(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 036 875 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
03.08.2022 Bulletin 2022/31

(21) Application number: **21000099.8**

(22) Date of filing: **07.04.2021**

(51) International Patent Classification (IPC):
G07C 9/00 *(2020.01)*

(52) Cooperative Patent Classification (CPC):
G07C 9/00944; G07C 9/00174; G07B 15/00; G07C 2009/0023; G07C 2009/00412; G07C 2009/00587; G07C 2009/00642; G07C 2209/08

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **01.02.2021 ES 202130079**

(71) Applicant: **Elparking Internet, S.L.U**
28016 Madrid (ES)

(72) Inventor: **Álvarez Novoa, Carlos**
28027 Madrid (ES)

(74) Representative: **Botella Reyna, Juan**
Avenida de Moratalaz, 40 1a pl.
28030 Madrid (ES)

(54) **TELEMATIC ACCESS CONTROL DEVICE**

(57) Telematic access control device consisting of a frame structure (1) that groups together elements for opening and closing the access itself, such as automatically opening doors or barriers, together with electronic and computer equipment for the telematic operation of the aforementioned elements. It uses Bluetooth Low Energy (BLE) technology to communicate with the users' mobile phones. It includes a module (2) for powering the electronic and computer equipment, which is integrated in a second module (3) in a "system on a chip" (SoC) with Bluetooth, incorporating a communication firmware based on a Bluetooth GAP profile (General Access Profile), with encryption and without the need for pairing the mobile phones and the device. It also has a module (4) for acoustic and visual warning means.

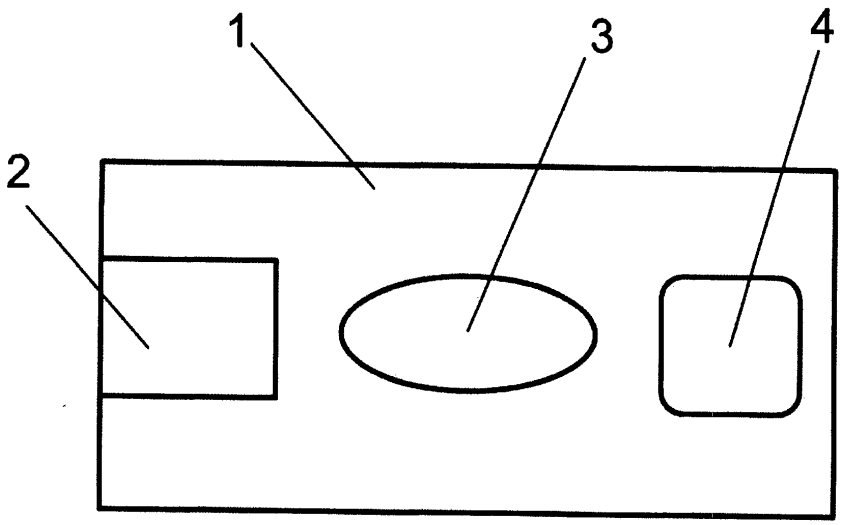

FIG-1

EP 4 036 875 A1

Description

[0001] The present invention, a telematic access control device, relates to a device that has been specially designed to be installed at entry/access control points for the general public, public events, public transport (bus, underground, train), or ticket validation points, by way of example.

[0002] Therefore, the object of the invention is a device that allows real-time validation of access by means of digital tickets that can be stored in electronic devices such as the mobile phones of users, whether or not the Internet is available, by means of a Bluetooth connection, without using connection or pairing. Pairing is the process normally used in Bluetooth to link a mobile phone with the telematic access control device, which is precisely avoided with this invention.

[0003] Therefore, the subject matter of the present invention will be of interest to the electronics and telematic devices industry.

BACKGROUND:

[0004] The prior art of this type of electronic devices in which the present invention is included comprises a plurality of devices and systems that have been developed as different communication technologies and electronic devices for use by the general public have been conceived.

