(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 August 2021 (19.08.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/160386 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/37* (2021.01)
H04L 9/32 (2006.01) *H04W 12/084* (2021.01)

(21) International Application Number:
PCT/EP2021/051096

(22) International Filing Date:
20 January 2021 (20.01.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202041006318 13 February 2020 (13.02.2020) IN

(71) Applicant: NOKIA TECHNOLOGIES OY [FI/FI]; Karakaari 7, 02610 Espoo (FI).

(72) Inventors: **BYKAMPADI, Nagendra S**; 59 A Eastwood layout, Haralur Road, Off Sarjapura Main Road, Karnataka, Bangalore 560102 (IN). **GEORGE, Jos**; Thaikudom (H), V.P. Marrikkar Road, Edappally, Kerala, Kochi 682024 (IN). **VAITHESWARAN, Sriram**; No. - 1J, W 3, Fernhill Gardens, secor 6, hsr layout, Bangalore 560102 (IN).

(74) Agent: **NOKIA EPO REPRESENTATIVES**; Nokia Technologies Oy, Karakaari 7, 02610 Espoo (FI).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH,

(54) Title: AUTHORIZATION SERVICE FOR PROVIDING ACCESS CONTROL

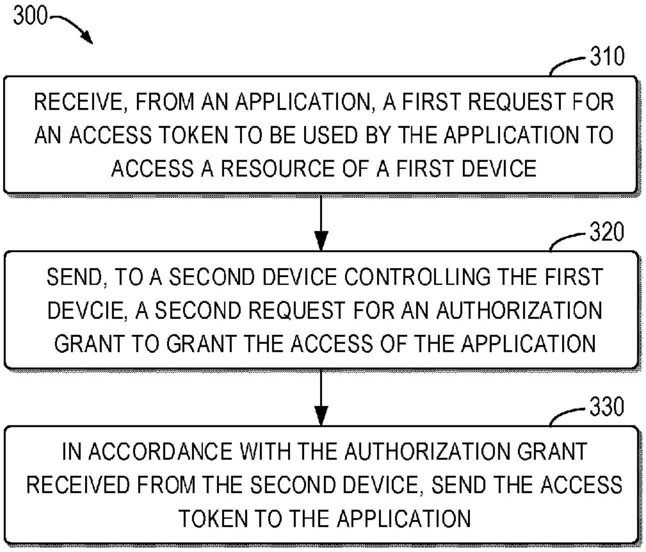
300
310
RECEIVE, FROM AN APPLICATION, A FIRST REQUEST FOR AN ACCESS TOKEN TO BE USED BY THE APPLICATION TO ACCESS A RESOURCE OF A FIRST DEVICE
320
SEND, TO A SECOND DEVICE CONTROLLING THE FIRST DEVCIE, A SECOND REQUEST FOR AN AUTHORIZATION GRANT TO GRANT THE ACCESS OF THE APPLICATION
330
IN ACCORDANCE WITH THE AUTHORIZATION GRANT RECEIVED FROM THE SECOND DEVICE, SEND THE ACCESS TOKEN TO THE APPLICATION

Fig. 3

(57) Abstract: Embodiments of the present disclosure relate to methods, apparatuses and computer readable storage media for authorizing access. In example embodiments, a method is provided. The method comprises receiving, from an application, a first request for an access token to be used by the application to access a resource of a first device; sending, to a second device controlling the first device, a second request for an authorization grant to grant the access of the application; and in accordance with the authorization grant received from the second device, sending the access token to the application. Embodiments of the present disclosure enable an authorization server to get a grant from the controller of a device before serving an access token to an application which tries to access resources of the device.

[Continued on next page]

GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

AUTHORIZATION SERVICE FOR PROVIDING ACCESS CONTROL

TECHNICAL FIELD

[0001] Embodiments of the present disclosure generally relate to the field of telecommunication, and in particular, to methods, apparatuses and computer readable storage media for authorizing access.

BACKGROUND

[0002] Using the fifth generation (5G) network, not only more humans are getting connected for their private and/or public uses, but also machines, robots, cars and/or devices will use the 5G network for their critical communications. To meet all of the requirements, the 5G core network (5GC) is designed to be extremely secure. At the same time, the 5GC will allow an application, such as an external application function (AF) or a 3rd party application, to request from network functions in the 5GC for data it needs to exchange with a device. For devices registered to the 5GC, the 5GC will facilitate secure communications. Access tokens from a Network Function (NF) Repository Function (NRF) will provide an additional mechanism to prevent unauthorized access to data that may have adverse effects on another device.

[0003] In many critical use cases, it is important to take consent from the owner or controller of a device, before accessing a protected resource of the device by an application using the authorization service from the ASF. However, at present, such functionality is not available in the ASF of the 5GC.

SUMMARY

[0004] In general, example embodiments of the present disclosure provide methods, apparatuses and computer readable storage media for authorizing access.

[0005] In a first aspect, there is provided an apparatus. The apparatus comprises at least one processor; and at least one memory including computer program codes; the at least one memory and the computer program codes are configured to, with the at least one processor, cause the apparatus to receive, from an application, a first request for an access token to be used by the application to access a resource of a first device; send, to a second device controlling the first device, a second request for an authorization grant to grant the access of the application; and in accordance with the authorization grant received from the second device, send the access token to the application.

[0006] In a second aspect, there is provided an apparatus. The apparatus comprises at least one processor; and at least one memory including computer program codes; the at least one memory and the computer program codes are configured to, with the at least one processor, cause the apparatus to receive, from an authorization server, a request for an authorization grant to grant access of an application to a resource of a first device; determine, based on the request, whether to grant the access; and in accordance with the determination to grant the access, generate the authorization grant; and send the authorization grant to the authorization server, to enable the authorization server to send to the application an access token for accessing the resource.

[0007] In a third aspect, there is provided a method. The method comprises receiving, from an application, a first request for an access token to be used by the application to access a resource of a first device; sending, to a second device controlling the first device, a second request for an authorization grant to grant the access of the application; and in accordance with the authorization grant received from the second device, sending the access token to the application.

[0008] In a fourth aspect, there is provided a method. The method comprises receiving, from an authorization server, a request for an authorization grant to grant access of an application to a resource of a first device; determining, based on the request, whether to grant the access; and in accordance with the determination to grant the access, generating the authorization grant; and sending the authorization grant to the authorization server, to enable the authorization server to send to the application an access token for accessing the resource.

[0009] In a fifth aspect, there is provided an apparatus. The apparatus comprises means for receiving, from an application, a first request for an access token to be used by the application to access a resource of a first device; means for sending, to a second device controlling the first device, a second request for an authorization grant to grant the access of the application; and means for in accordance with the authorization grant received from the second device, sending the access token to the application.

[0010] In a sixth aspect, there is provided an apparatus. The apparatus comprises means for receiving, from an authorization server, a request for an authorization grant to grant access of an application to a resource of a first device; means for determining, based on the request, whether to grant the access; and means for in accordance with the determination to grant the access, generate the authorization grant; and means for sending the authorization grant to the authorization server, to enable the authorization server to send to the application an access token for accessing the resource.

[0011] In a seventh aspect, there is a computer readable storage medium comprising program instructions stored thereon. The instructions, when executed by an apparatus, cause the apparatus to perform the method according to the above third or fourth aspect.

[0012] In an eighth aspect, there is provided a computer program product that is stored on a computer readable medium and includes machine-executable instructions. The machine-executable instructions, when being executed, cause a machine to perform the method according to the above third or fourth aspect.

[0013] It is to be understood that the summary section is not intended to identify key or essential features of embodiments of the present disclosure, nor is it intended to be used to limit the scope of the present disclosure. Other features of the present disclosure will become easily comprehensible through the following description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] Through the more detailed description of some example embodiments of the present disclosure in the accompanying drawings, the above and other objects, features and advantages of the present disclosure will become more apparent, wherein:

[0015] Fig. 1 illustrates a block diagram of an example environment according to some example embodiments of the present disclosure;

[0016] Fig. 2A illustrates an interaction diagram of an example process for initiating a request of an authorization grant according to some example embodiments of the present disclosure;

[0017] Fig. 2B illustrates an interaction diagram of an example process for according to some example embodiments of the present disclosure;

[0018] Fig. 3 shows a flowchart of an example method according to some example embodiments of the present disclosure;

[0019] Fig. 4 shows a flowchart of an example method according to some example embodiments of the present disclosure;

[0020] Fig. 5 illustrates a simplified block diagram of an apparatus that is suitable for implementing embodiments of the present disclosure; and

[0021] Fig. 6 illustrates a block diagram of an example computer readable medium in accordance with some example embodiments of the present disclosure.

