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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 September 2021 (10.09.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/176131 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04W 12/104* (2021.01)
H04L 29/06 (2006.01) *H04W 12/60* (2021.01)
H04W 12/084 (2021.01)

(21) International Application Number:
PCT/FI2021/050040

(22) International Filing Date:
22 January 2021 (22.01.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202041009301 04 March 2020 (04.03.2020) IN

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

(72) Inventors: **PRASAD, Pradyumna Ram**; No 203, Mythri sapphire Apt., 4th Main, BOB Colony, Puttenhalli, JP Nagar 7th Phase, Bangalore 560078 (IN). **MURALIDHARA, Harish**; 1155/14, Visveswaraya nagara 7th block, Near Neelakateshwara Temple, Karnataka, Bangalore 560056 (IN). **MAHADEVAIAH, Krishnamurthy**; 18, 2nd stage, 2nd block Nagarabhavi, Bangalore 560072 (IN). **BYKAMPADI, Nagendra**; 59 A Eastwood layout, Haralur Road, Off Sarjapura Main Road, Karnataka, Bangalore 560102 (IN).

(74) Agent: **NOKIA TECHNOLOGIES OY** et al.; Ari Aarnio, IPR Department, 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,

(54) Title: ENHANCED AUTHORIZATION IN COMMUNICATION NETWORKS

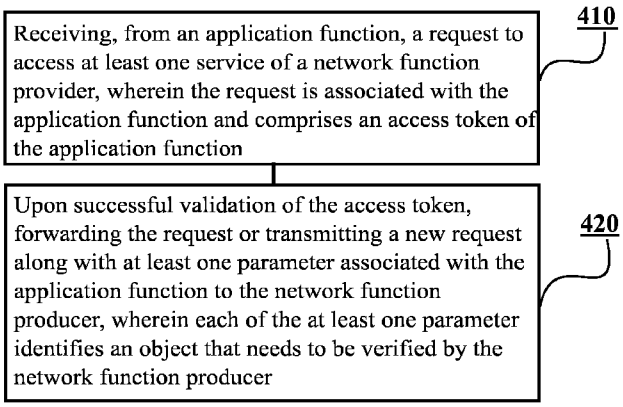

FIGURE 4

(57) Abstract: According to an example aspect of the present invention, there is provided a method for a network exposure function, the method comprising receiving, from an application function, a request to access at least one service of a network function producer, wherein the request is associated with the application function and comprises an access token of the application function and upon successful validation of the access token, forwarding the request or transmitting a new request along with at least one parameter associated with the application function to the network function producer, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer.

WO 2021/176131 A1

[Continued on next page]

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, 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))*

ENHANCED AUTHORIZATION IN COMMUNICATION NETWORKS

FIELD

[0001] Various example embodiments relate in general to communication networks, such as core networks of cellular communication systems, and more specifically, to enhancing authorization in such networks.

BACKGROUND

[0002] Authorization is needed in various communication networks to ensure that only users and network entities that have a right to access certain services can do that. Proper authorization needs to be ensured for example in core networks of cellular communication systems, such as in 5G core networks developed by the 3rd Generation Partnership Project, 3GPP. Using 5G as an example, in 5G core networks, Application Functions, AFs, need to have access to some services but access control needs to be enforced at the same time. The 3GPP still develops 5G core networks and there is a need to provide improved methods, apparatuses and computer programs for enhancing authorization in 5G core networks, and in other networks in the future as well.

SUMMARY

[0003] According to some aspects, there is provided the subject-matter of the independent claims. Some example embodiments are defined in the dependent claims.

[0004] The scope of protection sought for various example embodiments of the invention is set out by the independent claims. The example embodiments and features, if any, described in this specification that do not fall under the scope of the independent claims are to be interpreted as examples useful for understanding various example embodiments of the invention.

[0005] According to a first aspect of the present invention, there is provided a method for a network exposure function, the method comprising receiving, from an application function, a request to access at least one service of a network function producer, wherein the request is associated with the application function and comprises an access token of the application function and upon successful validation of the access token, forwarding the

request or transmitting a new request along with at least one parameter associated with the application function to the network function producer, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer.

[0006] Example embodiments of the first aspect may comprise at least one feature from the following bulleted list:

- the object may be a location, time-of-day or subscriber identity range;
- the method may further comprise transmitting, upon successfully verifying one parameter associated with the application function, another parameter associated with the application function to the network function producer without transmitting said one parameter;
- said one parameter may identify a subscriber identity range object and said another parameter identifies a location object;
- the method may further comprise transmitting, upon successfully verifying that a subscriber identity range of the application function comprises an identity of at least one subscriber associated with the application function, the request along with the at least one parameter associated with the application function to the network function provider;
- the method may further comprise transmitting, upon successfully verifying that a time-of-day is such that the application function is allowed to access the at least one service, the request along with the at least one parameter associated with the application function to the network function provider;
- the at least one parameter may comprise a subscriber identity range object indicating that an identity of at least one subscriber of the application function needs to be verified versus a subscriber identity range of the application function;
- the at least one parameter may comprise a location object indicating that a location of at least one subscriber of the application function needs to be verified versus a region wherein the application function is allowed to access the at least one service when the at least one subscriber is within the region;
- the at least one parameter may comprise a time-of-day object indicating that a time-of-day needs to be verified versus a time when the application function is allowed to access the at least one service;

- the method may further comprise receiving, from the application function, the at least one parameter associated with the application function.

[0007] According to a second aspect of the present invention, there is provided a method for a network function producer, the method comprising receiving, from a network exposure function, a request to access at least one service of the network function producer along with at least one parameter associated with an application function, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer, determining, based on the at least one parameter associated with the application function, whether to grant the request or not and transmitting a response to the network exposure function, wherein the response depends on whether the request is granted.

[0008] Example embodiments of the second aspect may comprise at least one feature from the following bulleted list:

- the object may be a location, time-of-day or subscriber identity range;
- the at least one parameter associated with the application function may identify a subscriber identity range object, and the method may further comprise, determining whether to grant the request or not by checking whether a subscriber identity range of the application function comprises an identity of at least one subscriber of the application function;
- the at least one parameter associated with the application function may identify a location object, and the method may further comprise, determining whether to grant the request or not by comparing a location of at least one subscriber of the application function versus a region wherein the application function is allowed to access the at least one service when the at least one subscriber is within the region;
- the at least one parameter associated with the application function may identify a time-of-day object, and the method may further comprise, determining whether to grant the request or not by checking whether a time-of-day is such that the application function is allowed to access the at least one service.

[0009] Example embodiments of the first or the second aspect may comprise at least one feature from the following bulleted list:

- the network function producer may be a unified data management network function;
- the network exposure function and the network function producer may operate according to at least one standard specification defined by a 3rd Generation Partnership Project, 3GPP;
- the network exposure function and the network function producer may be in a core network of a cellular communication network;
- the core network may be a 5G core network;
- the request and the at least one parameter may be associated with at least one subscriber of the application function.

[0010] According to a third aspect of the present invention, there is provided an apparatus, comprising one or more processors, and memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the first method. The at least one memory and the computer program code may be configured to, with the at least one processing core, cause the apparatus at least to perform, receive, from an application function, a request to access at least one service of a network function producer, wherein the request is associated with the application function and comprises an access token of the application function and upon successful validation of the access token, forward the request or transmit a new request along with at least one parameter associated with the application function to the network function producer, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer.

[0011] According to a fourth aspect of the present invention, there is provided an apparatus, comprising one or more processors, and memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the second method. The at least one memory and the computer program code may be further configured to, with the at least one processing core, cause the apparatus at least to perform, receive, from a network exposure function, a request to access at least one service of the network function producer along with at least one parameter associated with an application function, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer, determine, based on the at least one parameter associated with the

application function, whether to grant the request or not and transmit a response to the network exposure function, wherein the response depends on whether the request is granted.

[0012] According to a fifth aspect of the present invention, there is provided an apparatus, comprising means for performing the first method. The apparatus may comprise means for receiving, from an application function, a request to access at least one service of a network function producer, wherein the request is associated with the application function and comprises an access token of the application function and upon successful validation of the access token, means for forwarding the request or transmitting a new request along with at least one parameter associated with the application function to the network function producer, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer.

[0013] According to a sixth aspect of the present invention, there is provided an apparatus, comprising means for performing the second method. The apparatus may comprise means for receiving, from a network exposure function, a request to access at least one service of the network function producer along with at least one parameter associated with an application function, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer, means for determining, based on the at least one parameter associated with the application function, whether to grant the request or not and means for transmitting a response to the network exposure function, wherein the response depends on whether the request is granted.

[0014] According to a seventh aspect of the present invention, there is provided non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least perform the method of the first aspect. According to an eighth aspect of the present invention, there is provided non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least perform the method of the second aspect.

[0015] According to a ninth aspect of the present invention, there is provided a computer program configured to perform the method of the first aspect. According to a tenth aspect of the present invention, there is provided a computer program configured to perform the method of the second aspect.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] FIGURE 1 illustrates an exemplary system in accordance with at least some example embodiments;

[0017] FIGURE 2 illustrates signalling in accordance with at least some example embodiments;

[0018] FIGURE 3 illustrates an example apparatus capable of supporting at least some example embodiments;

[0019] FIGURE 4 illustrates a flow graph of a first method in accordance with at least some example embodiments;

[0020] FIGURE 5 illustrates a flow graph of a second method in accordance with at least some example embodiments.