[0005] Thus, this invention represents an advance over existing systems and technologies for contactless ticket validation through mobile devices, including NFC (Near field communication) technologies or QR codes (Quick Response codes) which can be read and processed by a programme that directs the user to a specific web address and thus serves to validate access to a place, vehicle, event, etc.

[0006] Therefore, the present invention may replace other systems known in the prior art for access control of the general public in cases that are as similar as possible to those that currently exist, but using different technology that allows a quick and easy implementation.

[0007] As background one could cite the Spanish Utility Model ES 1 074 924 U titled "Structure for control and access in ski slope turnstiles" by the inventor Arturo Vilas Salamero, which describes a structure for control and access in ski slope turnstiles based on suspending the control and access turnstiles above a support with displacement in both elevation and rotation. The aim of the invention is to facilitate the entry of skiers to the slopes, as well as to reduce access time and facilitate the work of ski resort employees, reducing waiting times at the control and access points to the slopes, improving the image and quality of the facilities. However, this invention, which intends to provide physical access control for the public, lacks the technological means of telematic control the present invention.

[0008] In line with the above, the validation of digital tickets using mobile phones is already in use today, but the methods used have shortcomings that the present invention solves.

[0009] The following table presents a descriptive table of access validation capabilities using three different technologies: QR, NFC and Bluetooth, in different types of devices currently in use.

	Validation with QR	Validation with NFC	Validation with Bluetooth
Available on all terminals	Yes	No	Yes
Standardised system	No	No	Yes
Requires additional chips	No	Yes	No
Maximum distance	-30-50cm	~10cm	10m
The user receives a reply	No	Yes	Yes

[0010] The use of Bluetooth technology, as opposed to NFC, is more widespread and makes it possible to reach practically 100% of the population with a mobile phone, as Bluetooth technology is open, known, standardised worldwide and is much more widespread in all ranges of mobile devices from their first generations, unlike NFC technology, which is present in the most modern generations of mobile phones and only in medium- and high-end terminals. In some manufacturers it is even disabled or its functionality is limited, as is the case, for example, of some Apple terminals with the IOS operating system.

[0011] On the other hand, in the prior art there are other Bluetooth solutions for similar use cases, such as opening doors or switching on lights, which use BLE with the GAP and GATT standard. In these cases, one problem is that the operation of this technology is slow, as it is intended to correctly establish a connection and follows certain processes, such as:

- Searching for the device (GAP)

- Connecting (GATT)
- Discovering services and their features (GATT)
- Reading or writing on a feature (GATT)
- Disconnecting (GATT)

[0012] Depending on the speed of the processor and the Bluetooth chip used by the mobile phone, this process can take as little as 2 seconds or up to 6 or 7 seconds for lower-end phones, which makes it impractical for mass access control.

[0013] The difference between the two methods is shown in the following diagram, this drawing corresponds to figure no. 2

[0014] For these reasons, the use of connection-oriented Bluetooth technology for access validation is not feasible, so that it has hereto been necessary to resort to other technologies, such as the aforementioned NFC or QR, with real-time capability.

[0015] For these reasons, the present invention represents an advance in the state of the art and fills the technological gap described above, making it possible to offer a fully functional device, with Bluetooth technology, adapted to any use case that is currently being performed, avoiding the use of NFC technology, by enabling access control processing at speeds of less than one second using low and medium range mobile phones.

DESCRIPTION

[0016] The telematic access control device described below mainly consists in a device that uses BLE (Bluetooth Low Energy) technology, which is a wireless PAN (Personal Area Network) technology that is advantageous over conventional Bluetooth in that BLE is designed to provide low energy consumption while maintaining a similar communication range.

[0017] In this invention, the GATT layer has been dispensed with and the GAP layer has been adapted to be able to transmit bidirectional information between the mobile and the access control device.

[0018] To use Bluetooth, a device must implement one of the defined Bluetooth profiles. These define the use of the Bluetooth channel as well as the channelling of the device to be paired.

[0019] Profiles are descriptions of general behaviours that devices can use to communicate, formalised to support unified usage. The way Bluetooth capabilities are used is therefore based on the profiles supported by each device. Profiles allow manufacturing devices that suit specific needs.

