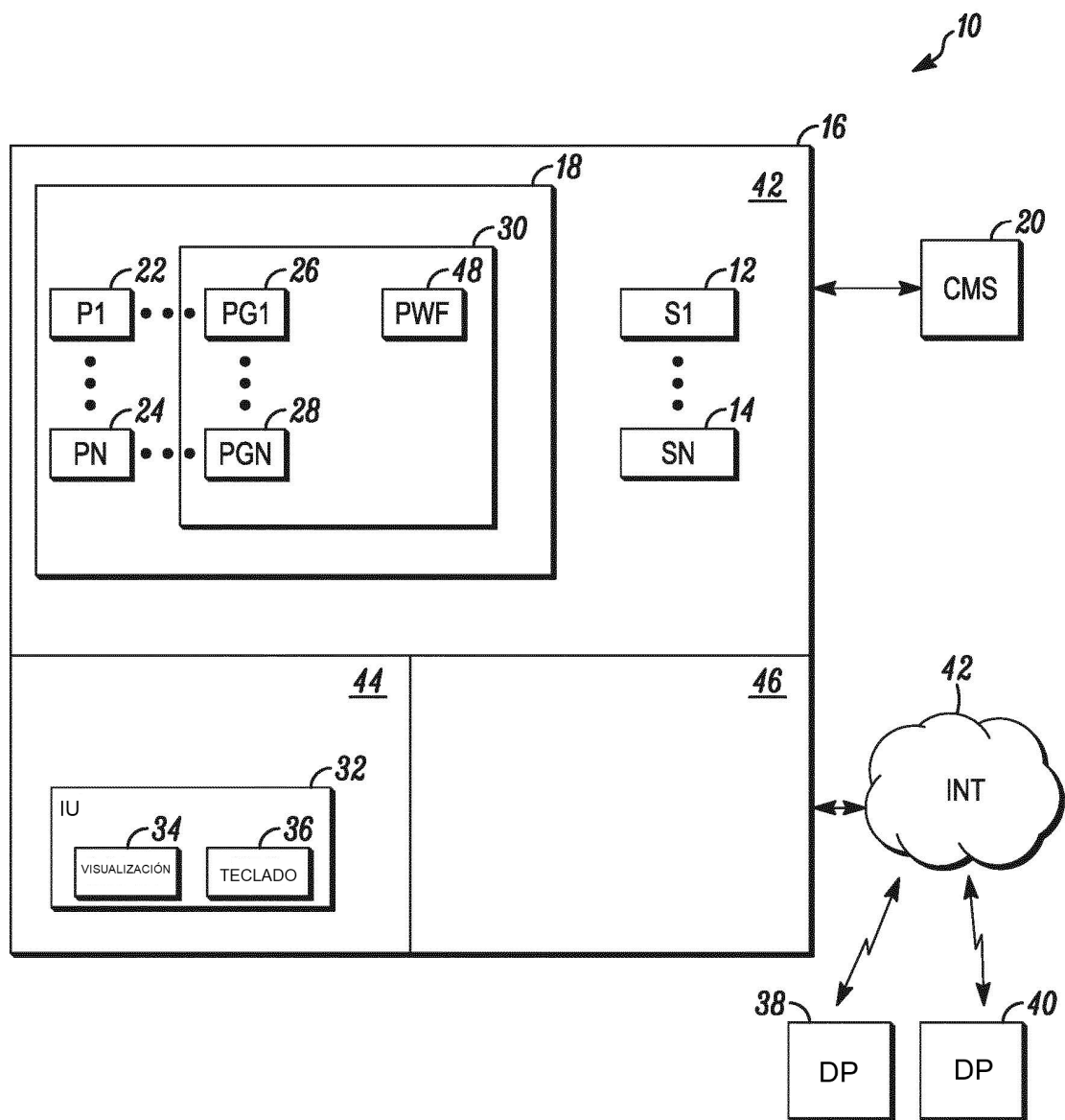


FIG. 1

Solución Implementada

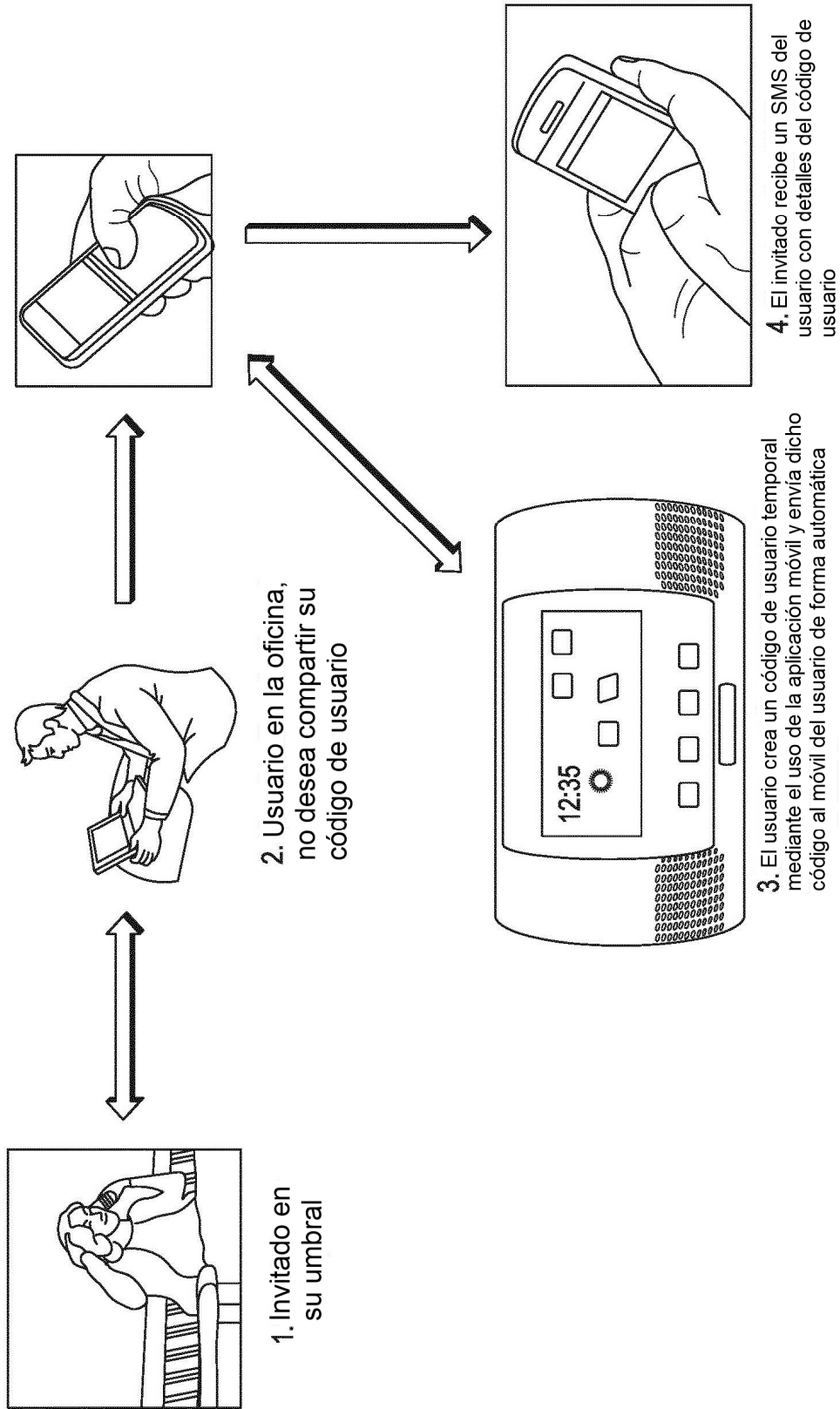


FIG. 2

Interfaz de usuario de aplicación móvil propuesta

- Pantalla de creación de usuario temporal para acceder/limitar el sistema de seguridad:

100

Nombre 102 JOHN K

Código de usuario 106 5678

Número de móvil 104 96327941799

Dirección del hogar 108 H. No 44, 1st main, M.G. Road, Bangalore

Contactos 122

Automático

Fecha & hora de inicio de expiración 110 01/11/2013 09:00 AM

Fecha & hora de fin de expiración 112 15/11/2013 07:30 PM

Número de Desactivaciones 114 10

Acceso Remoto 116

Acceso de Partición 118 P1

120 Guardar & Enviar Mensaje

- Provisión para tomar automáticamente el Nombre, Número de Móvil de los contactos en el móvil
- Dirección del hogar una vez establecida se habilitará por defecto
- Por defecto, la fecha de inicio de expiración serán la fecha y hora actuales

FIG. 3

### Mensaje al usuario de aplicación de móvil propuesto

- Mensaje enviado al móvil de usuario del Invitado de la siguiente manera:

200

|                                                           |                                             |
|-----------------------------------------------------------|---------------------------------------------|
| Nombre                                                    | :JOHN                                       |
| Código de Usuario                                         | :5678                                       |
| Dirección del Hogar                                       | :H. No 44, 1st main<br>M.G. Road, Bangalore |
| Fecha & hora de inicio de expiración de código de usuario | : 01/11/2013 09:00 AM                       |
| Fecha & hora de fin de expiración de código de usuario    | : 15/11/2013 07:30 PM                       |
| Número de Desactivaciones permitidas                      | :10                                         |

**FIG. 4**