[0022] Throughout the drawings, the same or similar reference numerals represent the same or similar element.

DETAILED DESCRIPTION

[0023] Principle of the present disclosure will now be described with reference to some example embodiments. It is to be understood that these embodiments are described only for the purpose of illustration and help those skilled in the art to understand and implement the present disclosure, without suggesting any limitation as to the scope of the disclosure. The disclosure described herein can be implemented in various manners other than the ones described below.

[0024] In the following description and claims, unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skills in the art to which this disclosure belongs.

[0025] References in the present disclosure to “one embodiment,” “an embodiment,” “an example embodiment,” and the like indicate that the embodiment described may include a particular feature, structure, or characteristic, but it is not necessary that every embodiment includes the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an example embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

[0026] It shall be understood that although the terms “first” and “second” etc. may be used herein to describe various elements, these elements should not be limited by these terms. These terms are only used to distinguish one element from another. For example, a first element could be termed a second element, and similarly, a second element could be termed a first element, without departing from the scope of example embodiments. As used herein, the term “and/or” includes any and all combinations of one or more of the listed terms.

[0027] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of example embodiments. As used herein, the singular forms “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms “comprises”, “comprising”, “has”, “having”, “includes” and/or “including”, when used herein, specify the presence of stated features, elements, and/or components etc., but do not preclude the presence or addition of one or more other features, elements, components and/ or combinations thereof.

[0028] As used in this application, the term “circuitry” may refer to one or more or all of the following:

(a) hardware-only circuit implementations (such as implementations in only analog and/or digital circuitry) and

(b) combinations of hardware circuits and software, such as (as applicable):

(i) a combination of analog and/or digital hardware circuit(s) with software/firmware and

(ii) any portions of hardware processor(s) with software (including digital signal processor(s)), software, and memory(ies) that work together to cause an apparatus, such as a mobile phone or server, to perform various functions) and

(c) hardware circuit(s) and or processor(s), such as a microprocessor(s) or a portion of a microprocessor(s), that requires software (e.g., firmware) for operation, but the software may not be present when it is not needed for operation.

[0029] This definition of circuitry applies to all uses of this term in this application, including in any claims. As a further example, as used in this application, the term circuitry also covers an implementation of merely a hardware circuit or processor (or multiple processors) or portion of a hardware circuit or processor and its (or their) accompanying software and/or firmware. The term circuitry also covers, for example and if applicable to the particular claim element, a baseband integrated circuit or processor integrated circuit for a mobile device or a similar integrated circuit in server, a cellular network device, or other computing or network device.

[0030] As used herein, the term “communication network” refers to a network following any suitable communication standards, such as Long Term Evolution (LTE), LTE-Advanced (LTE-A), Wideband Code Division Multiple Access (WCDMA), High-Speed Packet Access (HSPA), Narrow Band Internet of Things (NB-IoT), New Radio (NR) and so on. Furthermore, the communications between a terminal device and a network device in the communication network may be performed according to any suitable generation communication protocols, including, but not limited to, the first generation (1G), the second generation (2G), 2.5G, 2.75G, the third generation (3G), the fourth generation (4G), 4.5G, the future fifth generation (5G) communication protocols, and/or any other protocols either currently known or to be developed in the future. Embodiments of the present disclosure may be applied in various communication systems. Given the rapid development in communications, there will of course also be future type communication technologies and systems with which the present disclosure may be embodied. It should not be seen as limiting the scope of the present disclosure to only the aforementioned system.

[0031] As described above, using the 5G network, not only more humans are getting connected for their private and/or public uses, but also machines, robots, cars and/or devices will use the 5G network for their critical communications. To meet all of the requirements, the 5GC is designed to be extremely secure. At the same time, the 5GC will allow an external AF or a 3rd party application to request from network functions in the 5GC for data it needs to exchange with a device. For devices registered to the 5GC, the 5GC will facilitate secure communications. Access tokens from a NRF will provide an additional mechanism to prevent unauthorized access to data that may have adverse effects on another device.

[0032] Currently, OAuth 2.0 authorization framework has been proposed to enable a third-party application to obtain limited access to a web service enabled device, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the web service, or by allowing the third-party application to obtain access on its own behalf. In OAuth 2.0 authorization framework, the client may request access to resources controlled by a resource owner and hosted by a resource server and may be issued a different set of credentials from those of the resource owner. Instead of using the credentials of the resource owner to access protected resources, the client may obtain an access token, that is, a string denoting a specific scope, lifetime, and other access attributes. The access token may be issued to the client by an authorization server (such as, an authorization sever function or a NRF) with the approval of the resource owner. The client may use the access token to access the protected resources hosted by the resource server.

[0033] The 5GC comprises a lot of network entities, which provide different network functions. For example, the Network Function (NF) Repository Function (NRF) is the network entity in the 5GC which maintains NF profiles and available NF instances. It also provides service registration and discovery function so that NFs can discover each other. In addition, the NRF can provide an OAuth 2.0 authorization service to other NFs. It exposes a "Token Endpoint", where a NF service consumer can request an access token to access a NF service producer. The NRF may act as the OAuth 2.0 authorization server (aka ASF), the NF service consumer may act as the OAuth 2.0 client and the NF service producer may act as the OAuth 2.0 resource server. Examples of the NF service consumer may include, but not limited to, Access and Mobility Management Function (AMF), Session Management Function (SMF), Policy Control Function (PCF), Network Exposure Function (NEF), Network Slice Selection Function (NSSF), Short Message Service Function (SMSF) and Authentication Server Function (AUSF).

[0034] In the 5G network, NFs securely expose capabilities and events to third-party AFs via the NEF. The NEF also enables secure provision of information on authenticated and authorized AFs. The NEF shall authorize requests from AFs using the OAuth-based authorization mechanism. In a scenario, the NRF (that is, the authorization server) is configured to grant an AF (which is the client of the NRF) to access northbound Application Programming Interfaces (APIs) of the NEF.

[0035] Within the 5GC, the Unified Data Repository (UDR) provides unified data management services to other NFs, such as, AMF, SMF, SMSF, NEF, Gateway Mobile Location Center (GMLC) and AUSF via the UDR service based interfaces (also referred to as “NUDR interfaces” in the following). For example, the UDR can provide a subscriber data management service, a UE context management service, a UE authentication service, an event exposure service, a parameter provision service and a Non-IP Data Delivery (NIDD) authorization service via the NUDR interfaces.

[0036] In many critical 5G use cases, it is important to take consent from the owner or controller of a device, before accessing a protected resource from the device by an application using the authorization service from the ASF. However, at present, such functionality is not available in the ASF/NRF of the 5GC.

[0037] Embodiments of the present disclosure provide a solution for authorizing access to a device from an application function (AF). In this solution, the owner or controller of a device may receive a request for an authorization grant forwarded by the ASF per request from an external AF to access a resource of the device. The request from the ASF may include identity information of the external AF and information about the resource to be accessed. The owner or controller of the device will check validity of the external AF and availability of the device, and accordingly reply to the ASF the authorization grant for accessing the device. In response to receiving the authorization grant from the owner or controller of the device allowing the access to the device, the ASF will provide an access token to the external AF to access the resource of the device. Embodiments of the present disclosure enable the ASF to get a grant from the owner or controller of the device before serving an access token to the external AF which tries to access resources of the device. The grant received from the owner may include additional information that allows the ASF to further determine the granted scope of access by the AF to the device. Since the authorization grant is provided by a different device other than the device where the resources are located, this will improve security and reduce the attack surface for the authorization service.

[0038] Reference is now made to Fig. 1, which illustrates a block diagram of an environment 100 according to some example embodiments of the present disclosure. As shown in Fig. 1, for example, the environment 100 may include an application 110, a first device 120, an authorization server 130 and a second device 140 which controls the first device.

[0039] In the environment 100, it is assumed that the application 110, the first device 120 and the second device 140 are all registered to a same network, such as, a Land Mobile Network (PLMN). In sake of simplicity for discussion, it is also assumed that the above entities are all in CM-CONNECTED mode when they are registered to a same PLMN. It is to be understood that the structure of the environment 100 is shown only for purpose of illustration, without suggesting any limitation to the scope of the present disclosure. Embodiments of the present disclosure may also be applied to an environment with a different structure.