EXAMPLE EMBODIMENTS

[0021] Authorization may be enhanced by the procedures described herein for example for Application Functions, AFs, in communication networks, such as in 5G core networks or other core networks. At least in the case of 5G core networks, the network may comprise network functions such as a Network Exposure Function, NEF, and a Network Function Producer, NFP, such as a Unified Data Management, UDM, network function. According to some example embodiments of the present invention, authorization may be enhanced by exploiting at least one subject parameter identifying an object, such as a location, time-of-day or subscriber identity range associated with an AF or more specifically, in some example embodiments, associated with at least one subscriber of the AF. That is to say, the at least one subject parameter may be AF-specific.

[0022] A subject parameter may be referred to as a parameter or as an authorization parameter in general. The subject parameter may be specific to a subject of an access token, such as an OAuth token for example. That is to say, the subject of the access token may be a network function, such as the NEF or the AF, that uses the access token to access a service provided by another network function, such as the UDM.

[0023] Upon receiving a request related to at least one service of the NFP from an AF and validating an access token successfully, the NEF may forward the request, or transmit a new request, to the NFP together with the at least one subject parameter associated with the AF. In some example embodiments, the at least one subject parameter may be associated with at least one subscriber of the AF Thus, the NFP may check the least one subject parameter and decide whether to accept the request based on that, to improve authorization of AFs and subscribers of AFs. In some example embodiments, the NEF may also verify the least one subject parameter, thereby enabling two-staged authorization process.

[0024] In some example embodiments, the NEF may verify one subject parameter and the NFP may verify another subject parameter, to ensure that all relevant subject parameters are verified, even if the NEF or the NFP could not do that alone. As an example, the NEF may verify that a subscriber identity range of the AF comprises an identity of the at least one subscriber and the NFP may verify the location of the AF or the location of the at least one subscriber of the AF, thereby enabling proper authentication for various services, such as location-based services, because the NEF may not know the location of the AF or the at least one subscriber of the AF.

[0025] In some example embodiments, a framework that allows any AF specific aspect to be the subject to or basis for authorization by the target NF is provided. For instance, one of the common AF-specific attribute/object may be the set of subscribers assigned/allotted to it. On the other hand, in some example embodiments, the common AF-specific attribute/object may be AF's location etc. In general, the proposed access token may be generic enough to handle one or more of those AF-specific attributes.

[0026] FIGURE 1 illustrates an exemplary system in accordance with at least some example embodiments of the present invention. The exemplary system of FIGURE 1 comprises two Public Land Mobile Networks, PLMNs, 110 and 112, each equipped with at least one NF, 120 and 122, respectively. An NF may refer to an operational and/or a physical entity. An NF may be a specific network node or element, or a specific function or set of functions carried out by one or more entities, such as Virtual Network Elements, VNFs. At least some embodiments of the present invention may be applied in containerized deployments as well. One physical node may be configured to perform plural NFs. Examples of such network functions include a (radio) access or resource control or management

function, session management or control function, interworking, data management or storage function, authentication function or a combination of one or more of these functions.

[0027] In case of a 3rd Generation Partnership Project, 3GPP, Service-Based Architecture, SBA, of 5G core networks, NFs may comprise at least some of an Access and Mobility Function, AMF, a Session Management Function, SMF, a Network Slice Selection Function, NSSF, a NEF, an Network Repository Function, NRF, a UDM, an Authentication Server Function, AUSF, a Policy Control Function, PCF, an AF, Operations Administration and Maintenance, OAM, and Network Data Analysis Function, NWDAF. In some example embodiments, the AF may not be a NF though as defined by the 3GPP. Instead, the AF may be a complement to the NF. The AF may be a third party AF, e.g., for an enterprise.

[0028] In some example embodiments, the UDM may provide for example authentication and subscription information to the other NFs, such as NFs in 5G core network. The UDM may manage network user data in a single element. The UDM may be similar to Home Subscriber Service, HSS, in 4G networks. The UDM may provide authentication and subscription information to NFs which need information for controlling network access and sessions of subscribers. The UDM may be stateful, i.e., keep data locally, or stateless, i.e., store data externally in a User Data Repository, UDR.

[0029] UDM – Event Exposure, UDM-EE, is one example of a UDM. The UDM-EE may provide an event exposure service, which may be used by a NEF to subscribe to or unsubscribe from UDM event notifications. A NEF may request for events exposed by the AMF and in such a case the UDM may utilize the AMF's event exposure service. Other services provided by UDMs comprise at least a subscriber data management service, UE context management service and UE authentication service. A UDM may provide services concerning at least events of the following events; loss of connectivity, UE reachability for data, UE reachability for SMS, location reporting, change of SUPI PEI association, roaming status, communication failure and availability after DNN failure. Embodiments of the present invention are not limited to any specific service provided by a UMD though.

[0030] The PLMNs 110 and 112 may further comprise a Security Edge Protection Proxy, SEPP, 130 and 132, respectively. The SEPPs 130 and 132 may be configured to operate as a security edge node or gateway. The NFs may communicate with each other

using representational state transfer Application Programming Interfaces, APIs. These may be known as Restful APIs.

[0031] The SEPP 130, 132 may be a network node at the boundary of an operator's network that may receive a message, such as an HTTP request or HTTP response from the NF, applies protection for sending, and forwards the reformatted message through a chain of intermediate nodes, such as IP eXchanges, IPX, towards a receiving SEPP. The receiving SEPP receives a message sent by the sending SEPP and forwards the message towards an NF within its operator's network, e.g. the AUSF.

[0032] The NEF for example may comprise an Application Exposure Function, AEF, and a Common API Framework, CAPIF. The AEF may also be referred to as an API Exposing Function. In any case, the AEF may be a provider of Service APIs and/or a service communication entry point of a Service API to API invokers, such as AFs. The CAPIF may be a functionality that may be a part of the AEF of the NEF, or the NEF in general. The CAPIF may be defined in a 3GPP standard specification TS 29.222 for example.

[0033] The CAPIF may provide services such as CAPIF Discover Service API, CAPIF Publish Service API, CAPIF Events API, CAPIF API Invoker Management API, CAPIF Security API, CAPIF Monitoring API, CAPIF Logging API Invocation API, CAPIF Auditing API, CAPIF Access Control Policy API. In some example embodiments, security of APIs is considered. An AF may support impact of an application on traffic routing, access to the NEF and policy control, for example similarly as in the Evolved Packet Core, EPC.

[0034] An inter-PLMN interconnection allows secure communication between a service-consuming NF and a service-producing NF, referred to as a cNF 120 and a pNF 122 in FIGURE 1. In some example embodiments of the present invention, the cNF 120 may be referred to as an NF Consumer, NFC, and the pNF 122 may be referred to as an NFP. A Service Communication Proxy, SCP, 150 may be deployed for indirect communication between network functions. The SCP 150 may be an intermediate function/element for assisting in routing of messages, such as control plane messages such as Diameter Routing Agent, DRA, messages between NFs.

[0035] Direct communication may be applied between the cNF 120 and the pNF 122 for an NF service, or NF service communication may be performed indirectly via SCP(s)

150. In direct communication, the cNF 120 may perform discovery of the target pNF 122 by local configuration or via a local NRF, the cNRF 140. The cNF 120 may delegate the discovery of the target pNF 122 to the pSCP 150 used for indirect communication. In the latter case, the pSCP 152 uses the parameters provided by the cNF 120 to perform discovery and/or selection of the target NFP. The pSCP 152 address may be locally configured in cNF 120. In general, an SCP may be an intermediate function covering delegated NF discovery to help resolving the target NF producer instances and delegated routing to help route control plane messages between two NFs.

[0036] NF discovery and NF service discovery enable core network entities, such as the cNF 140 or the SCP 150, to discover a set of NF instance(s) and NF service instance(s) for a specific NF service or an NF type. The NRF is a function that is used to support the functionality of NFs and NF service discovery and status notification. The NRF may maintain an NF profile of available NF instances and their supported services. The NRF may notify about newly registered, updated, or deregistered NF instances along with its NF services to a subscribed cNF 120 or cSCP 150. Unless the expected NF and/or NF service information is locally configured on the requester NF, such as when the expected NF service or NF is in the same PLMN as the requester NF, the NF and NF service discovery may be implemented via the NRF. The NRF may be a logical function. The NRF may also support status notification. An NRF may be co-located together with an SCP.

[0037] In order for the cNF 120 or the cSCP 150 to obtain information about the NF and/or NF service(s) registered or configured in a PLMN/slice, the cNF 120 or the cSCP 150 may initiate, based on local configuration, a discovery procedure with the cNRF 140. The discovery procedure may be initiated by providing the type of the NF and optionally a list of the specific service(s) it is attempting to discover. The cNF 120 or the cSCP 150 may also provide other service parameters, such as slicing related information.

[0038] In case of indirect communication, during an NF service discovery in inter-PLMN (roaming) communication, the cSCP 150, on behalf of the cNF 120, may request service discovery from an NRF in its PLMN 110, i.e., the cNRF 140. The cNRF 140 may send a discovery request to an NRF, referred herein as the pNRF 142, in another PLMN 112, e.g. the home PLMN. The pNRF 142 in the other PLMN 112 may respond with a discovery response which may be forwarded to the cSCP via the cNRF 140 in the PLMN 110 of the

cNF 120. Then the cSCP may trigger service requests for the pNF via the cSEPP 130 and the pSEPP 132. When using indirect communication, a cNF 120 may provide the SCP an address or name of the NRF which may be used by the SCP.