[0020] The GATT layer, or Generic Attribute Profile, is the profile commonly used in BLE technology. However, in this invention the GAP profile, or General Access Profile, is used.

[0021] In this way, a high speed is achieved in the access validation process using Bluetooth technology available in most mobile phones.

[0022] Firstly, the mobile devices identify the access control devices, through which the user wishes to access, by means of GAP communication protocols, which is a specification of the BLE standard meant to enable users' mobile phones to identify access control devices in their proximity. This identification is achieved by the reception in the mobile telephone of specific messages issued by the access control devices, which can be of two types: Advertising Data and Scan Response, both with a maximum size of 31 bytes.

[0023] These messages are used by access control devices so that they can be seen by and communicate with mobile phones, according to certain operational applications specific to said access control.

[0024] In the present invention, the device uses 31-byte messages, not to identify a peripheral, but instead to send and receive messages between two or more devices.

[0025] This shortens the time required for access control using traditional Bluetooth technology. For example, in tests carried out with low-end mobile phones, the communication time required for the use case of a bus ticket validation was less than 300 ms at a distance of less than 50 cm, which exceeds that of traditional Bluetooth.

[0026] In view of the above, the disclosed device consists of three modules, one of which is interchangeable or can be installed multiple times.

[0027] More specifically, a first module is defined consisting of a power supply module; by default, this module allows the circuitry to be powered at 5VDC. Depending on the use or installation, this module can be changed to accept other types of voltages.

[0028] The second module is materialised as a "system on a chip" (SoC) with Bluetooth. This means that it comprises a computer or electronic system integrated in a single integrated circuit or chip.

[0029] This SOC comprises customised firmware of this GAP-based communication system. An encryption layer is implemented on top of the communication layer, which allows information to be securely exchanged directly with the device from compatible mobile phones without the need to establish a connection or pairing, making the user experience convenient and comfortable by providing an immediate response.

[0030] Pairing, or bonding, is a process used in computer networks that helps establish an initial link between computing devices to enable communications between them, especially in Bluetooth, where the pairing process is used to link

devices. This process is avoided by this invention.

[0031] The third module refers to a set of means for warning and informing users of what is happening during the validation process, and may comprise acoustic means to give an audible warning and/or visual means to inform of a correct validation or an error. This can be performed by a speaker or buzzer for the audible warning, a led or group of LEDs for the visual warning, or in case of having to show more information, it can be done by means of a display on the top of the device.

[0032] Based on this structure, an application is defined to be installed on the users' mobile phones, which allows validating and providing correct access to those people who have purchased a valid ticket that is still active.

[0033] Each device associated with each access has a unique ID and a unique factory-installed password.

[0034] The device remains on standby awaiting for the reception of a message carrying the encoded input. When a user approaches the entrance, the mobile phone application, either automatically or manually, starts sending the input to the device. The device receives the input, decrypts it, validates it and sends a response to the phone while emitting an acoustic and/or light signal.

[0035] Each input is unique per user and has a very limited lifetime to avoid fraudulent use.

[0036] It is worth noting that neither the user nor the device need to be connected to the internet, allowing validations in places without data communication coverage by a telephone company.

PREFERRED EMBODIMENT OF THE INVENTION

[0037] A detailed description of the telematic access control device is given below, with reference to the accompanying drawings, which show, by way of example and in a non-limiting sense, a preferred embodiment that may be subject to variations in details that do not imply a fundamental alteration of the essential features of said improvements.

[0038] These drawings illustrate:

In Figure 1: A structural schematic view of the telematic access control device.

[0039] According to the example of embodiment shown, the telematic access control device illustrated in this preferred embodiment essentially consists of an original structure comprising equipment on a frame (1) provided with a structure for controlling physical access by the general public. This structure groups together elements for opening and closing access to the public, such as doors or barriers that open automatically, as well as equipment for telematic actuation of these elements.

