

5G Advanced

5G System Architecture selected Exposure Function APIs from Subscriber-aware Northbound APIs Access to Resource-owner aware Northbound APIs Access for 5G Services

Ike Alisson

2023 - 09- 22

Rev PA06





1. 5G System APIs evolvement - from "preliminary" SNA to "normative" RNAA" specifications
 - 1.1 5GS support for Unified Access Control for Access Identities and Categories
 - 1.2 5G System Service Requirements related to APIs in 3GPP Rel.19
 - 1.3 Business Relationships in 5G System Common API Framework (CAPIF) for SNA
 - 1.4 5G System Network Capability External Exposure Application Function (AF) influence on Traffic Routing
 - 1.5 Business Relationships in 5G System Architecture Common API Framework (CAPIF) for RNAA (Resource Owner-aware Northbound API Access)
 - 1.6 5G CAPIF (Common API Framework) Deployment Model with 4G EPC CN SCEF and 5G SA CN NEF
 - 1.7 5G CAPIF Role in Charging
 - 1.8 Functional Model Description for the CAPIF for interaction of API Exposing Function (AEF)
 - 1.9 Deployment Options of API Providers
 - 1.10 5G Architecture for enabling Edge Applications deployments in relation with 5G Common API Framework

Annex

1. Shift from 2G/3G/4G "Best-effort Services" to 5G User Experience & Performance Service Guarantees
2. 5G Advanced enhanced API Core Function (CAPIF) Deployment Options with API Authorization Function and Service APIs

In **SNA**-related studies so far, **3GPP SA6 WG**, that is the Application Enablement and Critical Communication Applications Group for Vertical Markets with main Objective to provide Application Layer Architecture Specifications for 3GPP Verticals, including Architecture Requirements, Functional Architecture, Procedures, Information Flows, Inter-working with Non-3GPP Application Layer Solutions, and Deployment Models as appropriate and (**SA6**), currently responsible for Application Layer Specifications, **has used the term "Subscriber-aware Northbound API access,"** or **SNA** for its abbreviation.

However, the 5G Common API Framework (**CAPIF**) **System** should be **aware of the Resource Owner, rather than the Subscriber.**

Thus, the term "**Subscriber-aware Northbound API access**" is not appropriate for this Use Case (UC).

Subscriber-aware Northbound API Access (SNA) is replaced with **Resource owner-aware Northbound API access;**

Inappropriate term is used and it may confuse the Readers.

The Resource Owner Client(s) are **Application Clients (ACs)** used by **Resource Owners** of the API Provider Domain's Service Provider (SP).

The Resource Owner Client(s) interacts with the Authorization Function in CAPIF via **CAPIF-8**.

The Resource owner communicates with the Authorization Function in CAPIF to "Provide" and "Revoke" Resource owner Consent.

The Resource owner interactions are supported via a Resource owner Client, which is **a Client-side Entity**.

3GPP TSG-SA WG6 Meeting #52-bis-e
Online, 11th – 20th January 2022

S6-230407
(revision of S6-230156)

CHANGE REQUEST

CR 0101 rev 1 Current version: 18.0.0

For **HELP** on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.

Proposed change affects:

☐ UICC apps

☐ ME

☐ Radio Access Network

☒ Core Network

Title:

Source to WG:

Source to TSG:

Work item code:

Category:

Modify a terminology for SNA

NTT DOCOMO

SA6

SNAAPP

D

Use one of the following categories:

F (correction)

A (mirror corresponding to a change in an earlier release)

B (addition of feature),

C (functional modification of feature)

D (editorial modification)

Detailed explanations of the above categories can be found in 3GPP [TR 21.900](#).

Date:

Release:

2023-01-10

Rel-18

Use one of the following releases:

Rel-8 (Release 8)

Rel-9 (Release 9)

Rel-10 (Release 10)

Rel-11 (Release 11)

...

Rel-16 (Release 16)

Rel-17 (Release 17)

Rel-18 (Release 18)

Rel-19 (Release 19)

Reason for change:

Summary of change:

Consequences if not approved:

In SNA-related studies so far, SA6 and has used the term "subscriber-aware northbound API access," or SNA for its abbreviation. However, the CAPIF system should be aware of the resource owner, rather than the subscriber. Thus, the term "subscriber-aware northbound API access" is not appropriate for this use case.

Subscriber-aware northbound API access is replaced with resource owner-aware northbound API access; SNA is replaced with RNAA.

Inappropriate term is used and it may confuse the readers.

Clauses affected:

Other specs affected:
(show related CRs)

Other comments:

This CR's revision history:

3.1, 3.2, 4.17, 4.17.1, 5.2, 6.2.3

| | |
|-------------------------------------|-------------------------------------|
| Y | N |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Other core specifications

Test specifications

O&M Specifications

TS/TR ... CR ...

TS/TR ... CR ...

TS/TR ... CR ...

2. Further shift of APIs Capabilities to End-Users (Resource Owners former Subscribers) from early 5G Rel. 15 FMSS & SEES Features with enabled APIs Capabilities shift from MNOs to 3rd Party ISPs & ICPs - UE Services Enablement Clients (with 5GS support for UAC - Unified Access Control) with specified (Service(s)) Access Identities & Access Categories - below example of selected UCs Services (by 5GS specified Architectures for AEF - Application Enablement Frameworks) supported by specified UE Clients

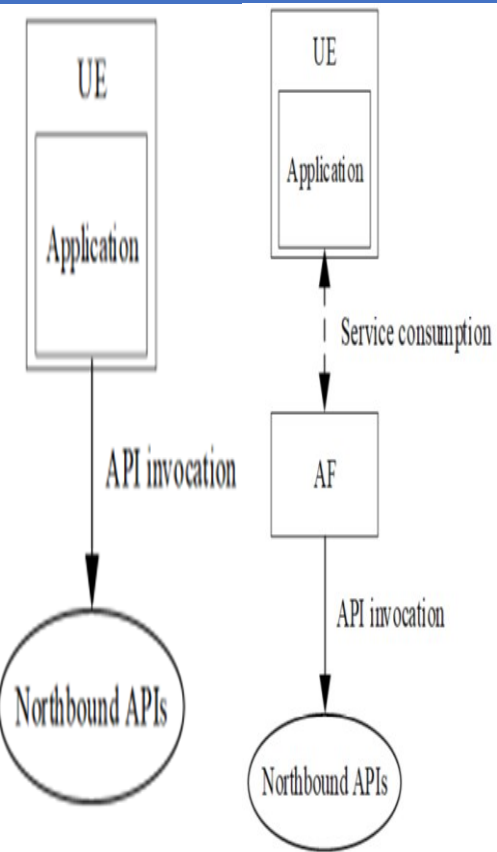


Fig.: UE-originated API Invocation

Fig.: AF-originated API Invocation

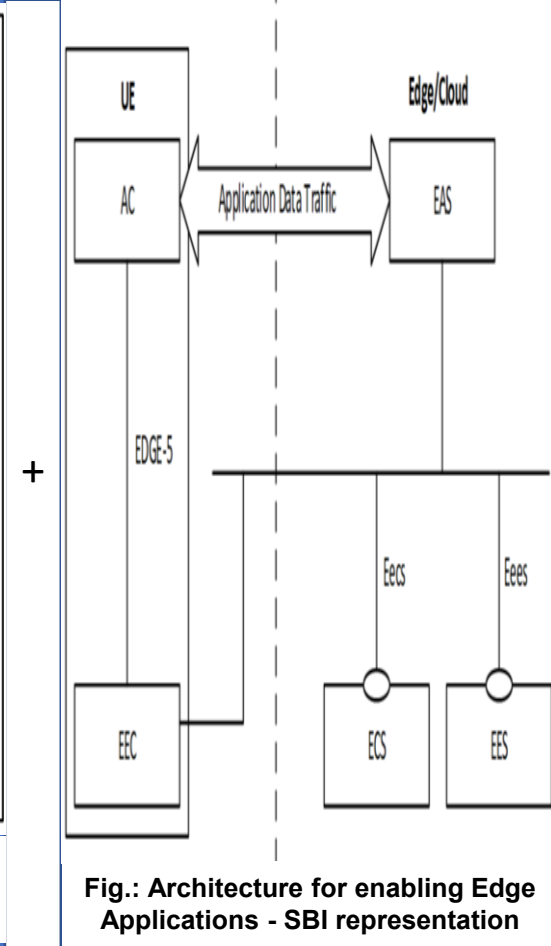
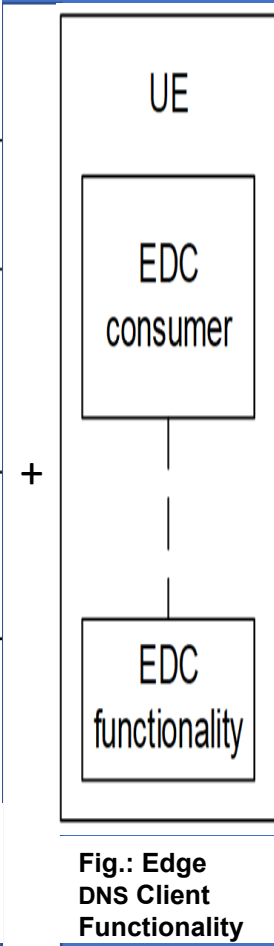
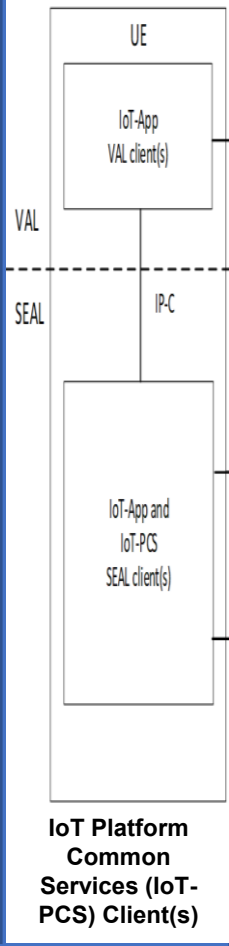
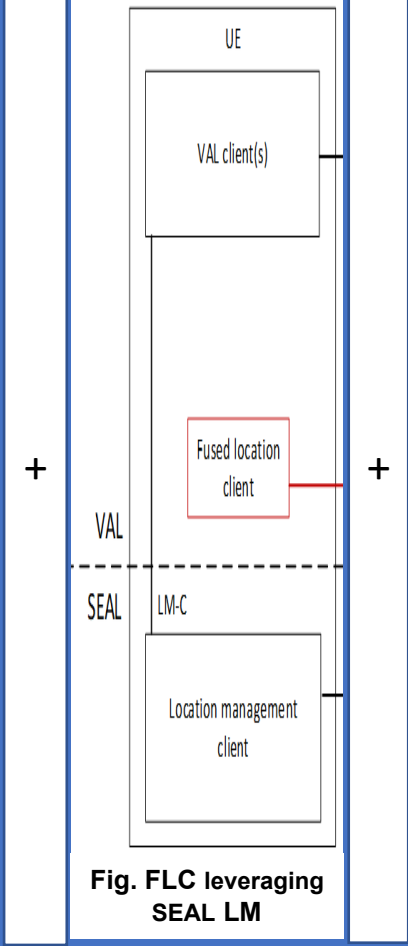
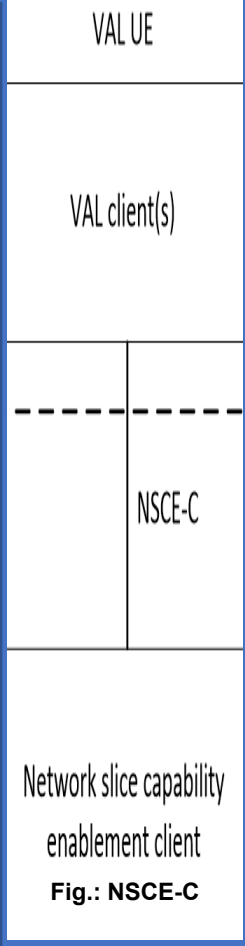
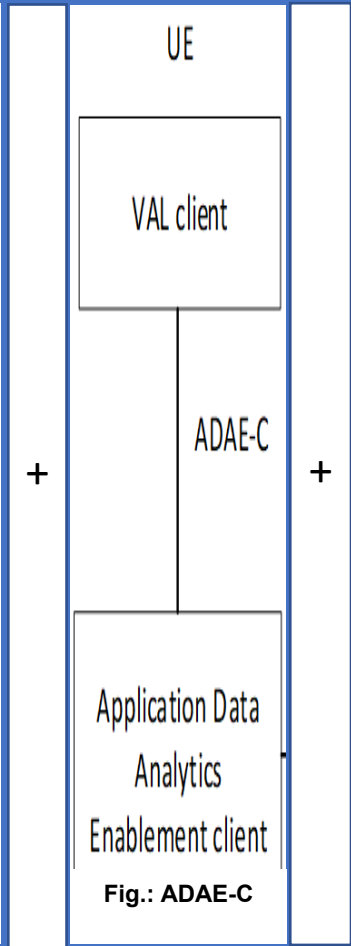


Fig.: Architecture for enabling Edge Applications - SBI representation

1. 3GPP Changing: Subscriber-aware Northbound API access (**SNA**) to Resource-owner aware Northbound APIs access (**RNAA**)



1.1 5GS support for Unified Access Control for Access Identities and Categories

Depending on Operator's Policies, Deployment Scenarios, Subscriber Profiles, and Available Services, different criterion will be used in determining which Access attempt should be allowed or blocked when congestion occurs in the 5G System.

These different criteria for **Access Control** are associated with **Access Identities** and **Access Categories**. The 5GS will provide a Single Unified Access Control where Operators Control Accesses based on these two (2)

In **Unified Access Control**, each Access attempt is categorized into one (1) or more of the Access Identities and one of the Access Categories.

Based on the Access Control Information applicable for the corresponding Access Identity and Access Category of the access attempt, the **UE performs a test whether the actual access attempt can be made or not.**

The **Unified Access Control** supports extensibility to allow inclusion of additional Standardized Access Identities and Access Categories and supports flexibility to allow operators to define Operator-defined Access Categories using their own criterion (e.g. Network Slicing, Application, and Application Server).

NOTE: When a **UE is configured for EAB** (Extended Access Barring) according to 5GS Service Accessibility, the **UE is also configured for Delay Tolerant Service for 5G system.**

The Unified Access Control Framework shall be applicable both to UEs accessing the 5G CN using E-UTRA and to UEs accessing the 5G CN using NR.

The Unified Access Control Framework shall be **applicable to UEs in RRC Idle, RRC Inactive, and RRC Connected** at the time of initiating a new access attempt (e.g. New Session Request).