[0039] It is to be noted that at least some of the entities or nodes 120, 122, 130, 132, 140, 142, 150, 152 may act in both service-consuming and service-providing roles and that their structure may also be similar or identical, even though their role in the example of FIGURE 1 in delivery of a particular message is identified by use of the prefix "c" or "p" indicating whether they are acting for the service-consuming or service-producing NF. It is to be noted that instead of "c" and "p", "v" for visited and "h" for home may be used to refer to at least some respective entities in the visited and home PLMNs.

[0040] In some example embodiments, OAuth based authorization and token exchange may be applied between the mobile networks. Thus, for example the pNRF 142, may be or perform functionalities of an OAuth server. The cNF 120 may be an OAuth client and the pNF 122 may operate as OAuth resource server, and both may be configured to support OAuth authorization framework as defined in RFC 6749.

[0041] In some example embodiments of the present invention, an AF may need to access or subscribe for a service of a NFP, such as a UDM. The service may be related to a network event, e.g., event monitoring or subscription. For that, the AF may transmit a request concerning at least one service of the NFP to the NEF. The request may be for example an event monitoring request or a subscription request. The NEF may then forward the request, or transmit a new request, to an appropriate NF, such as the UDM, using a Service Based Interface, SBI, for example.

[0042] Embodiments of the present invention may be generally used to avoid authorization gaps. For instance, performing authorization only at a level of AFs may not be sufficient in various use cases. Embodiments of the present invention therefore provide additional levels of authorization, e.g., based on at least one subject parameter that is associated with the AF or more specifically, in some example embodiments, associated with the at least one subscriber of the AF. For instance, the at least one subject parameter may be specific for the AF in question and identify an object, such as a subscriber identity range, or even specific for the at least one subscriber of the AF and identify an object, such as a location wherein access is allowed or time-of-day when access is allowed. For instance,

subscriber identity ranges may refer to identities such as SUPI, GPSI, MSISDN and external identities. The at least one subject parameter may need to be verified by the NEF and/or the NFP, such as the UDM, before providing the required service. In some example embodiments, the object, or a type of the object, may be identified in a subject parameter type (subjectParameterType) and the corresponding object, which may comprise a value for that specific subject parameter type, may also be present therein. That is to say, the object itself may be transmitted along with each of the at least one subject parameter.

[0043] The at least one subject parameter may relate to information that the NFP has and in such case a quick one-step authorization process by the NFP may be used to enhance authorization. In some example embodiments, the at least one subject parameter may relate to information that both, the NFP and the NEF, have. Thus a two-stage authorization process may be used, where the NEF may reject at least some of the requests directed toward NFPs, thereby helping to protect the NFPs from denial-of-service attacks, for example. Alternatively, or in addition, the at least one subject parameter may relate to information the NFP has but the NEF does not have, wherefore the NEF may not even be able to verify the at least one subject parameter. In such cases the-two stage authorization process may be used to enable authorization, e.g., for location-based services.

[0044] The at least one subject parameter may identify a location object, time-of-day object or subscriber identity range object. Location-based access may require verifying of the location of the AF or the at least one subscriber of the AF to determine whether a request for a service may be granted, i.e., the location object may indicate that the location needs to be verified. Verifying of the location may comprise comparing the location of the AF, or the location of the at least one subscriber of the AF, to a region wherein the AF is allowed to access the at least one service provided that, or when, the AF or the at least one subscriber is within the region, i.e., to see whether the location of the AF or the location of the at least one subscriber of the AF is within the region and if so, the AF is allowed to access the at least one service. That is to say, a NF, such as the UDM, may check the location object in an access token against the location of the AF or the at least one subscriber and if it matches, the AF may be allowed to access the at least one service. For instance, the request may be granted if the at least one subscriber is within the region and rejected if the at least one subscriber is outside of the region wherein the AF is allowed to access the at least one service.

[0045] The time-of-day object may be related to access or parameter provisioning for IoT devices, i.e., require verifying whether the AF is allowed to access the requested service at a certain time-of-day, to determine whether a request for a service may be granted. Verifying of the time-of-day may comprise comparing the time-of-day to a time when the AF is allowed to access the at least one service. If the time-of-day is such that the AF is allowed to access the at least one service, the request may be granted but otherwise the request may be denied.

[0046] The subscriber identity range object may require verifying that a subscriber identity range of the AF, e.g., the subscriber identity range that the AF can access for a given application type, comprises an identity of the at least one subscriber. That is to say, verification of the subscriber identity range may comprise comparing the identity of the at least one subscriber to the subscriber identity range, to see whether the identity is within the subscriber identity range. If the identity is within the subscriber identity range, the request may be accepted, i.e., the AF may be allowed to access the at least one service, but otherwise the request may be denied.

[0047] It should be noted that some examples about possible subject parameters and objects are provided above, but in general embodiments of the present invention may be exploited for various other subject parameters and objects that need to be verified, and for different scenarios as well.

[0048] Embodiments of the present invention address various issues. For example, it may be ensured that an AF cannot access data of subscribers belonging to the other AFs. In some example embodiments, subscribers belonging to different AFs may have overlapping DNNs though. So for example, if the subscriber identity range of AF1 is 10000XXXXX and the subscriber identity range of AF2 is 20000XXXXX, some embodiments of the present invention may be used to ensure that a NEF and/or NFP, such as a UDM, knows that AF1 is not meant to monitor events for a subscriber belonging to the subscriber identity range 20000XXXXX. Moreover, any NFP such as a UDM may be provided with information of the AF that sent the request concerning the at least one service of the NFP, thereby making it possible for the NFP to perform authorization as well.

[0049] To solve the aforementioned problem, a framework is provided wherein AccessTokenClaims, such as a request concerning at least one service of a NFP, are extended

to add subject specific parameters, thereby strengthening security by providing additional level of access control based on the specific parameters. The request concerning the at least one service of a NFP may be an event monitoring request or a subscription request if the NFP in question is a UDM. That is to say, the request may be a request to access the at least one service provided by the NFP.

[0050] FIGURE 2 illustrates signalling in accordance with at least some example embodiments. On the vertical axes are disposed, from the left to the right, UDM-EE 202, NEF 203, AF1 206 and AF2 207. NEF 203 may further comprise AEF 204, CAPIF 205. Time advances from the top towards the bottom. Even though example embodiments of FIGURE 2 are described using UDM-EE 202 as an example, the embodiments may be applied for any NFP in general. That is to say, embodiments of the present invention are not limited UDM-EE 202, instead any NFP may perform the same tasks.

[0051] At Step 210, AF1 and AF2 may retrieve tokens from NEF 203, or CAPIF 205 of NEF 203. The retrieved tokens may comprise, or be transmitted along with a subscriber identity range allocated for the AF in question. That is to say, at step 210 AF1 206 may transmit an access token request to NEF 203 (or CAPIF 205 of NEF 203). Upon receiving the access token request, NEF 203 (or CAPIF 205 of NEF 203) may generate an access token for AF1 206. The access token of AF1 206 may be transmitted to AF2 in an access token response, wherein the access token response may comprise the subscriber identity range of the AF1 as well. The generated access token may be signed by NEF 203 (or CAPIF 205 of NEF 203) using a private key of NEF 203 (or CAPIF 205 of NEF 203) respectively.

[0052] The subscriber identity range of the AF1 206 may comprise identities that may be allocated for the subscribers of AF1 206 by AF1 206. For instance, AF1 206 may be an IoT application with a subscriber identity range such as 10000XXXXX while AF2 207 may an IoT application with a subscriber identity range such as 20000XXXXX.

[0053] At step 220, AF1 206 may transmit a request to access at least one service of a NFP, such as UDM-EE 202, to NEF 203 (or AEF 204 of NEF 203). The request may be associated with at least one subscriber of AF1 206 and comprise the access token of AF1 206, i.e., the access token generated by NEF 203 (or CAPIF 205 or NEF 203), for AF1 206 at step 210.The request may comprise at least one subject parameter associated with the at least one subscriber of AF1 206, wherein each of the at least one subject

parameter may identify an object that needs to be verified by NEF 203 or the NFP, such as UDM-EE 202. Even though a request associated with at least one subscriber of AF1 206 is used as an example, the request may in general be associated with AF1 206. Similarly, the at least one subject parameter may be associated with AF1 206 in general.

[0054] The identified object may be for example a location, time-of-day or a subscriber identity range of AF1 206. In some example embodiments, the request may be a REST POST MonitoringEvent(MSISDN = 2000011111, EventType = UE_REACHABILITY_FOR_SMS), Authorization: Bearer Token(SubjectParameters)).

[0055] Step 220 is optional though. In some example embodiments, NEF 203 (or AEF 204 of NEF 203) may determine the at least one subject parameter by itself, e.g., if the at least one subject parameter comprises a subscriber identity range.

[0056] At step 230, NEF 203 (or AEF 204 of NEF 203) may validate the access token received from AF1 206. The access token received from AF1 206 may be determined as valid if it matches the access token provided by NEF 203 (or CAPIF 205 of NEF 203) for AF1 206. NEF 203 (or AEF 204 of NEF 203) may verify a digital signature in the access token for example.