[0040] The first device 120 or the second device 140 may refer to any end device that is capable of wireless communication. By way of example rather than limitation, the first device 120 or the second device 140 may also be referred to as a communication device, user equipment (UE), a Subscriber Station (SS), a Portable Subscriber Station, a Mobile Station (MS), or an Access Terminal (AT). The first device 120 may include, but not limited to, a mobile phone, a cellular phone, a smart phone, voice over IP (VoIP) phones, wireless local loop phones, a tablet, a wearable terminal device, a personal digital assistant (PDA), portable computers, desktop computer, image capture terminal devices such as digital cameras, gaming terminal devices, music storage and playback appliances, vehicle-mounted wireless terminal devices, wireless endpoints, mobile stations, laptop-embedded equipment (LEE), laptop-mounted equipment (LME), USB dongles, smart devices, wireless customer-premises equipment (CPE), an Internet of Things (loT) device, a watch or other wearable, a head-mounted display (HMD), a vehicle, a drone, a medical device and applications (e.g., remote surgery), an industrial device and applications (e.g., a robot and/or other wireless devices operating in an industrial and/or an automated processing chain contexts), a consumer electronics device, a device operating on commercial and/or industrial wireless networks, and the like. Although the first device 120 is shown as a vehicle and the second device 140 is shown as a mobile phone in Fig. 1, it is to be understood that embodiments of the present disclosure are also applicable to other terminal devices. In the following description, the terms “terminal device”, “communication device”, “terminal”, “user equipment” and “UE” may be used interchangeably.

[0041] The second device 140 may act as an owner or controller of the first device 120. The interaction between the first device 120 and the second device 140 can be an automated process or a non-automated process according to different scenarios and/or requirements.

[0042] The application 110 can be any type of application, which may be deployed on any physical computer, server or virtual machine. For example, the application 110 may be a Land Mobile Network (PLMN) registered third-party AF. The authorization server 130 can be implemented in a single device or across a plurality of devices. In some example embodiments, the authorization server 130 can be implemented as a new NF (such as, an ASF) or can be implemented at an existing NF (such as, the NRF). For example, the authorization server 130 can be implemented as a standalone NF or co-located with another NF in the 5GC. The authorization server 130 can provide an authorization service to the application 110.

[0043] In some example embodiments, the authorization server 130 may include an authorization module and a token module, which are not shown in Fig. 1. For example, in response to receiving from the application 110 a first request for an access token to be used for accessing a resource of the first device 120, the authorization module may send, to the second device 140, a second request for an authorization grant to grant the access of the application 110. In response to receiving the second request from the authorization server 130, the second device 140 may determine, based on the second request, whether to grant the access. For example, the second device 140 may check validity of the application as well as availability of the first device 120 for the access. In response to determining to grant the access, the second device 140 may send the authorization grant to the authorization server 130, to enable the authorization server 130 to send the access token to the application 110.

[0044] In some example embodiments, the first device 120 (for example, a car) may be owned by a human user and the second device 140 may be a terminal device (for example, a phone) operated by the human user. In this event, the authorization server 130 may reach the human user via the phone. For example, in response to receiving from the application 110 the first request, the authorization server 130 may send, to the human user, the second request for the authorization grant via a short message or through an application running on the phone. The human user can decide whether or not to grant the access of application 110. In response to determining to grant the access, the human user may cause the phone to send the authorization grant to the authorization server 130 via another short message or the application running on the phone. The application running on the phone may also enable the human user to smartly process the request for the authorization grant based on API keys or based on the identity information of the application 110. For example, as will be described in detail as below, the request for the authorization grant may comprise information about the application 110, which enables the application running on the phone to process the request for the authorization grant smartly.

[0045] Fig. 2A illustrates an interaction diagram of an example process 210 for initiating a request of an authorization grant according to some example embodiments of the present disclosure. The process 210 may involve the application 110, the second device 140 and the authorization server 130 as shown in Fig. 1. The process 210 may also involve an AMF 201 within the 5GC. Prior to the process 210, the application 110 may have registered with the authorization server 130 for an authorization service.

[0046] As shown in Fig. 2A, the application 110 may send 211, to the authorization server 130, a first request for an access token to be used for accessing a resource of the first device 120. In some example embodiments, the first request may include first identity information of the first device 120, for example, a Mobile Station International Subscriber Directory Number (MSISDN) of the first device 120; second identity information of the second device 140, for example, a MSISDN of the second device 140; and information about the resource to be accessed by the application 110. For example, the information about the resource may identify the requested scope of the access. In some example embodiments, the authorization server 130 can reject the first request if any of the above parameters (such as, the second identity information of the second device 140) is missing. Alternatively, in some example embodiments, the authorization server 130 may maintain a mapping relationship between identity information of devices and identity information of their owners in its database. As such, the application 110 may not need to include the second identity information in the first request.

[0047] As shown in Fig. 2A, in response to receiving the first request from the application 110, the authorization server 130 may initiate 212, towards the second device 140, a second request for an authorization grant to grant the access of the application 110. In some example embodiments, the authorization server 130 may invoke the Namf_Communication_N1N2MessageTransfer service operation to the AMF 201.

[0048] The second request may be sent to the second device 140 based on the second identity information of the second device 140. For example, if the first request comprises the second identity information of the second device 140, the authorization server 130 may extract the second identity information from the first request. If the first request comprises the first identity information of the first device 120 and the authorization server 130 maintains the mapping relationship between the first identity information of the first device 120 and the second identity information of the second device 140, the authorization server 130 may extract the first identity information from the first request and determine the second identity information based on the mapping relationship between the first identity information and the second identity information.

[0049] In some example embodiments, the second request may comprise at least one of the following: the first identity information of the first device 120; information about the resource to be accessed by the application 110, the information about the resource indicating the scope of the access requested by the application 110; and information about the application 110. In some example embodiments, the information about the application 110 may comprise at least one of the following: location information of the application 110; duration for which the application 110 has registered to the 5GC; third identity information of the application 110; one or more API keys to distinguish traffic for different access purposes; and the like. In some example embodiments, the authorization server 130 may obtain the information about the application 110 from the UDR in the 5GC. Such information about the application 110 can help the controller 140 of the first device 120 to determine whether the application 110 is legitimate or not and further decide whether or not to grant the access of application 110.

[0050] In some example embodiments, different API keys may indicate different access purposes. For example, it is assumed that the first device 120 is a self-driving car and the second device 140 that controls the first device 120 is a mobile phone of the owner of the car. One of the API keys may indicate that the application 110 needs to send new advertisements to the car infotainment system, while another of the API keys may indicate that the application needs to collect weekly maintenance data from the car, and so on. That is, different API keys can be used to segregate different kinds of access traffic. In some example embodiments, the 5GC can limit the number of transactions corresponding to one API key sent from the application 110 for accessing the first device 120. In some example embodiments, the number of transactions corresponding to one API key can be negotiated between the controller of a device (for example, the controller 140 of the first device 120) and the 5GC (for example, the authorization server 130), for example, via the authorization grant request (for example, the second request) and its corresponding response, or via a separate request and its corresponding response. In some example embodiments, one API key may correspond to one device to be accessed. For example, if one controller controls a plurality of devices to be accessed, the plurality of devices may correspond to different API keys. Alternatively, in some example embodiments, if one controller controls a plurality of devices to be accessed, the plurality of devices may share a same API key. Alternatively, in some example embodiments, if a device provides a plurality of resources for access, each of the plurality of resources may correspond to a separate API key.

[0051] As shown in Fig. 2A, the AMF 201 may forward 213 the second request to the second device 140 as part of a Downlink Non-Access Stratum (NAS) message. In some example embodiments, the payload of the message may include the first identity information of the first device 120 which needs a grant for the access. In some example embodiments, the AMF 201 may send 214, to the authorization server 130, a Namf_Communication_N1N2MessageTransfer response indicating whether the AMF 201 was able to successfully transfer the N1 and/or N2 message. Alternatively, in some example embodiments, the second device 140 may send an acknowledgement for the Downlink NAS message indicating successful reception of the second request from the authorization server 130 via an Uplink NAS message towards the AMF 201. If the authorization server 130 is subscribed for Namf_Communication_N1MessageNotify service operation from the AMF 201, the AMF 201 may forward this acknowledgement to the authorization server 130.

[0052] Upon receiving the second request from the authorization server 130, the second device 140 may verify validity of the application 110 based on the third identity information of the application 110. The second device 140 may also check the availability or readiness of the first device 120 for the access from the application 110. In some example embodiments, if the second device 140 determines that the application 110 is valid and the second device 140 is available for the access, the second device 140 may determine to grant the access and send an authorization grant to the authorization server 130. The authorization grant may indicate a scope of access granted by the second device. In some example embodiments, if the second device 140 determines that the application 110 is invalid and/or the second device 140 is unavailable for the access, the second device 140 may determine to deny the access without sending the authorization grant to the authorization server 130. In some cases, when the first device 120 is functioning, it may not be readily available for the access (such as, a software upgrade) from the application 110. In such cases, the second device 140 may negotiate a maintenance time window with the first device 120 and send the authorization grant to the authorization server 130 during this maintenance time window. Once receiving the authorization grant from the second device 140, the authorization server 130 will provide the access token to the application 110.