Release 193GPPV19.4.0 (2023-09)

Table: 5G System support for Unified Access Control Access Identities

| Access Identity number | UE configuration |
|--|--|
| 0 | UE is not configured with any parameters from this table |
| 1 (NOTE 1) | UE is configured for Multimedia Priority Service (MPS). |
| 2 (NOTE 2) | UE is configured for Mission Critical Service (MCS). |
| 3 | UE for which Disaster Condition applies (note 4) |
| 4-10 | Reserved for future use |
| 11 (NOTE 3) | Access Class 11 is configured in the UE. |
| 12 (NOTE 3) | Access Class 12 is configured in the UE. |
| 13 (NOTE 3) | Access Class 13 is configured in the UE. |
| 14 (NOTE 3) | Access Class 14 is configured in the UE. |
| 15 (NOTE 3) | Access Class 15 is configured in the UE. |
| NOTE 1: Access Identity 1 is used by UEs configured for MPS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN, PLMNs equivalent to HPLMN, and visited PLMNs of the home country. Access Identity 1 is also valid when the UE is explicitly authorized by the network based on specific configured PLMNs inside and outside the home country. | |
| NOTE 2: Access Identity 2 is used by UEs configured for MCS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN or PLMNs equivalent to HPLMN and visited PLMNs of the home country. Access Identity 2 is also valid when the UE is explicitly authorized by the network based on specific configured PLMNs inside and outside the home country. | |
| NOTE 3: Access Identities 11 and 15 are valid in Home PLMN only if the EHPLMN list is not present or in any EHPLMN. Access Identities 12, 13 and 14 are valid in Home PLMN and visited PLMNs of home country only. For this purpose, the home country is defined as the country of the MCC part of the IMSI. | |
| NOTE 4: The configuration is valid for PLMNs that indicate to potential Disaster Inbound Roamers that the UEs can access the PLMN. See clause 6.31. | |

Release 193GPPV19.4.0 (2023-09)

Table: 5G System support for Unified Access Control Access Categories

| Access Category number | Conditions related to UE | Type of access attempt |
|--|---|--|
| 0 | All | MO signalling resulting from paging |
| 1 (NOTE 1) | UE is configured for delay tolerant service and subject to access control for Access Category 1, which is judged based on relation of UE's HPLMN and the selected PLMN. | All except for Emergency, or MO exception data |
| 2 | All | Emergency |
| 3 | All except for the conditions in Access Category 1. | MO signalling on NAS level resulting from other than paging |
| 4 | All except for the conditions in Access Category 1. | MMTEL voice (NOTE 3) |
| 5 | All except for the conditions in Access Category 1. | MMTEL video |
| 6 | All except for the conditions in Access Category 1. | SMS |
| 7 | All except for the conditions in Access Category 1. | MO data that do not belong to any other Access Categories (NOTE 4) |
| 8 | All except for the conditions in Access Category 1 | MO signalling on RRC level resulting from other than paging |
| 9 | All except for the conditions in Access Category 1 | MO IMS registration related signalling (NOTE 5) |
| 10 (NOTE 6) | All | MO exception data |
| 11-31 | | Reserved standardized Access Categories |
| 32-63 (NOTE 2) | All | Based on operator classification |
| NOTE 1: The barring parameter for Access Category 1 is accompanied with information that define whether Access Category applies to UEs within one of the following categories: a) UEs that are configured for delay tolerant service; b) UEs that are configured for delay tolerant service and are neither in their HPLMN nor in a PLMN that is equivalent to it; c) UEs that are configured for delay tolerant service and are neither in the PLMN listed as most preferred PLMN of the country where the UE is roaming in the operator-defined PLMN selector list on the SIM/USIM, nor in their HPLMN nor in a PLMN that is equivalent to their HPLMN. When a UE is configured for EAB, the UE is also configured for delay tolerant service. In case a UE is configured both for EAB and for EAB override, when upper layer indicates to override Access Category 1, then Access Category 1 is not applicable. | | |
| NOTE 2: When there are an Access Category based on operator classification and a standardized Access Category to both of which an access attempt can be categorized, and the standardized Access Category is neither 0 nor 2, the UE applies the Access Category based on operator classification. When there are an Access Category based on operator classification and a standardized Access Category to both of which an access attempt can be categorized, and the standardized Access Category is 0 or 2, the UE applies the standardized Access Category. | | |
| NOTE 3: Includes Real-Time Text (RTT). | | |
| NOTE 4: Includes IMS Messaging. | | |
| NOTE 5: Includes IMS registration related signalling, e.g. IMS initial registration, re-registration, and subscription refresh. | | |
| NOTE 6: Applies to access of a NB-IoT-capable UE to a NB-IOT cell connected to 5GC when the UE is authorized to send exception data. | | |

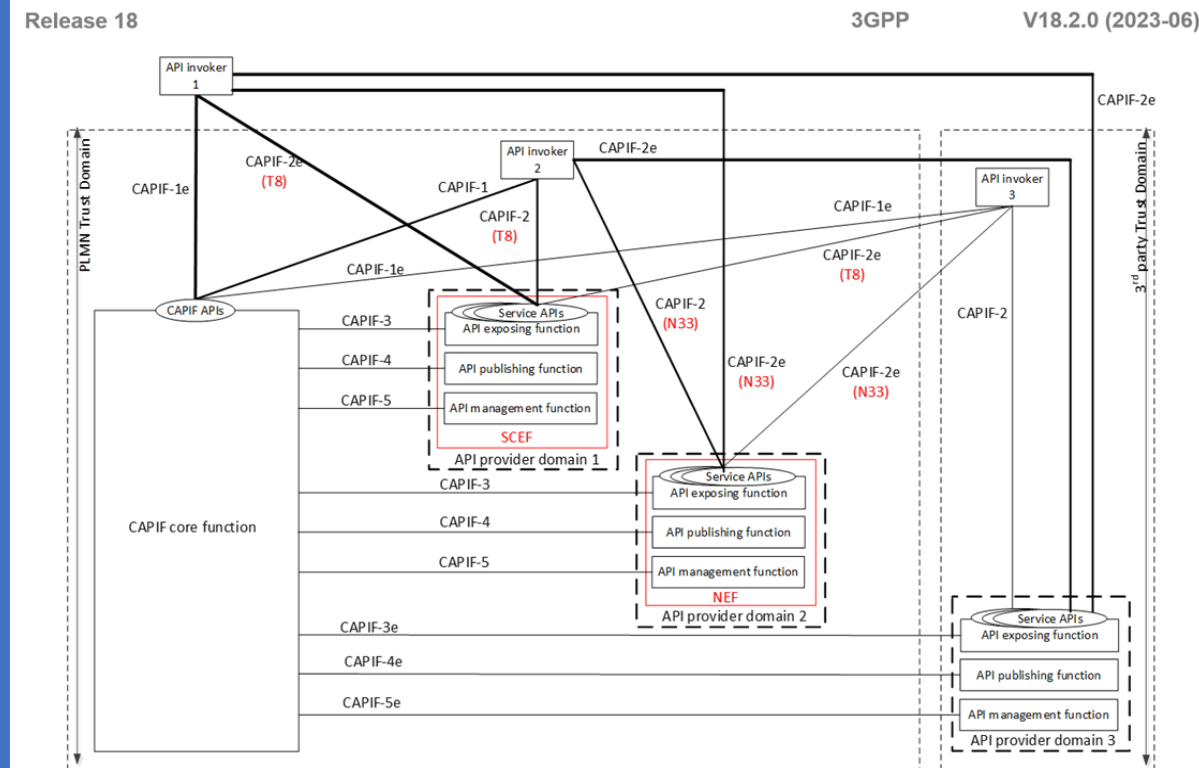
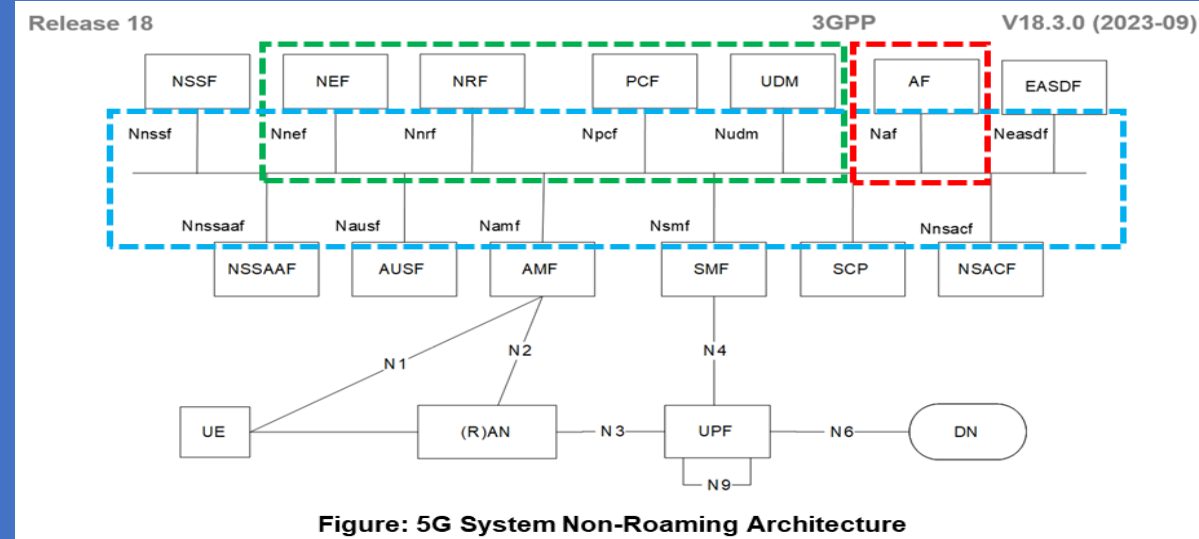
1. 3GPP Changing: Subscriber-aware Northbound API access (SNA) to Resource-owner aware Northbound APIs access (RNAA)

1.2 5G System Service Requirements related to APIs in 3GPP Rel.19

3GPP, already in Rel-15, provided support for 5GS CN **SEES (Service Exposure & Enablement Support) & (e)FMSS (Enhancement to Flexible Mobile Service Steering) Features** to allow the Operator to **expose Network Capabilities e.g. QoS Policy to 3rd-Party ISPs/ICPs.**

With the advent of 5G, New Network Capabilities needed to be exposed to the **3rd-Party** (e.g. to allow the **3rd-Party** to "customize" a Dedicated Physical or Virtual Network (VN) or a Dedicated Network Slice (**SST**) for diverse Use Cases (UCs);

- to allow the **3rd-Party** to manage a Trusted **3rd-Party Application** in a Service Hosting Environment (SHE)
- to improve User Experience, and
- to efficiently utilize Backhaul and Application Resources).



5G System Service Requirements related to Network Capability Exposure and relevant APIs - 1

3GPP 5GS **SEES (Service Exposure & Enablement Support) & (e)FMSS (Enhancement to Flexible Mobile Service Steering)** Features allow the Operator to expose Network Capabilities e.g. **QoS Policy to 3rd-Party ISPs/ICPs**. With the advent of **5G, New Network Capabilities** need to be exposed to the **3rd-Party** (e.g. to allow the **3rd-Party** to customize a Dedicated Physical or Virtual Network or a Dedicated *Network Slice (SST)* for diverse UCs; to allow the **3rd-Party** to manage a trusted **3rd-Party Application** in a Service Hosting Environment to improve *User Experience*, & efficiently utilize Backhaul & Application Resources.

A **5G Network** shall provide suitable APIs to allow a Trusted 3rd-Party to create, modify, and delete **Network Slices (SST) used** for the Third-Party.

The **5G Network** shall provide suitable **APIs to allow a Trusted 3rd-Party** to monitor the **Network Slice** used for the 3rd-Party.

The **5G System** shall support a mechanism to provide **time stamps with a common time base at the monitoring API**, for services **that cross Multiple Network Slices and 5G Networks**.

The **5G System** shall provide suitable APIs to coordinate **Network Slices in multiple 5G Networks** so that the selected communication services of a non-public network can be extended through a PLMN (e.g. the service is supported by a slice in the non-public network and a slice in the PLMN).

The **5G Network** shall provide suitable **APIs to allow a Trusted 3rd-Party** to define and update the Set of Services and Capabilities supported in a **Network Slice (SST)** used for the 3rd-Party.

The **5G Network** shall provide **suitable APIs to allow a Trusted 3rd-Party** to configure the Information, which associates **a UE to a Network Slice (SST)** used for the 3rd-Party.

The **5G Network** shall provide suitable **APIs to allow a Trusted 3rd-Party** to configure the information which associates **a Service to a Network Slice (SST used for the 3rd-Party**.