[0040] The device uses Bluetooth Low Energy (BLE) technology and integrates three modules, one of them being a first module (2) for powering the electronic and computer equipment, which is integrated in a second module (3) in the form of a so-called 'system on a chip' (SoC) with Bluetooth. This means that it comprises a computer or electronic system integrated in a single integrated circuit or chip.

[0041] Moreover, the SoC incorporates customised firmware for this communication system, which is based on the Bluetooth General Access Profile (GAP), together with an encryption layer implemented on top of the communication layer.

[0042] In this way, this structure makes it possible to securely exchange information directly with the device from compatible mobile phones without the need for pairing, taking advantage of the initial link between a mobile terminal and the telematic access control device.

[0043] In addition to the above, the device has a third module (4) comprising a set of means for warning and informing users of what is happening during the validation process, which may comprise acoustic means to give an audible warning and/or visual means to indicate the correct validation or an error. This can be performed by a speaker or buzzer for the audible warning, a led or group of LEDs for the visual warning, or in case of having to show more information, it can be done by means of a display on the top of the device.

[0044] In addition, the telematic access control device has an application that communicates with mobile phones in its proximity, validating the access or entry of the general public automatically or manually by means of the emission by the mobile phone of a digital input to the device, which receives it, decrypts it, validates it and sends a response to the phone while emitting an acoustic and/or light signal, allowing or denying access or entry.

[0045] Finally, to prevent or hinder a fraudulent use of the device, each digital input is unique for each user and the access opens for a very limited time only.

[0046] The shape, materials and dimensions and, in general, everything that is accessory and secondary, may vary provided that this does not change or modify the essence of the improvements described above.

Claims

1. Telematic access control device consisting of a structure comprising a frame (1) of a physical access control device for the general public, which groups together elements for opening and closing the access itself, such as automatically

opening doors or barriers, together with electronic and computer equipment for telematic operation of the aforementioned elements, which, using the technology known as BLE, Bluetooth Low Energy, communicates with the users' mobile phones, **characterised in that** the device comprises three modules, one of them being a first module (2) for power supply of the aforementioned electronic and computer equipment, which is integrated in a second module (3) materialised in a "system on a chip" (SoC) with Bluetooth, said SoC incorporating a communication firmware based on a Bluetooth GAP profile (General Access Profile), together with an encryption layer provided on top of the communication layer without the need for pairing by means of the initial link between a mobile terminal and the telematic access control device itself, all of this together with a third module (4) comprising a set of acoustic and visual user warning and information means.

2. Telematic access control device, according to claim 1, **characterised in that** by means of an application resident in the users' mobile phones, said device communicates with said mobile phones when they are in its proximity, validating the access or entry of the public automatically or manually, by means of the emission by the mobile phone of a digital input to the device, which receives, decrypts, validates and sends a response to the phone, and at the same time emits an acoustic and/or light signal and allows or denies access or entry.

3. Telematic access control device, according to any of the previous claims, **characterised in that** each digital input is unique per user and the access opens for a very limited time, making fraudulent use of the same impossible.

