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

(11) EP 3 739 553 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.11.2020 Bulletin 2020/47

(51) Int Cl.:
G07C 9/00 *(2020.01)* ***H04W 48/02*** *(2009.01)*
H04W 48/16 *(2009.01)*

(21) Application number: **19461537.3**

(22) Date of filing: **11.05.2019**

(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

(71) Applicant: **Ekinno Lab Sp. z o.o.**
44-100 Gliwice (PL)

(72) Inventor: **Kubala, Radoslaw**
41-813 Zabrze (PL)

(74) Representative: **Kancelaria Eupatent.pl Sp. z.o.o**
Ul. Kilinskiego 185
90-348 Lodz (PL)

(54) A METHOD AND SYSTEM FOR ACCESS CONTROL

(57) A method for controlling an access restriction device (200), the method comprising: monitoring the vicinity of the access restriction device (200) to detect, via a wireless communication module (204) an access request message from a user device (100), the access request message comprising a user ID (identifier); forwarding the access request message to a backend server (300); upon receiving an action request from the backend server (300), activating an access restriction module (205) to allow access via the access restriction device (200).

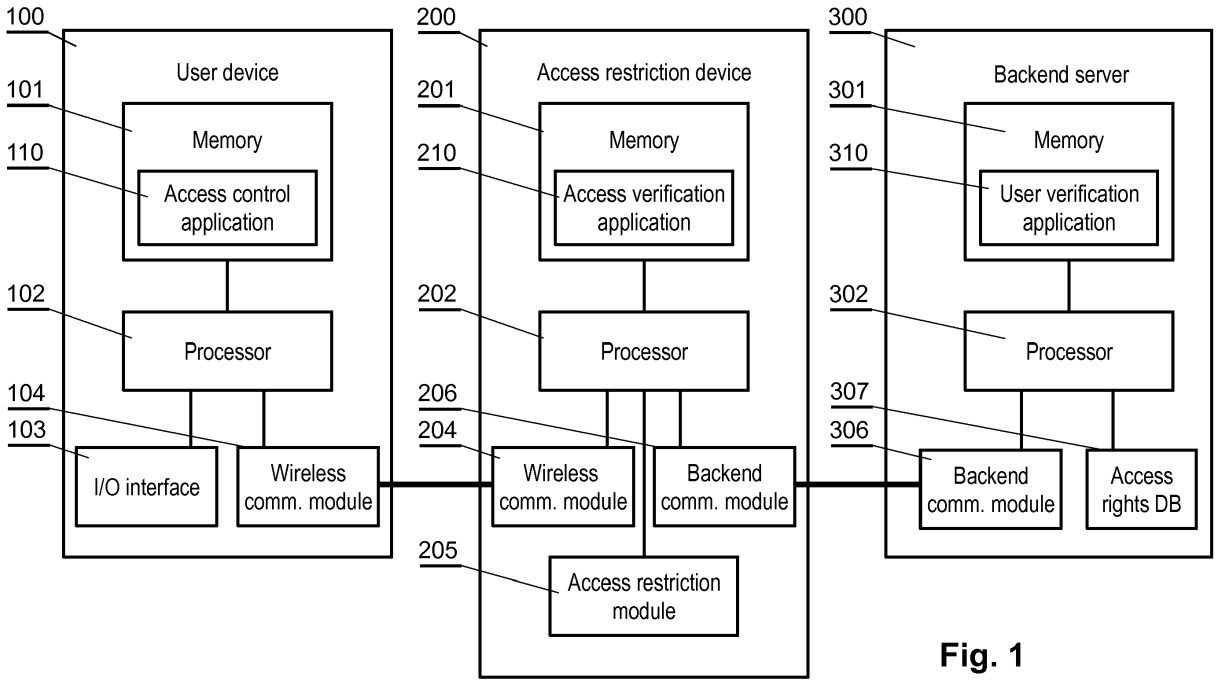

Fig. 1

EP 3 739 553 A1

Description

TECHNICAL FIELD

[0001] The present invention relates to access control, in particular remote control of access to areas protected by access restriction devices, such as doors or barriers, wherein the access is activated via a user mobile device.

