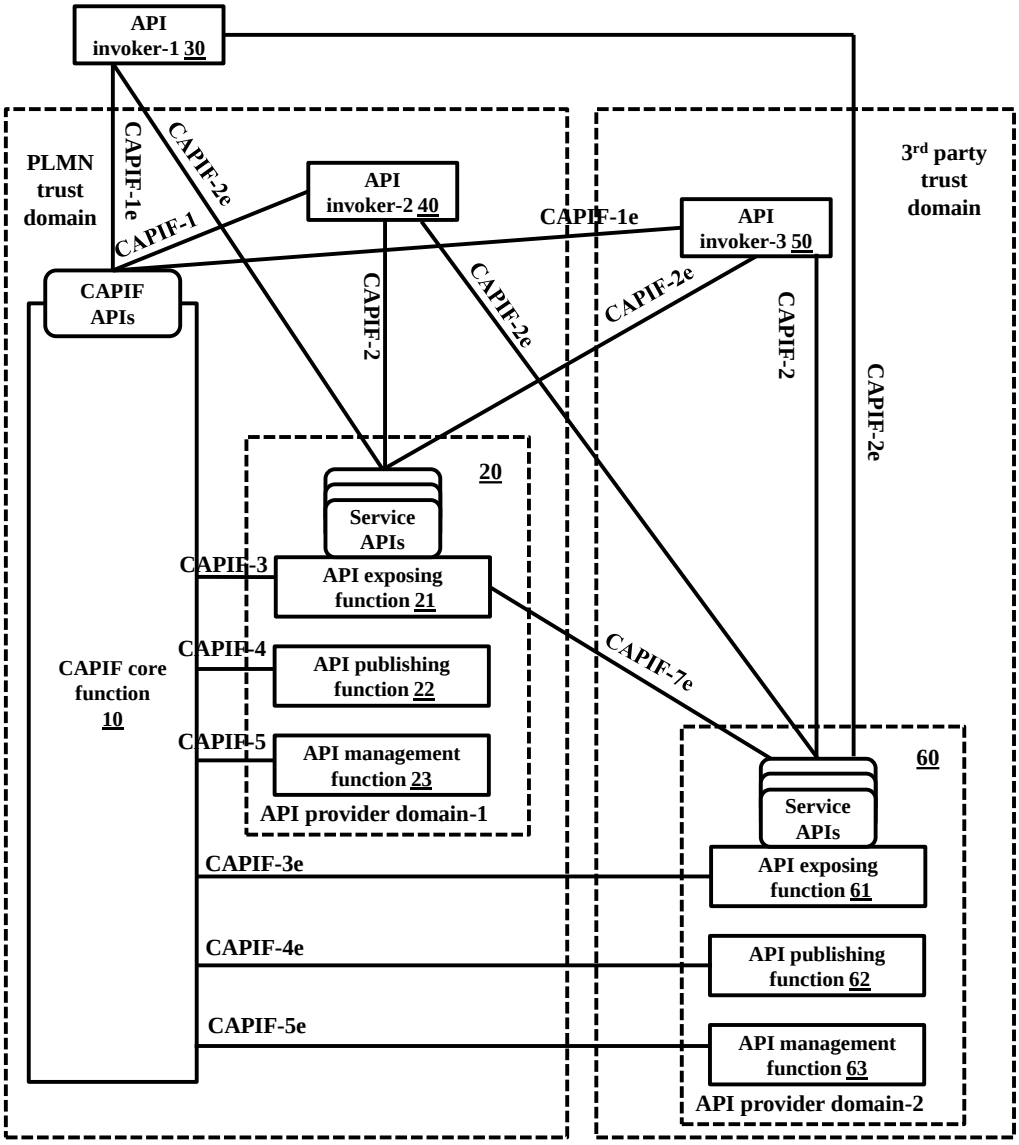

FIG. 1
(Prior art)