[0057] In some example embodiments, NEF 203 (or AEF 204 of NEF 203) may also verify at least some of the objects identified by the subject parameters received from AF1 206. For instance, if the at least one subject parameter associated with the at least one subscriber of AF1 206 identifies an object such as a subscriber identity range, NEF 203 (or AEF 204 of NEF 203) may check whether an identity of the at least one subscriber is within the subscription range. That is to say, NEF 203 (or AEF 204 of NEF 203) may successfully verify that the subscriber identity range of AF1 206 comprises the identity of the at least one subscriber. NEF 203 (or AEF 204 of NEF 203) may directly deny the request if the subscriber identity range of AF1 206 does not comprise the identity of the at least one subscriber. Authentication and security may be thus improved, as AF2 207 cannot access data of subscribers of AF1. Security threats, such as denial-of-service attacks, may be identified quickly as well, if there are for example multiple unauthorized requests from various sources towards subscribers of one particular AF.

[0058] For instance, the request transmitted by AF1 206 may be a REST POST MonitoringEvent(MSISDN = 2000011111, EventType = UE_REACHABILITY_FOR_SMS), Authorization: Bearer Token(SubjectParameters)), wherein the identity of the at least one subscriber of AF1 206 is MSISDN=2000011111. So if the subject parameters comprise a subscriber identity range object, but the subscriber identity range of AF1 is 10000XXXXX, NEF 203 (or AEF 204 of NEF 203) may notice that the identity of the at least one subscriber, as obtained from the request at step 220, is not within the subscriber identity range of AF1. Consequently, the request may be denied by NEF 203 (or AEF 204 of NEF 203) right away, without transmitting the at least one parameter to the NFP.

[0059] In some example embodiments, if the at least one subject parameter associated with the at least one subscriber of AF1 206 identifies an object such as a time-of-day, NEF 203 (or AEF 204 of NEF 203) may check whether the at least one subscriber is allowed to access the requested service at a certain time-of-day. The request may be denied directly by NEF 203 (or AEF 204 of NEF 203) if AF1 206 is not allowed to access the at least one service at that time-of-day.

[0060] Upon successful validation of the access token received from AF1 206, and possibly verifying at least some of the objects identified by the subject parameters, NEF 203 (or AEF 204 of NEF 203) may forward the request along with the at least one subject parameter associated with the at least one subscriber of AF1 206 to the NFP, such as UDM-EE 202. In some example embodiments, NEF 203 (or AEF 204 of NEF 203) may also process the request internally, i.e., it may initiate a new request to UDM-EE 202 to access the at least one service and/or several requests to other network function services in response to receiving the request at step 220. Verification of the at least one subject parameter by NEF 203 (or AEF 204 of NEF 203) is optional though. In some example embodiments, NEF 203 (or AEF 204 of NEF 203) may just forward the request, or transmit a new request, along with the at least one subject parameter without verifying, as long as the validation of the access token is successful, to enable quick one-stage authorization process.

[0061] In some example embodiments, NEF 203 (or AEF 204 of NEF 203) may verify one subject parameter and transmit, upon successfully verifying said one parameter, only another subject parameter to the NFP, such as UDM-EE 202, without transmitting said one

subject parameter. That is to say, said one subject parameter may not be transmitted in the request or in connection with the request, i.e., the NFP may not receive any information about the parameter verified by NEF 203 (or AEF 204 of NEF 203).

[0062] For instance, said one subject parameter may be related to a subscriber identity range and said another subject parameter may be related to a location. NEF 203 (or AEF 204 of NEF 203) may not have information about the location of the at least one subscriber and thus, NEF 203 (or AEF 204 of NEF 203) may only verify that a subscriber identity range of AF1 206 comprises an identity of the at least one subscriber and transmit said another subject parameter related to a location to the NFP, thereby enabling authorization for location-based services. Alternatively, or in addition, NEF 203 (or AEF 204 of NEF 203) may verify the time-of-day object.

[0063] The NFP, such as UDM-EE, may then determine whether the request may be granted, i.e., access to the at least one service may be authorized, by verifying a location of the at least one subscriber of the application function. However, there is no need to transmit the request to the NFP if the verifying fails at NEF 203. Thus, authorization for location-based services may be performed efficiently.

[0064] Upon receiving the request concerning the at least one service of the NFP, such as UDM-EE 202, along with the at least one subject parameter associated with at least one subscriber of AF1 206, the NFP may determine based on the at least one subject parameter associated with the at least one subscriber of AF1 206, whether the request may be granted. That is to say, the NFP may determine whether access to the requested service may be granted and respond to AF1 206 accordingly via NEF 203 (AEF 204 of NEF 203).

[0065] For instance, if the at least one subject parameter associated with the at least one subscriber of AF1 206 comprises a subscriber identity range object, the NFP may determine whether the request may be granted by verifying that a subscriber identity range of AF1 206 comprises an identity of the at least one subscriber and if so, transmit a positive response (201 Context Created (CreatedEeSubscription) to NEF 203 (or AEF 204 of NEF 203). In such a case, NEF 203 (or AEF 204 of NEF 203) may forward the response (200 OK) to AF1 206.

[0066] However, if the subscriber identity range of AF1 206 does not comprise the identity of the at least one subscriber, the NFP may transmit a negative response (403 Forbidden) to NEF 203 (or AEF 204 of NEF 203), which may forward the negative response to AF1 206. For instance, the request received from NEF 203 (or AEF 204 of NEF 203) may be REST POST Nudm_ee APIs(MSISDN = 2000011111, EventType = UE_REACHABILITY_FOR_SMS), Authorization: Bearer Token(SubjectParameters)), wherein the identity of the at least one subscriber of AF1 206 is MSISDN=2000011111.

[0067] So if the subject parameters comprise a subscriber identity range object, but the subscriber identity range of AF1 is 10000XXXXX, the NFP may notice that the identity of the at least one subscriber is not within the subscriber identity range of AF1 206. Consequently, the request may be denied by the NFP. If the subscriber identity range is verified by both, NEF 203 (or AEF 204 of NEF 203) and the NFP, authentication may be improved by performing two-staged verifying.

[0068] In some example embodiments, if the at least one subject parameter associated with the at least one subscriber of AF1 206 comprises a location object, the NFP may determine whether the request may be granted by checking a location of the at least one subscriber of AF1 206. Depending on whether the location, i.e., the current location, of the at least one subscriber is within a region, wherein AF1 206 is allowed to access to the at least one service when the at least one subscriber is within the region, the NFP may determine whether to grant the request, or not. Hence, authorization may be enabled for location-based services as well, even if NEF 203 (or AEF 204 of NEF 203) would not know the current location of the at least one subscriber.

[0069] Similarly, if the at least one subject parameter associated with the at least one subscriber of AF1 206 comprises a time-of-day object, the NFP may determine whether the request may be granted by checking a time-of-day of the at least one subscriber of AF1 206. Depending on whether the time-of-day, i.e., the current time, is such that access to the at least one service is allowable, the NFP may determine whether to grant the request, or not.

[0070] In some example embodiments of the present invention, AccessTokenClaims may be enhanced with a new object called “SubjectSpecificInfo”.The SubjectSpecificInfo may be an object that contains an array of heterogenous subject parameters. The subject parameters may include sub objects such as location, time-of-day, subscriber identity ranges

(SUPI/GPSI/MSISND/external Identity), etc. Some part of the SubjectSpecificInfo may be consumed by an NEF while the other sections may be consumed by the NFP, such as the UDM, to which the NEF forwards the request or transmits the new request, depending on a use case.

[0071] According to some embodiments of the present invention, some changes may be made to 3GPP standard specifications TS 29.222 and 29.510. For instance, AccessTokenClaims defined in TS29222_CAPIF_Security_API.yaml and TS29510_Nnrf_AccessToken.yaml may be modified as below.

[0072] The "SubjectSpecificInfo" may have a list of parameters. Each of the parameters may be defined using the schema defined by "SubjectParameter", which may act as a union of all the possible parameters and their types that may be used to define an AF's parameters. The generic framework makes it easy to add new types to the allowed parameters. The exemplary schema below presents a few options for location, time-of-day services and different types of subscriber identity range identifiers:

```
components:
    schemas:
        AccessTokenClaims:
          type: object
          required: "subjectSpecificInfo"
          properties:
          … … …
        subjectSpecificInfo:
            type: array
            items:
            "$ref": "/components/schemas/SubjectParameter"
        scheduledCommunicationTime:
            $ref:
            'TS29571_CommonData.yaml#/components/schemas/ScheduledCommun
            icationTimeRm'
        userLocation:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
```

```
        supiRanges:
          type: array
          items:
          $ref: '#/components/schemas/SupiRange'
          minItems: 1
        gpsiRanges:
          type: array
          items:
          $ref: '#/components/schemas/IdentityRange'
          minItems: 1
        externalGroupIdentifiersRanges:
          type: array
          items:
          $ref: '#/components/schemas/IdentityRange'
          minItems: 1
      SubjectParameter:
        type: object
        required:
        - subjectParameterType
        properties:
          scheduledCommunicationTime:
            $ref:
            'TS29571_CommonData.yaml#/components/schemas/ScheduledCommun
            icationTimeRm'
          userLocation:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
          supiRanges:
          type: array
            items:
            $ref: '#/components/schemas/SupiRange'
            minItems: 1
          gpsiRanges:
```

```
        type: array
        items:
        $ref: '#/components/schemas/IdentityRange'
        minItems: 1
      externalGroupIdentifiersRanges:
        type: array
        items:
        $ref: '#/components/schemas/IdentityRange'
        minItems: 1
      subjectParameterType:
        type: string
        enum:
              - USER_LOCATION
              - TIME_OF_DAY
              - SUPI_RANGE
              - GPSI_RANGE
              - EXTERNAL_GRP_DENTITY_RANGE
    anyOf:
    - properties:
      subjectParameterType:
        const: USER_LOCATION
    required:
      - userLocation
    - properties:
      subjectParameterType:
        const: TIME_OF_DAY
    required:
      - scheduledCommunicationTime
    - properties:
      subjectParameterType:
        const: SUPI_RANGE
    required:
```

```
    - supiRanges
  - properties:
    subjectParameterType:
      const: GPSI_RANGE
  required:
    - gpsiRanges
  - properties:
    subjectParameterType:
      const: EXTERNAL_GRP_DENTITY_RANGE
  required:
    - externalGroupIdentifiersRanges
```