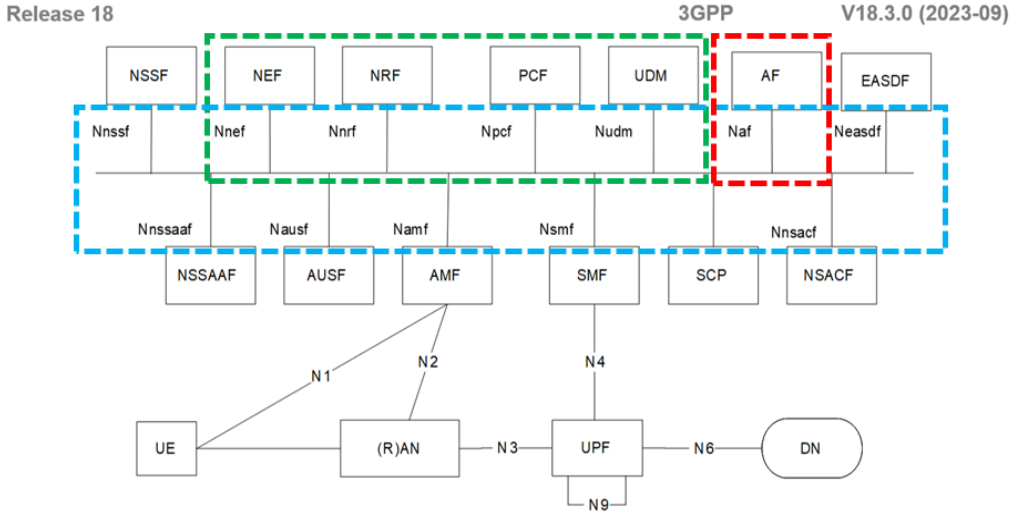


Figure: 5G System Non-Roaming Architecture

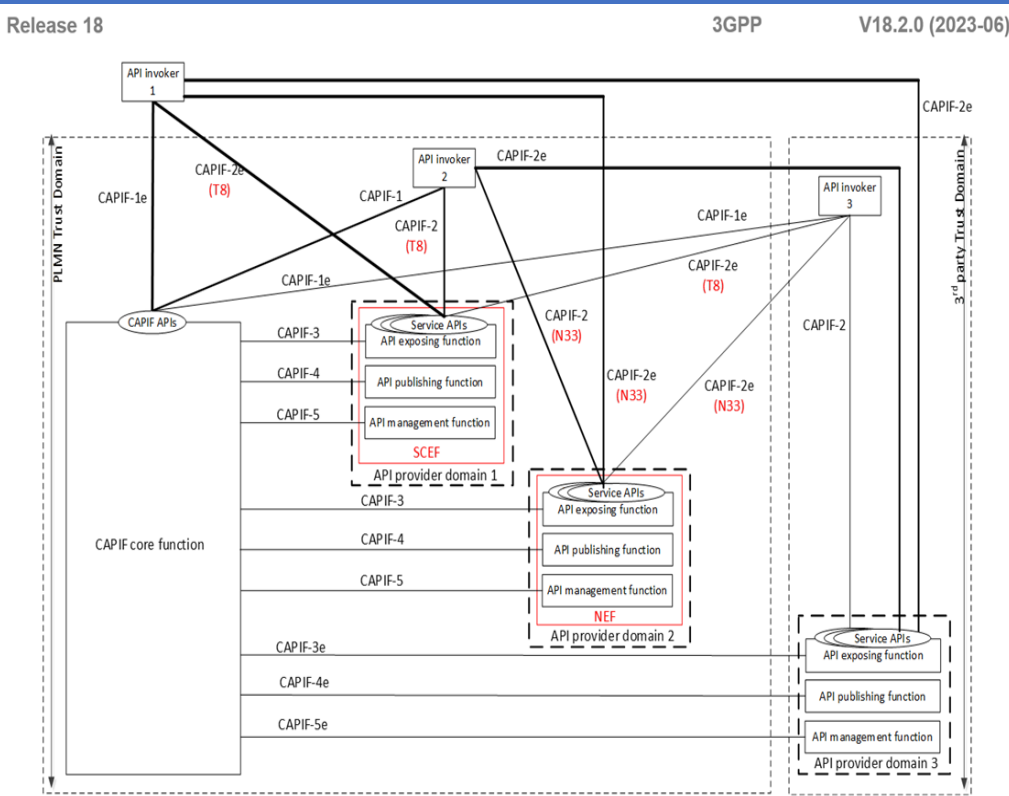


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

5G System Service Requirements related to Network Capability Exposure and relevant APIs - 2

The 5G Network shall provide suitable **APIs** to allow a **Trusted 3rd-Party** to assign a **UE** to a Network Slice used for the **3rd-Party**, to move a UE from one (1) Network Slice (SST) used for **the 3rd-Party** to another Network Slice (SST) used for **the 3rd-Party**, and to remove a UE from a Network Slice (SST) used for the **3rd-Party** based on:

- **Subscription,**
- **UE Capabilities, and**
- **Services provided by the Network Slice (SST).**

A 5G Network shall provide suitable **APIs to allow a Trusted Third-Party** to manage this Trusted 3rd-Party owned Application(s) in the Operator's Service Hosting Environment.

The 5G Network shall provide suitable **APIs to allow a 3rd-Party** to monitor this Trusted 3rd-Party owned Application(s) in the Operator's Service Hosting Environment.

The 5G Network shall provide suitable **APIs to allow a Trusted 3rd-Party** to scale a Network Slice (SST) used for the 3rd-Party, i.e. to adapt its Capacity.

A 5G Network shall provide suitable **APIs to allow one Type of Traffic (from Trusted 3rd-Party owned Applications in the Operator's Service Hosting Environment)** to/from a UE to be off-loaded to a Service Hosting Environment close to the UE's Location.

The 5G Network shall provide suitable **APIs to allow a Trusted 3rd-Party Application to request appropriate QoE from the Network.**

The 5G Network shall expose a suitable **API to an Authorized 3rd-Party** to provide the Information regarding the Availability Status of a Geographic Location that is associated with that 3rd-Party.

The 5G Network shall expose a suitable **API to allow an Authorized 3rd-Party** to monitor the Resource utilization of the Network Service (Radio Access Point and the Transport Network (Front, Backhaul)) that are associated with the 3rd-Party.

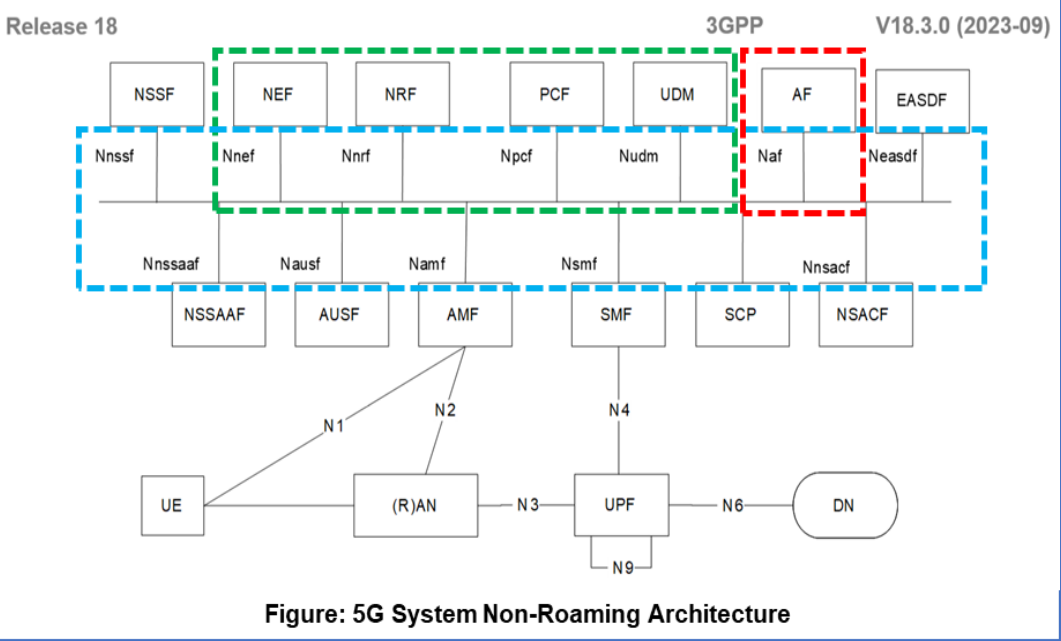


Figure: 5G System Non-Roaming Architecture

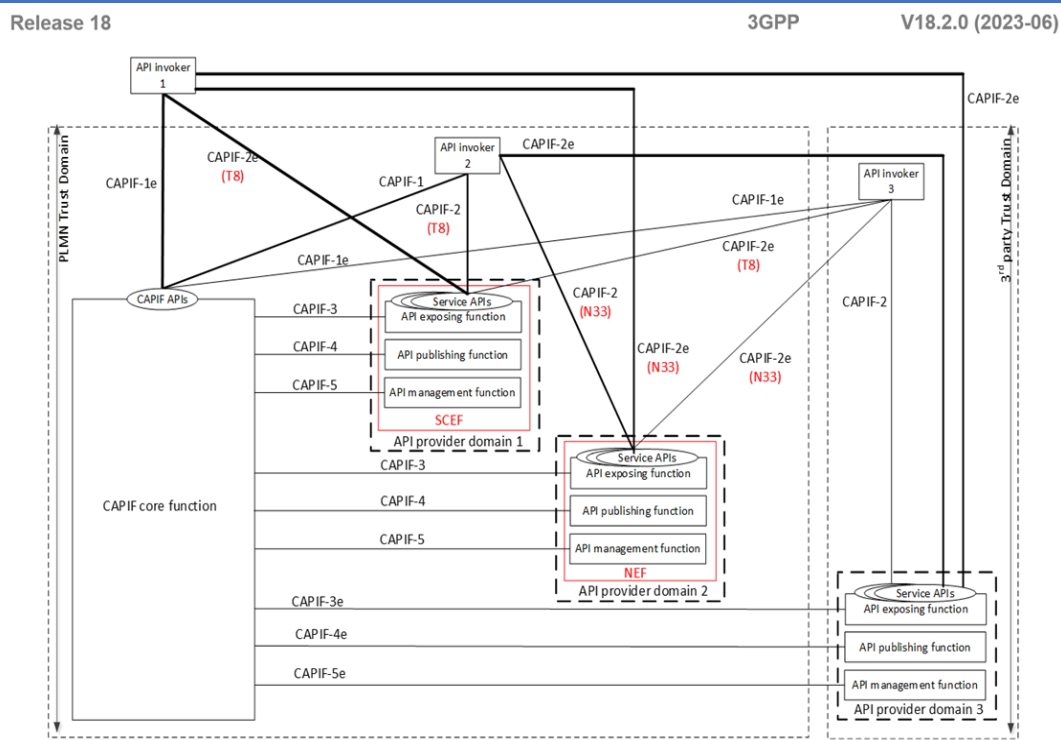


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

5G System Service Requirements related to Network Capability Exposure and relevant APIs - 3

The 5G Network shall expose a suitable **API to allow an Authorized 3rd-Party** to define and reconfigure the properties of the Communication Services offered to the 3rd-Party.

The 5G System shall support the means for disengagement (tear down) of Communication Services by an Authorized 3rd-Party.

The 5G Network shall expose a **suitable API to** provide the Security Logging **Information of UEs**, for example, the Active 3GPP Security Mechanisms (e.g.:

- Data Privacy,
- Authentication,
- Integrity Protection to an Authorized 3rd-Party.

The 5G Network shall be able to acknowledge within 100 ms a Communication Service Request from an Authorized 3rd-Party via a suitable API.

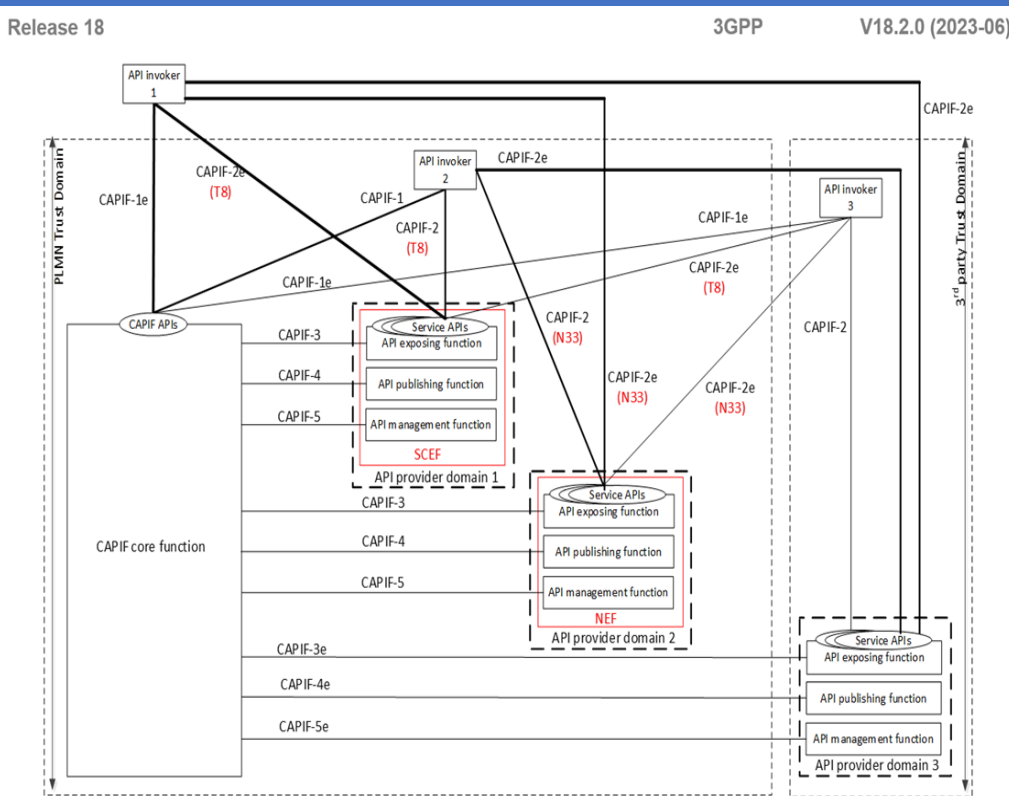
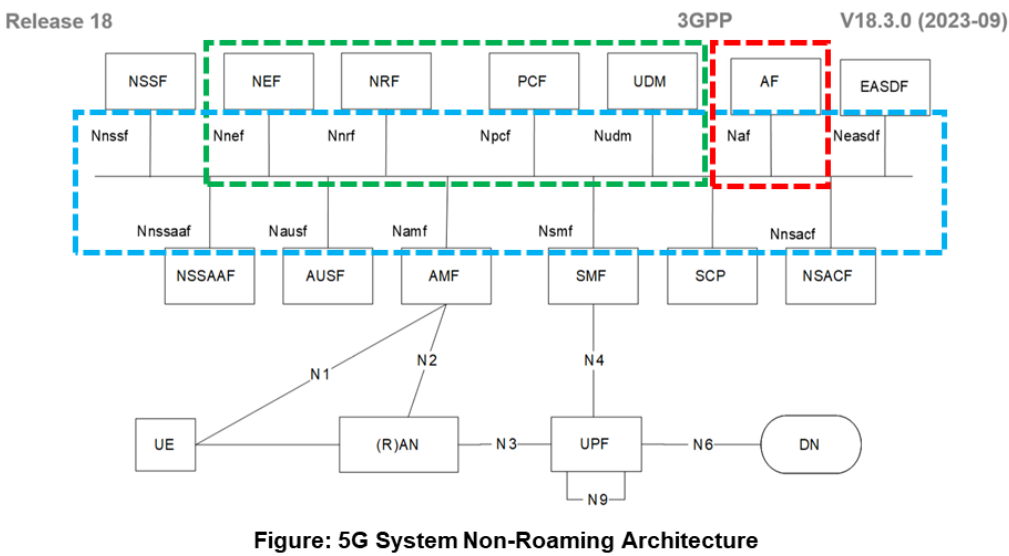
The 5G Network shall provide suitable **APIs to allow a Trusted 3rd-Party** to monitor the Status (e.g. Locations, Lifecycle, Registration Status) of its own UEs.

NOTE 3: The Number of UEs could be in the range from single digit to tens (10s) of thousands (1000s).

The 5G Network shall provide suitable **APIs to allow a Trusted 3rd-Party** to get the Network Status Information of a **Private Slice** dedicated for the 3rd-Party, e.g. the Network Communication Status between **the Slice (SST)** and a specific UE.

The 5G System shall provide a **suitable API** by which an authorized third-party shall be able to authorize (multiple) UEs under control of the **third-party to act as a Relay UE or remote UE**.