BACKGROUND

[0002] There are known various solutions to remotely control access restriction devices, such as door locks or road barrier actuators.

[0003] One solution is to send an activation command directly from a user mobile device to the access restriction device. A system of this type is disclosed in US7205908, which describes a system and method for proximity control of a barrier comprising a stationary wireless signal receiving device and a mobile transmitting device. The wireless signal receiving device may monitor at least one transmitting device within a predetermined coverage area and may be a radio frequency receiver or a spread spectrum receiver located near the barrier. The disadvantage of that solution is that it requires the user to be registered as an authorized user directly at the access restriction device.

[0004] Another solution is to send an activation command from a user mobile device to a remote server that controls the operation of the access restriction device. A system of this type is disclosed in US9367978, which describes application software for a mobile device that can provide an owner or operator of a premises with the ability to remotely grant a guest authorization to access an access control device on or in the premises. The access control device can control the operation of the one or more secondary devices, so that with the owner authorization, the guest can access the access control device to cause an action at the premises with the secondary device. However, that requires the user mobile device to handle long-range communication to communicate with the server.

[0005] Therefore, there is a need to improve the access control systems to achieve at least one of the following technical objectives: ease of use usability, secure access, low requirements for the user mobile device.

SUMMARY

[0006] The object of the invention is a method for controlling an access restriction device, the method comprising: monitoring the vicinity of the access restriction device to detect, via a wireless communication module an access request message from a user device, the access request message comprising a user ID (identifier); forwarding the access request message to a backend server; upon receiving an action request from the backend server, activating an access restriction module to allow access via the access restriction device.

[0007] The access request message may be encrypted with a public key known to the backend server.

[0008] The access request message may be encrypted by a user-unique secret value known to the access control application and the backend server.

[0009] The access request message may further comprise a command to execute a particular action by the access restriction device.

[0010] The access request message may be broadcast by the user device via a wireless communication interface.

[0011] The wireless communication interface may be compliant with Bluetooth Low Energy.

[0012] The object of the invention is also a controller for an access restriction device comprising a processor configured to operate an access verification application for performing the steps of the method as described herein.

BRIEF DESCRIPTION OF DRAWINGS

[0013] The invention is shown by means of example embodiments on a drawing, wherein:

Fig. 1 shows a structure of modules of the system for access control;
Fig. 2 shows communication between system modules;
Fig. 3 shows example of a database with user access rights;
Fig. 4 shows an example embodiment of the system.

DETAILED DESCRIPTION

[0014] The system comprises three main cooperating components: a user application 110 operated at a user device 100, an access restriction device 200 and an backend server 300.

[0015] The user device 100 comprises a memory 101 for storing typical software components such as an operating system of the device, and in particular an access control application 110 and a processor 102 for executing the operating system and the access control application 110. The device is operable by the user via an input/output interface 103, including a display and an input controller, for example a touch display. The device further comprises a wireless user communication module 104, preferably a low energy device, such as a BLE (Bluetooth Low Energy) communication module. The user device is preferably a mobile device, such as a mobile smartphone, but can be also a dedicated device e.g. a specialized module connected to an onboard car system, or even a low-power beacon device that only transmits the access request message.

[0016] The access restriction device 200 may be a lockable door or a road barrier. It a memory 201 for storing typical software components such as an operating sys-

tem of the access restriction device, and in particular an access verification application 210 and a processor 202 for executing the operating system and the access verification application 210. The device further comprises a wireless user communication module 204, in particular a BLE (Bluetooth Low Energy) communication module, that is able to communicate with the user communication module 104 of the user device. The user communication module 204 may have a range of communication adapted to the particular type of the access restriction device 200, for example the module 204 installed at office door may have the range of communication limited to 50 cm, while the module 204 installed at a garage door may have the range of communication limited to 10 m. The access restriction device further comprises a controllable access restriction module 205 (such as a lock or a barrier actuator) that is operable by the processor. Furthermore, the device comprises a backend communication module 206 to communicate with the backend server 300, for example any type of interface allowing access to the Internet or other type of network via which the backend server 300 is accessible.