[0073] FIGURE 3 illustrates an example apparatus capable of supporting at least some example embodiments. Illustrated is device 300, which may comprise, for example, an NEF or NFP (such as UDM-EE), or a device controlling functioning thereof. Comprised in device 300 is processor 310, which may comprise, for example, a single- or multi-core processor wherein a single-core processor comprises one processing core and a multi-core processor comprises more than one processing core. Processor 310 may comprise, in general, a control device. Processor 310 may comprise more than one processor. Processor 310 may be a control device. Processor 310 may comprise at least one Application-Specific Integrated Circuit, ASIC. Processor 310 may comprise at least one Field-Programmable Gate Array, FPGA. Processor 310 may comprise an Intel Xeon processor for example. Processor 310 may be means for performing method steps in device 300, such as determining, causing transmitting and causing receiving. Processor 310 may be configured, at least in part by computer instructions, to perform actions.

[0074] A processor may comprise circuitry, or be constituted as circuitry or circuitries, the circuitry or circuitries being configured to perform phases of methods in accordance with example embodiments described herein. 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 network function, 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.

[0075] 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.

[0076] Device 300 may comprise memory 320. Memory 320 may comprise random-access memory and/or permanent memory. Memory 320 may comprise at least one RAM chip. Memory 320 may comprise solid-state, magnetic, optical and/or holographic memory, for example. Memory 320 may be at least in part accessible to processor 310. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be means for storing information. Memory 320 may comprise computer instructions that processor 310 is configured to execute. When computer instructions configured to cause processor 310 to perform certain actions are stored in memory 320, and device 300 overall is configured to run under the direction of processor 310 using computer instructions from memory 320, processor 310 and/or its at least one processing core may be considered to be configured to perform said certain actions. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be at least in part external to device 300 but accessible to device 300.

[0077] Device 300 may comprise a transmitter 330. Device 300 may comprise a receiver 340. Transmitter 330 and receiver 340 may be configured to transmit and receive, respectively, information in accordance with at least one cellular standard, such as a standard defined by the 3GPP. Transmitter 330 may comprise more than one transmitter. Receiver 340 may comprise more than one receiver. Transmitter 330 and/or receiver 340 may be configured to operate in accordance with a suitable communication standard.

[0078] Device 300 may comprise User Interface, UI, 350. UI 350 may comprise at least one of a display, a keyboard, a touchscreen, a vibrator arranged to signal to a user by causing device 300 to vibrate, a speaker and a microphone. A user may be able to operate device 300 via UI 350, for example to configure device 300 and/or functions it runs.

[0079] Processor 310 may be furnished with a transmitter arranged to output information from processor 310, via electrical leads internal to device 300, to other devices comprised in device 300. Such a transmitter may comprise a serial bus transmitter arranged to, for example, output information via at least one electrical lead to memory 320 for storage therein. Alternatively to a serial bus, the transmitter may comprise a parallel bus transmitter. Likewise processor 310 may comprise a receiver arranged to receive information in processor 310, via electrical leads internal to device 300, from other devices comprised in device 300. Such a receiver may comprise a serial bus receiver arranged to, for example, receive information via at least one electrical lead from receiver 340 for processing in processor 310. Alternatively to a serial bus, the receiver may comprise a parallel bus receiver.

[0080] Device 300 may comprise further devices not illustrated in FIGURE 3. In some example embodiments, device 300 lacks at least one device described above. For example, device 300 may not have UI 350.

[0081] Processor 310, memory 320, transmitter 330, receiver 340 and/or UI 350 may be interconnected by electrical leads internal to device 300 in a multitude of different ways. For example, each of the aforementioned devices may be separately connected to a master bus internal to device 300, to allow for the devices to exchange information. However, as the skilled person will appreciate, this is only one example and depending on the embodiment various ways of interconnecting at least two of the aforementioned devices may be selected without departing from the scope of the present invention.

[0082] FIGURE 4 is a flow graph of a first method in accordance with at least some example embodiments. The phases of the illustrated first method may be performed by a NEF, or by a control device configured to control the functioning thereof, possibly when installed therein.

[0083] The first method may comprise, at step 410, receiving, from an application function, a request to access at least one service of a network function producer, wherein the request is associated with the application function and comprises an access token of the application function. Also, the first method may comprise, at step 420, upon successful validation of the access token, forwarding the request or transmitting a new request along with at least one parameter associated with the application function to the network function producer, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer.

[0084] FIGURE 5 is a flow graph of a second method in accordance with at least some example embodiments. The phases of the illustrated second method may be performed by an NFP, such as a UDM-EE, or by a control device configured to control the functioning thereof, possibly when installed therein.

[0085] The second method may comprise, at step 510, receiving, from a network exposure function, a request to access at least one service of the network function producer along with at least one parameter associated with an application function, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer. Also, the second method may comprise, at step 520, determining, based on the at least one parameter associated with the application function, whether to grant the request or not. Finally, the second method may comprise, at step 530, transmitting a response to the network exposure function, wherein the response depends on whether the request is granted.

[0086] It is to be understood that the embodiments disclosed are not limited to the particular structures, process steps, or materials disclosed herein, but are extended to equivalents thereof as would be recognized by those ordinarily skilled in the relevant arts. It should also be understood that terminology employed herein is used for the purpose of describing particular example embodiments only and is not intended to be limiting.

[0087] Reference throughout this specification to one example embodiment or an example embodiment means that a particular feature, structure, or characteristic described in connection with the example embodiment is included in at least one example embodiment. Thus, appearances of the phrases “in one example embodiment” or “in an example embodiment” in various places throughout this specification are not necessarily all referring

to the same example embodiment. Where reference is made to a numerical value using a term such as, for example, about or substantially, the exact numerical value is also disclosed.

[0088] As used herein, a plurality of items, structural elements, compositional elements, and/or materials may be presented in a common list for convenience. However, these lists should be construed as though each member of the list is individually identified as a separate and unique member. Thus, no individual member of such list should be construed as a de facto equivalent of any other member of the same list solely based on their presentation in a common group without indications to the contrary. In addition, various example embodiments and examples may be referred to herein along with alternatives for the various components thereof. It is understood that such example embodiments, examples, and alternatives are not to be construed as de facto equivalents of one another, but are to be considered as separate and autonomous representations.

[0089] In an example embodiment, an apparatus, such as, for example, an NEF or NFP (such as UDM-EE), or a device controlling functioning thereof, may comprise means for carrying out the example embodiments described above and any combination thereof.

[0090] In an example embodiment, a computer program may be configured to cause a method in accordance with the example embodiments described above and any combination thereof. In an exemplary example embodiment, a computer program product, embodied on a non-transitory computer readable medium, may be configured to control a processor to perform a process comprising the example embodiments described above and any combination thereof.

[0091] In an example embodiment, an apparatus, such as, for example, an NEF or NFP (such as UDM-EE), or a device controlling functioning thereof, may comprise at least one processor, and at least one memory including computer program code, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the apparatus at least to perform the example embodiments described above and any combination thereof.

[0092] Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more example embodiments. In the preceding description, numerous specific details are provided, such as examples of lengths, widths,

shapes, etc., to provide a thorough understanding of example embodiments of the invention. One skilled in the relevant art will recognize, however, that the invention may be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

[0093] While the forgoing examples are illustrative of the principles of the example embodiments in one or more particular applications, it will be apparent to those of ordinary skill in the art that numerous modifications in form, usage and details of implementation may be made without the exercise of inventive faculty, and without departing from the principles and concepts of the invention. Accordingly, it is not intended that the invention be limited, except as by the claims set forth below.

[0094] The verbs “to comprise” and “to include” are used in this document as open limitations that neither exclude nor require the existence of also un-recited features. The features recited in depending claims are mutually freely combinable unless otherwise explicitly stated. Furthermore, it is to be understood that the use of "a" or "an", that is, a singular form, throughout this document does not exclude a plurality.

INDUSTRIAL APPLICABILITY

[0095] At least some example embodiments find industrial application at least in 5G core networks, wherein it is desirable to enhance authorization of 3rd party AFs, and possibly in other core networks in the future as well.

