

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 737 648**

21 Número de solicitud: 201800163

51 Int. Cl.:

G06F 1/26

(2006.01)

12

SOLICITUD DE PATENTE

A1

22 Fecha de presentación:

13.07.2018

43 Fecha de publicación de la solicitud:

15.01.2020

71 Solicitantes:

SMARTCITY URBISENS, S.L. (100.0%)
Ctra. N 550, Km 78 s/n
15890 Padrón (A Coruña) ES

72 Inventor/es:

GARCIA FERNÁNDEZ, Iván;
GARCÍA FERNÁNDEZ, Damián y
ABAL MARTÍNEZ, Francisco Javier

74 Agente/Representante:

HERRERA DÁVILA, Álvaro

54 Título: **Puerto de comunicaciones para dispositivos electrónicos con identificación y autenticación**

57 Resumen:

Puerto de comunicaciones para dispositivos electrónicos con identificación y autenticación. Constituido a partir de dos líneas de alimentación eléctrica, donde una de ellas es constante y la otra puede presentar o no energía según sea necesario, comunicación serie, identificador único para cada dispositivo y sistema de verificación de la identidad del dispositivo al que está conectado.

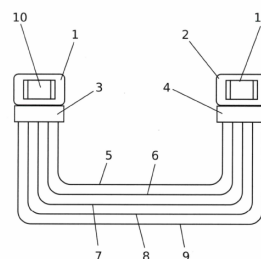


FIG 1

DESCRIPCIÓN

Puerto de comunicaciones para dispositivos electrónicos con identificación y autenticación.

5 Objeto de la invención

La presente invención se refiere a un puerto de comunicaciones cuyo objetivo es facilitar el desarrollo de productos para su aplicación en el mercado del Internet de las cosas y especialmente las SmartCities.

10 La transformación digital de las urbes es uno de los retos principales de los gobiernos a nivel mundial; como consecuencia directa de este reto, nace el concepto de Ciudades Inteligentes (Smart Cities) que engloba a varias industrias esenciales para las urbes. Entre estas son destacables el transporte, la gestión de residuos, la e-Sanidad o la gestión energética entre
15 otros.

Todos ellos son servicios cuya digitalización permitirá generar modelos de previsión mucho más eficaces a la hora de gestionar las ciudades. Esto dará cobertura universal a los ciudadanos con mejores herramientas y en un menor tiempo.

20 La importancia que adquirirán las Ciudades Inteligentes en los próximos años, está ligada a la revolución tecnológica actual del Internet de las cosas (IoT, por sus siglas en inglés). Este es un concepto todavía difuso para los consumidores tradicionales, pero que juega un papel clave en la recogida y digitalización de los datos que sirven de base a los modelos de gestión
25 eficientes.

No sólo la digitalización de las ciudades supone un reto tecnológico a corto plazo, sino que la mejora de gestión que conlleva debe aplicarse a campos tan diversos como la vivienda, agricultura, o industria. Y es en estos campos donde el IoT ofrece ya soluciones como las
30 Casas inteligentes (Smart Home), Agricultura inteligente (Smart Agriculture), o la industria 4.0.

En el proceso de digitalización en la gestión de ciudades, viviendas, industria o agricultura, se requiere que se provean de medios para capturar datos del mundo real (sensores) y de modos de actuar sobre este (actuadores).

35 Actualmente, sólo el 1% de todas las herramientas, productos o servicios inventados están conectados a Internet, pero debido a la creciente necesidad de digitalización, el número de sensores y actuadores será cada día mayor. Según las estimaciones de Cisco en el año 2020 el 40% de los datos procederán de sensores, generando un mercado valorado en 14,5 billones.

40 Las previsiones sobre el crecimiento demográfico y la emigración a las ciudades, imponen que la digitalización de ciudades, industrias y viviendas deben realizarse de una forma rápida. A pesar de ello las grandes multinacionales que mueven la evolución tecnológica del mundo generan sólo un 20% de innovación por cada 80% de operación.

45 En contraposición, las pequeñas empresas y desarrolladores independientes tienen un gran margen de maniobra y facilidades de innovación rápida. A pesar de ello y debido a las barreras de entrada en el mercado, su aportación al proceso de digitalización se ve fuertemente obstaculizado. Entre las barreras de entrada más importantes destacan los elevados costes del desarrollo de soluciones completas, el alto grado de especialización necesario en áreas
50 tecnológicas diversas y la dificultad para conseguir vías de comercialización adecuadas.