Arun Kishore Narasani
Patent Agent: IN/PA 1049

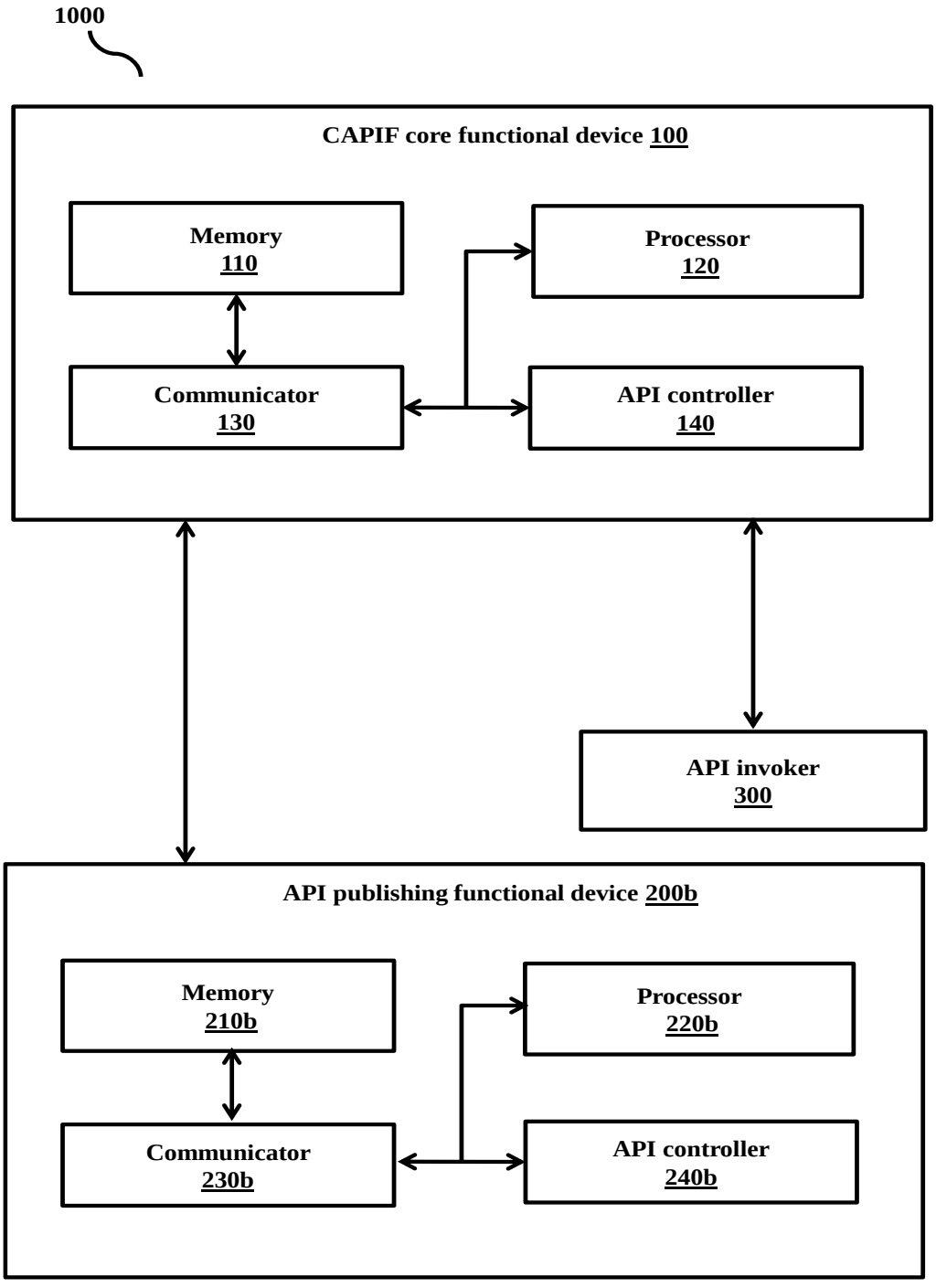

FIG. 2

Arun Kishore Narasani
Patent Agent: IN/PA 1049

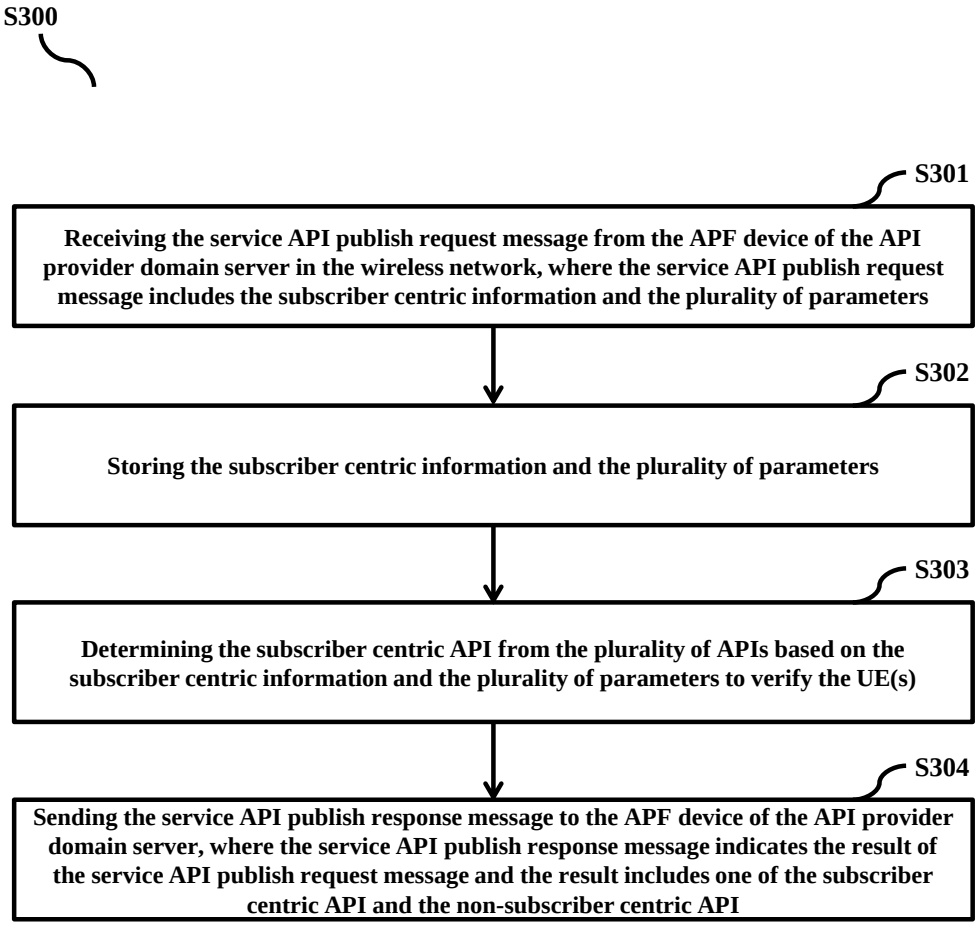

FIG. 3

Arun Kishore Narasani
Patent Agent: IN/PA 1049

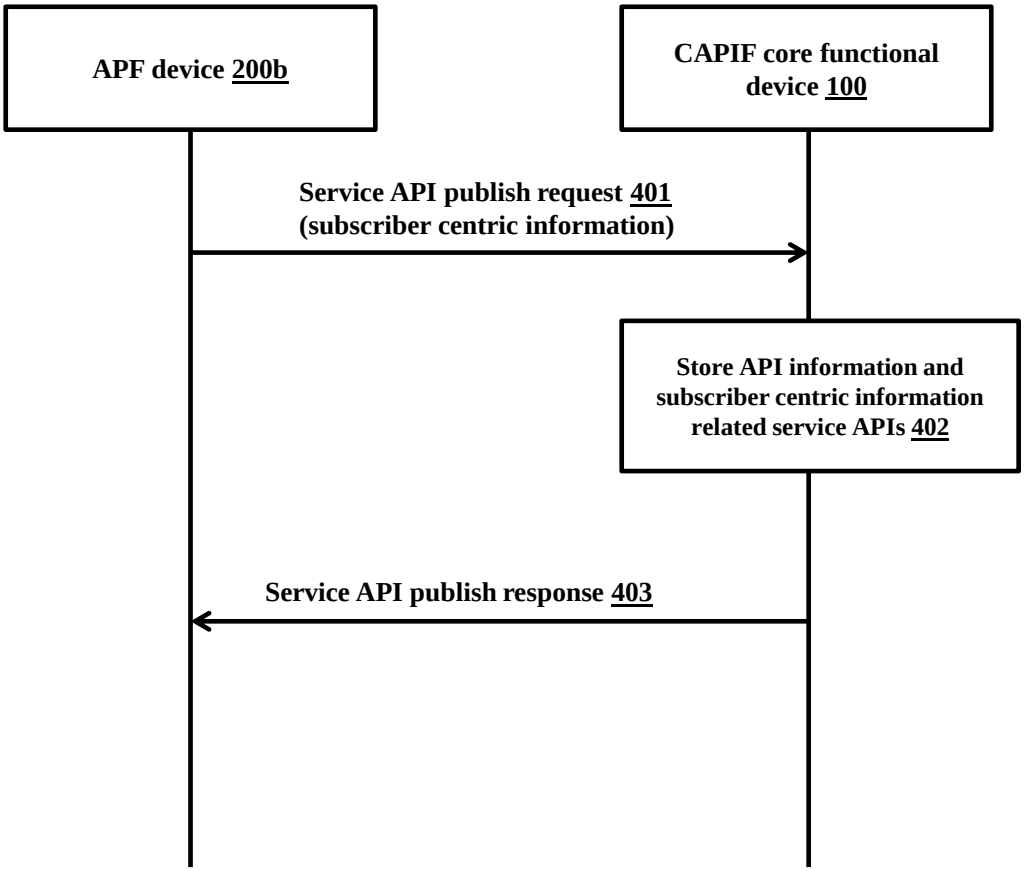

FIG. 4

Arun Kishore Narasani
Patent Agent: IN/PA 1049

Name of the Applicant: Samsung Electronics Co., Ltd.

Total No Of Sheets: 1

Application Number: **Sheet No.: 1/1**

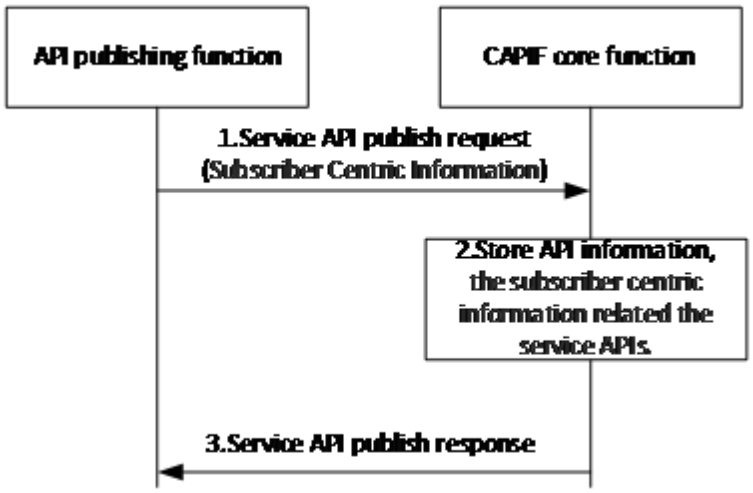

FIG. 1

Arun Kishore Narasani
Patent Agent: IN/PA 1049

FORM 2

The Patent Act 1970

(39 of 1970)

&

The Patent Rules, 2005

COMPLETE SPECIFICATION

(SEE SECTION 10 AND RULE 13)

TITLE OF THE INVENTION

"Method and system for determining subscriber-centric API in wireless network"

APPLICANT:

Name	: Samsung Electronics Co., Ltd.
Nationality	: Republic of Korea
Address	: 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi- do 443-742, Republic of Korea

The following specification particularly describes and ascertains the nature of this invention and the manner in which it is to be performed:

FIELD OF INVENTION

[0001] The present invention relates to a wireless network, and more specifically related to a method and a system for determining a subscriber-centric Application Programming Interface (API) in the wireless network. The present application is based on and claims priority from an Indian Provisional Application Number **202141013564** filed on 26th March 2021, the disclosure of which is hereby incorporated by reference herein.