The **5G System** shall provide a **suitable API** by which an authorized third-party shall be able to enable/disable (multiple) UEs under control of the third-party **to act as a Relay UE or remote UE**.



5G System Service Requirements related to Network Capability Exposure and relevant APIs - 4

The 5G System shall support APIs to allow the Non-Public Network (NPN) to be managed by the MNO's Operations System.

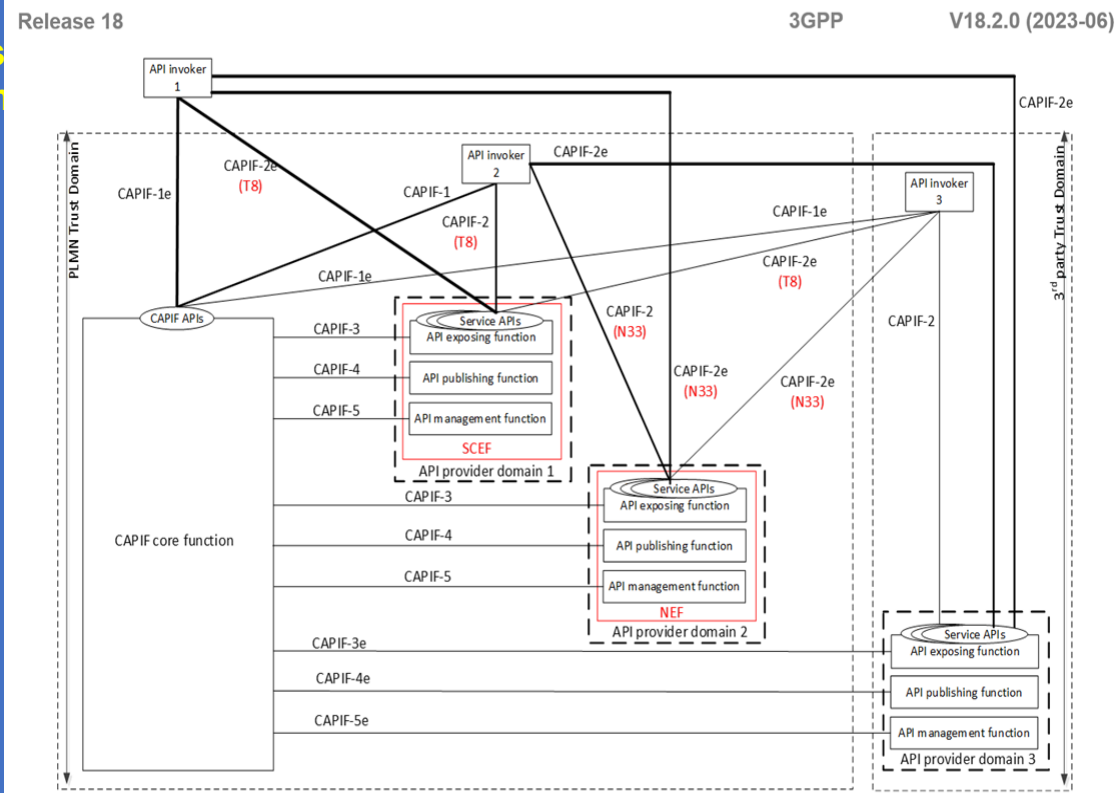
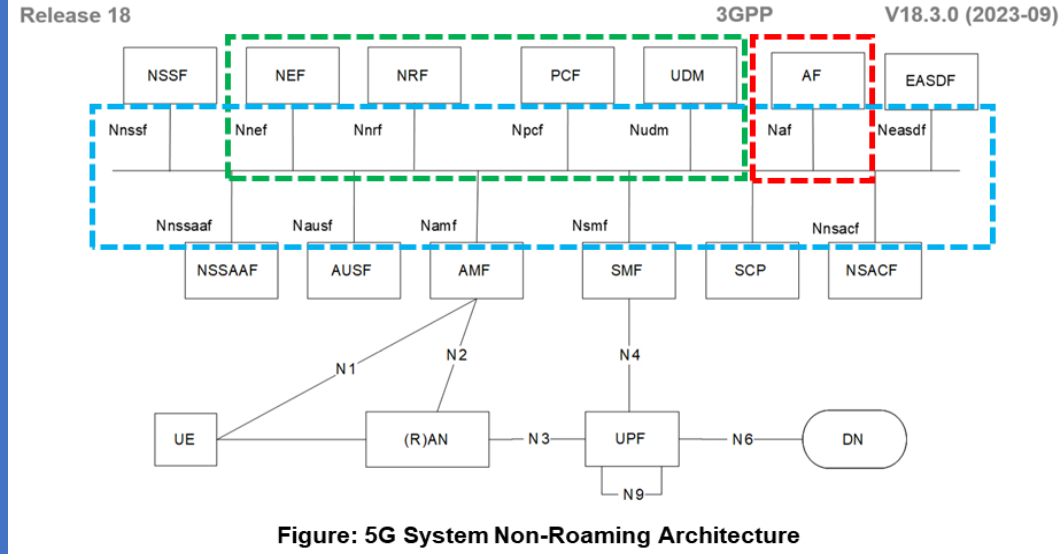
The 5G System shall provide suitable APIs to allow 3rd-Party Infrastructure (i.e. Physical/Virtual Network Entities at RAN/Core Level) to be used in a Private Slice.

A 5G System shall provide suitable APIs to enable a 3rd-Party to manage its own Non-Public Network (NPN) and its Private Slice(s) in the PLMN in a combined manner.

The 5G System shall support suitable APIs to allow an MNO to offer Automatic Configuration Services (e.g., Interference Management) to Non-Public Networks (NPNs) deployed by 3rd Parties and connected to the MNO's Operations System through Standardized Interfaces.

The 5G System shall be able to:

- provide a 3rd-Party with Secure Access to APIs (e.g. triggered by an Application that is visible to the 5G System), by Authenticating and Authorizing both the 3rd-Party and the UE using the 3rd-Party's Service.
- provide a UE with Secure Access to APIs (e.g. triggered by an Application that is not visible to the 5G System), by authenticating and authorizing the UE.
- allow the UE to provide/revoke consent for Information (e.g., Location, Presence) to be shared with the 3rd-Party.
- preserve the Confidentiality of the UE's External Identity (e.g. MSISDN) against the 3rd-Party.
- provide a 3rd-Party with Information to identify Networks and APIs on those Networks.



5G System Service Requirements related to Network Capability Exposure and relevant APIs - 5

The 5G System shall provide means by which an MNO informs a 3rd Party of changes in UE Subscription information.

The 5G System shall also provide a means for an Authorized 3rd Party to request this Information at any time from the MNO.

NOTE 4: Examples of UE subscription information include IP address, 5G LAN-VN Membership, and Configuration Parameters for Data Network Access.

NOTE 5: These changes can have strong impacts in the stability of the 3rd-Party Service.

The 5G System shall provide means by which an MNO can inform Authorized 3rd Parties of changes in the:

- RAT type that is serving a UE;
- Cell ID;
- RAN Quality of Signal Information;
- Assigned Frequency Band.

This information listed above shall be provided with a suitable Frequency via OAM and/or 5G Core Network.

NOTE 6: The information aids the 3rd Party User to take proactive actions so that it can achieve High Service Availability in Delivery of its Services.

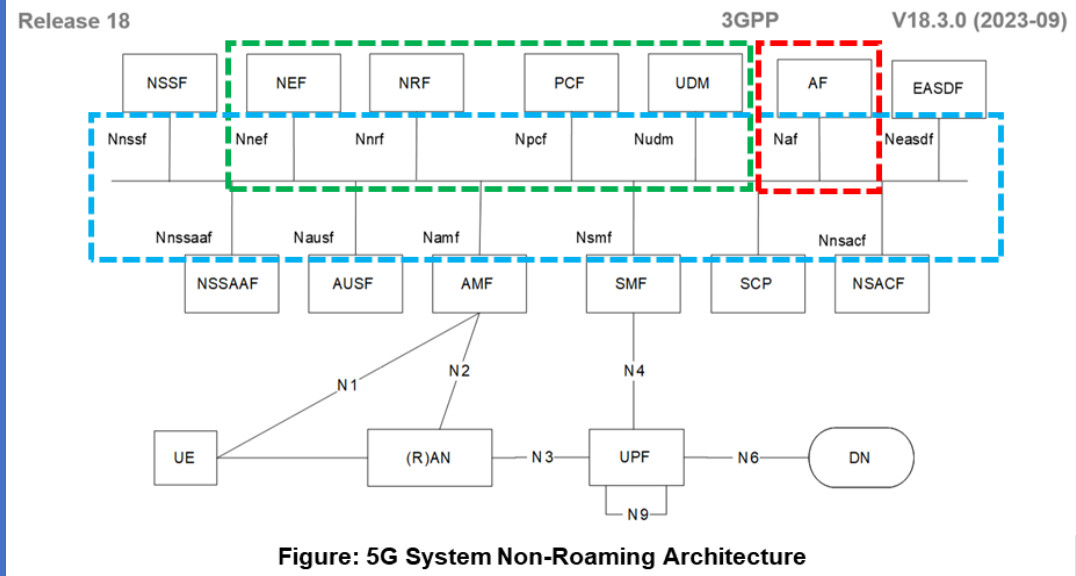


Figure: 5G System Non-Roaming Architecture

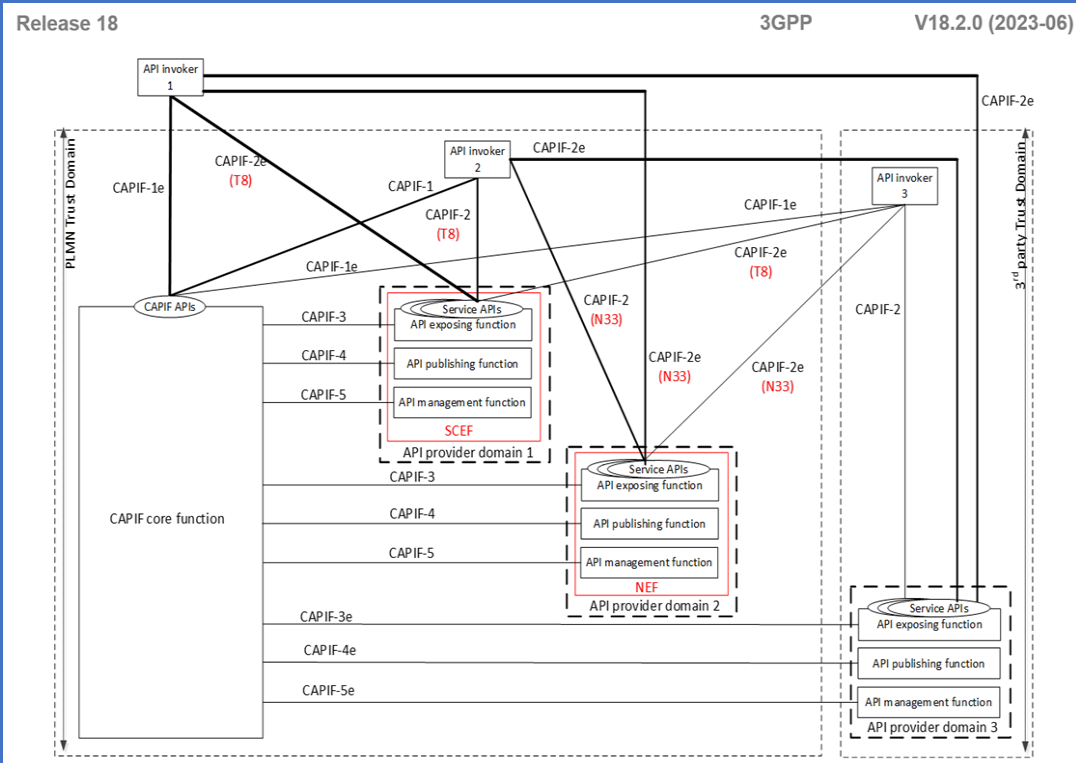


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

1. 3GPP Changing: Subscriber-aware Northbound API access (SNA) to Resource-owner aware Northbound APIs access (RNAA)

1.3 Business Relationships in 5G System Architecture Common API Framework (CAPIF) in SNA (Subscriber-aware Northbound Apis Access)

This solution addresses **the Business Relationship** between

- the User (UE),
- the AF and
- the Northbound API Provider in the AF-originated API Invocation scenario.

Considering the Business Relationship, **the Resource Owner** (which is **a UE-side Entity**) is **a new entity** that has not been in the existing CAPIF business relationship, thus the business relationship should be updated to include the Resource Owner.

The Figure shows the typical Business Relationship in SNA, that can be applied to both:

- **AF-originated API Invocation** scenario and
- **UE-originated API invocation** scenario,

as the **API invoker** in the Figure can either be:

- **an Application on the UE** or
- **the AF.**

The API Invoker has Service Agreement with a CAPIF Provider, and the API Provider provides APIs associated with the Resource Owner.

The CAPIF Provider and the API Provider can be part of the same Organization (e.g. PLMN Operator), as described in CAPF specification. When the CAPIF Provider is a PLMN Operator, the **Resource Owner may be a Subscriber of the PLMN.**

NOTE: In the current Release, both the CAPIF Provider and the API Provider should belong to the same Organization (e.g., PLMN Operator).

This Solution enhances the existing CAPIF Business Relationship by introducing the **Resource Owner**, which is viable.

Release 18

3GPP

V18.1.0 (2023-03)

Solution #1: Business relationship in SNA

Figure shows the typical business relationship in SNA. This business relationship can be applied to both AF- and UE-originated API invocation scenario, as the API invoker in figure can either be an application on the UE or the AF.