Las consecuencias directas que estas barreras de entrada provocan al mercado son la pérdida de talento, oportunidades y dinamismo. El reto que las urbes afrontan en un futuro cercano requiere de innovación y crecimiento rápidos, por lo que este talento no debe desaprovecharse.

5 La presente invención está diseñada para suplir las necesidades de desarrollo de productos IoT, y sus ventajas son las siguientes:

- Reduce el consumo global de la electrónica necesaria para una determinada aplicación al poder apagar componentes de la misma.

10

- Permite identificar a todos los componentes de una instalación.

- Asegura la identidad de los dispositivos conectados, aportando seguridad.

15

- Puede fabricarse con componentes actualmente existentes en el mercado.

- Las tecnologías usadas como base están plenamente probadas y validadas en el mercado.

20 La aplicación industrial de esta invención se encuentra dentro del sector de diseño y fabricación de dispositivos electrónicos, y más concretamente dispositivos electrónicos con tasa de transferencia de datos moderada/baja para los sectores de IoT, SmartCities, domótica, seguridad, control logístico y automoción.

25 **Antecedentes de la invención**

Aunque no se ha encontrado ninguna invención idéntica a la descrita, exponemos a continuación los documentos encontrados que reflejan el estado de la técnica relacionado con la misma.

30

Así el documento ES2468690A1 se refiere a un método, dispositivo, sistema y producto informático para la distribución física de contenidos digitales que comprende las etapas de identificar a un usuario en un sistema integrado de gestión a través de un código unívoco de identificación de un dispositivo móvil; seleccionar los contenidos digitales en una plataforma de contenidos digitales a través de un dispositivo de distribución de contenidos digitales; generar al menos un código de descarga que incluye un código único de descarga asociado con un único contenido y el código unívoco de identificación del dispositivo móvil de usuario identificado; y descargar el contenido digital seleccionado en el dispositivo móvil de usuario. La citada invención hace alusión a la necesidad de identificación de un usuario a través de un código de un dispositivo móvil, mientras que la invención de la patente principal manifiesta la comunicación entre dispositivos de cualquier tipo.

35

40

45

50

EP1174158A1 describe una estación de origen que comprende medios para difundir un programa difundido a al menos una pluralidad de grupos de estaciones de destino; que la estación de origen comprende, además, medios para enviar un primer parámetro de periodo de registro a un primer grupo de estaciones de destino, en la cual el primer parámetros de periodo de registro especifica un primer periodo durante el cual el primer grupo de estaciones de destino se deben registrar para el programa difundido en la estación de origen, y en la cual cualesquiera intentos de solicitudes de registro que se produzcan fuera del primer periodo se bloquean. La invención principal, a diferencia de la citada, se fundamenta en la interacción entre dos dispositivos para el intercambio de alimentación eléctrica y datos a través de un conjunto mínimo de conexiones.

ES2634332B1 se refiere a un dispositivo para la gestión segura de evidencias electrónicas con credenciales vinculantes (testigo digital) sobre el que el usuario u objeto que obtiene, genera o recibe evidencias delega su identidad de forma vinculante e insoluble mediante credenciales vinculantes, y caracterizado por que comprende: a. Un gestor de operaciones entre el usuario u objeto y el dispositivo, responsable de establecer las políticas que relacionan al usuario u objeto con el objetivo y que permite vincular la identidad de un usuario u objeto con su dispositivo generándose al menos una credencial vinculante; b. un núcleo de confianza, responsable de asegurar la integridad de la evidencia electrónica, impedir el acceso no autorizado y permitir su transferencia a una entidad autorizada, y que comprende a su vez: mecanismos criptográficos aceptados dentro de un elemento seguro (chip hw, anti-tampering) para establecer un canal de comunicaciones seguro; y medios de almacenamiento seguro con control de acceso, protegidos en un elemento seguro (puede ser el mismo elemento seguro que el que contiene los mecanismos criptográficos u otro distinto), para almacenar claves y otros datos protegidos, por ejemplo los hashes de las evidencias electrónicas y las credenciales vinculantes; y c. un gestor de evidencias electrónicas para objetos, que coordina las operaciones (y establece las políticas a aplicar sobre dichas operaciones) de adquisición o generación de evidencias electrónicas, almacenamiento seguro, transferencia de la evidencia electrónica a otro testigo de la cadena, y, en su caso, de borrado o eliminación de evidencias. La citada invención tiene como finalidad la mitigación de los efectos de la ciberdelincuencia, campo distinto al de la patente principal.