BACKGROUND

[0002] 3rd Generation Partnership Project (3GPP) offers network services to third-party Application Functions (AF) through northbound Application Programming Interfaces (APIs). The majority of the northbound APIs are associated with User Equipment (UE(s)) and may have an impact on service experience of the UE(s). A Network Exposure Function (NEF) and Service Capability Exposure Function (SCEF) are key functional entities that offer the 3GPP network services through the northbound APIs, as specified in 3GPP Technical Specification (TS) 29.522 and 3GPP TS 29.122 respectively.

[0003] Furthermore, the 3GPP also defines architectures for enabling a vertical specific application(s) over 3GPP networks. The architectures also define a service(s) as the northbound APIs, at an enabler layer for consumption by the vertical-specific application(s). For example, Service Enabler Architecture Layer (SEAL) for verticals as specified in 3GPP TS 23.434. Furthermore, the 3GPP specified Common API Framework (CAPIF) in TS 23.222, to define common aspects that apply to all the northbound APIs. Some of the key functionalities of the CAPIF include API discovery, API management (publishing APIs), authentication, and authorization of Application Function (API invoker) using the northbound APIs.

[0004] The AF may invoke the northbound API, related to the UE (subscriber with 3GPP credentials) or a set of UEs using an external

identifier(s) in an API request. In such scenarios, an API exposing function (e.g. NEF, SCEF, etc.) serving the northbound APIs, authenticates and authorizes the AF for an API invocation and may additionally need to authorize the UE(s) in a context of API invocation and that the AF is authorized to invoke the northbound API related to the specific UE(s) in the API request. Not all the northbound APIs defined by the 3GPP are subscriber-centric, which means that such APIs do not affect the service experience of the UE(s). Some northbound APIs are subscriber-centric and some are not. In such a scenario, for a CAPIF Core Function (CCF) to be able to authorize the UE(s) and verify that the AF (API invoker) can invoke a service API related to UE(s), the CCF should be able to determine if the service API is subscriber-centric or affects the service experience of the UE(s). But in a conventional system, the CCF cannot checks whether the service API is subscriber-centric or not and verify the UE(s) in the context of AF's API invocation.

[0005] Thus, it is desired to provide a useful alternative for determining the subscriber-centric APIs in the wireless network.

OBJECT OF INVENTION

[0006] The principal object of the embodiments herein is to provide a method and a Common API Framework (CAPIF) core functional device for determining a subscriber-centric API from a plurality of APIs based on received service API publish request message from an API Publishing Function (APF) device of an API provider domain server. The service API publish request message includes subscriber-centric information and a plurality of parameters. The CAPIF core functional device enables for verification of a UE(s) in a context of an API invocation in response to determining the subscriber-centric API from the plurality of APIs. As a result, the CAPIF core functional device, the UE(s), and other network entities establish a secure wireless network. The proposed method allows the

CAPIF core functional device to authorize API invocation not only based on the API invoker invoking the service API, but also on the granularity for which subscribers (UEs) the API is invoked. This is to allow for more granular authorization for subscriber-aware northbound APIs.

[0007] Another object of the embodiment herein is to enable the CAPIF core functional device and an API Exposing Functional (AEF) device (e.g. NEF, SCEF, etc.) of the API provider domain server to selectively verify the UE(s) in the context of the API invocation only for a service API invocation that is in context of the UE(s), along with authentication and authorization of an API invoker (e.g. Application Function (AF)), in response to determining that the invoked service API is subscriber-centric API from the plurality of APIs.

[0008] Another object of the embodiment herein is to verify or not verify the UE(s) in the context of the API invocation based on a trust or business relationship between the API provider domain server and the API invoker in response to determining the invoked service API is subscriber-centric API from the plurality of APIs.

[0009] Another object of the embodiment herein is to verify the UE(s) in the context of the API invocation based on configured local policies in response to determining the invoked service API is subscriber-centric API from the plurality of APIs.

SUMMARY

[0010] Accordingly, the embodiment herein is to provide a method for determining a subscriber-centric Application Programming Interface (API) in a wireless network. The method includes receiving, by a Common API Framework (CAPIF) core functional device, a service API publish request message from an API Publishing Function .

[0011] In an embodiment, the plurality of information elements includes API publisher information, service API information, and shareable

information. The API publisher information includes identity, authentication, and authorization information (where the identity, authentication, and authorization information is used to validate the service API publish request), the service API information includes a service API name, a service API type, a communication type, a description, serving area information, an AEF location, subscriber-centric information, interface details, protocols, version numbers, data format and session Identity (ID), and the shareable information indicates whether the service API or a service API category is sharable to other CAPIF core functional device.

[0012] In an embodiment, the method includes enabling, by the CAPIF core functional device, to verify the UE(s) in the context of the API invocation in response to determining that the invoked service API is subscriber-centric API from the plurality of APIs. Further, the method includes verifying, by the CAPIF core functional device, the UE(s) in the context of the API invocation based on the subscriber-centric information and the plurality of parameters in subsequent CAPIF procedures.

[0013] In an embodiment, the APF device of the API provider domain server includes the subscriber-centric information as common information applicable for all service APIs in the service API publish request message or separately for each service API.

[0014] In an embodiment, the APF device of the API provider domain server includes the service API information along with the subscriber-centric information of the service API information at the CAPIF core functional device using an update service APIs procedure.

[0015] In an embodiment, the APF device of the API provider domain server defines the session ID, the session ID is used to select the service API by the CAPIF core functional device, and an API Invoker to bind the service API used to a particular UE session.

[0016] In an embodiment, the method includes verifying or not verifying, by the CAPIF core functional device, the UE(s) in the context of the API invocation based on a trust or business relationship between the API provider domain server, and an API invoker.

[0017] In an embodiment, the APF device of the API provider domain server includes receiving, by the APF device of the API provider domain server, on-boarded API invokers information from the CAPIF core functional device, and selectively adding, by the APF device of the API provider domain server, the API invoker information in a publish APIs procedure when the service APIs in the service API publish request message needs to verify the UE(s) in the context of the service API invocation and the service API in the service API publish request message is invoked by the API invokers.

[0018] In an embodiment, the method includes determining, by the CAPIF core functional device, the subscriber-centric API from the plurality of APIs based on the data model of the service API. Further, the method includes performing, by the CAPIF core functional device, one of, verifying the UE(s) in the context of the API invocation in response to determine the subscriber-centric API, and selectively applying verification of the UE(s) in the context of the API invocation based on configured local policies

[0019] Accordingly, the embodiment herein is to provide the CAPIF core functional device for determining the subscriber-centric API in the wireless network. The CAPIF core functional device includes an API controller coupled with a processor and a memory. The API controller receives the service API publish request message from the APF device of the API provider domain server in the wireless network. Further, the API controller stores the subscriber-centric information and the plurality of parameters. Further, the API controller determines the subscriber-centric API from the plurality of APIs based on the subscriber-centric information

and the plurality of parameters to verify the UE(s). Further, the API controller sends the service API publish response message to the APF device of the API provider domain server, where the service API publish response message indicates the result of the service API publish request message and the result includes one of the subscriber-centric API or a non-subscriber-centric API.

[0020] Accordingly, the embodiment herein is to provide the APF device of the API provider domain server for selectively adding the API invoker information. The APF device includes an API controller coupled with a processor and a memory. The API controller receives on-boarded API invoker's information from the CAPIF core functional device. Further, the API controller selectively adds the API invoker information in the publish APIs procedure when the service APIs in the service API publish request message need to verify the UE(s) and the service API in the service API publish request message is invoked by the API invokers.

[0021] These and other aspects of the embodiments herein will be better appreciated and understood when considered in conjunction with the following description and the accompanying drawings. It should be understood, however, that the following descriptions, while indicating preferred embodiments and numerous specific details thereof, are given by way of illustration and not of limitation. Many changes and modifications may be made within the scope of the embodiments herein, and the embodiments herein include all such modifications.