[0053] Fig. 2B illustrates an interaction diagram of an example process 220 for replying an authorization grant according to some example embodiments of the present disclosure. The process 220 may involve the application 110, the first device 120, the second device 140 and the authorization server 130 as shown in Fig. 1. The process 220 may also involve the AMF 201 within the 5GC and Radio Access Network (RAN) 202. For example, the process 220 may be performed subsequent to the process 210 and in response to the second device 140 deciding to grant the access of the application 110 to the first device 120.

[0054] As shown in Fig. 2B, the second device 140 may send 221 a service request comprising an authorization grant for the access to the RAN 202. The RAN 202 may forward 222 the service request comprising the authorization grant to the AMF 201 in a N2 message. Once the AMF 201 receives the N2 message, the AMF 201 will connect to the authorization server via a standard API and send 223 this message to the authorization server 130. The authorization server 130 may validate 224 the authorization grant given by the second device 140. The authorization server 130 may send, to the second device 140, an acknowledgement that the authorization grant is successfully received. As shown in Fig. 2B, the acknowledgement may be sent 225 to the AMF 201 and then forwarded 226 to the RAN 202 by the AMF 201. The RAN 202 may then forward 227 the acknowledgement to the second device 140.

[0055] The authorization server 130 may send 228 the access token for accessing the first device 120 to the application 110. In some example embodiments, in addition to the access token, the authorization server 130 may also send information related to the access token to the application 110, such as, the expiration time of the access token. In response to receiving the access token from the authorization server 130, the application 110 may send 229, to the first device 120, a device access request for accessing the resource of the first device 120. The device access request may include the access token received from the authorization server 130. The first device 120 may verify 230 validity of the access token and check the scope of the access from the access token. If the access token is valid, the first device 120 may serve the device access request and send 231 a device access response to the application 110.

[0056] It can be seen that, embodiments of the present disclosure provide a solution for authorizing access. In this solution, the owner or controller of a device may receive a request for an authorization grant forwarded by the authorization server per request from an application to access a resource of the device. The request from the authorization server may include identity information of the application and the scope of the access. The owner or controller of the device will check validity of the application and availability of the device, and accordingly reply to the authorization server the authorization grant for accessing the device. In response to receiving the authorization grant from the owner or controller of the device, the authorization server will provide an access token to the application to access the resource of the device. Embodiments of the present disclosure enable the ASF to get a grant from the owner or controller of the device before serving an access token to the external AF which tries to access resources of the device. Since the authorization grant is provided by a different device other than the device where the resources are located, this will improve security and reduce the attack surface for the authorization service.

[0057] Fig. 3 shows a flowchart of an example method 300 according to some example embodiments of the present disclosure. The method 300 can be implemented at the authorization server 130 as shown in Fig. 1. For the purpose of discussion, the method 300 will be described from the perspective of the authorization server 130 with reference to Fig. 1. It is to be understood that the method 300 may include additional blocks not shown and/or may omit some shown blocks, and the scope of the present disclosure is not limited in this regard.

[0058] At block 310, the authorization server 130 receives, from the application 110, a first request for an access token to be used by the application 110 to access a resource of the first device 120.

[0059] In some example embodiments, the first request comprises at least one of the following: first identity information of the first device 120; second identity information of the second device 140; and information about the resource to be accessed by the application 110, the information indicating a first scope of access requested by the application 110.

[0060] At block 320, the authorization server 130 sends, to the second device 140 controlling the first device 120, a second request for an authorization grant to grant the access of the application 110.

[0061] In some example embodiments, sending the second request to the second device 140 comprises: determining second identity information of the second device 140 based on the first request; and sending the second request to the second device 140 based on the second identity information.

[0062] In some example embodiments, determining the second identity information comprises: extracting the second identity information from the first request.

[0063] In some example embodiments, determining the second identity information comprises: extracting first identity information of the first device 120 from the first request; and determining the second identity information based on a mapping relationship between the first identity information and the second identity information.

[0064] In some example embodiments, the second request comprises at least one of the following: first identity information of the first device 120; information about the resource to be accessed by the application 110, the information about the resource indicating a first scope of access requested by the application 110; and information about the application 110.

[0065] In some example embodiments, the information about the application 110 comprises at least one of the following: location information of the application 110; duration for which the application 110 has registered to a network; third identity information of the application 110; and API keys to distinguish traffic for different access purposes.

[0066] In some example embodiments, sending the second request to the second device 140 comprises: sending the second request to the second device 140 via an Access and Mobility Management Function.

[0067] In some example embodiments, the method 300 further comprises: receiving the authorization grant from the second device 140 via the Access and Mobility Management Function, the authorization grant indicating a second scope of access granted by the second device 140; and in accordance with the authorization grant received from the second device 140, sending to the second device 140 an acknowledgement that the authorization grant is received.

[0068] At block 330, in accordance with the authorization grant received from the second device 140, the authorization server 130 sends the access token to the application 110.

[0069] Fig. 4 shows a flowchart of an example method 400 according to some example embodiments of the present disclosure. The method 400 can be implemented at the second device 140 which controls the first device 120 as shown in Fig. 1. For the purpose of discussion, the method 400 will be described from the perspective of the second device 140 with reference to Fig. 1. It is to be understood that the method 400 may include additional blocks not shown and/or may omit some shown blocks, and the scope of the present disclosure is not limited in this regard.

[0070] At block 410, the second device 140 receives, from the authorization server 130, a request for an authorization grant to grant access of the application 110 to a resource of the first device 120.

[0071] In some example embodiments, the request comprises at least one of the following: first identity information of the first device 120; information about the resource to be accessed by the application 110, the information about the resource indicating a first scope of access requested by the application 110; and information about the application 110.

[0072] In some example embodiments, the information about the application 110 comprises at least one of the following: location information of the application 110; duration for which the application 110 has registered to a network; third identity information of the application 110; and API keys to distinguish traffic for different access purposes.

[0073] At block 420, the second device 140 determines, based on the request, whether to grant the access.

[0074] In some example embodiments, the request comprises third identity information of the application, and determining whether to grant the access comprises: verifying validity of the application 110 based on the third identity information; determining whether the first device 120 is available for the access; in accordance with the verification that the application 110 is valid and the determination that the first device 120 is available for the access, determining to grant the access; and in accordance with the verification that the application 110 is invalid and/or the determination that the first device 120 is unavailable for the access, determining to deny the access.

[0075] At block 430, in accordance with the determination to grant the access, the second device 140 generates the authorization grant.

[0076] In some example embodiments, the request indicates a first scope of access requested by the application, and generating the authorization grant comprises: determining, based on the first scope of access, a second scope of access to be granted to the application 110; and generating the authorization grant indicating the second scope of access.

[0077] At block 440, the second device 140 sends the authorization grant to the authorization server 130, to enable the authorization server 130 to send to the application 110 an access token for accessing the resource.

[0078] In some example embodiments, sending the authorization grant to the authorization server 130 comprises: sending the authorization grant to the authorization server 130 via an

Access and Mobility Management Function.

[0079] In some example embodiments, the method 400 further comprises: receiving, from the authorization server, an acknowledgement that the authorization grant is received via the Access and Mobility Management Function.

[0080] In some example embodiments, an apparatus capable of performing the method 300 may comprise means for performing the respective steps of the method 300. The means may be implemented in any suitable form. For example, the means may be implemented in a circuitry or software module.

[0081] In some example embodiments, the apparatus capable of performing the method 300 (for example, the authorization server 130) comprises: means for receiving, from an application, a first request for an access token to be used by the application to access a resource of a first device; means for sending, to a second device controlling the first device, a second request for an authorization grant to grant the access of the application; and means for in accordance with the authorization grant received from the second device, sending the access token to the application.

[0082] In some example embodiments, the first request comprises at least one of the following: first identity information of the first device; second identity information of the second device; and information about the resource to be accessed by the application, the information indicating a first scope of access requested by the application.

[0083] In some example embodiments, the means for sending the second request to the second device comprises: means for determining second identity information of the second device based on the first request; and means for sending the second request to the second device based on the second identity information.

[0084] In some example embodiments, the means for determining the second identity information comprises: means for extracting the second identity information from the first request.

[0085] In some example embodiments, the means for determining the second identity information comprises: mean for extracting first identity information of the first device from the first request; and means for determining the second identity information based on a mapping relationship between the first identity information and the second identity information.

[0086] In some example embodiments, the second request comprises at least one of the following: first identity information of the first device; information about the resource to be accessed by the application, the information about the resource indicating a first scope of access requested by the application; and information about the application.