ACRONYMS LIST

3GPP	3rd Generation Partnership Project
AEF	Application Exposure Function
AF	Application Function
AMF	Access and Mobility Function
API	Application Programming Interfaces
AUSF	Authentication Server Function
CAPIF	Common API Framework
DRA	Diameter Routing Agent
EPC	Evolved Packet Core
HSS	Home Subscriber Service
IPX	IP eXchanges
KPI	Key Performance Indicator
NEF	Network Exposure Function
NF	Network Function
NFC	NF Consumer
NFP	NF Producer
NRF	Network Repository Function
NSSF	Network Slice Selection Function
NWDAF	Network Data Analysis Function
OAM	Operations Administration and Maintenance
PCF	Policy Control Function
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
QoS	Quality of Service
SBA	Service-Based Architecture
SBI	Service-Based Interface
SCP	Service Communication Proxy
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
TLS	Transport Layer Security
UDM	Unified Data Management

UDR	User Data Repository
VNF	Virtual Network Function

REFERENCE SIGNS LIST

110, 112	PLMNs
120, 122	NFs
130, 132	SEPPs
140, 142	NRFs
150, 152	SCPs
202	UDM-EE
203	NEF
204	AEF
205	CAPIF
206	AF1
207	AF2
210 – 260	Steps of the process of FIGURE 2
300 – 350	Structure of the apparatus of FIGURE 3
410 – 420	Phases of the first method in FIGURE 4
510 – 520	Phases of the first method in FIGURE 5

WE CLAIM:

1. A method for a network exposure function, the method comprising:
   - receiving, from an application function, a request to access at least one service of a network function producer, wherein the request is associated with the application function and comprises an access token of the application function; and
   - upon successful validation of the access token, forwarding the request or transmitting a new request along with at least one parameter associated with the application function to the network function producer, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer.

2. A method according to claim 1, wherein the object is a location, time-of-day or subscriber identity range.

3. A method according to claim 1 or claim 2, further comprising:
   - transmitting, upon successfully verifying one parameter associated with the application function, another parameter associated with the application function to the network function producer without transmitting said one parameter.

4. A method according to claim 3, wherein said one parameter identifies a subscriber identity range object and said another parameter identifies a location object.

5. A method according to any of the preceding claims, further comprising:
   - transmitting, upon successfully verifying that a subscriber identity range of the application function comprises an identity of at least one subscriber associated with the application function, the request along with the at least one parameter associated with the application function to the network function provider.

6. A method according to any of the preceding claims, further comprising:
   - transmitting, upon successfully verifying that a time-of-day is such that the application function is allowed to access the at least one service, the request along

with the at least one parameter associated with the application function to the network function provider.

7. A method according to any of the preceding claims, wherein the at least one parameter comprises a subscriber identity range object indicating that an identity of at least one subscriber of the application function needs to be verified versus a subscriber identity range of the application function.

8. A method according to any of the preceding claims, wherein the at least one parameter comprises a location object indicating that a location of at least one subscriber of the application function needs to be verified versus a region wherein the application function is allowed to access the at least one service when the at least one subscriber is within the region.

9. A method according to any of the preceding claims, wherein the at least one parameter comprises a time-of-day object indicating that a time-of-day needs to be verified versus a time when the application function is allowed to access the at least one service.

10. A method according to any of the preceding claims, further comprising:

- receiving, from the application function, the at least one parameter associated with the application function.

11. A method for a network function producer, the method comprising:

- receiving, from a network exposure function, a request to access at least one service of the network function producer along with at least one parameter associated with an application function, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer;
- determining, based on the at least one parameter associated with the application function, whether to grant the request or not; and
- transmitting a response to the network exposure function, wherein the response depends on whether the request is granted.

12. A method according to claim 11, wherein the object is a location, time-of-day or subscriber identity range.

13. A method according to claim 11 or claim 12, wherein the at least one parameter associated with the application function identifies a subscriber identity range object, and the method further comprises:

- determining whether to grant the request or not by checking whether a subscriber identity range of the application function comprises an identity of at least one subscriber of the application function.

14. A method according to any of claims 11 to 13, wherein the at least one parameter associated with the application function identifies a location object, and the method further comprises:

- determining whether to grant the request or not by comparing a location of at least one subscriber of the application function versus a region wherein the application function is allowed to access the at least one service when the at least one subscriber is within the region.

15. A method according to any of claims 11 to 14, wherein the at least one parameter associated with the application function identifies a time-of-day object, and the method further comprises:

- determining whether to grant the request or not by checking whether a time-of-day is such that the application function is allowed to access the at least one service.

16. A method according to any of the preceding claims, wherein the network function producer is a unified data management network function.

17. A method according to any of the preceding claims, wherein the network exposure function and the network function producer operate according to at least one standard specification defined by a 3rd Generation Partnership Project, 3GPP.

18. A method according to any of the preceding claims, wherein the network exposure function and the network function producer are in a core network of a cellular communication network.

19. A method according to claim 18, wherein the core network is a 5G core network.

20. A method according to any of the preceding claims, wherein the request and the at least one parameter are associated with at least one subscriber of the application function.

21. An apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to perform:

- receive, from an application function, a request to access at least one service of a network function producer, wherein the request is associated with the application function and comprises an access token of the application function; and
- upon successful validation of the access token, forward the request or transmit a new request along with at least one parameter associated with the application function to the network function producer, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer.

22. An apparatus according to claim 21, wherein the at least one memory and the computer program code are further configured to, with the at least one processing core, cause the apparatus at least to perform a method according to any of claims 2 – 10 or 16 -20.

23. An apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to perform:

- receive, from a network exposure function, a request to access at least one service of the network function producer along with at least one parameter associated with an application function, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer;

- determine, based on the at least one parameter associated with the application function, whether to grant the request or not; and
- transmit a response to the network exposure function, wherein the response depends on whether the request is granted.

24. An apparatus according to claim 23, wherein the at least one memory and the computer program code are further configured to, with the at least one processing core, cause the apparatus at least to perform a method according to any of claims 12 -20.

25. An apparatus comprising:

- means for receiving, from an application function, a request to access at least one service of a network function producer, wherein the request is associated with the application function and comprises an access token of the application function; and
- upon successful validation of the access token, means for forwarding the request or transmitting a new request along with at least one parameter associated with the application function to the network function producer, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer.

26. An apparatus according to claim 25, further comprising means for performing a method according to any of claims 2 – 10 or 16 -20.

27. An apparatus comprising:

- means for receiving, from a network exposure function, a request to access at least one service of the network function producer along with at least one parameter associated with an application function, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer;
- means for determining, based on the at least one parameter associated with the application function, whether to grant the request or not; and
- means for transmitting a response to the network exposure function, wherein the response depends on whether the request is granted.

28. A apparatus according to claim 27, further comprising means for performing a method according to any of claims 12 -20.

29. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least perform a method according to any claims 1 – 10 or 16 -20, or 11 – 20.

30. A computer program configured to perform a method according to any of claims 1 – 10 or 16 -20, or 11 – 20.

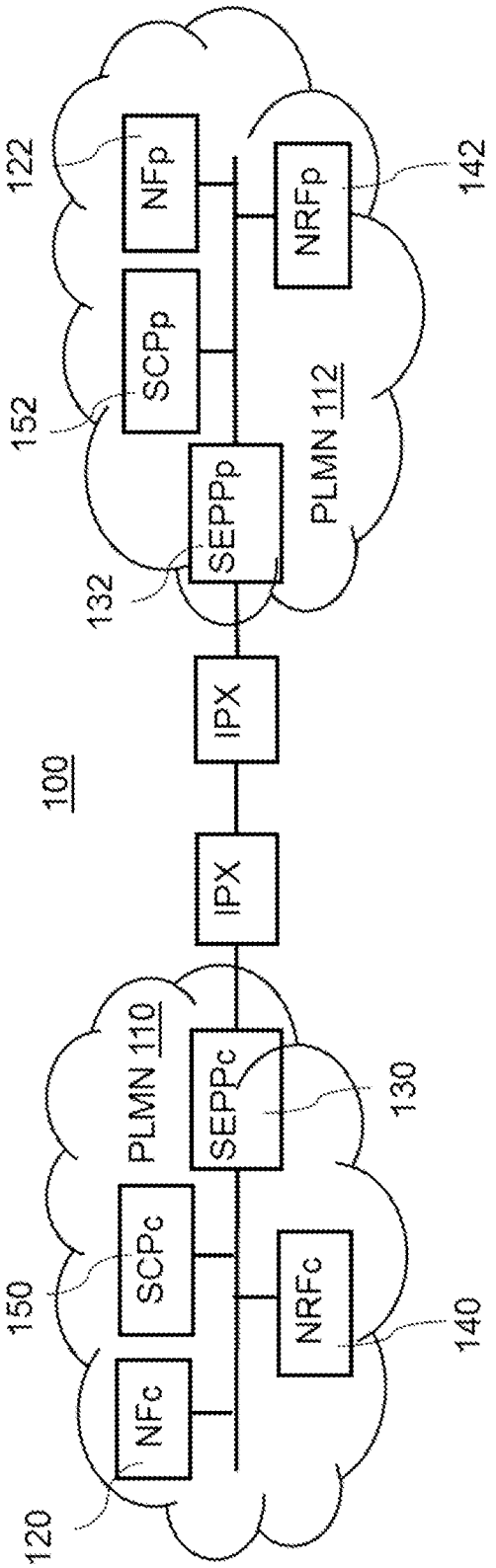
122
NFp
NRFp
142
SCPp
152
PLMN 112
SEPPp
132
IPX
100
IPX
PLMN 110
SEPPc
130
150
SCPc
NRFc
140
NFc
120