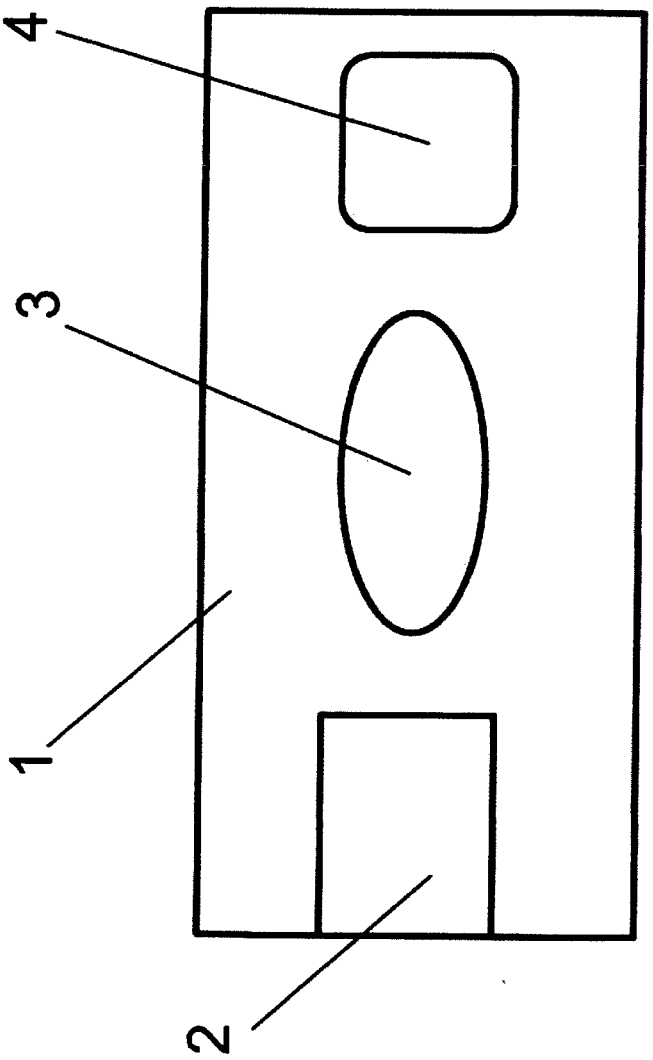

FIG-1

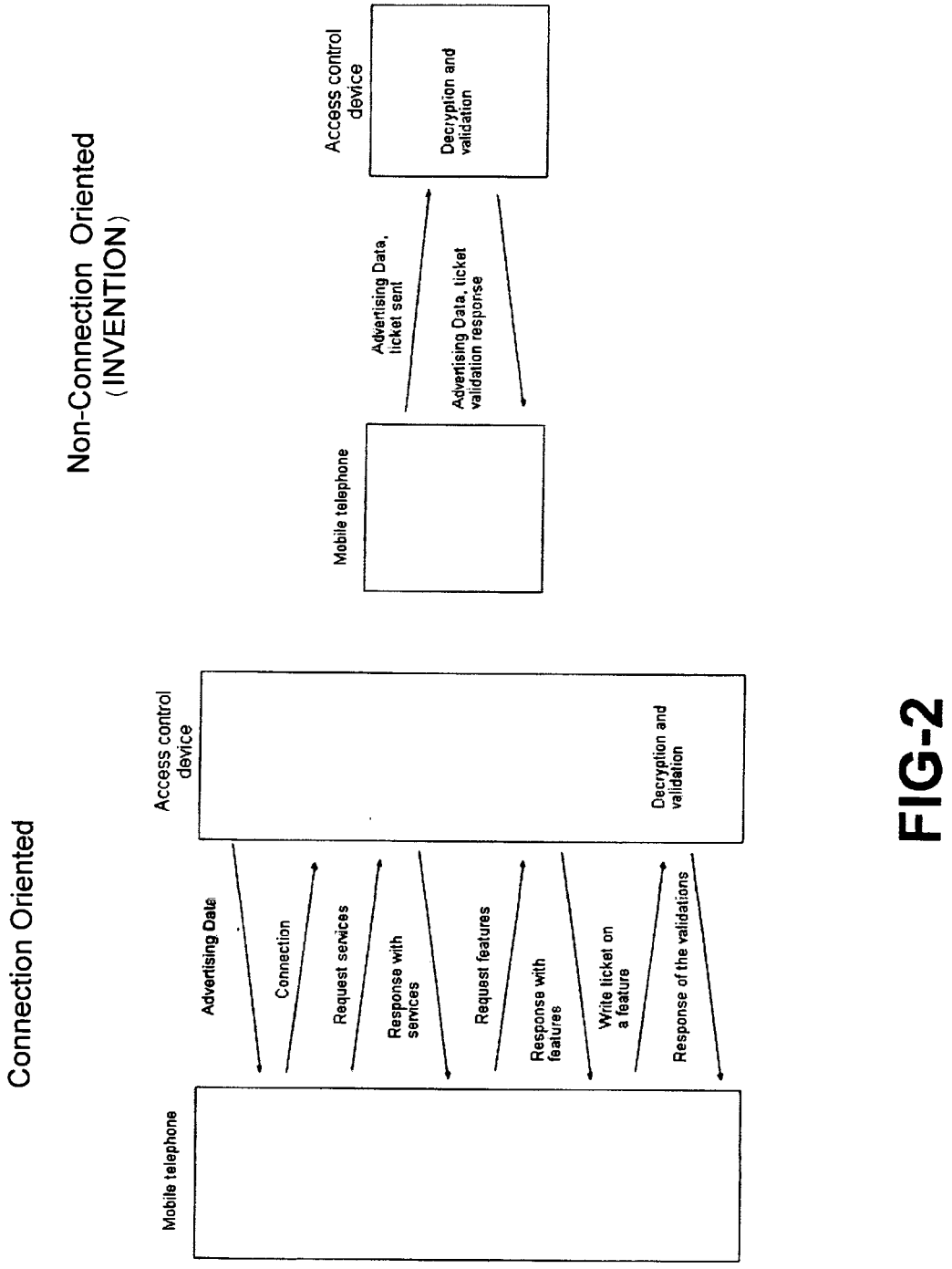
Non-Connection Oriented
(INVENTION)
Access control device
Decryption and validation
Mobile telephone
Advertising Data, ticket sent
Advertising Data, ticket validation response
Connection Oriented
Access control device
Decryption and validation
Mobile telephone
Advertising Data
Connection
Request services
Response with services
Request features
Response with features
Write ticket on a feature
Response of the validations