[0017] The backend server 300 comprises a memory 301 for storing typical software components such as an operating system of the backend server, and in particular a user verification application 310 and a processor 302 for executing the operating system and the user verification application 310. The server also comprises an access rights database 307 that stores information about users registered in the system and their permissions to activate particular access restriction devices 200. Furthermore, the server comprises a backend communication module 306 to communicate with the communication module 206 of the access restriction device 200.

[0018] The system operates as shown in Fig. 2.

[0019] When the user access control application is active, it continuously broadcasts, in step 11, an access request message, comprising at least a user ID (identifier). Optionally, the access request message may include other information, such as the requested command for the access restriction device, in case the device is capable of performing more than one action (for example, the road barrier control device may be optionally requested to turn on the light). Preferably, the access request message is encrypted with a secret user-unique value, as explained later. In case the access restriction device is a simple bi-state device (such as ON/OFF or OPEN/CLOSED), it is enough to transmit the user ID, since it is evident that the user intention is to have the access restriction device to move to an access enablement state (such as ON or OPEN). Since the broadcasting of the access request message data is performed via a low energy wireless communication module 204, the power usage performed by this step is relatively low. In order to avoid the broadcasting at times when it is not necessary, the access control application may be activated when the user device detects that it is located at a particular area (based on GPS, WiFi or other localizing module), at a particular time of day, upon detecting a signal from another module or upon manual activation by the user.

[0020] The access verification application 210 is configured to continuously monitor the vicinity of the access restriction device 200 in order to detect the access request messages broadcast by the user devices, via the wireless communication module 204. When the access request message is detected, the access verification application forwards the access request message (along with the device identifier (ID) at which the message was received) to the backend server 300.

[0021] At the backend server 300, the user verification application 310 receives the access request message, decrypts it (if it was encrypted, in order to check its authenticity, by checking whether it is decipherable by the security value associated with that user and/or whether it contains a correct timestamp) and reads the user ID. Next it checks, in step 13, in the access rights database 307, whether the particular user has access rights to activate the particular access restriction device 200 (or to perform a particular action as requested at the access request message). If the user does not have a permission, no action is taken or a response is sent to the access verification application that the action is denied. In case the user does have access rights, an action request (such as to activate the device or to perform the particular requested action) is sent in step 14 to the access verification application.

[0022] The access request message may be encrypted, for example with a public key of the backend server and a time stamp corresponding to the time of generating the message and/or other unique data that allows the message to change, such that the contents of the message, in particular the user ID, can be read only at the backend server 300. This increases the security of the system, as a malicious third party will not be able to determine the user ID, even if the broadcast access restriction message is captured.

[0023] Fig. 3 presents an example of access rights database 307. The access restriction devices D1, D2, D3 are bistate devices, therefore it is enough to specify whether the user has permission to access or not. The access restriction device D4 has more elaborate functionality, such as Open or Lights functions. The user U1 is allowed to access devices D1, D2 and D4 (with Open and Lights function permissions). The user U2 is allowed to access devices D2 and D4 (with Open function permission only). The user U3 is allowed to access device D3 only.

[0024] As an optional feature, the database 307 may comprise a "secret" value unique for the user that is a symmetrical key used to verify the authenticity of messages sent by the user application. In that case, the user may send packets containing a User ID (and preferably a timestamp to effect a change of the message content, so as to avoid transmitting repeatedly the same message and its re-use by unauthorized entities) that are encrypt-

ed by the secret value S1-S3 that is known to the access control application at the user device and the backend server.

[0025] Once the action request is received by the access verification application 210, in step 15 it sends an activation command to the access restriction module 205, such as to open a door lock or lift a road barrier.