BRIEF DESCRIPTION OF FIGURES

[0022] This invention is illustrated in the accompanying drawings, throughout which like reference letters indicate corresponding parts in the various figures. The embodiments herein will be better understood from the following description with reference to the drawings, in which:

[0023] FIG. 1 illustrates an example schematic diagram of a functional model for a CAPIF to support 3rd party API providers, according to prior art;

[0024] FIG. 2 illustrates a block diagram of a system to determine a subscriber-centric Application Programming Interface (API) in a wireless network, according to the embodiments as disclosed herein;

[0025] FIG. 3 is a flow diagram illustrating a method for determining the subscriber-centric API in the wireless network, according to the embodiments as disclosed herein; and

[0026] FIG. 4 is a sequential diagram illustrating the method for determining the subscriber-centric API in the wireless network, according to the embodiments as disclosed herein.

DETAILED DESCRIPTION OF INVENTION

[0027] The embodiments herein and the various features and advantageous details thereof are explained more fully with reference to the non-limiting embodiments that are illustrated in the accompanying drawings and detailed in the following description. Descriptions of well-known components and processing techniques are omitted so as to not unnecessarily obscure the embodiments herein. Also, the various embodiments described herein are not necessarily mutually exclusive, as some embodiments can be combined with one or more other embodiments to form new embodiments. The term "or" as used herein, refers to a non-exclusive or, unless otherwise indicated. The examples used herein are intended merely to facilitate an understanding of ways in which the embodiments herein can be practiced and to further enable those skilled in the art to practice the embodiments herein. Accordingly, the examples should not be construed as limiting the scope of the embodiments herein.

[0028] As is traditional in the field, embodiments may be described and illustrated in terms of blocks which carry out a described function or functions. These blocks, which may be referred to herein as managers, units, modules, hardware components or the like, are physically implemented by analog and/or digital circuits such as logic gates, integrated circuits, microprocessors, microcontrollers, memory circuits, passive electronic components, active electronic components, optical components, hardwired circuits and the like, and may optionally be driven by firmware. The circuits may, for example, be embodied in one or more semiconductor chips, or on substrate supports such as printed circuit boards and the like. The circuits constituting a block may be implemented by dedicated hardware, or by a processor (e.g., one or more programmed microprocessors and associated circuitry), or by a combination of dedicated hardware to perform some functions of the block and a processor to perform other functions of the

block. Each block of the embodiments may be physically separated into two or more interacting and discrete blocks without departing from the scope of the disclosure. Likewise, the blocks of the embodiments may be physically combined into more complex blocks without departing from the scope of the disclosure.

[0029] The accompanying drawings are used to help easily understand various technical features and it should be understood that the embodiments presented herein are not limited by the accompanying drawings. As such, the present disclosure should be construed to extend to any alterations, equivalents and substitutes in addition to those which are particularly set out in the accompanying drawings.

[0030] Throughout this document, the term "subscriber-centric API" means a northbound API that affects the service experience of UE(s) or a service API is in a context of the UE(s). The terms "northbound API" and "service API" mean the same and are used interchangeably throughout this document. Throughout this document, the term "verifies the UE" means, authentication, and/or authorizes the UE or takes UE's consent. The terms "CAPIF", "CAPIF core functional device" and "CAPIF core function" mean the same and are used interchangeably throughout this document. The terms "API Exposing Functional (AEF) device" and "API Exposing Function (AEF) device" mean the same and are used interchangeably throughout this document. The terms "entity", and "device" mean the same and are used interchangeably throughout this document.

[0031] FIG. 1 illustrates an example schematic diagram of a functional model for a CAPIF (10) to support 3rd party API providers, according to prior art.

[0032] The CAPIF core function (10) in a Public Land Mobile Network (PLMN) trust domain supports service APIs (20) from both the PLMN trust domain and a 3rd party trust domain having a business

relationship with the PLMN. API invokers (e.g. 40, 50, and 30) may exist within the PLMN trust domain, or within the 3rd party trust domain, or outside of both the PLMN trust domain and the 3rd party trust domain. The API provider domain server-1 (20) offers service APIs from a PLMN operator. The API provider domain server-2 (60) offers service APIs from the 3rd party. When the 3rd party API providers are a trusted 3rd party of the PLMN, the API provider domain server-1 (20) also offers the service APIs from the 3rd party.

[0033] The API invoker-2 (40) within the PLMN trust domain interacts with the CAPIF core function (10) via CAPIF-1, invokes the service APIs in the PLMN trust domain via CAPIF-2, and invokes the service APIs in the 3rd party trust domain via CAPIF-2e. The API invoker-3 (50) within the 3rd party trust domain interacts with the CAPIF core function (10) via CAPIF-1e, invokes the service APIs in the PLMN trust domain via CAPIF-2e, and invokes the service APIs in 3rd party trust domain via CAPIF-2. The API invoker-1 (30) from outside the PLMN trust domain and 3rd party trust domain, interacts with the CAPIF core function (10) via CAPIF-1e and invokes the service APIs in the PLMN trust domain and the service APIs in the 3rd party trust domain via CAPIF-2e.

[0034] An API exposing function (21), an API publishing function (22), and an API management function (23) of the API provider domain server-1 (20) within the PLMN trust domain interacts with the CAPIF core function (10) via CAPIF-3, CAPIF-4, and CAPIF-5 respectively. An API exposing function (61), an API publishing function (62), and an API management function (63) of the API provider domain server-2 (60) within the 3rd party trust domain interacts with the CAPIF core function (10) in the PLMN trust domain via CAPIF-3e, CAPIF-4e, and CAPIF-5e respectively. The API exposing functions (21, 61) provide the service APIs to the API

invokers (30, 40, and 50), offered by the respective trust domains. The API exposing function (21) within the PLMN trust domain interacts with the API exposing function (61) in the 3rd party trust domain via CAPIF-7e.

[0035] In a conventional system, the CCF (10) cannot determine whether a service API is subscriber-centric or not and verify a UE(s) in an AF's API invocation. In addition, the API provider domain server (e.g. 20 and/or 60) may want to verify or not verify the UE(s) based on a service agreement between the API Provider domain server (e.g. 20 and/or 60) and the API invokers (or said Application Function (AF)) (e.g. 30, 40 and 50), additionally the UE in the context of the API invocation, along with the authentication and authorization of the AF. Some examples of scenarios are shown below.

a) As in the context of Business to Consumer (B2C) application (e.g. shopping application, social media application, etc.), a user of the UE uses an application(s) provided by an application service provider on the UE. In such instances, the application service provider may choose to access 3GPP network services via northbound APIs, which may impact UE's service experience. For example, upgradation of a UE's Quality of Service (QoS) profile for the application service provider's application traffic on the UE, and retrieval of a UE's location from a core network.

b) As in the context of Machine Type Communication (MTC) service providers may have a service agreement with a Public Land Mobile Network (PLMN) under which a dedicated AF may request network services on behalf of all the devices belonging to the MTC service provider. In such a case, block permission may suffice as all the devices belong to a single user (e.g. MTC provider).

[0036] The following are some instances of APIs that are not subscriber-centric according to definition of API.

a. The UE(s) in a given location (monitoring events configuration directly via Mobility Management Device (MME)/ Serving GPRS Support Node (SGSN)), as specified in clause 4.4.2.2.3 of 3GPP TS 29.122.

b. Packet Flow Description (PFDs) associated with an application identifier (procedures for PFD management), as specified in clause 4.4.10 of 3GPP TS 29.122.

c. Reporting network status API, in clause 5.9, of 3GPP TS 29.122.

[0037] The aforementioned issue also applies to the northbound APIs offered by 3GPP vertical enabler layers for use by vertical-specific applications. Some examples of the vertical enabler layers specified by the 3GPP are, a Service Enabler Architecture Layer (SEAL) for verticals as specified in 3GPP TS 23.434, Vehicle-to-Everything (V2X) services as specified in 3GPP TS 23.486, Architecture for enabling Edge Applications as specified in 3GPP TS 23.558, Application layer support for Unmanned Aerial System (UAS) as specified in 3GPP TS 23.255, and like so. These vertical enabler layer architectures define functional entities on UE side. Such UE side functional identities are defined in the respective architectures like Vertical Application Layer (VAL) User ID, VAL UE ID in SEAL, and EEC ID in EDGE APP (3GPP TS 23.558) and like so. It is possible that the vertical enabler layer functional entities that expose the northbound APIs, maybe subscriber-centric that affect the service experience of the UE(s) side functional entities.