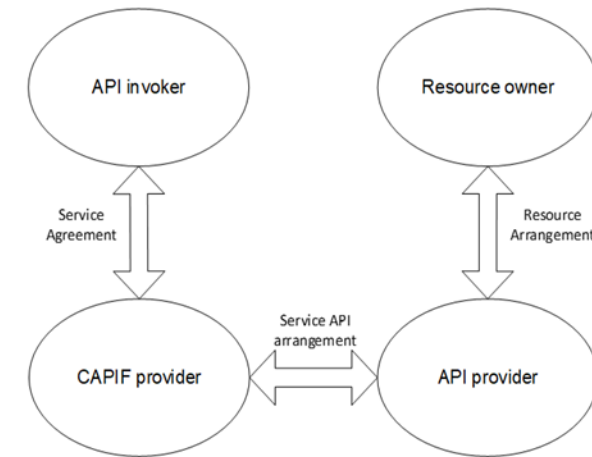


Figure: 5G Common API Framework (CAPIF) Business Relationships in Subscriber-aware Northbound API Access (SNA)

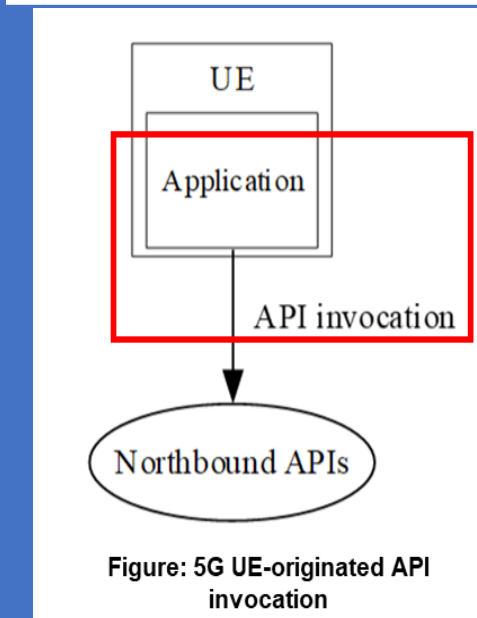


Figure: 5G UE-originated API invocation

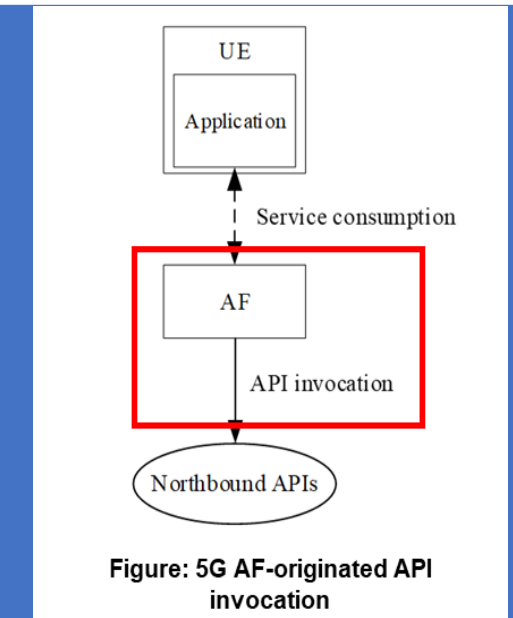


Figure: 5G AF-originated API invocation

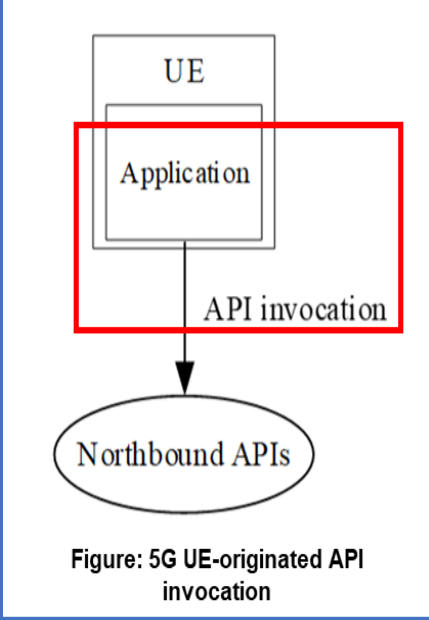
1. 3GPP Changing: Subscriber-aware Northbound API access (SNA) to Resource-owner aware Northbound APIs access (RNAA)

1. UE-originated API Invocation - the UE-originated API invocation as specified in 5G Service Requirements, 3GPP, Rel-19, June 2023

- The 5G System (5GS) shall be able to provide a UE with secure access to APIs (e.g. triggered by an Application that is not visible to the 5GS), by
- "Authenticating" and "Authorizing" the UE.

In this scenario, the "Application on the UE" invokes the Northbound APIs (NAPs). The scenario is illustrated in the Figure.

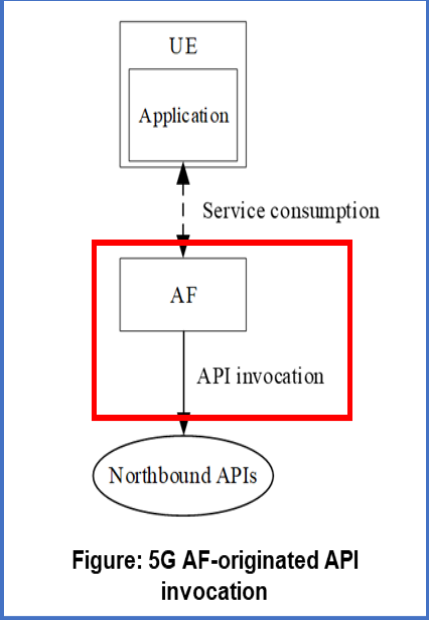
From CAPIF point of view, the Application on the UE, plays the role of the "API Invoker", as defined in 5G Common API Framework (CAPIF).



2. AF-originated API invocation

In the AF-originated API Invocation, the AF invokes the NAPs APIs, and the Application on the UE consumes the Service from the AF.

The scenario is illustrated in the Figure.



Use case examples

AF-originated API invocation (Gaming)

General

This use case is an example of AF-originated API invocation with a gaming application. In this use case, the end user (also a subscriber of the MNO) allows the AF (game provider's server) to invoke the QoS API (offered by MNO) to modify the QoS of the end user.

5G API Core Function procedure for API Invoker obtaining Resource owner Consent prior to the Service APIs Invocation

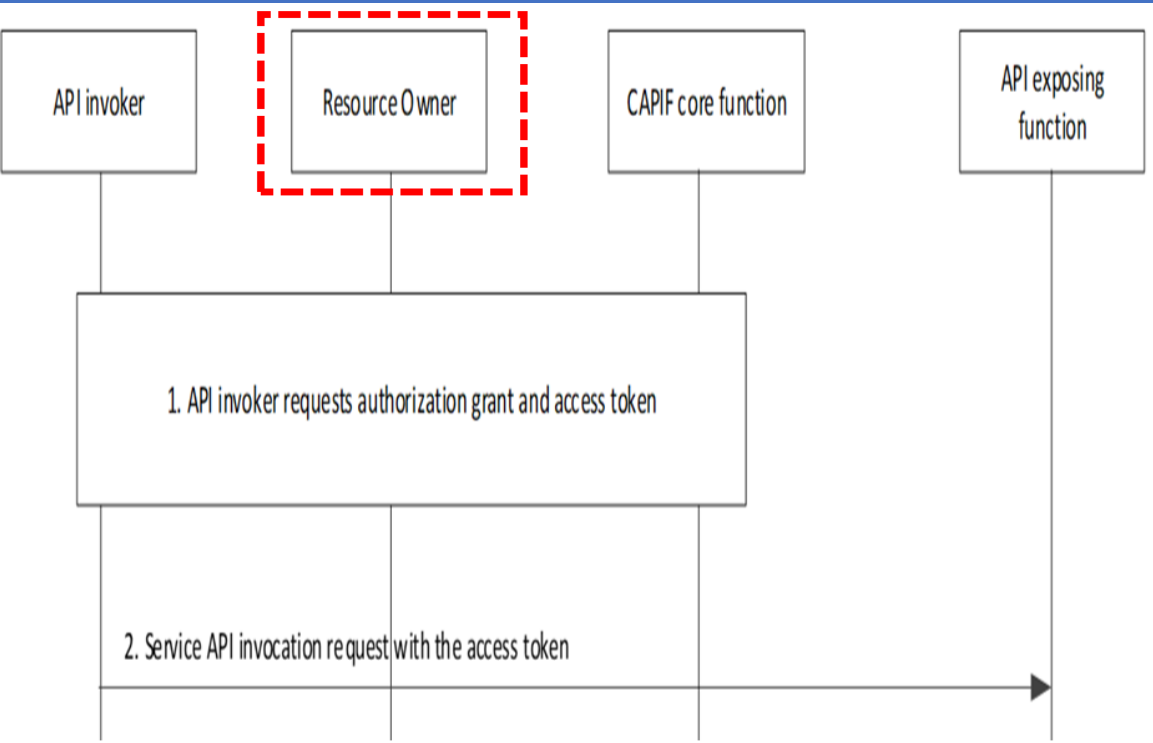


Fig.: 5G API Core Function procedure for API Invoker obtaining Resource owner Consent prior to the Service APIs Invocation

UE-originated API invocation (Location tracking)

General

This use case is an example of UE-originated API invocation with a location tracking application. In this use case, the end user (also a subscriber of the MNO) on UE X allows the end user on UE Y to invoke an API to track the location of the end user on UE X.

5G API Core Function Procedure for obtaining Resource owner Consent in a nested API Invocation

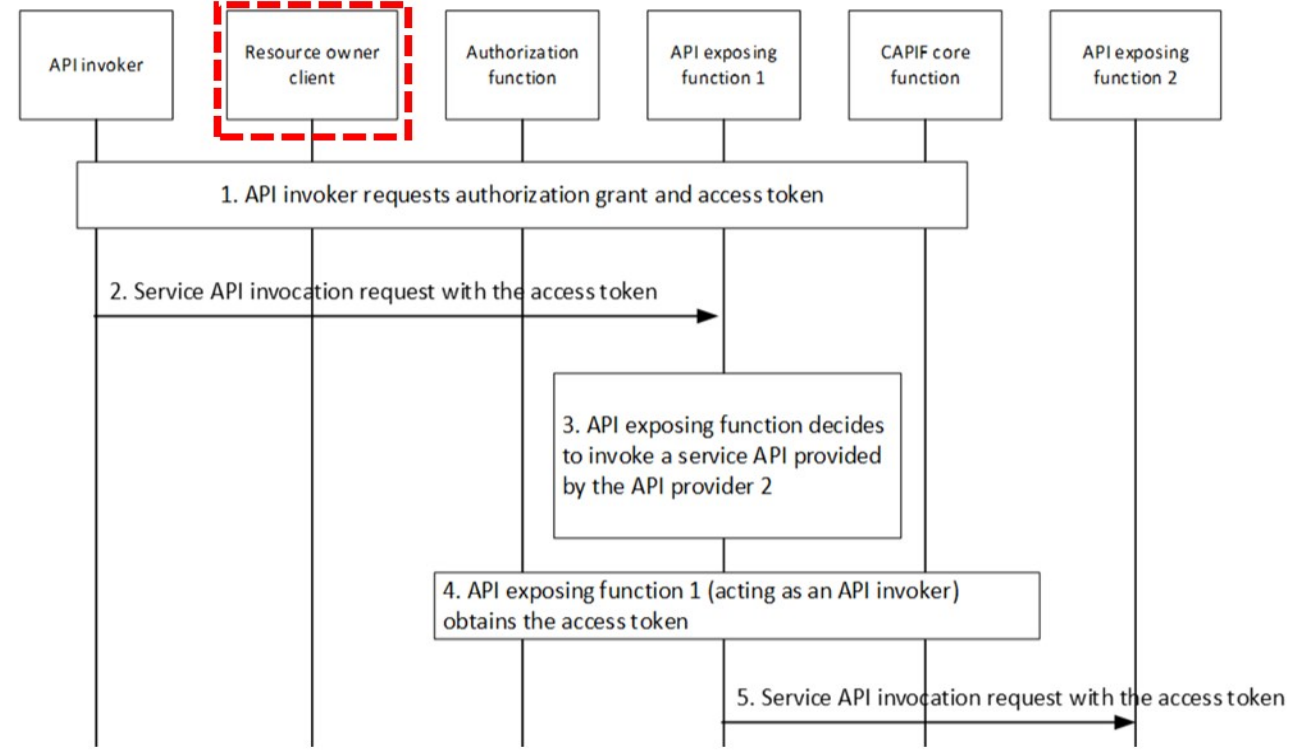


Fig.: 5G API Core Function Procedure for obtaining Resource owner Consent in a nested API Invocation

1. 3GPP Changing: Subscriber-aware Northbound API access (SNA) to Resource-owner aware Northbound APIs access (RNAAI)

Release 18

3GPP

V18.2.2 (2023-07)

1.4 5G System Network Capability External Exposure Application Function (AF) influence on Traffic Routing- 1

AF influence on Traffic Routing may apply in the case of Home Routed (HR) deployments with Session Breakout (HR SBO).

In that case when an AF belonging to the V-PLMN (or with an offloading SLA with the V-PLMN) desires to provide Traffic Influence policies it may invoke at the V-NEF the API defined in this clause and provide the information listed in the Table, but the corresponding Traffic Influence information is provided directly from V-NEF to V-SMF bypassing the PCF.

An AF may send requests to influence SMF routing decisions for Traffic of PDU Session.

The AF requests may influence UPF (re)selection and (I-)SMF (re)selection and allow routing User Traffic to a Local Access to a Data Network (identified by a DNAI).

The AF may issue requests on behalf of Applications not owned by the PLMN serving the UE.

If the Operator does not allow an AF to access the Network directly, the AF shall use the NEF to interact with the 5GC.

Table : Information element contained in AF request

| Information Name | Applicable for PCF or NEF (NOTE 1) | Applicable for NEF only | Category |
|--|---|---|----------------------|
| Traffic Description | Defines the target traffic to be influenced, represented by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information. | The target traffic can be represented by AF-Service-Identifier, instead of combination of DNN and optionally S-NSSAI. | Mandatory |
| Potential Locations of Applications | Indicates potential locations of applications, represented by a list of DNAI(s). | The potential locations of applications can be represented by AF-Service-Identifier. | Conditional (NOTE 2) |
| Target UE Identifier(s) | Indicates the UE(s) that the request is targeting, i.e. one or a list of individual UE(s), a group of UE represented by Internal Group Identifier(s) (NOTE 3), or any UE accessing the combination of DNN, S-NSSAI and DNAI(s). | GPSI can be applied to identify the individual UE, or External Group Identifier(s) can be applied to identify a group of UE (NOTE 3). External Subscriber Category(s) (NOTE 5). | Mandatory |
| Spatial Validity Condition | Indicates that the request applies only to the traffic of UE(s) located in the specified location, represented by areas of validity. | The specified location can be represented by geographical area. | Optional |
| AF transaction identifier | The AF transaction identifier | N/A | Mandatory |
| N6 Traffic Routing requirements | Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation (NOTE 4). | N/A | Optional (NOTE 2) |
| Application Relocation Possibility | Indicates whether an application can be relocated once a location of the application is selected by the 5GC. | N/A | Optional |
| UE IP address preservation indication | Indicates UE IP address should be preserved. | N/A | Optional |
| Temporal Validity | Time interval(s) or duration(s). | N/A | Optional |
| Information on AF subscription to corresponding SMF events | Indicates whether the AF subscribes to change of UP path of the PDU Session and the parameters of this subscription. | N/A | Optional |
| Information for EAS IP Replacement in 5GC | Indicates the Source EAS identifier and Target EAS identifier, (i.e. IP addresses and port numbers of the source and target EAS). | N/A | Optional |
| User Plane Latency Requirement | Indicates the user plane latency requirements | N/A | Optional |
| Information on AF change | N/A | Indicates the AF instance relocation and relocation information. | Optional |
| Indication for EAS Relocation | Indicates the EAS relocation of the application(s). | N/A | Optional |
| Indication for Simultaneous Connectivity over the source and target PSA at Edge Relocation | Indicates that simultaneous connectivity over the source and target PSA should be maintained at edge relocation and provides guidance to determine when the connectivity over the source | N/A | Optional |
| EAS Correlation indication | Indicates selecting a common EAS for the application identified by the Traffic Description for the set of UEs. | | Optional |
| Common EAS IP address | the common EAS for the application identified by the Traffic Description for a set of UEs the AF request aims at. | | Optional |
| Traffic Correlation ID | Identification of a set of UEs targeted at by the AF request, and accessing the application identified by the Traffic Description. | | Optional |
| FQDN(s) | FQDN(s) used for influencing EASDF-based DNS query procedure as defined in clause 6.2.3.2.2 of TS 23.501 and TS 23.502. | | Optional |

NOTE 1: When the AF request targets existing or future PDU Sessions of multiple UE(s) or of any UE and is sent via the NEF, as described in clause 6.3.7.2, the information is stored in the UDR by the NEF and notified to the PCF by the UDR.