[0026] Fig. 4 shows an example embodiment of operation of a road barrier 200, e.g. a barrier allowing access to a parking space. A user with a smartphone 100 drives a car and approaches the parking space. At that time, the smartphone geolocation module recognizes that the user is in the vicinity of the road barrier to be operated and sends a command to activate the access control application 110 to broadcast the access request message in step 11. The access request message is received by the access verification application 210 at the road barrier 200 and forwarded to the backend server 300 in step 12. The backend server 300 checks whether a user with the user ID contained in the access request message has permission rights to open that road barrier and if so, sends a command to open the barrier in step 14. The access verification application 210, upon receiving the command from the server, activates the road barrier actuator 205 to open the barrier. The same backend server 300 can also handle access control for other access restriction barriers D2, D3, D4 located at various other locations.

[0027] The advantage of the system is that it provides safety, ease of use and low resources to operate. The user device only needs to be capable of broadcasting the access request message via a low-power wireless communication interface, such as BLE. The user device does not need to be capable of communicating with the backend server, since the access request message is forwarded to the server by the access restriction device. The access restriction application (controller) can be universal and mounted to any kinds of access restriction devices and does not have to include the database of users, since the database can be central and provided at the backend server, while the controller at the access restriction device must be only able to receive messages from users, forward them to the backend server and respond to instructions received from the server. The presented method and system therefore provides an alternative solution for controlling access rights.

Claims

1. A method for controlling an access restriction device (200), the method comprising:

- monitoring the vicinity of the access restriction device (200) to detect, via a wireless communication module (204) an access request message from a user device (100), the access request message comprising a user ID (identifier);
- forwarding the access request message to a backend server (300);
- upon receiving an action request from the backend server (300), activating an access restriction module (205) to allow access via the access restriction device (200).

2. The method according to claim 1, wherein the access request message is encrypted with a public key known to the backend server (300).

3. The method according to claim 1, wherein the access request message is encrypted by a user-unique secret value (S1-S3) known to the access control application and the backend server (300).

3. The method according to any of previous claims, wherein the access request message further comprises a command to execute a particular action by the access restriction device (200).

4. The method according to any of previous claims, wherein the access request message is broadcast by the user device (100) via a wireless communication interface (104).

5. The method according to any of previous claims, wherein the wireless communication interface (104) is compliant with Bluetooth Low Energy (BLE).

6. A controller for an access restriction device (200) comprising a processor (202) configured to operate an access verification application (210) for performing the steps of the method of any of previous claims 1-5.