[0038] Not all the northbound APIs defined by the 3GPP vertical enabler layers are subscriber-centric, which means that such APIs do not affect the service experience of the UE side functional entities. Some northbound APIs are subscriber-centric and some are not. In such a scenario, for the CAPIF Core Function (CCF) (10) to be able to authorize the UE side functional device and verify that the AF (API Invoker) can invoke a service API related to the UE side functional device, the CCF (10) should be able to

determine if a service API is subscriber-centric or affects the service experience of UE side functional device. But in the conventional system, the CCF (10) cannot determine if the service API is subscriber-centric or not and verify the UE(s) in the AF's API invocation.

[0039] The 3GPP defined northbound APIs determine the UE(s) with various identifiers, namely, Mobile Subscriber ISDN (MSISDN), external identifier, Generic Public Subscription Identifier (GPSI), Internet Protocol (IP) address of the UE(s), and like so. 3GPP defined vertical enabler layer, determine the UE side functional device, Such UE side functional identities are defined in the respective architectures like the VAL User ID, the VAL UE ID in the SEAL, the EEC ID in the EDGE APP (3GPP TS 23.558) and like so. The above-stated shortcoming applies to all of these UE or UE side functional device identification mechanisms.

[0040] Accordingly, the embodiment herein is to provide a method for determining a subscriber-centric Application Programming Interface (API) in a wireless network. The method includes receiving, by a Common API Framework (CAPIF) core functional device, a service API publish request message from an API Publishing Functional (APF) device of an API provider domain server in the wireless network, where the service API publish request message includes subscriber-centric information and a plurality of parameters. Further, the method includes storing, by the CAPIF core functional device, the subscriber-centric information and the plurality of parameters. Further, the method includes determining, by the CAPIF core functional device, the subscriber-centric API from a plurality of APIs (e.g. subscriber-centric API or non-subscriber-centric API/ or said service APIs) based on the subscriber-centric information and the plurality of parameters to verify a User Equipment(s) (UE(s)). Further, the method includes sending, by the CAPIF core functional device, a service API publish response message to the APF device of the API provider domain server, where the

service API publish response message indicates a result of the service API publish request message and the result includes one of the subscriber-centric API or a non-subscriber-centric API.

[0041] Accordingly, the embodiment herein is to provide the CAPIF core functional device for determining the subscriber-centric API in the wireless network. The CAPIF core functional device includes an API controller coupled with a processor and a memory. The API controller receives the service API publish request message from the APF device of the API provider domain server in the wireless network. Further, the API controller stores the subscriber-centric information and the plurality of parameters. Further, the API controller determines the subscriber-centric API from the plurality of APIs based on the subscriber-centric information and the plurality of parameters to verify the UE(s). Further, the API controller sends the service API publish response message to the APF device of the API provider domain server, where the service API publish response message indicates the result of the service API publish request message and the result includes one of the subscriber-centric API or a non-subscriber-centric API.

[0042] Accordingly, the embodiment herein is to provide the APF device of the API provider domain server for selectively adding the API invoker information. The APF device includes an API controller coupled with a processor and a memory. The API controller receives on-boarded API invoker's information from the CAPIF core functional device. Further, the API controller selectively adds the API invoker information in the publish APIs procedure when the service APIs in the service API publish request message need to verify the UE(s) and the service API in the service API publish request message is invoked by the API invokers.

[0043] Unlike existing methods and systems, the proposed method allows the CAPIF core functional device to determine the subscriber-centric

API from the plurality of APIs based on received service API publish request message from the API Publishing Function (APF) device of the API provider domain server. The service API publish request message includes the subscriber-centric information and the plurality of parameters. The CAPIF core functional device enables for verification of the UE(s) in the context of the API invocation in response to determining the subscriber-centric API from the plurality of APIs. As a result, the CAPIF core functional device, the UE(s), and other network devices/entities establish a secure wireless network. The proposed method allows the CAPIF core functional device to authorize API invocation not only based on the API invoker invoking the service API, but also on the granularity for which subscribers (UEs) the API is invoked. This is to allow for more granular authorization for subscriber-aware northbound APIs.

[0044] Unlike existing methods and systems, the proposed method allows to enable the CAPIF core functional device and an API Exposing Functional (AEF) device (e.g. NEF, SCEF, etc.) of the API provider domain server to selectively verify the UE(s) in the context of the API invocation only for the service API invocation that is in context of the UE(s), along with authentication and authorization of an API invoker (e.g. Application Function (AF) (e.g. 30, 40 and 50)), in response to determining that the subscriber-centric API from the plurality of APIs.

[0045] Unlike existing methods and systems, the proposed method allows the CAPIF core functional device to verify or not verify the UE(s) in the context of the API invocation based on a trust or business relationship between the API provider domain server and the API invoker in response to determining the subscriber-centric API from the plurality of APIs.

[0046] Unlike existing methods and systems, the proposed method allows the CAPIF core functional device to verify the UE(s) in the context

of the API invocation based on configured local policies in response to determining the subscriber-centric API from the plurality of APIs.

[0047] Referring now to the drawings and more particularly to FIGS. 2 through 4, where similar reference characters denote corresponding features consistently throughout the figures, there are shown preferred embodiments.

[0048] FIG. 2 illustrates a block diagram of a system (1000) to determine a subscriber-centric Application Programming Interface (API) in a wireless network, according to the embodiments as disclosed herein. The system (1000) includes a Common API Framework (CAPIF) core functional device (100), an API provider domain server (200) (not shown in FIG. 2), an API invoker(s) (300), and a UE(s) (400) (not shown in FIG. 2).

[0049] The API provider domain server (200) includes an API Exposing Functional (AEF) device (200a), an API Publishing Functional (APF) device (200a), and an API Management Functional (AMF) device (200c). Example of the UE(s) (400) include, but are not limited to a smartphone, a tablet computer, a Personal Digital Assistance (PDA), an Internet of Things (IoT) device, a wearable device, etc.

[0050] In an embodiment, the CAPIF core functional device (100) includes a memory (110), a processor (120), a communicator (130), and an API controller (140).

[0051] In an embodiment, the memory (110) stores a subscriber centric API(s), a non-subscriber centric API(s), subscriber-centric information, a plurality of parameters, API invoker information, other applicable parameters, and a plurality of information elements in a data model of a service API. The memory (110) stores instructions to be executed by the processor (120). The memory (110) may include non-volatile storage elements. Examples of such non-volatile storage elements may include magnetic hard discs, optical discs, floppy discs, flash memories, or forms of

electrically programmable memories (EPROM) or electrically erasable and programmable (EEPROM) memories. In addition, the memory (110) may, in some examples, be considered a non-transitory storage medium. The term "non-transitory" may indicate that the storage medium is not embodied in a carrier wave or a propagated signal. However, the term "non-transitory" should not be interpreted that the memory (110) is non-movable. In some examples, the memory (110) can be configured to store larger amounts of information than the memory. In certain examples, a non-transitory storage medium may store data that can, over time, change (e.g., in Random Access Memory (RAM) or cache). The memory (110) can be an internal storage unit or it can be an external storage unit of the CAPIF core functional device (100), a cloud storage, or any other type of external storage.

[0052] The processor (120) communicates with the memory (110), the communicator (130), and the API controller (140). The processor (120) is configured to execute instructions stored in the memory (110) and to perform various processes. The processor (120) may include one or a plurality of processors, maybe a general-purpose processor, such as a central processing unit (CPU), an application processor (AP), or the like, a graphics-only processing unit such as a graphics processing unit (GPU), a visual processing unit (VPU), and/or an Artificial intelligence (AI) dedicated processor such as a neural processing unit (NPU).

[0053] The communicator (130) is configured for communicating internally between internal hardware components and with external devices (e.g. API invoker, API provider domain server, other CAPIF core functional device, etc.) via one or more networks (e.g. Radio technology). The communicator (130) includes an electronic circuit specific to a standard that enables wired or wireless communication.

[0054] The API controller (140) is implemented by processing circuitry such as logic gates, integrated circuits, microprocessors,

microcontrollers, memory circuits, passive electronic components, active electronic components, optical components, hardwired circuits, or the like, and may optionally be driven by firmware. The circuits may, for example, be embodied in one or more semiconductor chips, or on substrate supports such as printed circuit boards and the like.