NOTE 2: The potential locations of applications and N6 traffic routing requirements may be absent only if the request is for subscription to notifications about UP path management events only or request is for indication of selecting Common EAS for a set of UEs.

NOTE 3: Internal Group ID can only be used by an AF controlled by the operator and only towards PCF. If a list of Internal/External Group IDs is provided by the AF, the AF request applies to the UEs that belong to every one of these groups, i.e. a single UE needs to be a member of every group in the list of Internal/External Group IDs.

NOTE 4: The indication of traffic correlation can be used for 5G VN groups as described in clause 5.29.

NOTE 5: External Subscriber category(s) can be combined with External Group ID(s) or any UE. If a list of External Subscriber categories are provided by the AF, the AF request applies to the UEs that belong to every one of these Subscriber categories.

NOTE 6: FQDN(s) is used for influencing EASDF-based DNS query procedure as defined in clause 6.2.3.2.2 of TS 23.501 and TS 23.502.

1. 5G System Network Capability External Exposure Application Function (AF) influence on Traffic Routing- 2

The AF may be in charge of the (re)selection or re-location of the Applications within the Local Part of the DN.

The AF may request to get notified about events related with PDU Sessions.

In the case of AF instance change, the AF may send request of AF re-location information.

The AF requests that target existing or future PDU Sessions of multiple UE(s) or of any UE are sent via the NEF and may target multiple PCF(s).

The PCF(s) transform(s) the AF requests into Policies that apply to PDU Sessions.

When the AF has subscribed to UP Path Management Event Notifications from SMF(s) (including notifications on how to reach a GPSI over N6), such notifications are sent either "directly to the AF" or via an NEF (without involving the PCF).

For AF interacting with PCF directly or via NEF, the AF requests may contain the information as described in the Table:

Release 18

3GPP

V18.2.2 (2023-07)

Table : Information element contained in AF request

| Information Name | Applicable for PCF or NEF (NOTE 1) | Applicable for NEF only | Category |
|---|---|---|----------------------|
| Traffic Description | Defines the target traffic to be influenced, represented by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information. | The target traffic can be represented by AF-Service-Identifier, instead of combination of DNN and optionally S-NSSAI. | Mandatory |
| Potential Locations of Applications | Indicates potential locations of applications, represented by a list of DNAI(s). | The potential locations of applications can be represented by AF-Service-Identifier. | Conditional (NOTE 2) |
| Target UE Identifier(s) | Indicates the UE(s) that the request is targeting, i.e. one or a list of individual UE(s), a group of UE represented by Internal Group Identifier(s) (NOTE 3), or any UE accessing the combination of DNN, S-NSSAI and DNAI(s). | GPSI can be applied to identify the individual UE, or External Group Identifier(s) can be applied to identify a group of UE (NOTE 3). External Subscriber Category(s) (NOTE 5). | Mandatory |
| Spatial Validity Condition | Indicates that the request applies only to the traffic of UE(s) located in the specified location, represented by areas of validity. | The specified location can be represented by geographical area. | Optional |
| AF transaction identifier | The AF transaction identifier | N/A | Mandatory |
| N6 Traffic Routing requirements | Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation (NOTE 4). | N/A | Optional (NOTE 2) |
| Application Relocation Possibility | Indicates whether an application can be relocated once a location of the application is selected by the 5GC. | N/A | Optional |
| UE IP address preservation indication | Indicates UE IP address should be preserved. | N/A | Optional |
| Temporal Validity Condition | Time interval(s) or duration(s). | N/A | Optional |
| Information on AF subscription to corresponding SMF events | Indicates whether the AF subscribes to change of UP path of the PDU Session and the parameters of this subscription. | N/A | Optional |
| Information for EAS IP Replacement in 5GC | Indicates the Source EAS identifier and Target EAS identifier, (i.e. IP addresses and port numbers of the source and target EAS). | N/A | Optional |
| User Plane Latency Requirement | Indicates the user plane latency requirements | N/A | Optional |
| Information on AF change | N/A | Indicates the AF instance relocation and relocation information. | Optional |
| Indication for EAS Relocation | Indicates the EAS relocation of the application(s) | N/A | Optional |
| Indication for Simultaneous Connectivity over the source and target PSA at Edge Relocation | Indicates that simultaneous connectivity over the source and target PSA should be maintained at edge relocation and provides guidance to determine when the connectivity over the source | N/A | Optional |
| EAS Correlation indication | Indicates selecting a common EAS for the application identified by the Traffic Description for the set of UEs. | | Optional |
| Common EAS IP address | the common EAS for the application identified by the Traffic Description for a set of UEs the AF request aims at. | | Optional |
| Traffic Correlation ID | Identification of a set of UEs targeted at by the AF request, and accessing the application identified by the Traffic Description. | | Optional |
| FQDN(s) | FQDN(s) used for influencing EASDF-based DNS query procedure as defined in 6.2.3.2.2 of 3GPP TS 23.501 | | Optional |
| NOTE 1: When the AF request targets existing or future PDU Sessions of multiple UE(s) or of any UE and is sent via the NEF, as described in clause 6.3.7.2, the information is stored in the UDR by the NEF and notified to the PCF by the UDR. | | | |
| NOTE 2: The potential locations of applications and N6 traffic routing requirements may be absent only if the request is for subscription to notifications about UP path management events only or request is for indication of selecting Common EAS for a set of UEs. | | | |
| NOTE 3: Internal Group ID can only be used by an AF controlled by the operator and only towards PCF. If a list of Internal/External Group IDs is provided by the AF, the AF request applies to the UEs that belong to every one of these groups, i.e. a single UE needs to be a member of every group in the list of Internal/External Group IDs. | | | |
| NOTE 4: The indication of traffic correlation can be used for 5G VN groups as described in clause 5.29. | | | |
| NOTE 5: External Subscriber category(s) can be combined with External Group ID(s) or any UE. If a list of External Subscriber categories are provided by the AF, the AF request applies to the UEs that belong to every one of these Subscriber categories. | | | |
| NOTE 6: FQDN(s) is used for influencing EASDF-based DNS query procedure as defined in clause 6.2.3.2.2 of 3GPP TS 23.501. | | | |

1. 3GPP Changing: Subscriber-aware Northbound API access (SNA) to Resource-owner aware Northbound APIs access (RNAA)

1.5 Business Relationships in 5G System Architecture Common API Framework (CAPIF) for RNAA (Resource Owner-aware Northbound API Access) applied to:

The **API invoker** is typically provided by a **3rd Party Application Provider** who has Service Agreement with a CAPIF Provider.

The API Provider hosts one (1) or more Service APIs and has a Service API arrangement with CAPIF Provider to offer the Service APIs to the API Invoker.

The CAPIF Provider and the API Provider can be part of the same Organization (e.g. PLMN Operator), in which case the Business Relationship between the two (2) is internal to a single Organization.

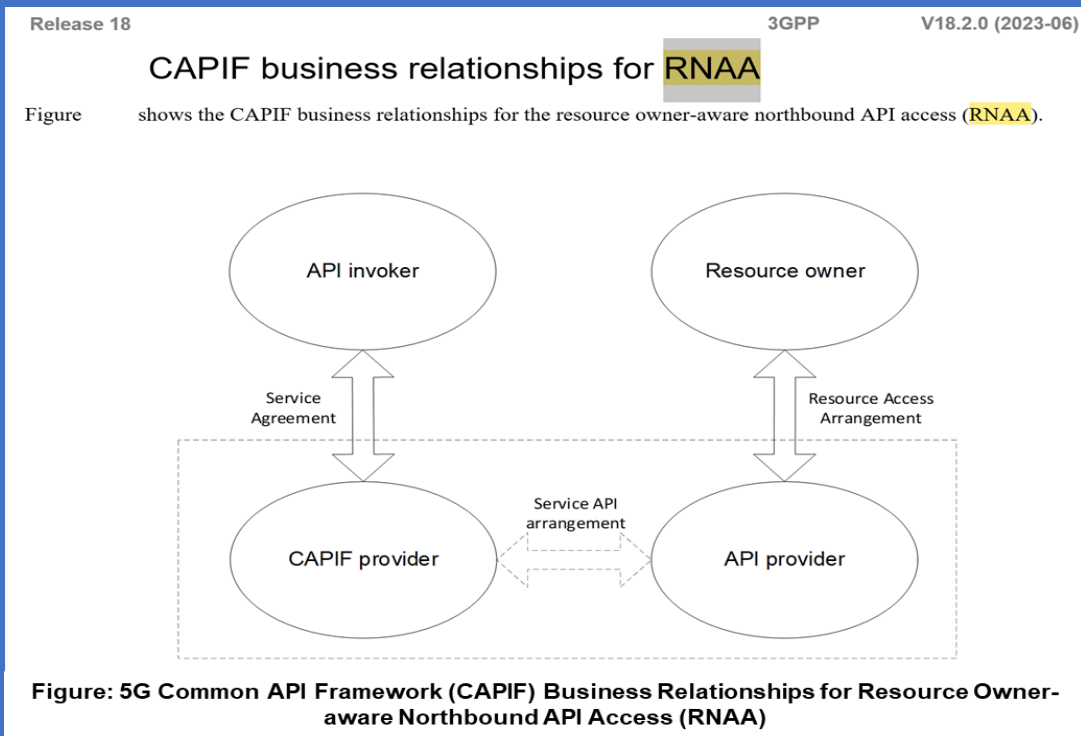
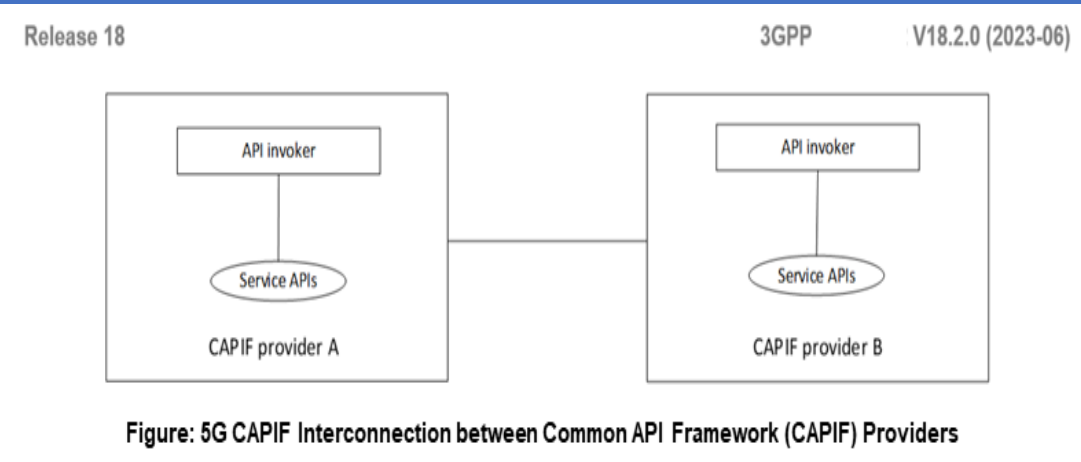
The CAPIF Provider and the API Provider can be part of different Organizations, in which case the Business Relationship between the two 2) must exist.

The Resource Owner is an Entity capable of granting Access to a protected Resource related to the Resource exposed by the API Provider.

The API invoker and the resource owner can be the same Entity or separate Entities.

In the current release, the Resource Owner is a User of a UE and can provide Authorization Information using the UE.

NOTE: In the current Release, both the CAPIF Provider and the API Provider should belong to the same Organization (e.g., PLMN Operator) and *the Service API arrangement is not required explicitly.*



The Figure shows the Architectural Model for the RNAA which allows the Resource Owner to provide "Authorization" to the API Invocation.

The Resource Owner Client(s) are Application Clients used by Resource Owners of the API Provider Domain's Service Provider.

The Authorization Function is an internal entity of the CAPIF Core Function (CCF). The resource owner client(s) interacts with the authorization function in the CAPIF core function via CAPIF-8. The resource owner communicates with the authorization function in the CAPIF core function to provide and revoke resource owner consent. The resource owner interactions are supported via a resource owner client, which is a client-side entity.

The API exposing function (e.g. 5G CN NEF, 4G/LTE CN SCEF) acts as a Resource Owner Consent Enforcement Point as specified in 3GPP TS 33.501 [8] and interacts with the authorization function in the CAPIF core function via CAPIF-3. The API exposing function can retrieve the resource owner consent parameters from the authorization function.

The API exposing function (e. g. NEF) acts as a Resource owner Consent Enforcement point as specified in 5GS and interacts with the Authorization Function via CAPIF-9.

The API Exposing Function can retrieve the Resource owner Consent Parameters from the Authorization function. The API invoker interacts with Authorization Function via CAPIF-10/CAPIF-10e.

NOTE: In the current release, 3rd party API providers (i.e., API providers outside the PLMN trust domain) are not supported for RNAA.

NOTE 1: RNAA is supported for both 4G and 5G Network. The API invoker interacts with Authorization Function in the CAPIF core function via CAPIF-1/CAPIF-1e.

NOTE 2: In the current release, 3rd party API Providers (i.e., API Providers outside the PLMN Trust Domain) are not supported for RNAA.

NOTE 3: The terms "Functional Architecture" and "Functional Model" mean the same and have been used interchangeably in this specification.

NOTE 4: The Functional Model described in this Specification applies to both PLMN(s) and to SNPN(s).