[0087] In some example embodiments, the information about the application comprises at least one of the following: location information of the application; duration for which the application has been registered to a network; third identity information of the application; and API keys to distinguish traffic for different access purposes.

[0088] In some example embodiments, the means for sending the second request to the second device comprises: means for sending the second request to the second device via an Access and Mobility Management Function.

[0089] In some example embodiments, the apparatus capable of performing the method 300 further comprises: means for receiving the authorization grant from the second device via the Access and Mobility Management Function, the authorization grant indicating a second scope of access granted by the second device; and means for in accordance with the authorization grant received from the second device, sending to the second device an acknowledgement that the authorization grant is received.

[0090] In some example embodiments, an apparatus capable of performing the method 400 may comprise means for performing the respective steps of the method 400. The means may be implemented in any suitable form. For example, the means may be implemented in a circuitry or software module.

[0091] In some example embodiments, the apparatus capable of performing the method 400 (for example, the second device 140) comprises: means for receiving, from an authorization server, a request for an authorization grant to grant access of an application to a resource of a first device; means for determining, based on the request, whether to grant the access; and means for in accordance with the determination to grant the access, generating the authorization grant; and means for sending the authorization grant to the authorization server, to enable the authorization server to send to the application an access token for accessing the resource.

[0092] In some example embodiments, the request comprises at least one of the following: first identity information of the first device; information about the resource to be accessed by the application, the information about the resource indicating a first scope of access requested by the application; and information about the application.

[0093] In some example embodiments, the information about the application comprises at least one of the following: location information of the application; duration for which the application has registered to a network; third identity information of the application; and API keys to distinguish traffic for different access purposes.

[0094] In some example embodiments, the request comprises third identity information of the application, and the means for determining whether to grant the access comprises: means for verifying validity of the application based on the third identity information; means for determining whether the first device is available for the access; means for in accordance with the verification that the application is valid and the determination that the first device is available for the access, determining to grant the access; and means for in accordance with the verification that the application is invalid and/or the determination that the first device is unavailable for the access, determining to deny the access.

[0095] In some example embodiments, the request indicates a first scope of access requested by the application, and the means for generating the authorization grant comprises: means for determining, based on the first scope of access, a second scope of access to be granted to the application; and means for generating the authorization grant indicating the second scope of access.

[0096] In some example embodiments, the means for sending the authorization grant to the authorization server comprises: means for sending the authorization grant to the authorization server via an Access and Mobility Management Function.

[0097] In some example embodiments, the apparatus capable of performing the method 400 further comprises: means for receiving, from the authorization server, an acknowledgement that the authorization grant is received via the Access and Mobility Management Function.

[0098] Fig. 5 is a simplified block diagram of a device 500 that is suitable for implementing embodiments of the present disclosure. For example, the first device 120, the second device 140 and/or the authorization server 130 as shown in Fig. 1 can be implemented by the device 500. For example, the application 110 as shown in Fig. 1 can be implemented at the device 500. As shown, the device 500 includes one or more processors 510, one or more memories 520 coupled to the processor 510, and one or more communication modules 540 coupled to the processor 510.

[0099] The communication module 540 is for bidirectional communications. The communication module 540 has at least one antenna to facilitate communication. The communication interface may represent any interface that is necessary for communication with other network elements.

[00100] The processor 510 may be of any type suitable to the local technical network and may include one or more of the following: general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs) and processors based on multicore processor architecture, as non-limiting examples. The device 500 may have multiple processors, such as an application specific integrated circuit chip that is slaved in time to a clock which synchronizes the main processor.

[00101] The memory 520 may include one or more non-volatile memories and one or more volatile memories. Examples of the non-volatile memories include, but are not limited to, a Read Only Memory (ROM) 524, an electrically programmable read only memory (EPROM), a flash memory, a hard disk, a compact disc (CD), a digital video disk (DVD), and other magnetic storage and/or optical storage. Examples of the volatile memories include, but are not limited to, a random access memory (RAM) 522 and other volatile memories that will not last in the power-down duration.

[00102] A computer program 530 includes computer executable instructions that are executed by the associated processor 510. The program 530 may be stored in the ROM 524. The processor 510 may perform any suitable actions and processing by loading the program 530 into the RAM 522.

[00103] The embodiments of the present disclosure may be implemented by means of the program 530 so that the device 500 may perform any process of the disclosure as discussed with reference to Figs. 1-4. The embodiments of the present disclosure may also be implemented by hardware or by a combination of software and hardware.

[00104] In some example embodiments, the program 530 may be tangibly contained in a computer readable medium which may be included in the device 500 (such as in the memory 520) or other storage devices that are accessible by the device 500. The device 500 may load the program 530 from the computer readable medium to the RAM 522 for execution.

The computer readable medium may include any types of tangible non-volatile storage, such as ROM, EPROM, a flash memory, a hard disk, CD, DVD, and the like. Fig. 6 shows an example of the computer readable medium 600 in form of CD or DVD. The computer readable medium has the program 530 stored thereon.

[00105] It should be appreciated that future networks may utilize network functions virtualization (NFV) which is a network architecture concept that proposes virtualizing network node functions into “building blocks” or entities that may be operationally connected or linked together to provide services. A virtualized network function (VNF) may comprise one or more virtual machines running computer program codes using standard or general type servers instead of customized hardware. Cloud computing or data storage may also be utilized. In radio communications, this may mean node operations to be carried out, at least partly, in a central/centralized unit, CU, (e.g. server, host or node) operationally coupled to distributed unit, DU, (e.g. a radio head/node). It is also possible that node operations will be distributed among a plurality of servers, nodes or hosts. It should also be understood that the distribution of labour between core network operations and base station operations may vary depending on implementation.

[00106] In an embodiment, the server may generate a virtual network through which the server communicates with the distributed unit. In general, virtual networking may involve a process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network. Such virtual network may provide flexible distribution of operations between the server and the radio head/node. In practice, any digital signal processing task may be performed in either the CU or the DU and the boundary where the responsibility is shifted between the CU and the DU may be selected according to implementation.

[00107] Therefore, in an embodiment, a CU-DU architecture is implemented. In such case the apparatus 500 may be comprised in a central unit (e.g. a control unit, an edge cloud server, a server) operatively coupled (e.g. via a wireless or wired network) to a distributed unit (e.g. a remote radio head/node). That is, the central unit (e.g. an edge cloud server) and the distributed unit may be stand-alone apparatuses communicating with each other via a radio path or via a wired connection. Alternatively, they may be in a same entity communicating via a wired connection, etc. The edge cloud or edge cloud server may serve a plurality of distributed units or a radio access networks. In an embodiment, at least some of the described processes may be performed by the central unit. In another embodiment, the apparatus 500 may be instead comprised in the distributed unit, and at least some of the described processes may be performed by the distributed unit.

[00108] In an embodiment, the execution of at least some of the functionalities of the apparatus 500 may be shared between two physically separate devices (DU and CU) forming one operational entity. Therefore, the apparatus may be seen to depict the operational entity comprising one or more physically separate devices for executing at least some of the described processes. In an embodiment, such CU-DU architecture may provide flexible distribution of operations between the CU and the DU. In practice, any digital signal processing task may be performed in either the CU or the DU and the boundary where the responsibility is shifted between the CU and the DU may be selected according to implementation. In an embodiment, the apparatus 500 controls the execution of the processes, regardless of the location of the apparatus and regardless of where the processes/functions are carried out.

[00109] Generally, various embodiments of the present disclosure may be implemented in hardware or special purpose circuits, software, logic or any combination thereof. Some aspects may be implemented in hardware, while other aspects may be implemented in firmware or software which may be executed by a controller, microprocessor or other computing device. While various aspects of embodiments of the present disclosure are illustrated and described as block diagrams, flowcharts, or using some other pictorial representations, it is to be understood that the block, apparatus, system, technique or method described herein may be implemented in, as non-limiting examples, hardware, software, firmware, special purpose circuits or logic, general purpose hardware or controller or other computing devices, or some combination thereof.

[00110] The present disclosure also provides at least one computer program product tangibly stored on a non-transitory computer readable storage medium. The computer program product includes computer-executable instructions, such as those included in program modules, being executed in a device on a target real or virtual processor, to carry out the methods 300 and/or 400 as described above with reference to Figs. 3-4. Generally, program modules include routines, programs, libraries, objects, classes, components, data structures, or the like that perform particular tasks or implement particular abstract data types. The functionality of the program modules may be combined or split between program modules as desired in various embodiments. Machine-executable instructions for program modules may be executed within a local or distributed device. In a distributed device, program modules may be located in both local and remote storage media.