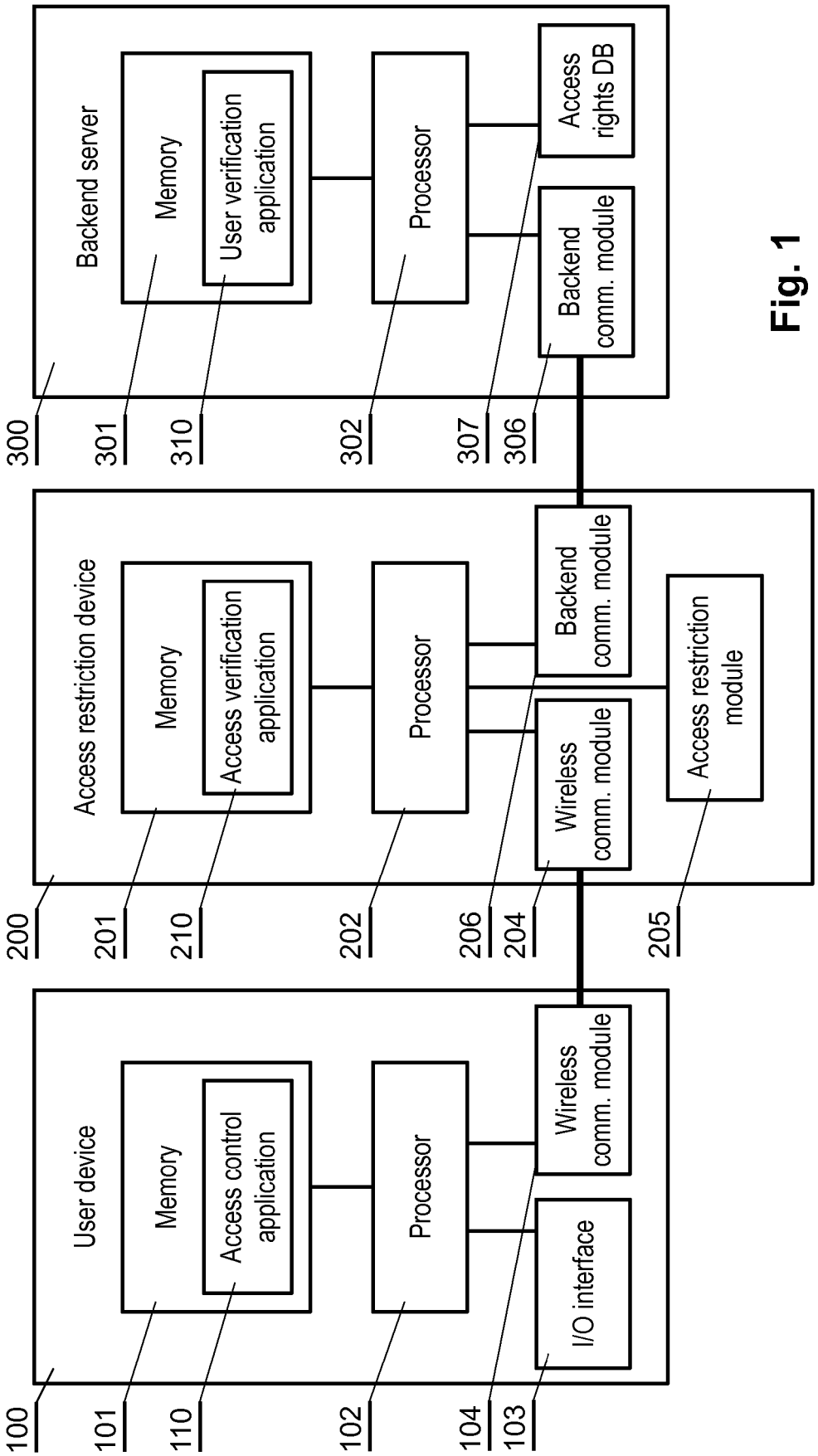
Backend server
Memory
User verification application
Processor
Access rights DB
Backend comm. module
300
301
310
302
307
306
Access restriction device
Memory
Access verification application
Processor
Backend comm. module
Wireless comm. module
Access restriction module
200
201
210
202
206
204
205
User device
Memory
Access control application
Processor
Wireless comm. module
I/O interface
100
101
110
102
104
103