FIGURE 1

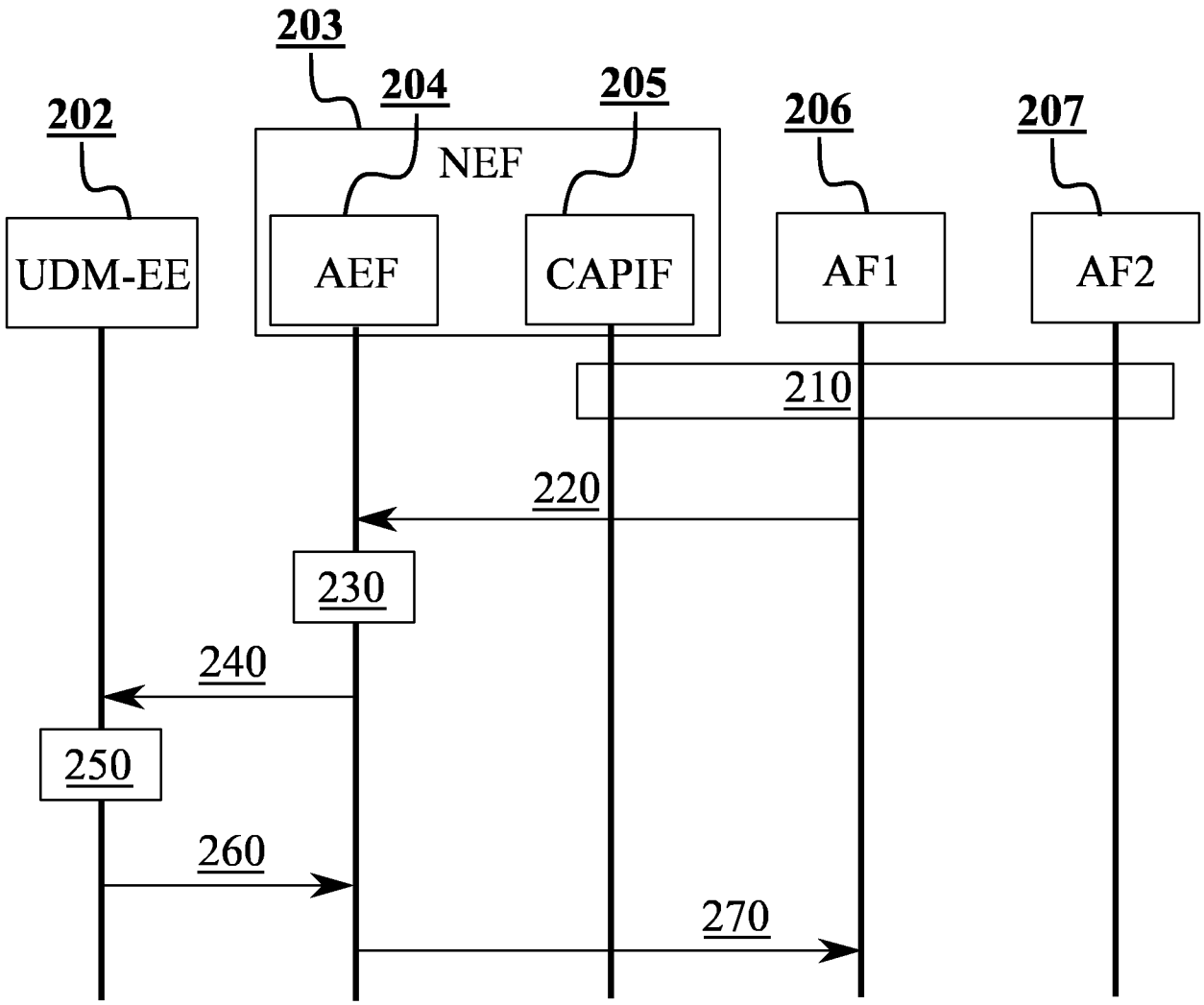
203
204
205
202
206
207
NEF
UDM-EE
AEF
CAPIF
AF1
AF2
210
220
230
240
250
260
270

FIGURE 2

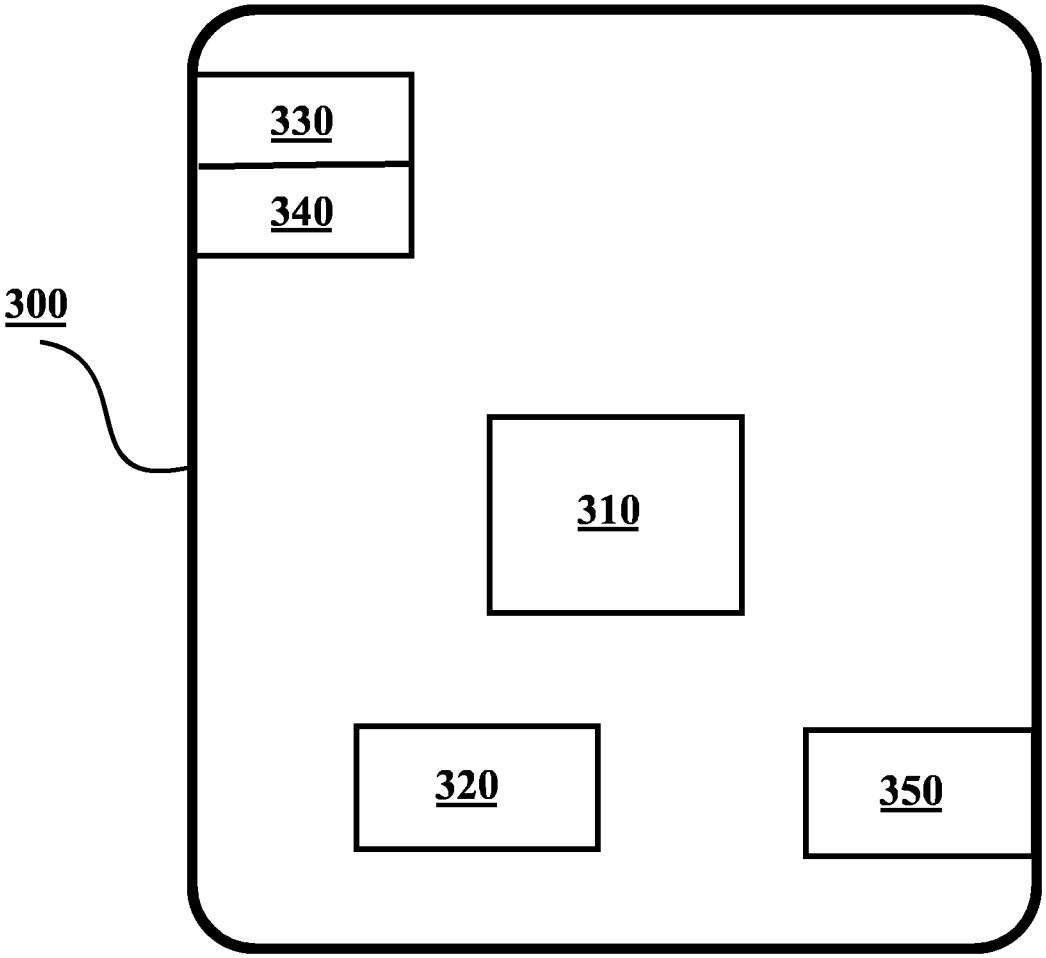

FIGURE 3

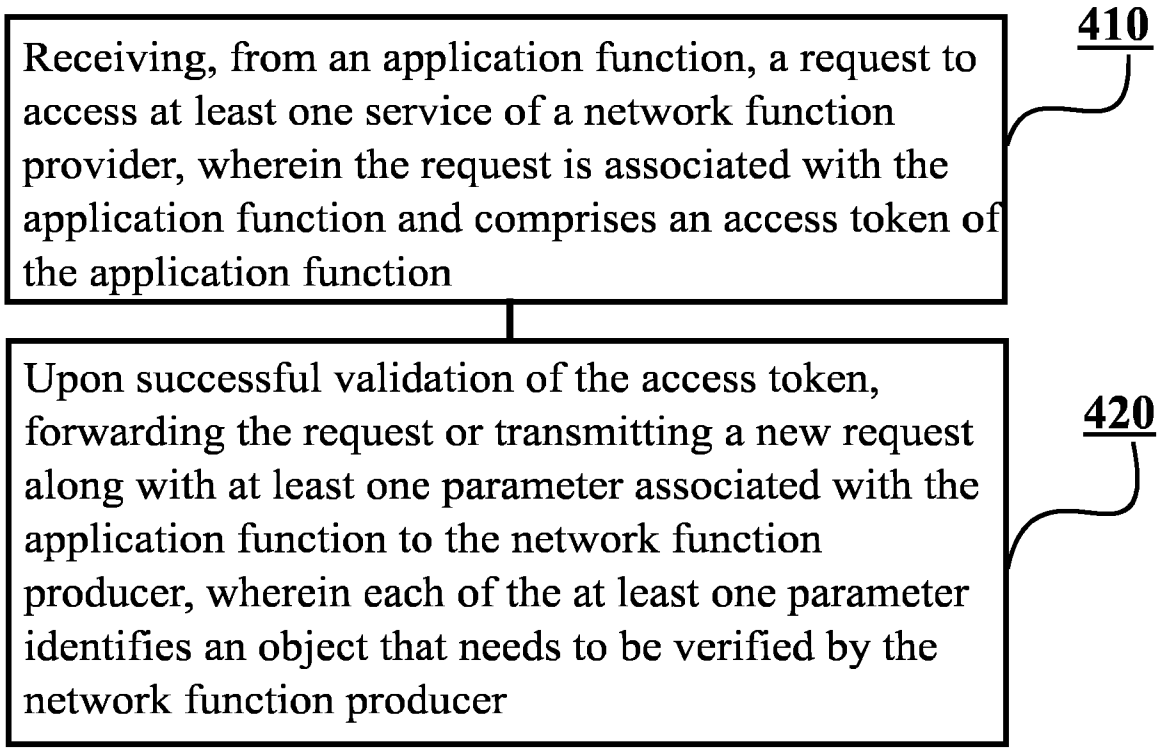
Receiving, from an application function, a request to access at least one service of a network function provider, wherein the request is associated with the application function and comprises an access token of the application function
410
Upon successful validation of the access token, forwarding the request or transmitting a new request along with at least one parameter associated with the application function to the network function producer, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer
420