[0055] In an embodiment, the API controller (140) receives a service API publish request message from the APF device (200a) of the API provider domain server (200) in the wireless network, where the service API publish request message includes the published service APIs, subscriber-centric information and the plurality of parameters. Further, the API controller (140) stores the subscriber-centric information and the plurality of parameters to the memory (110). The subscriber-centric information includes a plurality of subscriber centric northbound APIs, verification of the UE(s) (400) in a context of an API invocation, a plurality of information elements in a data model of a service API that identify the UE(s) (400), an API invoker information, and other applicable parameters (Other applicable parameters are based on the data model of the published service API; there is no fixed set of the plurality of parameters. NEF and SCEF expose a lot of APIs, each with its own data model). The plurality of information elements includes API publisher information, service API information, and shareable information. The API publisher information includes identity, authentication, and authorization information (where the identity, authentication, and authorization information is used to validate the service API publish request). The service API information includes a service API name, a service API type, a communication type, a description, serving area information, an AEF location, the subscriber-centric information, interface details, protocols, version numbers, data format, and session Identity (ID), as described in 3GPP TS 23.222. The shareable information indicates whether the service

API or a service API category is sharable to other CAPIF core functional device (100).

[0056] In an embodiment, the API controller (140) determines the subscriber-centric API from a plurality of APIs based on the subscriber-centric information and the plurality of parameters to verify the UE(s) (400). Further, the API controller (140) sends a service API publish response message to the APF device (200b) of the API provider domain server (200), where the service API publish response message indicates a result of the service API publish request message and the result includes the subscriber centric API or the non-subscriber centric API.

[0057] In an embodiment, the API controller (140) enables to verify the UE(s) (400) in the context of the API invocation in response to determining the subscriber-centric API from the plurality of APIs. Further, the API controller (140) verifies the UE(s) (400) in the context of an API invocation based on the subscriber-centric information and the plurality of parameters in subsequent CAPIF procedures (subsequent CAPIF procedures explained in FIG. 4).

[0058] In an embodiment, the API controller (140) verifies or does not verify the UE(s) (400) in the context of the API invocation based on a trust or business relationship between the API provider domain server (200), and the API invoker (300).

[0059] In an embodiment, the API controller (140) determines the subscriber-centric API from the plurality of APIs based on the data model of the service API. Further, the API controller (140) verifies the UE(s) (400) in the context of the API invocation in response to determine the subscriber-centric API. Further, the API controller (140) selectively applies verification of the UE(s) (400) in the context of an API invocation based on configured local policies.

[0060] In an embodiment, the APF device (200b) includes a memory (210b), a processor (220b), a communicator (230b), and an API controller (240b).

[0061] In an embodiment, the memory (210b) stores the subscriber centric API(s), the non-subscriber centric API(s), the subscriber-centric information, the plurality of parameters, the API invoker information, other applicable parameters, and the plurality of information elements in the data model of the service API. The memory (210b) stores instructions to be executed by the processor (220b). The memory (210b) may include non-volatile storage elements. Examples of such non-volatile storage elements may include magnetic hard discs, optical discs, floppy discs, flash memories, or forms of electrically programmable memories (EPROM) or electrically erasable and programmable (EEPROM) memories. In addition, the memory (210b) may, in some examples, be considered a non-transitory storage medium. The term "non-transitory" may indicate that the storage medium is not embodied in a carrier wave or a propagated signal. However, the term "non-transitory" should not be interpreted that the memory (210b) is non-movable. In some examples, the memory (210b) can be configured to store larger amounts of information than the memory. In certain examples, a non-transitory storage medium may store data that can, over time, change (e.g., in Random Access Memory (RAM) or cache). The memory (210b) can be an internal storage unit or it can be an external storage unit of the APF device (200b), a cloud storage, or any other type of external storage.

[0062] The processor (220b) communicates with the memory (210b), the communicator (230b), and the API controller (240b). The processor (220b) is configured to execute instructions stored in the memory (210b) and to perform various processes. The processor (220b) may include one or a plurality of processors, maybe a general-purpose processor, such as a central processing unit (CPU), an application processor (AP), or the like, a graphics-

only processing unit such as a graphics processing unit (GPU), a visual processing unit (VPU), and/or an Artificial intelligence (AI) dedicated processor such as a neural processing unit (NPU).

[0063] The communicator (230b) is configured for communicating internally between internal hardware components and with external devices (e.g. API invoker, CAPIF core functional device, etc.) via one or more networks (e.g. Radio technology). The communicator (230b) includes an electronic circuit specific to a standard that enables wired or wireless communication.

[0064] The API controller (240b) is implemented by processing circuitry such as logic gates, integrated circuits, microprocessors, microcontrollers, memory circuits, passive electronic components, active electronic components, optical components, hardwired circuits, or the like, and may optionally be driven by firmware. The circuits may, for example, be embodied in one or more semiconductor chips, or on substrate supports such as printed circuit boards and the like.

[0065] In an embodiment, the API controller (240b) receives on-boarded API invoker's information from the CAPIF core functional device (100). Further, the API controller (240b) selectively adds the API invoker information in a publish APIs procedure when the service APIs in the service API publish request message need to verify the UE(s) (400) and the service API in the service API publish request message is invoked by the API invoker (300).

[0066] In an embodiment, the API controller (240b) includes the subscriber-centric information as common information applicable for all service APIs in the service API publish request message or separately for each service API.

[0067] In an embodiment, the API controller (240b) includes the service API information along with the subscriber-centric information of the

service API information at the CAPIF core functional device (100) using an update service APIs procedure.

[0068] In an embodiment, the API controller (240b) defines the session ID, the session ID is used to select the service API by the CAPIF core functional device (100) and the API Invoker (300) to bind the service API used to a particular UE session.

[0069] Although the FIG. 2 shows various hardware components of the CAPIF core functional device (100), the APF device (200b), and the API invoker (300) but it is to be understood that other embodiments are not limited thereon. In other embodiments, the CAPIF core functional device (100), the APF device (200b), and the API invoker (300) may include less or more components. Further, the labels or names of the components are used only for illustrative purpose and does not limit the scope of the invention. One or more components can be combined to perform the same or substantially similar function to determine the subscriber-centric AP in the wireless network.

[0070] FIG. 3 is a flow diagram (S300) illustrating a method for determining the subscriber-centric API in the wireless network, according to the embodiments as disclosed herein. The CAPIF core functional device (100) performs various steps (S301-S304) to determine the subscriber-centric AP in the wireless network.

[0071] At S301, the method includes receiving the service API publish request message from the APF device (200a) of the API provider domain server (200) in the wireless network, where the service API publish request message includes the subscriber-centric information and the plurality of parameters. At S302, the method includes storing the subscriber-centric information and the plurality of parameters. At S303, the method includes determining the subscriber-centric API from the plurality of APIs based on the subscriber-centric information and the plurality of parameters to verify

the UE(s) (400). At S304, the method includes sending the service API publish response message to the APF device (200b) of the API provider domain server (200), where the service API publish response message indicates the result of the service API publish request message and the result includes the subscriber centric API or the non-subscriber centric API.

[0072] The various actions, acts, blocks, steps, or the like in the flow diagram (S300) may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[0073] FIG. 4 is a sequential diagram illustrating the method for determining the subscriber-centric API in the wireless network, according to the embodiments as disclosed herein.

[0074] Referring to the FIG. 4 consider the proposed method illustrating a scenario of the APF device (200b) publishes service APIs information to the CAPIF core functional device (100) using "CAPIF_Publish_Service_API" API as specified in 3GPP TS 23.222, along with adding the subscriber-centric information, indicating the service APIs that are subscriber-centric. The subscriber-centric information includes the northbound APIs that are subscriber-centric and need verification of the UE(s) (not shown in FIG. 4) in the context of the API invocation, information elements in the data model of the service API(s) that determine the UE(S), may include API invoker(s) information and any other applicable parameters.