Fig. 1

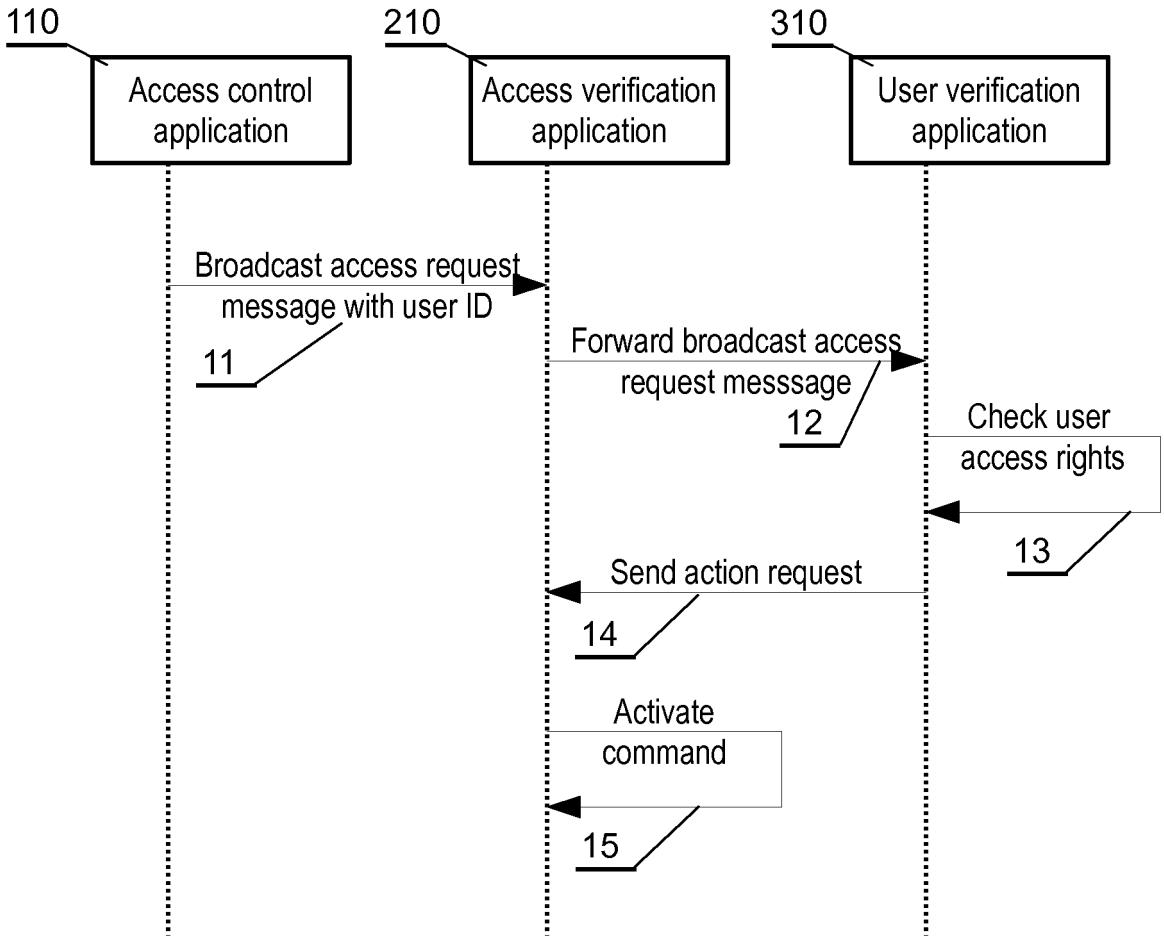

Fig. 2

User ID	Device ID	Access rights	Secret
U1	D1	YES	S1
U1	D2	YES	S1
U1	D4	Open, Lights	S1
U2	D2	YES	S2
U2	D4	Open	S2
U3	D3	YES	S3