Conclusiones: Como se desprende de la investigación realizada, ninguno de los documentos encontrados soluciona los problemas planteados como lo hace la invención propuesta.

25 Descripción de la invención

El puerto de comunicaciones para dispositivos electrónicos con identificación y autenticación objeto de la presente invención se constituye para la interconexión de dos o más dispositivos que intercambian alimentación eléctrica y datos a través de un conjunto mínimo de hilos.

Se definen tres roles en la comunicación a través de este puerto: controlador, gestor y esclavo.

El controlador decide sobre las necesidades de alimentación del puerto.

El gestor gobierna al esclavo e interpreta sus mensajes y peticiones.

Y el esclavo atiende las peticiones del gestor, pudiendo tomar la iniciativa de la comunicación cuando el gestor se lo permita o por medio de interrupciones.

Se definen dos tipos de alimentación en el puerto. Una de estas es constante y la otra, denominada "alimentación controlada", se activa en función de los requerimientos de la aplicación y las necesidades que el esclavo transmita.

El intercambio de mensajes entre el gestor y el esclavo se realiza en serie y de forma asíncrona usando los hilos TX y RX. Estos responden a la especificación USART, universalmente aceptada para comunicaciones serie entre dispositivos, aunque no es limitativa.

Cada uno de los dispositivos tiene una cadena de datos que identifica al fabricante modelo y número de serie. Con esta cadena los dos dispositivos se identifican mutuamente.

La identidad de cada dispositivo podrá comprobarse usando el módulo de verificación de identidad. Si el resultado de ese control es positivo, los dos dispositivos podrán comunicarse con confianza en su interlocutor.

La conexión entre los dispositivos se inicia intercambiando mensajes de identificación, verificación y parámetros de funcionamiento. Tras lo cual, pueden enviar mensajes del dominio de su aplicación.

5 Breve descripción de los dibujos

Para una mejor comprensión de la presente descripción se acompañan unos dibujos que representan una realización preferente de la presente invención:

10 Figura 1: Vista esquemática de la interconexión de dos dispositivos usando el puerto de comunicaciones objeto de la presente invención.

Las referencias numéricas que aparecen en dichas figuras corresponden a los siguientes elementos constitutivos de la invención:

15

1. Dispositivo 1

2. Dispositivo 2

20

3. Conector para el dispositivo 1

4. Conector para el dispositivo 2

25

5. Hilo de comunicaciones con alimentación continua

6. Hilo de comunicaciones con alimentación controlada

7. Hilo de comunicaciones para el envío de datos TX

30

8. Hilo de comunicaciones para la recepción de datos RX

9. Hilo de masa eléctrica

35

10. Módulo de verificación de identidad del dispositivo 1

11. Módulo de verificación de identidad del dispositivo 2

Descripción de una realización preferente

40

Una realización preferente del puerto de comunicaciones para dispositivos electrónicos con identificación y autenticación objeto de la presente invención, con alusión a las referencias numéricas, puede realizarse con dos placas de circuito impreso, que corresponden a los dos dispositivos (1, 2) a comunicar.

45

Una de las placas estará compuesta por un microcontrolador y un zócalo (3) donde conectar la segunda placa. Este dispositivo tendrá el rol de esclavo.

50

La segunda placa estará compuesta por un microcontrolador, un relé, y un zócalo (4) que pueda conectarse a la primera placa. Este segundo dispositivo tendrá los roles de gestor y controlador.

Ambos dispositivos cuentan con su respectivo módulo de identidad de dispositivo (10, 11).

En esta configuración, el dispositivo esclavo obtendrá su alimentación de la alimentación controlada (6). La alimentación constante (5) podría usarse para alimentar otros sensores o dispositivos adicionales que el dominio de la aplicación requiriese.

- 5 La alimentación controlada (6) del puerto será proporcionada por el dispositivo gestor. Esta línea (6) de alimentación sería la propia de la placa conectada a través de un relé. Éste estaría regido por el microcontrolador, que decidiría cuando es necesaria para el dispositivo esclavo.