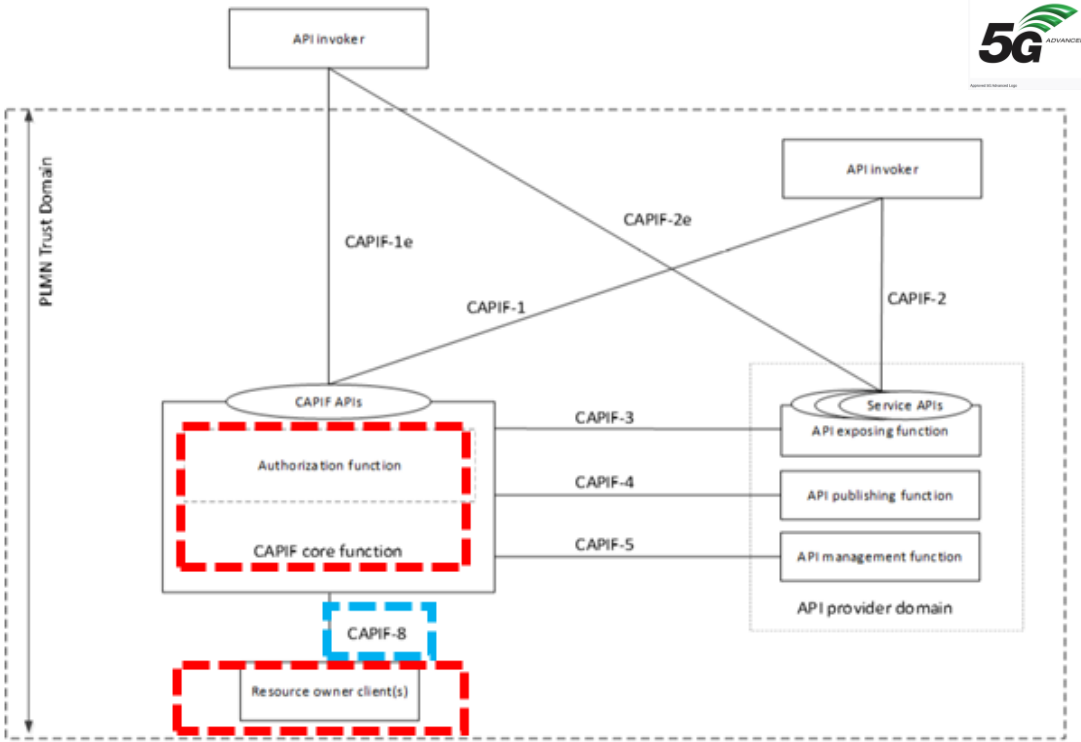


Figure: 5G Resource Owner-aware Northbound API Access (RNAA) Architecture support in 5G Common API Framework (CAPIF)

3GPP **5GS** can deploy the *CAPIF Core Function (CCF)* along with the **5G CN NEF**.

The **5G CN NEF** can implement the Functionalities of the API Provider Domain Functions.

The **5G CN NEF** can implement:

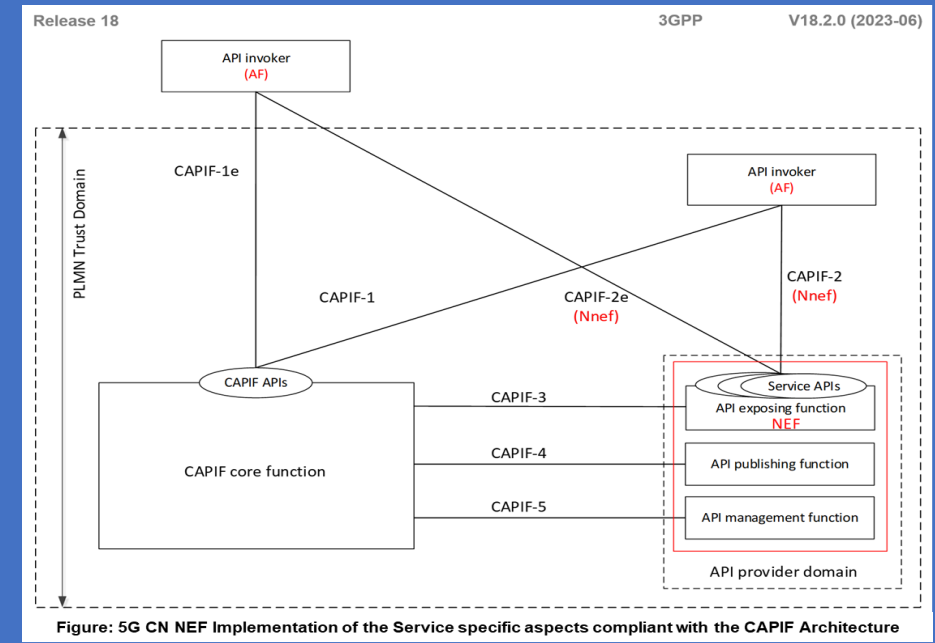
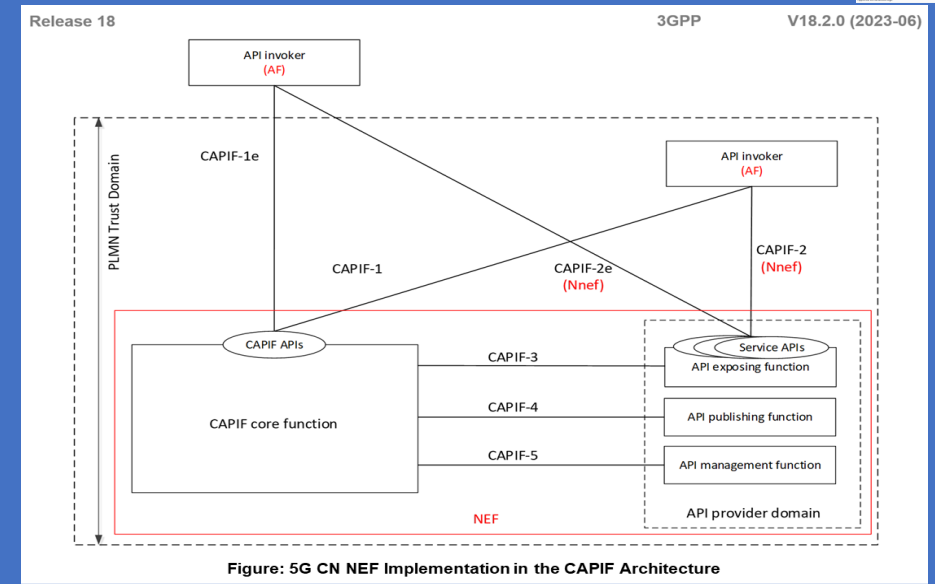
- the **CAPIF Core Function (CCF)** Functionalities,
- the **API Exposing Function**,
- the **API Publishing Function** and
- the **API Management function**.

According to the 5GS CAPIF Architecture, CAPIF-2 and CAPIF-2e consist of Framework aspects and Service specific aspects. The Service specific aspects are out of scope of CAPIF.

Nnef can implement the Service specific aspects of CAPIF-2 and CAPIF-2e, and can provide the service APIs exposed by NEF (AEF) to the AF (API invoker).

The **NEF** can implement the CAPIF-3 Reference Point/Interface to the CAPIF Core Function (CCF).

The **NEF** can additionally provide CAPIF-1 and CAPIF-1e (CAPIF APIs) to the AF (API invokers).



Distributed deployment of the 5G CN NEF compliant with the CAPIF Architecture

The Figure illustrates the Distributed deployment Model where the **5G CN NEF** implements the Service specific aspect compliant with the **5G CN CAPIF Architecture**.

The 3GPP 5GS can deploy the CAPIF Core Function (CCF), the NEF-2 (API Exposing Function as a Gateway (GW) along with the NEF-1.

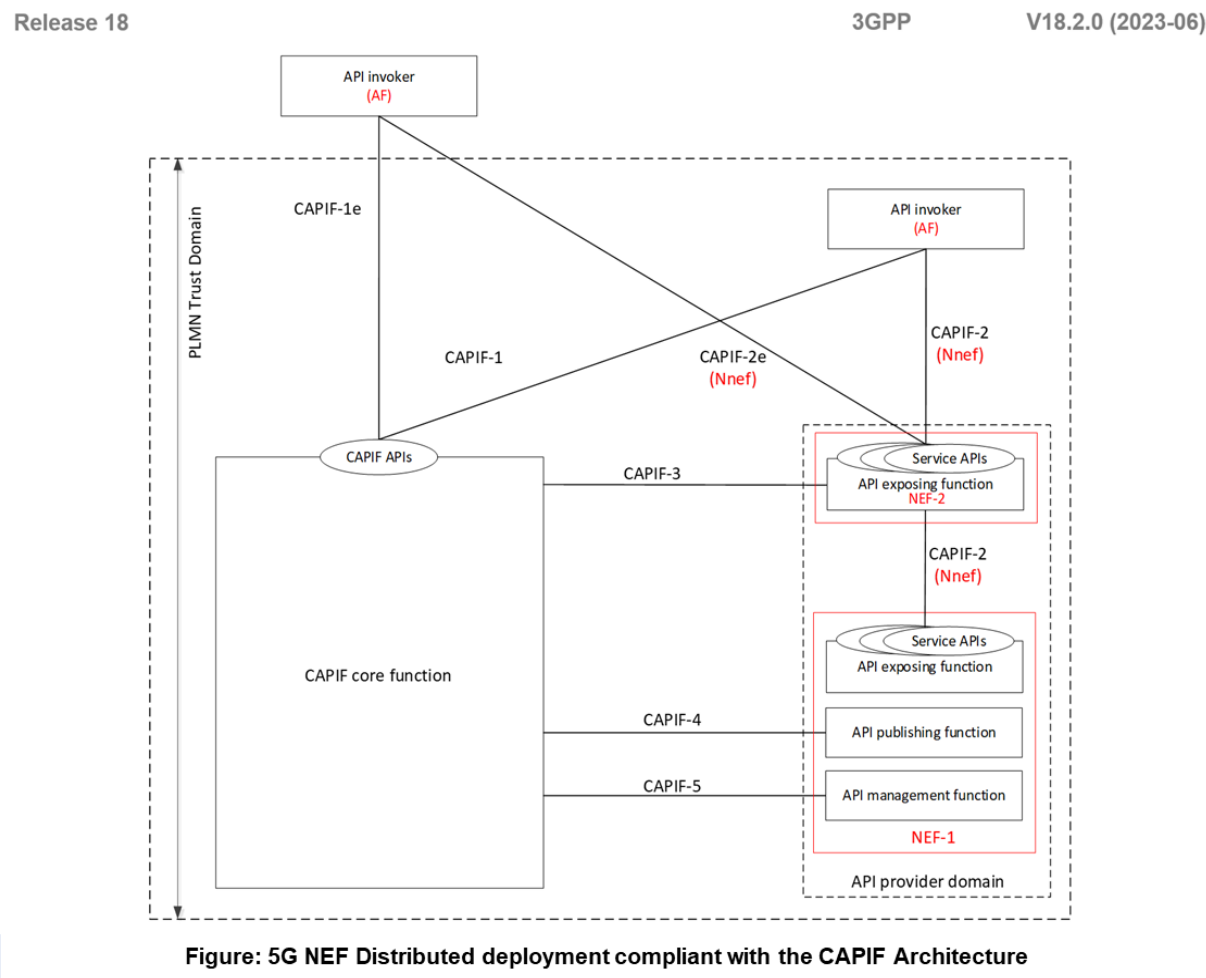
The 5G CN NEF can implement the Functionalities of API Provider Domain Functions.

According to the 5G CAPIF Architecture, CAPIF-2 or CAPIF-2e consists of Framework aspects and Service specific aspects.

The Service specific aspects are out of scope of the CAPIF.

The 5G CN Nnef can implement the Service specific aspects of CAPIF-2 and CAPIF-2 or CAPIF-2e can provide the Service APIs exposed by the NEF-2 (AEF as a Gateway (GW)) to the AF (API invoker).

The **NEF-2 (AEF)** can implement the CAPIF-3 Reference Point to the CAPIF Core Function (CCF) and the NEF-1 can implement the CAPIF-4 and CAPIF-5 Reference Points to the CAPIF Core Function (CCF).



1. 3GPP Changing: Subscriber-aware Northbound API access (SNA) to Resource-owner aware Northbound APIs access (RNAA)

1.6 5G CAPIF Deployment Model with 4G EPC CNSCEF and 5G SA CN NEF

The **4G EPC SCEF** and the **5G SA CN NEF** could be integrated with a single CAPIF Core Function (CCF) to offer their respective Service APIs to the API Invokers.

The **CAPIF Core Function (CCF)**, the **4G EPC SCEF** and the **5G SA CN NEF** are deployed in the **PLMN Trust Domain**, where the **CAPIF Core Function (CCF)** takes the Role of a **Unified Gateway (GW)** and provides **Services** to different **API Invokers**.

The API invokers obtains the **T8** and **N33** Service API Information and the corresponding entry point details from the CAPIF Core Function (CCF) via CAPIF-1 or CAPIF-1e Reference Points.

The API invokers can interact independently with the **4G EPC SCEF**, the **5G SA CN NEF** and the 3rd Party API Exposing Functions via CAPIF-2 or CAPIF-2e Reference Points.

In this case, **SCEF T8** and **NEF N33** can be re-used to implement the Service specific aspects of CAPIF-2 or CAPIF-2e Reference Points for the corresponding Service API Interactions of the SCEF and the NEF respectively.

The **SCEF** and the **NEF** applies any Service API Access Policy Control to the Interactions between the **API Invokers** and the **T8** and **N33** Service APIs respectively by communicating with the same CAPIF Core Function (CCF) via the CAPIF-3 Reference Point.