FIG-2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 00 0099

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2019/164716 A1 (CYPRESS SEMICONDUCTOR CORP [US]) 29 August 2019 (2019-08-29) * paragraph [0008] - paragraph [0087] * * figures 1-12 *	1	INV. G07C9/00
Y	EP 3 188 136 A1 (MARQUES SA [PT]) 5 July 2017 (2017-07-05) * abstract * * * paragraph [0017] - paragraph [0100] * * figures 1-4 *	1-3	
Y	IT 2018 0000 0672 A1 (SALARI SANDRO) 10 July 2019 (2019-07-10) * page 12, line 249 - page 27, line 574 * * figure 1 *	1-3	
Y	US 2018/132180 A1 (KVETNY EDUARD [IL] ET AL) 10 May 2018 (2018-05-10) * abstract * * * figures 1-4 * * paragraph [0020] - paragraph [0055] *	1-3	TECHNICAL FIELDS SEARCHED (IPC)
A	US 2013/176107 A1 (DUMAS PHILIP C [US] ET AL) 11 July 2013 (2013-07-11) * abstract * * * paragraph [0032] - paragraph [0108] *	1-3	G07C G07B
A	WO 2019/217610 A1 (STRATTEC SECURITY COPRORATION [US]) 14 November 2019 (2019-11-14) * abstract * * * paragraph [0002] * * paragraph [0026] - paragraph [0038] *	1-3	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	17 September 2021	Pañeda Fernández, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 21 00 0099

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

17-09-2021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2019164716 A1	29-08-2019	CN 111771337 A	13-10-2020
		DE 112019000884 T5	29-10-2020
		US 10367540 B1	30-07-2019
		US 2020007183 A1	02-01-2020
		US 2020212953 A1	02-07-2020
		US 2021083715 A1	18-03-2021
		WO 2019164716 A1	29-08-2019
EP 3188136 A1	05-07-2017	NONE	
IT 201800000672 A1	10-07-2019	---	
US 2018132180 A1	10-05-2018	US 2016381637 A1	29-12-2016
		US 2018132180 A1	10-05-2018
		WO 2016209521 A1	29-12-2016
US 2013176107 A1	11-07-2013	US 2013176107 A1	11-07-2013
		US 2015211259 A1	30-07-2015
		US 2015213658 A1	30-07-2015
		US 2015213663 A1	30-07-2015
WO 2019217610 A1	14-11-2019	CN 112384918 A	19-02-2021
		US 2019347882 A1	14-11-2019
		WO 2019217610 A1	14-11-2019

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- ES 1074924 U **[0007]**