[00111] Program code for carrying out methods of the present disclosure may be written in any combination of one or more programming languages. These program codes may be provided to a processor or controller of a general purpose computer, special purpose computer, or other programmable data processing apparatus, such that the program codes, when executed by the processor or controller, cause the functions/operations specified in the flowcharts and/or block diagrams to be implemented. The program code may execute entirely on a machine, partly on the machine, as a stand-alone software package, partly on the machine and partly on a remote machine or entirely on the remote machine or server.

[00112] In the context of the present disclosure, the computer program codes or related data may be carried by any suitable carrier to enable the device, apparatus or processor to perform various processes and operations as described above. Examples of the carrier include a signal, computer readable medium, and the like.

[00113] The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable medium may include but not limited to an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples of the computer readable storage medium would include an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing.

[00114] Further, while operations are depicted in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Likewise, while several specific implementation details are contained in the above discussions, these should not be construed as limitations on the scope of the present disclosure, but rather as descriptions of features that may be specific to particular embodiments. Certain features that are described in the context of separate embodiments may also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment may also be implemented in multiple embodiments separately or in any suitable sub-combination.

[00115] Although the present disclosure has been described in languages specific to structural features and/or methodological acts, it is to be understood that the present disclosure defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

WE CLAIM:

1. An apparatus comprising:

at least one processor; and

at least one memory including computer program codes;

the at least one memory and the computer program codes are configured to, with the at least one processor, cause the apparatus to:

receive, from an application, a first request for an access token to be used by the application to access a resource of a first device;

send, to a second device controlling the first device, a second request for an authorization grant to grant the access of the application; and

in accordance with the authorization grant received from the second device, send the access token to the application.

2. The apparatus of claim 1, wherein the first request comprises at least one of the following:

first identity information of the first device;

second identity information of the second device; and

information about the resource to be accessed by the application, the information indicating a first scope of access requested by the application.

3. The apparatus of claim 1, wherein the apparatus is caused to:

determine second identity information of the second device based on the first request; and

send the second request to the second device based on the second identity information.

4. The apparatus of claim 3, wherein the apparatus is caused to:

extract the second identity information from the first request.

5. The apparatus of claim 3, wherein the apparatus is caused to:

extract first identity information of the first device from the first request; and

determine the second identity information based on a mapping relationship between the first identity information and the second identity information.

6. The apparatus of claim 1, wherein the second request comprises at least one of the following:

first identity information of the first device;

information about the resource to be accessed by the application, the information about the resource indicating a first scope of access requested by the application; and

information about the application.

7. The apparatus of claim 6, wherein the information about the application comprises at least one of the following:

location information of the application;

duration for which the application has registered to a network;

third identity information of the application; and

Application Programming Interface keys to distinguish traffic for different access purposes.

8. The apparatus of claim 1, wherein the apparatus is caused to:

send the second request to the second device via an Access and Mobility Management Function.

9. The apparatus of claim 8, wherein the apparatus is further caused to:

receive the authorization grant from the second device via the Access and Mobility Management Function, the authorization grant indicating a second scope of access granted by the second device; and

in accordance with the authorization grant received from the second device, send to the second device an acknowledgement that the authorization grant is received.

10. An apparatus comprising:

at least one processor; and

at least one memory including computer program codes;

the at least one memory and the computer program codes are configured to, with the at least one processor, cause the apparatus to:

receive, from an authorization server, a request for an authorization grant to grant access of an application to a resource of a first device;

determine, based on the request, whether to grant the access;

in accordance with the determination to grant the access, generate the authorization grant; and

send the authorization grant to the authorization server, to enable the authorization server to send to the application an access token for accessing the resource.

11. The apparatus of claim 10, wherein the request comprises at least one of the following:

first identity information of the first device;

information about the resource to be accessed by the application, the information about the resource indicating a first scope of access requested by the application; and

information about the application.

12. The apparatus of claim 11, wherein the information about the application comprises at least one of the following:

location information of the application;

duration for which the application has registered to a network;

third identity information of the application; and

Application Programming Interface keys to distinguish traffic for different access purposes.

13. The apparatus of claim 10, wherein the request comprises third identity information of the application, and wherein the apparatus is caused to:

verify validity of the application based on the third identity information;

determine whether the first device is available for the access;

in accordance with the verification that the application is valid and the determination that the first device is available for the access, determine to grant the access; and

in accordance with the verification that the application is invalid and/or the determination that the first device is unavailable for the access, determine to deny the access.

14. The apparatus of claim 10, wherein the request indicates a first scope of access

requested by the application, and wherein the apparatus is caused to:

determine, based on the first scope of access, a second scope of access to be granted to the application; and

generate the authorization grant indicating the second scope of access.

15. The apparatus of claim 10, wherein the apparatus is caused to:

send the authorization grant to the authorization server via an Access and Mobility Management Function.

16. The apparatus of claim 10, wherein the apparatus is further caused to:

receive, from the authorization server, an acknowledgement that the authorization grant is received via the Access and Mobility Management Function.

17. A method comprising:

receiving, from an application, a first request for an access token to be used by the application to access a resource of a first device;

sending, to a second device controlling the first device, a second request for an authorization grant to grant the access of the application; and

in accordance with the authorization grant received from the second device, sending the access token to the application.

18. The method of claim 17, wherein the first request comprises at least one of the following:

first identity information of the first device;

second identity information of the second device; and

information about the resource to be accessed by the application, the information indicating a first scope of access requested by the application.

19. The method of claim 17, wherein sending the second request to the second device comprises:

determining second identity information of the second device based on the first request; and

sending the second request to the second device based on the second identity information.

20. The method of claim 19, wherein determining the second identity information comprises:

extracting the second identity information from the first request.

21. The method of claim 19, wherein determining the second identity information comprises:

extracting first identity information of the first device from the first request; and

determining the second identity information based on a mapping relationship between the first identity information and the second identity information.

22. The method of claim 17, wherein the second request comprises at least one of the following:

first identity information of the first device;

information about the resource to be accessed by the application, the information about the resource indicating a first scope of access requested by the application; and

information about the application.

23. The method of claim 22, wherein the information about the application comprises at least one of the following:

location information of the application;

duration for which the application has registered to a network;

third identity information of the application; and

Application Programming Interface keys to distinguish traffic for different access purposes.

24. The method of claim 17, wherein sending the second request to the second device comprises:

sending the second request to the second device via an Access and Mobility Management Function.

25. The method of claim 24, further comprising:

receiving the authorization grant from the second device via the Access and Mobility Management Function, the authorization grant indicating a second scope of access granted by the second device; and

in accordance with the authorization grant received from the second device, sending to the second device an acknowledgement that the authorization grant is received.

26. A method comprising:

receiving, from an authorization server, a request for an authorization grant to grant access of an application to a resource of a first device;

determining, based on the request, whether to grant the access;

in accordance with the determination to grant the access, generating the authorization grant; and

sending the authorization grant to the authorization server, to enable the authorization server to send to the application an access token for accessing the resource.

27. The method of claim 26, wherein the request comprises at least one of the following:

first identity information of the first device;

information about the resource to be accessed by the application, the information about the resource indicating a first scope of access requested by the application; and

information about the application.

28. The method of claim 27, wherein the information about the application comprises at least one of the following:

location information of the application;

duration for which the application has registered to a network;

third identity information of the application; and

Application Programming Interface keys to distinguish traffic for different access purposes.

29. The method of claim 26, wherein the request comprises third identity information of the application, and determining whether to grant the access comprises:

verifying validity of the application based on the third identity information;

determining whether the first device is available for the access;

in accordance with the verification that the application is valid and the determination that the first device is available for the access, determining to grant the access; and

in accordance with the verification that the application is invalid and/or the determination that the first device is unavailable for the access, determining to deny the access.

30. The method of claim 26, wherein the request indicates a first scope of access requested by the application, and generating the authorization grant comprises:

determining, based on the first scope of access, a second scope of access to be granted to the application; and

generating the authorization grant indicating the second scope of access.

31. The method of claim 26, wherein sending the authorization grant to the authorization server comprises:

sending the authorization grant to the authorization server via an Access and Mobility Management Function.

32. The method of claim 26, further comprising:

receiving, from the authorization server, an acknowledgement that the authorization grant is received via the Access and Mobility Management Function.

33. An apparatus comprising:

means for receiving, from an application, a first request for an access token to be used by the application to access a resource of a first device;

means for sending, to a second device controlling the first device, a second request for an authorization grant to grant the access of the application; and

means for in accordance with the authorization grant received from the second device, sending the access token to the application.

34. An apparatus comprising:

means for receiving, from an authorization server, a request for an authorization grant to grant access of an application to a resource of a first device;

means for determining, based on the request, whether to grant the access;

means for in accordance with the determination to grant the access, generating the authorization grant; and

means for sending the authorization grant to the authorization server, to enable the authorization server to send to the application an access token for accessing the resource.