- 10 La alimentación constante del puerto será la alimentación de la propia placa y los hilos TX (7) y RX (8) se conectarán al zócalo de forma que el dispositivo esclavo los reciba en su orden correcto. También comprende un hilo de masa eléctrica (9).

- 15 Los módulos de verificación de identidad podrían implementarse por software. Este usaría algoritmos de encriptación donde la clave privada de cada dispositivo se haya grabado en el dispositivo con el que va a comunicarse.

REIVINDICACIONES

- 5 1.- Puerto de comunicaciones para dispositivos electrónicos con identificación y autenticación, constituido para la interconexión de al menos dos dispositivos caracterizado por disponer de al menos dos líneas de alimentación eléctrica, donde una de ellas presenta o no energía dependiendo de la lógica del dispositivo controlador y disponer además de otras líneas de comunicaciones serie.
- 10 2.- Puerto de comunicaciones para dispositivos electrónicos con identificación y autenticación, según reivindicación 1, caracterizado porque dispone de un identificador único para cada dispositivo y un método para verificar que dicho identificador pertenece al dispositivo conectado al puerto.

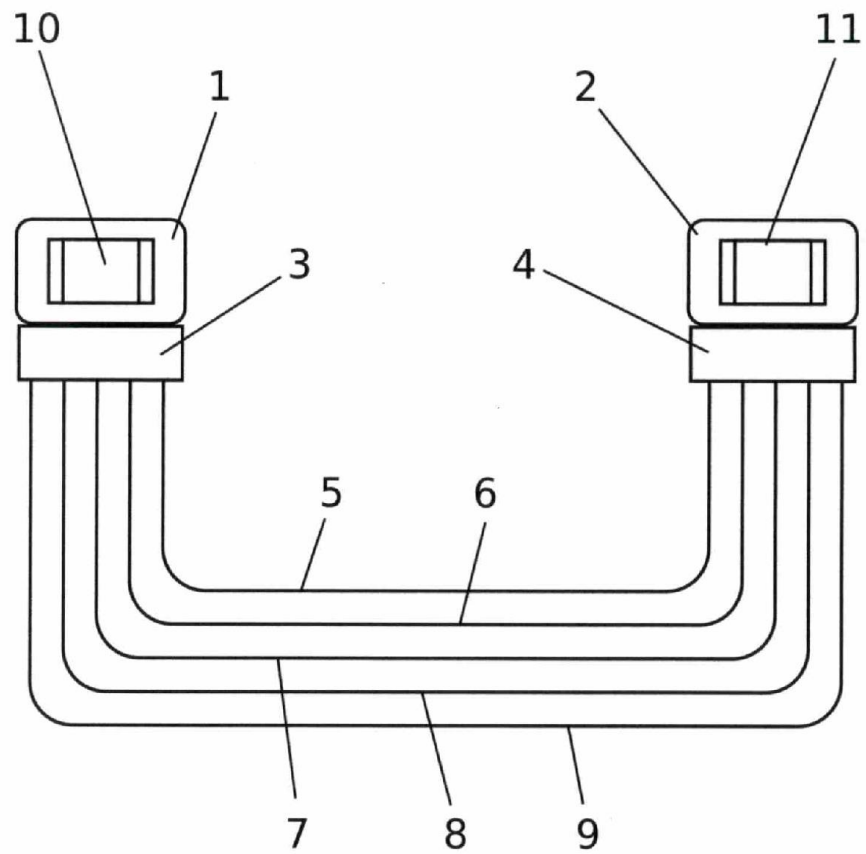


FIG 1



- ②① N.º solicitud: 201800163
②② Fecha de presentación de la solicitud: 13.07.2018
③② Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

⑤① Int. Cl.: **G06F1/26** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	⑤⑥ Documentos citados	Reivindicaciones afectadas
X	US 5842027 A (OPRESCU FLORIN et al.) 24/11/1998, abstract; pág. 4, párr. 2, 4; pág. 5, párr. 3, 5; fig. 1, 4,	1-2
A	WIKIPEDIA. Authentication.13/12/2017 [en línea][Recuperado el 04/07/2019]. Recuperado de Internet <URL: http://web.archive.org/web/20171213131703/https://en.wikipedia.org/wiki/Authentication >. párrafo. [1 - 2];	1-2

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
04.07.2019

Examinador
A. Oropesa García

Página
1/2

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

G06F

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

INVENES, EPODOC, internet