FIGURE 4

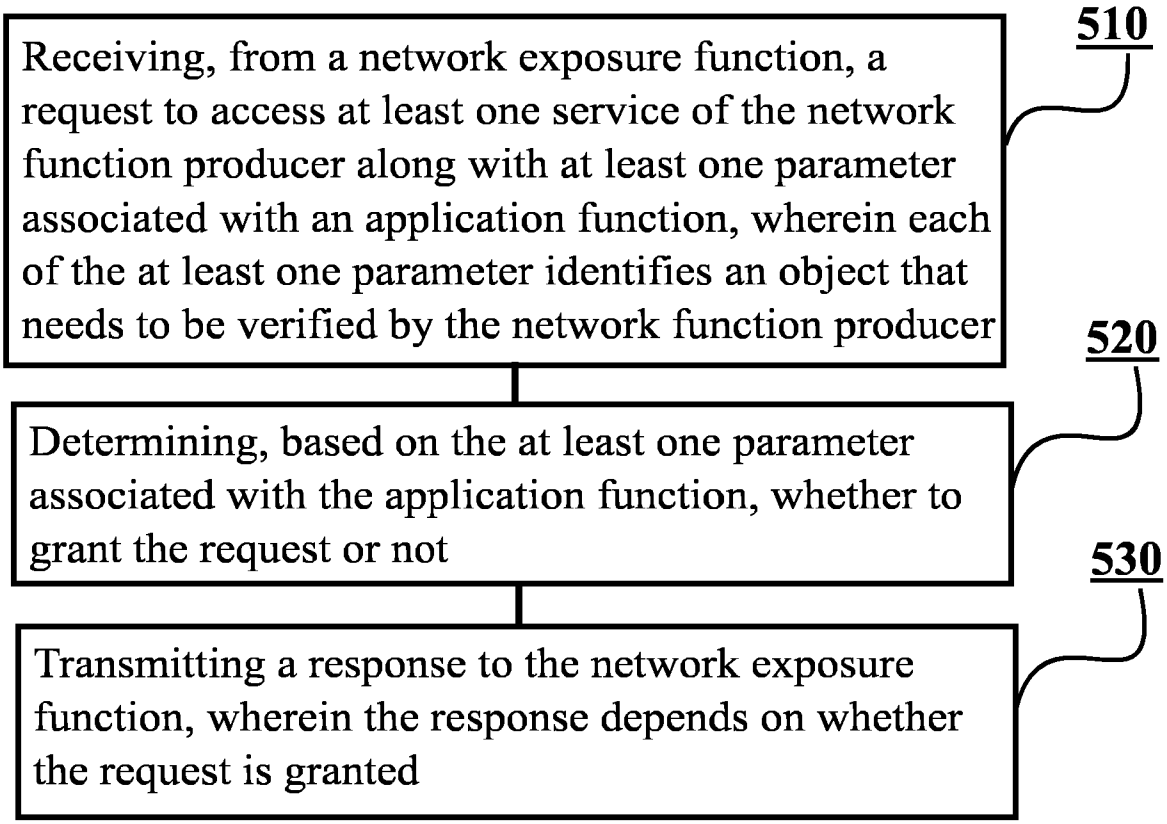
510
Receiving, from a network exposure function, a request to access at least one service of the network function producer along with at least one parameter associated with an application function, wherein each of the at least one parameter identifies an object that needs to be verified by the network function producer
520
Determining, based on the at least one parameter associated with the application function, whether to grant the request or not
530
Transmitting a response to the network exposure function, wherein the response depends on whether the request is granted

FIGURE 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2021/050040

A. **CLASSIFICATION OF SUBJECT MATTER**

See extra sheet

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)

IPC: H04L, H04W, G06F

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

FI, SE, NO, DK

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

EPODOC, EPO-Internal full-text databases, Full-text translation databases from Asian languages, WPIAP, XP3GPP, XPAIP, XPCPVO, XPESP, XPETSI, XPI3E, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPMISC, XPOAC, XPRD, XPSPRNG, XPTK, COMPDX, INSPEC, TDB, PRH-Internal, Internet, ACM, Springer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017149837 A1 (SONDHI AJAY [US] et al.) 25 May 2017 (25.05.2017) the whole document, in particular Figs. 5-6, 18; paragraphs [0061], [0074]-[0075], [0093], [0096], [0111]-[0112], [0197]	1-30
A	WO 2020002764 A1 (NOKIA TECHNOLOGIES OY [FI]) 02 January 2020 (02.01.2020) the whole document, in particular Figs. 1, 3; page 5, line 27 – page 6, line 4; page 10, lines 25-30; page 12, lines 4-13	16-19

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"D"	document cited by the applicant in the international application	"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
"E"	earlier application or patent but published on or after the international filing date	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search	Date of mailing of the international search report
22 April 2021 (22.04.2021)	23 April 2021 (23.04.2021)

Name and mailing address of the ISA/FI
Finnish Patent and Registration Office
FI-00091 PRH, FINLAND
Facsimile No. +358 29 509 5328

Authorized officer
Yrjö Raivio
Telephone No. +358 29 509 5000

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	3GPP TS 33.501 V16.1.0 (2019-12). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 16). [online], 2019-12-31, [retrieved on 2021-04-21]. Retrieved from <https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g10.zip>, the whole document, in particular Fig. 13.4.1.1-2; Sections 12.1, 12.4, 13.4.1.1	1-30
A	3GPP TS 29.522 V16.2.0 (2019-12). 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Network Exposure Function Northbound APIs; Stage 3 (Release 16). [online], 2019-12-23, [retrieved on 2021-04-21]. Retrieved from <https://www.3gpp.org/ftp/Specs/archive/29_series/29.522/29522-g20.zip>, the whole document, in particular Figs. 4.2-1, 4.2-2; Sections 4.2, 4.4.2	1-30
A	3GPP TS 29.503 V16.2.0 (2019-12). 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Unified Data Management Services; Stage 3 (Release 16). [online], 2019-12-20, [retrieved on 2021-04-21]. Retrieved from <https://www.3gpp.org/ftp/Specs/archive/29_series/29.503/29503-g20.zip>, the whole document, in particular Fig. 4.1-1; Section 4.1	1-30

US 2017149837 A1	25/05/2017	US 10084823 B2	25/09/2018
		CN 104255007 A	31/12/2014
		CN 104255007 B	14/07/2017
		CN 105659558 A	08/06/2016
		CN 105659558 B	31/08/2018
		EP 2761522 A2	06/08/2014
		EP 2761522 B1	22/06/2016
		EP 3047626 A1	27/07/2016
		EP 3047626 B1	25/10/2017
		IN 2443CHN2014 A	07/08/2015
		JP 2015501021 A	08/01/2015
		JP 6018210 B2	02/11/2016
		JP 2016535880 A	17/11/2016
		JP 6033990 B2	30/11/2016
		US 2013086645 A1	04/04/2013
		US 8935757 B2	13/01/2015
		US 2013086657 A1	04/04/2013
		US 9043886 B2	26/05/2015
		US 2015089597 A1	26/03/2015
		US 9197623 B2	24/11/2015
		US 2015089617 A1	26/03/2015
		US 9237145 B2	12/01/2016
		US 2015089596 A1	26/03/2015
		US 9350718 B2	24/05/2016
		US 2015089622 A1	26/03/2015
		US 9374356 B2	21/06/2016
		US 2016080361 A1	17/03/2016
		US 9407628 B2	02/08/2016
		US 2016028737 A1	28/01/2016
		US 9450963 B2	20/09/2016
		US 2015087879 A1	26/03/2015
		US 9463336 B2	11/10/2016
		US 2015089570 A1	26/03/2015
		US 9531697 B2	27/12/2016
		US 2015089571 A1	26/03/2015
		US 9544294 B2	10/01/2017
		US 2016226859 A1	04/08/2016
		US 9565178 B2	07/02/2017
		US 2015089623 A1	26/03/2015
		US 9578014 B2	21/02/2017
		US 2015089569 A1	26/03/2015
		US 9699170 B2	04/07/2017
		US 2017302655 A1	19/10/2017
		US 9860234 B2	02/01/2018
		US 2017021194 A1	26/01/2017
		WO 2013049461 A2	04/04/2013

		WO 2015042349 A1	26/03/2015
WO 2020002764 A1	02/01/2020	CN 112335274 A	05/02/2021

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2021/050040

CLASSIFICATION OF SUBJECT MATTER

IPC
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 12/084 (2021.01)
H04W 12/104 (2021.01)
H04W 12/60 (2021.01)