35. A computer readable storage medium comprising program instructions stored thereon, the instructions, when executed by an apparatus, causing the apparatus to:

receive, from an application, a first request for an access token to be used by the application to access a resource of a first device;

send, to a second device controlling the first device, a second request for an authorization grant to grant the access of the application; and

in accordance with the authorization grant received from the second device, send the access token to the application.

36. A computer readable storage medium comprising program instructions stored thereon, the instructions, when executed by an apparatus, causing the apparatus to:

receive, from an authorization server, a request for an authorization grant to grant access of an application to a resource of a first device;

determine, based on the request, whether to grant the access;

in accordance with the determination to grant the access, generate the authorization grant; and

send the authorization grant to the authorization server, to enable the authorization server to send to the application an access token for accessing the resource.

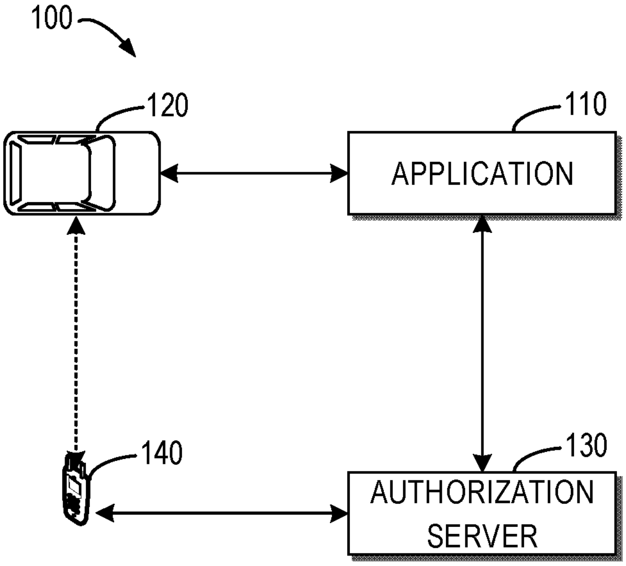

Fig. 1

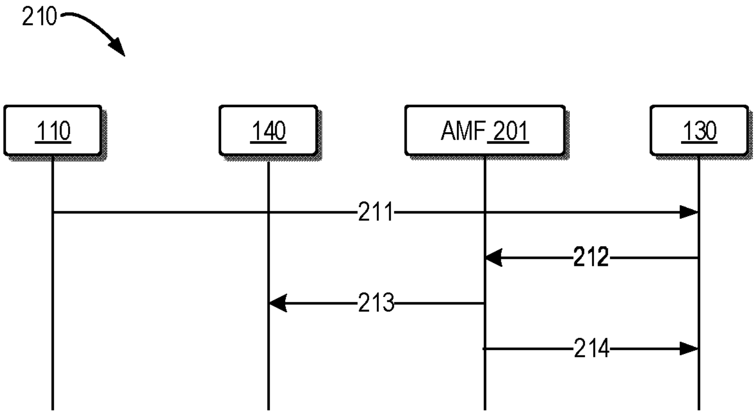
210
110
140
AMF 201
130
211
212
213
214

Fig. 2A

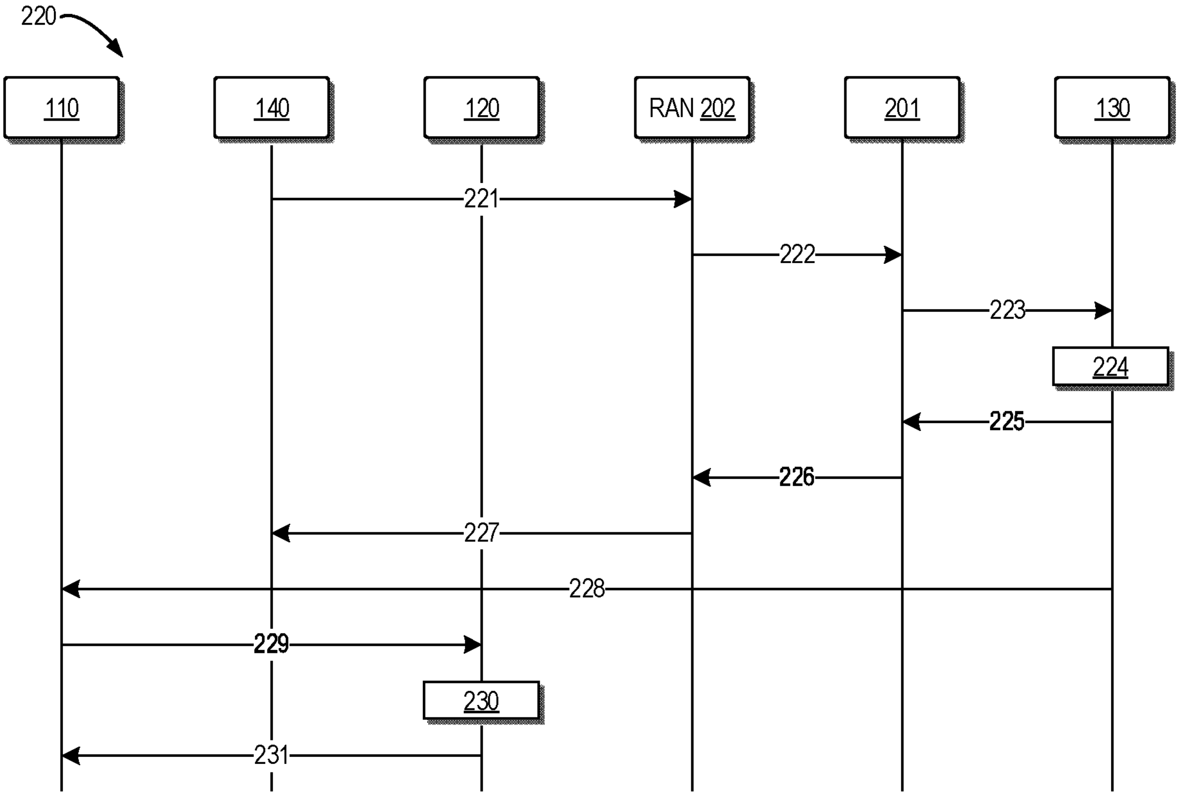
220
110
140
120
RAN 202
201
130
221
222
223
224
225
226
227
228
229
230
231

Fig. 2B

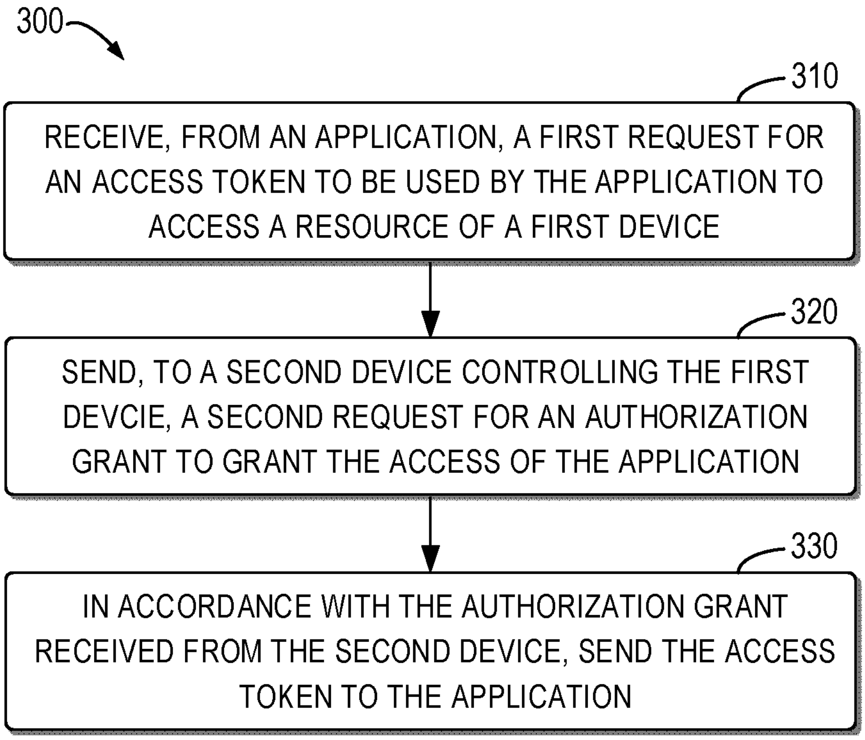
300
310
RECEIVE, FROM AN APPLICATION, A FIRST REQUEST FOR AN ACCESS TOKEN TO BE USED BY THE APPLICATION TO ACCESS A RESOURCE OF A FIRST DEVICE
320
SEND, TO A SECOND DEVICE CONTROLLING THE FIRST DEVCIE, A SECOND REQUEST FOR AN AUTHORIZATION GRANT TO GRANT THE ACCESS OF THE APPLICATION
330
IN ACCORDANCE WITH THE AUTHORIZATION GRANT RECEIVED FROM THE SECOND DEVICE, SEND THE ACCESS TOKEN TO THE APPLICATION