Fig. 3

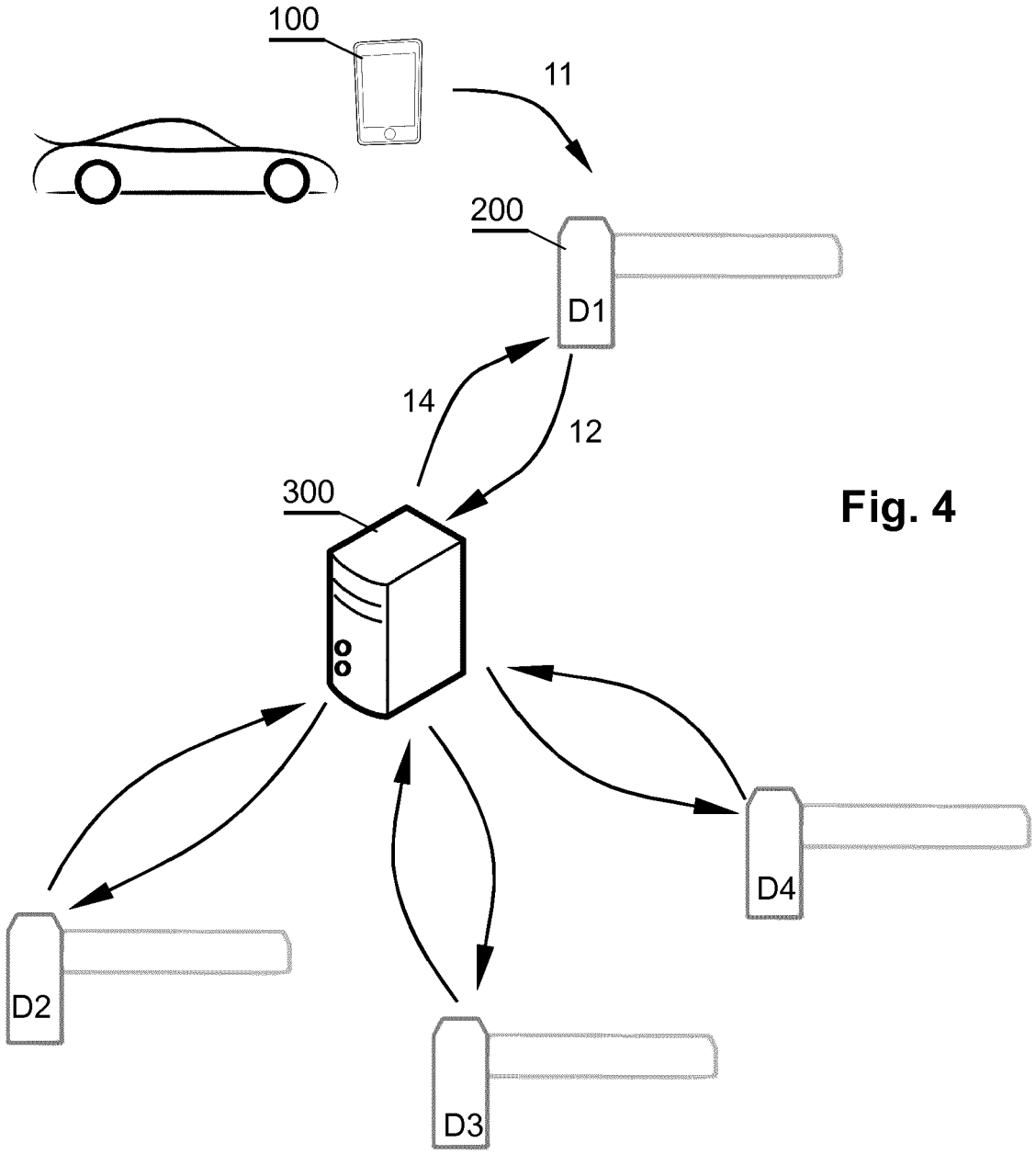

Fig. 4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 19 46 1537

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	US 2018/293823 A1 (GILLOT DAVID [BE] ET AL) 11 October 2018 (2018-10-11) * abstract * * figures 1a, 4, 6 * * claims 8-9 * * paragraph [0003] - paragraph [0020] * * paragraph [0098] - paragraph [0103] *	1-6	INV. G07C9/00 H04W48/02 H04W48/16
X	US 2018/047227 A1 (BEAVERS TIMOTHY RYAN [US] ET AL) 15 February 2018 (2018-02-15) * abstract * * figures 1, 4, 7 * * paragraph [0038] - paragraph [0053] * * paragraph [0104] - paragraph [0105] *	1-6	
A	US 2016/196706 A1 (TEHRANCHI ALI [US] ET AL) 7 July 2016 (2016-07-07) * abstract * * figures 2,4 * * paragraph [0056] - paragraph [0077] * * claims 10, 20 *	1-6	
			TECHNICAL FIELDS SEARCHED (IPC) G07C H04W

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	4 October 2019	Saraceni, Alessandro

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 19 46 1537

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.

04-10-2019

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018293823 A1	11-10-2018	EP 3362995 A1	22-08-2018
		US 2018293823 A1	11-10-2018
		WO 2017064107 A1	20-04-2017
US 2018047227 A1	15-02-2018	NONE	
US 2016196706 A1	07-07-2016	US 2016196706 A1	07-07-2016
		US 2019147680 A1	16-05-2019
		US 2019213815 A1	11-07-2019

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

- US 7205908 B **[0003]**
- US 9367978 B **[0004]**