[0075] A precondition for an interaction between the APF device (200b) and the CAPIF core functional device (100) is a discovery of the external interface of the CAPIF core functional device (100). There are several ways that this can be achieved:

a) Through a ‘static’ assigned IP address, or well-known hostname that is shared between a Mobile Network Operator (MNO) and a third party. Though this approach is inflexible (one cannot change the address/name once assigned, nor is it possible to easily implement a ‘load sharing’ or improved assignment of resources subsequently.

b) Assignment of a Uniform Resource Identifier (URI) to an interface exposed by the CAPIF core functional device (100) that can be resolved through a multi-step process based upon use of a Domain Name Server (DNS) service record (DNS SRV RR) or Name Authority Pointer (NAPTR) record (NAPTR RR) as specified in IETF RFC 2782 or IETF RFC 2915 respectively.

[0076] This allows schemes in which different dynamic weights can be assigned to different potential names that can then be resolved to IP addresses. This approach simplifies the configuration of mechanism that will access the CAPIF core functional device (100) interface (it can remain the same over time and be given to any third party since in practice it will be resolved in a multi-stage process allowing for flexibility and changes in deployment over time.

[0077] At 401, the APF device (200b) sends the service API publish request message to the CAPIF core functional device (100), with the details of the service API, the subscriber-centric information, and other applicable parameters. The subscriber-centric information includes the northbound APIs that are subscriber-centric and need verification of the UE(s) in the context of the API invocation, information elements, as shown in Table-1, in the data model of the service API that determines the UE(S), may include API invoker(s) information and any other applicable parameters.

Information element	Status	Description
API publisher information	M	The information of the API publisher may include identity, authentication, and authorization information
Service API information	M	The service API information includes the service API name, service API type, communication type, description, Serving Area Information (optional), AEF location (optional), Subscriber-centric Information, interface details (e.g. IP address, port number, URI), protocols, version numbers, and data format. The session ID is provided corresponding to the session that provides the service. This is the corresponding session ID known to the AF over N5 or the session ID known to the UE over N1.
Shareable information	O (see NOTE)	Indicates whether the service API or the service API category can be published to other CCFs. And if sharing, a list of CAPIF provider domain server information where the service API or the service API category can be published is contained.
NOTE: If the shareable information is not present, the service API is not allowed to be shared.		

Table-1

[0078] At 402, upon receiving the service API publish request message, the CAPIF core functional device (100) stores the service API information and the subscriber-centric information provided by the API publishing function at the CAPIF core functional device (100) (API registry).

The CAPIF core functional device (100) uses the subscriber-centric information in determining the service APIs for which the UE(s) (400) in the context of the service API invocation need to be verified. Upon determining the service APIs that are subscriber-centric, the CAPIF core functional device (100) uses this information in subsequent CAPIF procedures of TS 23.222, as listed below, to determine and verify the UE(s) (400) in the context of API invocation. The AEF device verifies the UE(s) (400) in the context of the service API invocation if the published service API is subscriber-centric.

a) CAPIF_Security API, Obtain_Security_Method operation: API invoker requests the service API security method from CCF.

b) CAPIF_Security API, Obtain_Authorization operation: API invoker requests authorization from CCF to access relevant service API.

c) CAPIF_Access_Control_Policy API: Allows the AEF to obtain the policy to perform access control on the service API invocations.

[0079] At 403, the CAPIF core functional device (100) sends a service API publish response message to the APF device (200b) indicating the result of the service API publish request.

[0080] In an embodiment, the APF device (200b) may include the subscriber-centric information as common information applicable for all the service APIs in the service API Publish request message or separately for each service API.

[0081] In an embodiment, the APF device (200b) may include the subscriber-centric information within the service API information or outside of the service API information as a separate information element.

[0082] In an embodiment, the APF device (200b) may update the service API information, along with the service API's subscriber-centric information, at the CAPIF core functional device (100) using the update service APIs procedure as specified in TS 23.222.

[0083] In an embodiment, the APF device (200b) may specify the session ID specifically 'bound' to the published API. This will be used to select the service API by the CAPIF core functional device (100) or the API invoker subsequently. This will be used to bind the service API used to the particular UE session so that the API invoker will specifically be able to operate upon the session relevant to the intended service by means of the service API.

[0084] In an embodiment, based on the trust or business relationship between the API provider domain server (AEF, APF, and AMF) and Application Function (API Invoker), the API provider domain server may decide to have the CCF verify or skip the verification of the UE(s) in the context of the API invocation. In such a scenario, if the API provider domain server wishes the CAPIF core functional device (100) to verify the UE(s) (400) in the context of the service API invocation, when invoked by a set of API invokers (AFs) (300), then the APF shall include the set of API invoker's information in subscriber-centric information for the service API, in the service API publish request message. Upon receipt of such information from the APF, the CAPIF core functional device (100) determine that for the service API invocations from the set of API invoker (300) provided in the API publish request message, the CAPIF core functional device (100) verifies the UE(s) in the context of the service API invocation. The absence of API invoker information in the subscriber-centric information for a service API means for all the invocations of the service APIs, from any API invoker (300), the UE(s) in the context of the API needs to be verified.

[0085] If the API provider domain server wishes the CAPIF core functional device (100) to skip the verification of the UE(s) in the context of a service API invocation from a set of API invoker`s (AFs) (300), then the APF shall exclude the set of API invoker`s information from the subscriber-centric information for the service API in the service API publish request or

an update service API request message. The absence of subscriber-centric information for the service API indicates the CAPIF core functional device (100) to skip the verification of the UE(s) (400) in the context of the service API invocation from all API invokers (AFs) (300).

[0086] In an embodiment, the APF device (200b) may receive the on-boarded API invoker`s information from the CAPIF core functional device (100). The APF device (200b) may use the API invoker information obtained from the CAPIF core functional device (100), to selectively include the API invoker information in the Publish APIs procedure, if the service APIs in the API Publish request to need the subscriber (UE) verification, when the service API in the publish API request is invoked by the API invoker (300).

[0087] In an embodiment, when the northbound APIs are exposed by the 3GPP vertical enabler layers for the consumption by vertical-specific applications, and the UE side functional device is in the context of the API invocation, then the APF device (200b) publishes the vertical enabler layer service APIs to the CAPIF core functional device (100), with the subscriber-centric information. The subscriber-centric information includes the vertical enabler layer northbound APIs that are subscriber-centric and need verification of the UE side functional device/entities in the context of the API invocation, the information elements in the data model of the service API that determines the UE side functional device, may include API invoker(s) information and any the other applicable parameters.

[0088] In an embodiment, the CAPIF core functional device (100) may use CAPIF interconnection interface (CAPIF-6/6e as specified in TS 23.222) to publish the service APIs information to the partner CCF and may include the subscriber-centric information related to the service APIs, along with other applicable parameters in the service API publish request message.

[0089] The CAPIF core functional device (100) determines based on the data model of the API. In this scenario, the CAPIF core functional device

(100) checks whether the service API is subscriber-centric or not, based on the data model of the service API. Using the data model definition of the service API, the CAPIF core functional device (100) determines that the service API is subscriber-centric. Using this information, the CAPIF core functional device (100) verifies in the UE(s) in the context of such API invocations. Additionally, the CAPIF core functional device (100) selectively applies the verification of the UE(s) in the context of API invocation based on the configured local policies.

[0090] The embodiments disclosed herein can be implemented using at least one hardware device and performing network management functions to control the elements.

[0091] The foregoing description of the specific embodiments will so fully reveal the general nature of the embodiments herein that others can, by applying current knowledge, readily modify and/or adapt for various applications such specific embodiments without departing from the generic concept, and, therefore, such adaptations and modifications should and are intended to be comprehended within the meaning and range of equivalents of the disclosed embodiments. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation. Therefore, while the embodiments herein have been described in terms of preferred embodiments, those skilled in the art will recognize that the embodiments herein can be practiced with modification within the scope of the embodiments as described herein.