Fig. 3

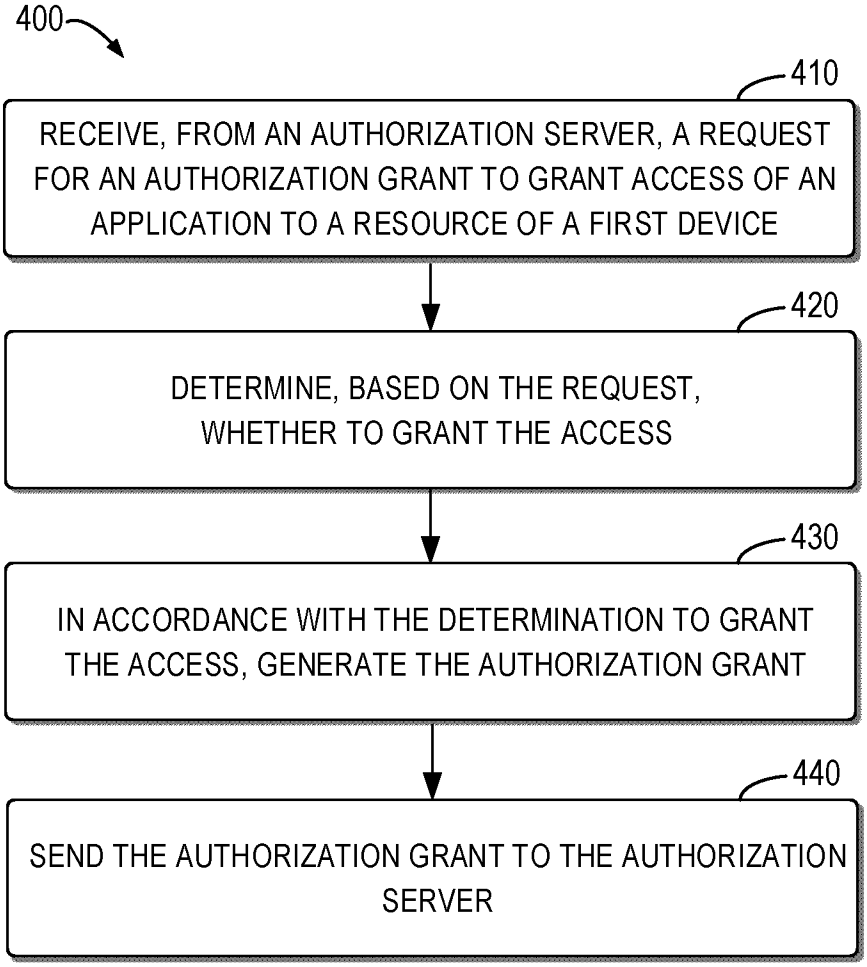
400
410
RECEIVE, FROM AN AUTHORIZATION SERVER, A REQUEST FOR AN AUTHORIZATION GRANT TO GRANT ACCESS OF AN APPLICATION TO A RESOURCE OF A FIRST DEVICE
420
DETERMINE, BASED ON THE REQUEST, WHETHER TO GRANT THE ACCESS
430
IN ACCORDANCE WITH THE DETERMINATION TO GRANT THE ACCESS, GENERATE THE AUTHORIZATION GRANT
440
SEND THE AUTHORIZATION GRANT TO THE AUTHORIZATION SERVER

Fig. 4

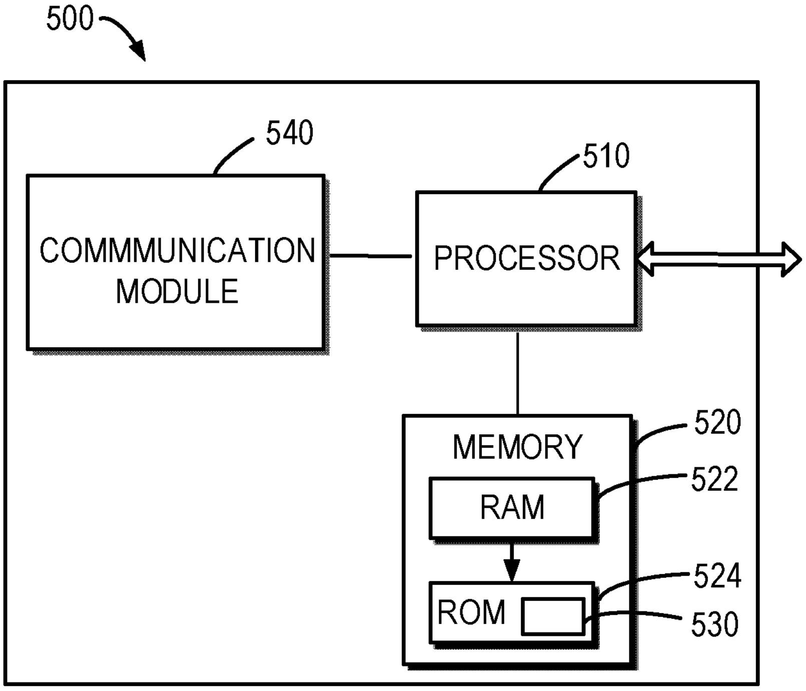
500
540
COMMMUNICATION MODULE
510
PROCESSOR
520
MEMORY
522
RAM
524
ROM
530

Fig. 5

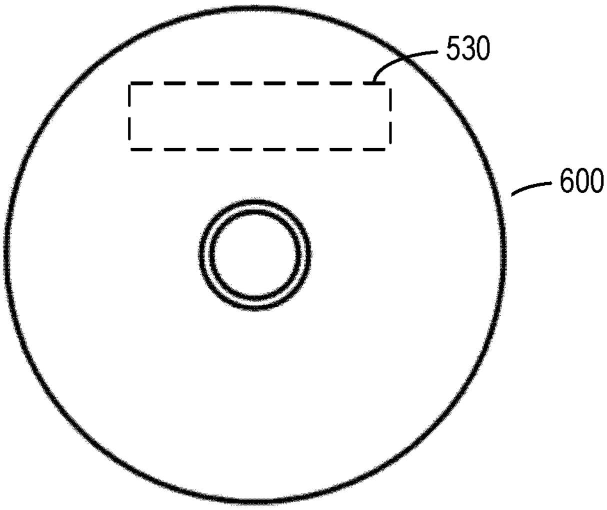
530
600

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/051096

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/32 H04W12/37 H04W12/084
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	D Hardt: "RFC 6749 The OAuth 2.0 Authorization Framework", , 31 October 2012 (2012-10-31), pages 1-76, XP055218558, Retrieved from the Internet: URL:https://www.rfc-editor.org/rfc/pdfrfc/rfc6749.txt.pdf [retrieved on 2015-10-06]	1-6,10, 11,13, 14, 17-22, 26,27, 29,30, 33-36
Y	Section 1.2 Section 3.2.1 Section 3.3	7-9,12, 15,16, 23-25, 28,31,32

	-/--	

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 March 2021	17/03/2021
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Bharucha, Zubin

1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/051096

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 10 2016 222541 A1 (AUDI AG) 17 May 2018 (2018-05-17)	7,12,23, 28
A	paragraph [0001] paragraph [0013] paragraph [0020] paragraph [0022] paragraph [0027] paragraph [0035] - paragraph [0037] paragraph [0045] - paragraph [0046] figure 1 -----	1-6, 8-11, 13-22, 24-27, 29-36
Y	"3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Network Function Repository Services; Stage 3 (Release 16)", 3GPP STANDARD; TECHNICAL SPECIFICATION; 3GPP TS 29.510, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. CT WG4, no. V16.2.0 20 December 2019 (2019-12-20), pages 1-167, XP051840882, Retrieved from the Internet: URL:ftp://ftp.3gpp.org/Specs/archive/29_series/29.510/29510-g20.zip 29510-g20.docx [retrieved on 2019-12-20]	8,9,15, 16,24, 25,31,32
A	Section 5.4.2.2.1 Section 5.4.2.2.2 -----	1-7, 10-14, 17-23, 26-30, 33-36

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2021/051096

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102016222541 A1	17-05-2018	CN 110035932 A	19-07-2019
		DE 102016222541 A1	17-05-2018
		KR 20190084293 A	16-07-2019
		US 2020062215 A1	27-02-2020
		WO 2018091168 A1	24-05-2018