CLAIMS

We claim:

1. A method for determining a subscriber centric Application Programming Interface (API) in a wireless network, the method comprising:

receiving, by a Common API Framework (CAPIF) core functional device (100), a service API publish request message from an API Publishing Functional (APF) device (200b) of an API provider domain server (200) in the wireless network, wherein the service API publish request message comprises subscriber-centric information and a plurality of parameters;

storing, by the CAPIF core functional device (100), the subscriber-centric information and the plurality of parameters;

determining, by the CAPIF core functional device (100), a subscriber centric API from a plurality of APIs based on the subscriber-centric information and the plurality of parameters to verify at least one User Equipment (UE) (400); and

sending, by the CAPIF core functional device (100), a service API publish response message to the APF device (200b) of the API provider domain server (200), wherein the service API publish response message indicates a result of the service API publish request message and the result comprises one of the subscriber centric API and a non-subscriber centric API.

2. The method as claimed in claim 1, wherein the API provider domain server (200) comprises an API Exposing Functional (AEF) device (200a), the APF device (200b), and an API Management Functional (AMF) device (200c).

3. The method as claimed in claim 1, wherein the subscriber-centric information comprises at least one of a plurality of subscriber centric

northbound APIs, verification of the at least one UE (400) in a context of an API invocation, a plurality of information elements in a data model of a service API that identifies the at least one UE (400), an API invoker information, and other applicable parameters.

4. The method as claimed in claim 3, wherein the plurality of information elements comprises at least one of API publisher information, service API information, and shareable information.

5. The method as claimed in claim 4, wherein the API publisher information comprises identity, authentication, and authorization information, the service API information comprises at least one of a service API name, a service API type, a communication type, a description, serving area information, an AEF location, subscriber-centric information, interface details, protocols, version numbers, a data format and a session Identity (ID), and the shareable information indicates whether the service API or a service API category is sharable to other CAPIF core functional device (100).

6. The method as claimed in claim 1, wherein the method comprises:

enabling, by the CAPIF core functional device (100), to verify the at least one UE (400) in a context of an API invocation in response to determining that the subscriber centric API from the plurality of APIs; and

verifying, by the CAPIF core functional device (100), the at least one UE (400) in the context of the API invocation based on the subscriber-centric information and the plurality of parameters in subsequent CAPIF procedures.

7. The method as claimed in claim 1, wherein the APF device (200b) of the API provider domain server (200) comprises the subscriber-centric information as common information applicable for all service

APIs in the service API publish request message or separately for each service API.

8. The method as claimed in claim 1, wherein the APF device (200b) of the API provider domain server (200) comprises the service API information along with the subscriber-centric information of the service API information at the CAPIF core functional device (100) using an update service APIs procedure.

9. The method as claimed in claim 1, wherein the APF device (200b) of the API provider domain server (200) defines the session ID, the session ID is used to select the service API by at least one of the CAPIF core functional device (100) and an API invoker (300) to bind the service API used to a particular UE session.

10. The method as claimed in claim 1, wherein the method comprises:

verifying or not verifying, by the CAPIF core functional device (100), the at least one UE (400) in a context of an API invocation based on a trust or business relationship between the API provider domain server (200), and an API invoker (300).

11. The method as claimed in claim 1, wherein the APF device (200b) of the API provider domain server (200) comprises:

receiving, by the APF device (200b) of the API provider domain server (200), on-boarded API invokers information from the CAPIF core functional device (100); and

selectively adding, by the APF device (200b) of the API provider domain server (200), the API invoker information in a publish APIs procedure when the service APIs in the service API publish request message need to verify the at least one UE (400) and the service APIs in the service API publish request message is invoked by the API invoker (300).

12. The method as claimed in claim 11, wherein the method further comprises:

when the API provider domain server (200) wishes the CAPIF core functional device (100) to skip the verification of the UE (400) in the context of a service API invocation from a set of API invoker (300), then the APF device (200b) excludes the set of API invoker`s information from the subscriber-centric information for the service API in the service API publish request message or an update service API request message; and

in absence of subscriber-centric information for the service API indicates the CAPIF core functional device (100) to skip the verification of the UE (400) in the context of the service API invocation from all API invoker (300).

13. The method as claimed in claim 1, wherein the method comprises:

determining, by the CAPIF core functional device (100), the subscriber centric API from the plurality of APIs based on a data model of a service API; and

performing, by the CAPIF core functional device (100), at least one of:

verifying the at least one UE (400) in a context of an API invocation in response to determining the subscriber centric API; and

selectively applying verification of the at least one UE (400) in the context of the API invocation based on configured local policies.

14. A Common API Framework (CAPIF) core functional device (100) for determining a subscriber centric Application Programming Interface (API) in a wireless network, the CAPIF core functional device (100) comprising:

a memory (110);

a processor (120); and

an API controller (140), operably connected to the memory (110) and the processor (120), configured to:

receive a service API publish request message from an API Publishing Functional (APF) device (200a) of an API provider domain server (200) in the wireless network, wherein the service API publish request message comprises subscriber-centric information and a plurality of parameters;

store the subscriber-centric information and the plurality of parameters;

determine the subscriber centric API from a plurality of APIs based on the subscriber-centric information and the plurality of parameters to verify at least one User Equipment (UE) (400); and

send a service API publish response message to the APF device (200b) of the API provider domain server (200), wherein the service API publish response message indicates a result of the service API publish request message and the result comprises one of the subscriber centric API or a non-subscriber centric API.

15. The CAPIF core functional device (100) as claimed in claim 14, wherein the CAPIF core functional device (100) comprises:

enable to verify the at least one UE (400) in a context of an API invocation in response to determining that the subscriber centric API from the plurality of APIs; and

verify the at least one UE (400) in the context of an API invocation based on the subscriber-centric information and the plurality of parameters in subsequent CAPIF procedures.

16. The CAPIF core functional device (100) as claimed in claim 14, wherein the CAPIF core functional device (100) comprises:

verify or not verify the at least one UE (400) in a context of an API invocation based on a trust or business relationship between the API provider domain server (200), and an API invoker (300).

17. The CAPIF core functional device (100) as claimed in claim 14, wherein the CAPIF core functional device (100) comprises:

determine the subscriber centric API from a plurality of APIs based on a data model of a service API; and

perform at least one of:

verifying the at least one UE (400) in a context of an API invocation in response to determining the subscriber centric API; and

selectively applying verification of the at least one UE (400) in the context of an API invocation based on configured local policies.

18. An API Publishing Functional (APF) device (200b) of an API provider domain server (200) for selectively adding Application Programming Interface (API) invoker information, the APF device (200b) comprising:

a memory (210b);

a processor (220b); and

an API controller (240b), operably connected to the memory (210b) and the processor (220b), configured to:

receive on-boarded API invokers information from a CAPIF core functional device (100); and

selectively add API invoker information in a publish APIs procedure when service APIs in a service API publish request message need to verify at least one UE (400) and the service APIs in the service API publish request message is invoked by an API invoker (300).

19. The APF device (200b) as claimed in claim 18, wherein the APF device (200b) of the API provider domain server (200) comprises subscriber-centric information as common information applicable for all service APIs in the service API publish request message or separately for each service API.

20. The APF device (200b) as claimed in claim 18, wherein the APF device (200b) of the API provider domain server (200) comprises service API information along with centric information of the service API information at the CAPIF core functional device (100) using an update service APIs procedure.

21. The APF device (200b) as claimed in claim 18, wherein the APF device (200b) of the API provider domain server (200) defines a session ID, the session ID is used to select the service API by at least one of the CAPIF core functional device (100) and an API invoker (300) to bind the service API used to a particular UE session.

Dated this : 18th day of March 2022



Signature:

Arun Kishore Narasani

Patent Agent: IN/PA 1049

ABSTRACT

“Method and system for determining subscriber-centric API in wireless network”

A method includes receiving the service API publish request message from an APF device (200a) of an API provider domain server (200) in the wireless network, where the service API publish request message includes the subscriber-centric information and the plurality of parameters. Further, the method includes storing the subscriber-centric information and the plurality of parameters. Further, the method includes determining, by a Common API Framework (CAPIF) core functional device (100), a subscriber-centric API from the plurality of APIs based on the subscriber-centric information and the plurality of parameters to verify a UE(s) (400). Further, the method includes sending the service API publish response message to the APF device (200b) of the API provider domain server (200), where the service API publish response message indicates the result of the service API publish request message and the result includes one of the subscriber centric API or a non-subscriber centric API.

FIG. 3