Release 18

3GPP

V18.2.0 (2023-06)

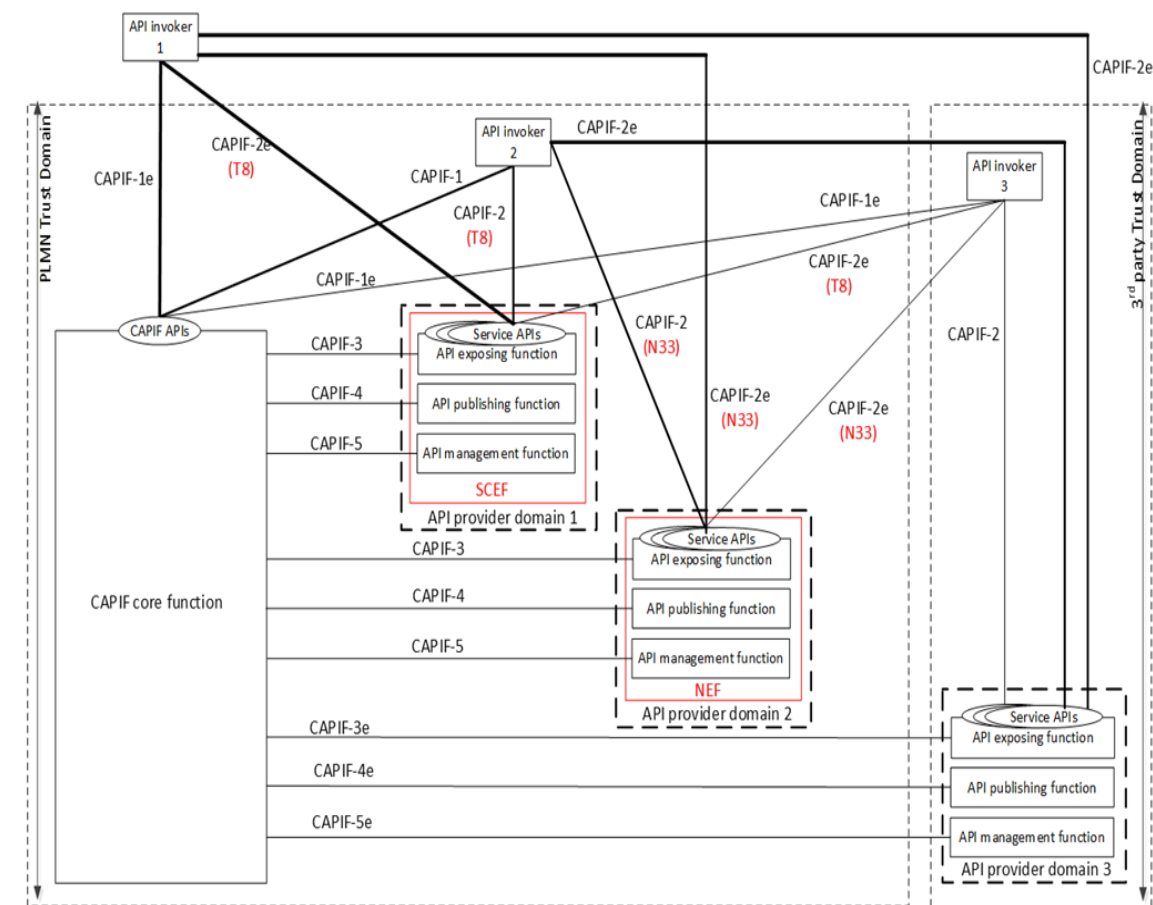


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

1.7 5G CAPIF Role in Charging

There are two (2) Charging Mechanisms - Offline Charging and Online Charging.

The Role of CAPIF in both these Charging Mechanisms is illustrated in the Figure for information purpose.

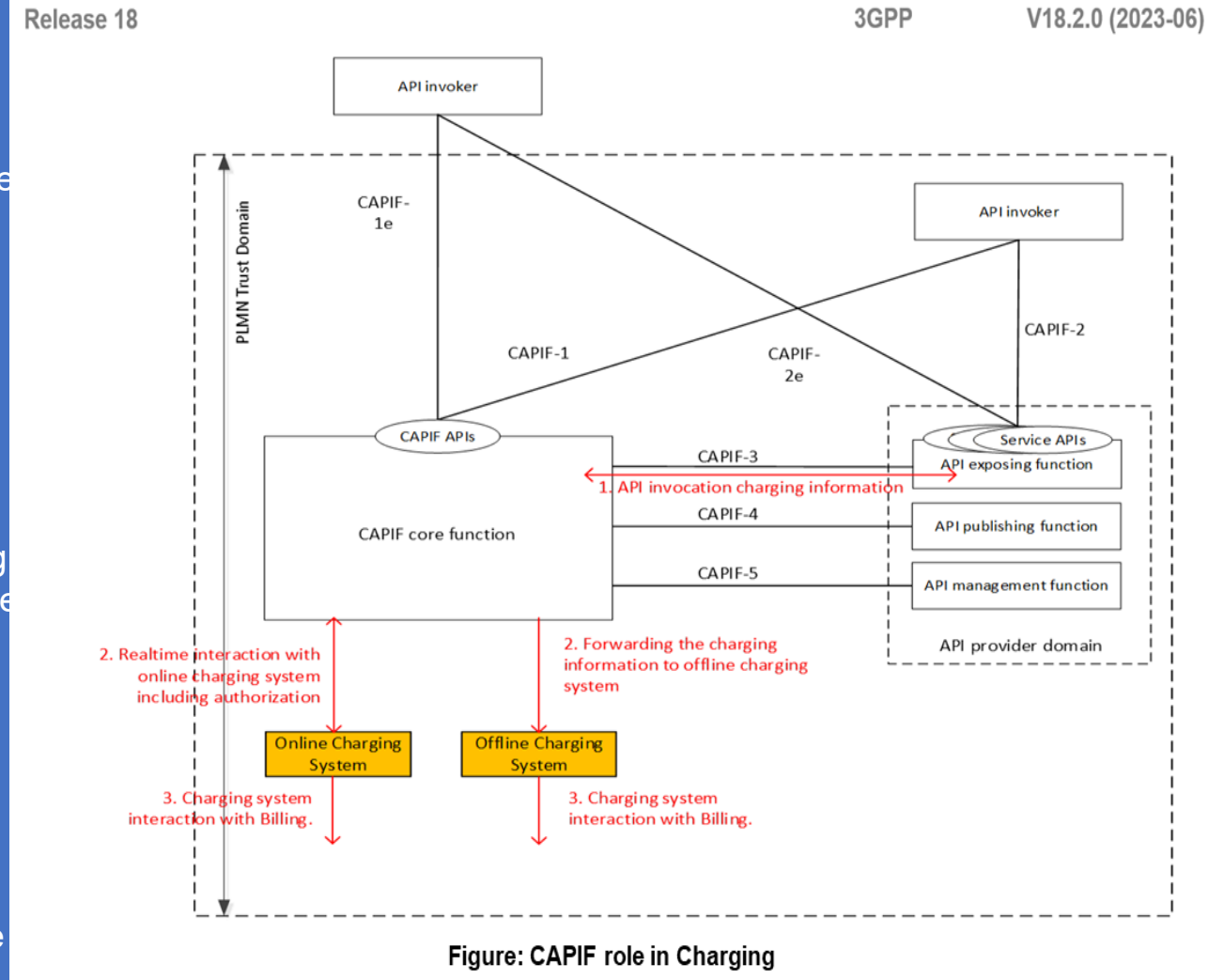
The API Invocations are subjected to Charging (On-line, Off-line) as illustrated in the Figure.

The API Exposing Function provides the API Invocation Charging Information to the CAPIF Core Function (CCF).

The CAPIF Core Function (CCF) further interacts with an Online Charging System in Real-Time by providing the Charging Information and further the CAPIF Core Function (CCF) receives the Authorization corresponding to the Charging Information.

The API invocations are subjected to Offline charging as illustrated. The API Exposing Function provides the API Invocation Charging Information to the CAPIF Core Function.

The CAPIF Core Function (CCF) provides the Charging Information to the Offline Charging System. The Offline Charging System generates the CDRs for the API Invocation and further transfers the CDR files to the Billing Domain.



1. 3GPP Changing: Subscriber-aware Northbound API access (SNA) to Resource-owner aware Northbound APIs access (RNAA)

1.8 Functional Model Description for the CAPIF for interaction of API Exposing Function (AEF)

As illustrated in the Figure, the interactions between the API Exposing Functions (AEF) within the PLMN Trust Domain is via **CAPIF-7**.

The CAPIF Core Function (CCF) provides CAPIF APIs to the API Invoker over CAPIF-1 and CAPIF-1e.

The API Exposing Function provides the Service APIs to the API Invoker over CAPIF-2 and CAPIF-2e.

NOTE 1: *The communication between the API Exposing Function and the CAPIF Core Function (CCF), between the API Publishing Function and the CAPIF Core Function (CCF) and between the API Management Function and the CAPIF Core Function (CCF) over CAPIF-3, CAPIF-4 and CAPIF-5 respectively can be API based.*

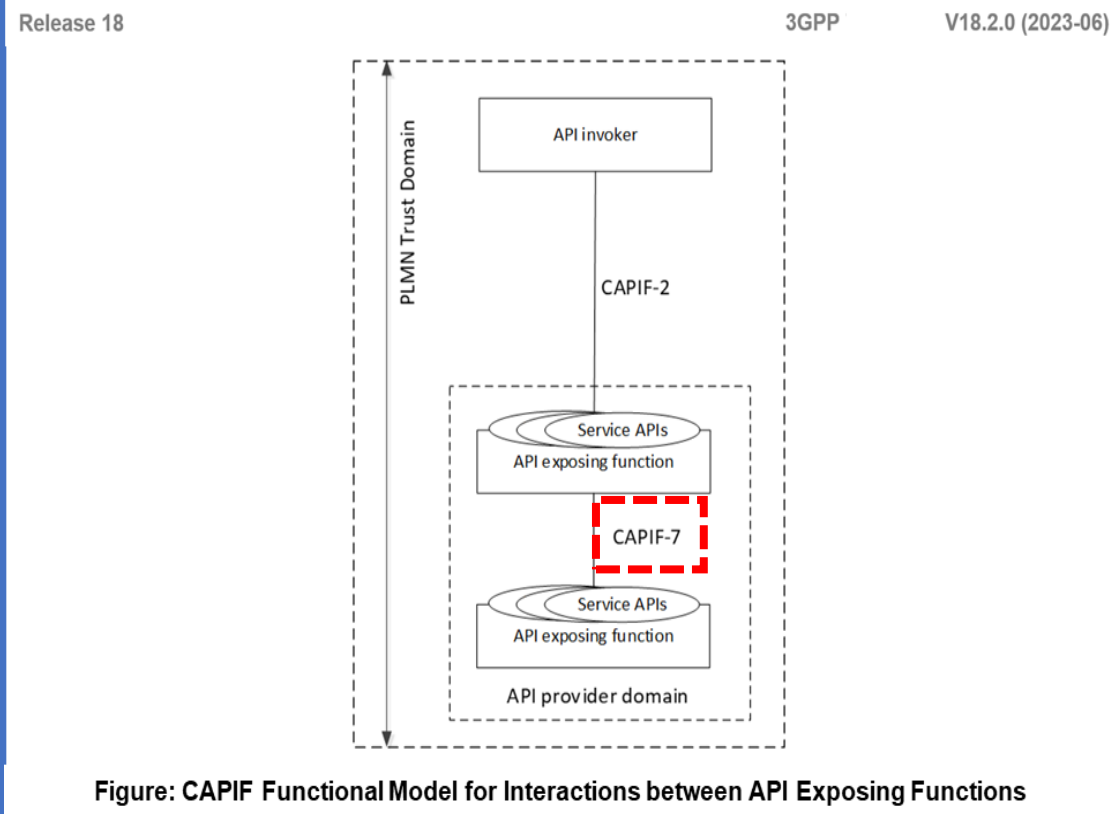


Figure: CAPIF Functional Model for Interactions between API Exposing Functions

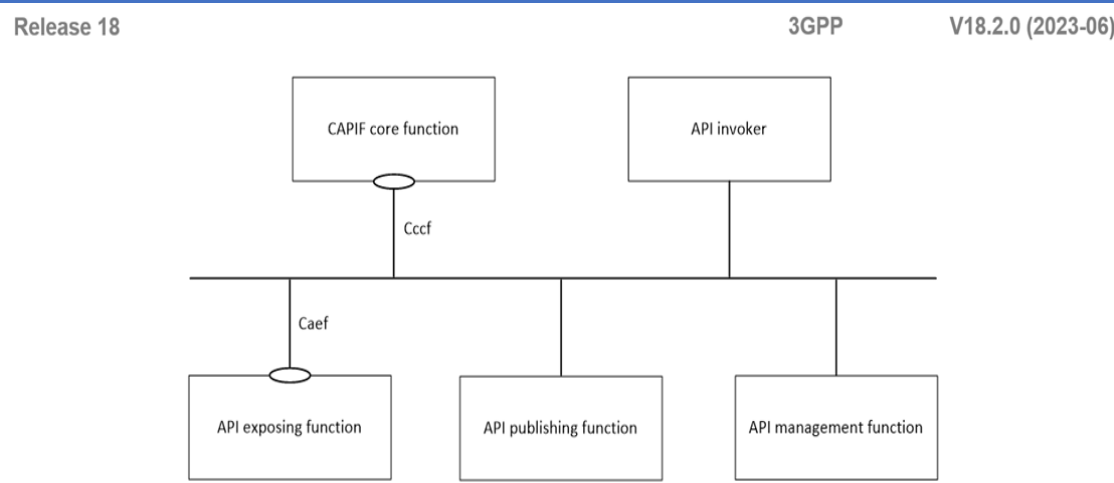


Figure: 5G CAPIF Functional Model Representation using Service-based Interfaces (SBIs)

CAPIF Functional Model description to support 3rd Party API Providers

The CAPIF core function in the PLMN trust domain supports service APIs from both the PLMN trust domain and the 3rd party trust domain having business relationship with PLMN.

The API invokers 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 1 offers the Service APIs from the PLMN Operator.

The API provider Domain 2 offers the Service APIs from the 3rd Party.

When the 3rd Party API Provider is a Trusted 3rd Party of the PLMN, the API Provider Domain 1 also offers the Service APIs from the 3rd Party.

The API Invoker 2 within the PLMN Trust Domain interacts with the CAPIF Core Function (CCF) via CAPIF-1, and 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 Exposing Function (AEF), the API Publishing Function and the API Management Function of the API Provider Domain 1 within the PLMN Trust Domain interacts with the CAPIF core function via CAPIF-3, CAPIF-4 and CAPIF-5 respectively. The API exposing function, the API publishing function and the API management function of the API provider domain 2 within the 3rd party trust domain interacts with the CAPIF core function in the PLMN trust domain via CAPIF-3e, CAPIF-4e and CAPIF-5e respectively. The API Exposing Function within the PLMN trust domain and the 3rd party trust domain provides the service APIs to the API invoker, offered by the respective trust domains.

The interactions between the API Exposing Functions within the PLMN Trust Domain is via **CAPIF-7** (not shown in the Figure for simplicity).

The API Exposing Function within the PLMN Trust Domain interacts with the API Exposing Function in the 3rd Party Trust Domain via **CAPIF-7e**.

NOTE 1: The Communication between the API Exposing Function and the CCF, between the API Publishing Function and the CCF and between the API Management Function and the CCF over CAPIF-3/3e, CAPIF-4/4e and CAPIF-5/5e respectively can be API based.

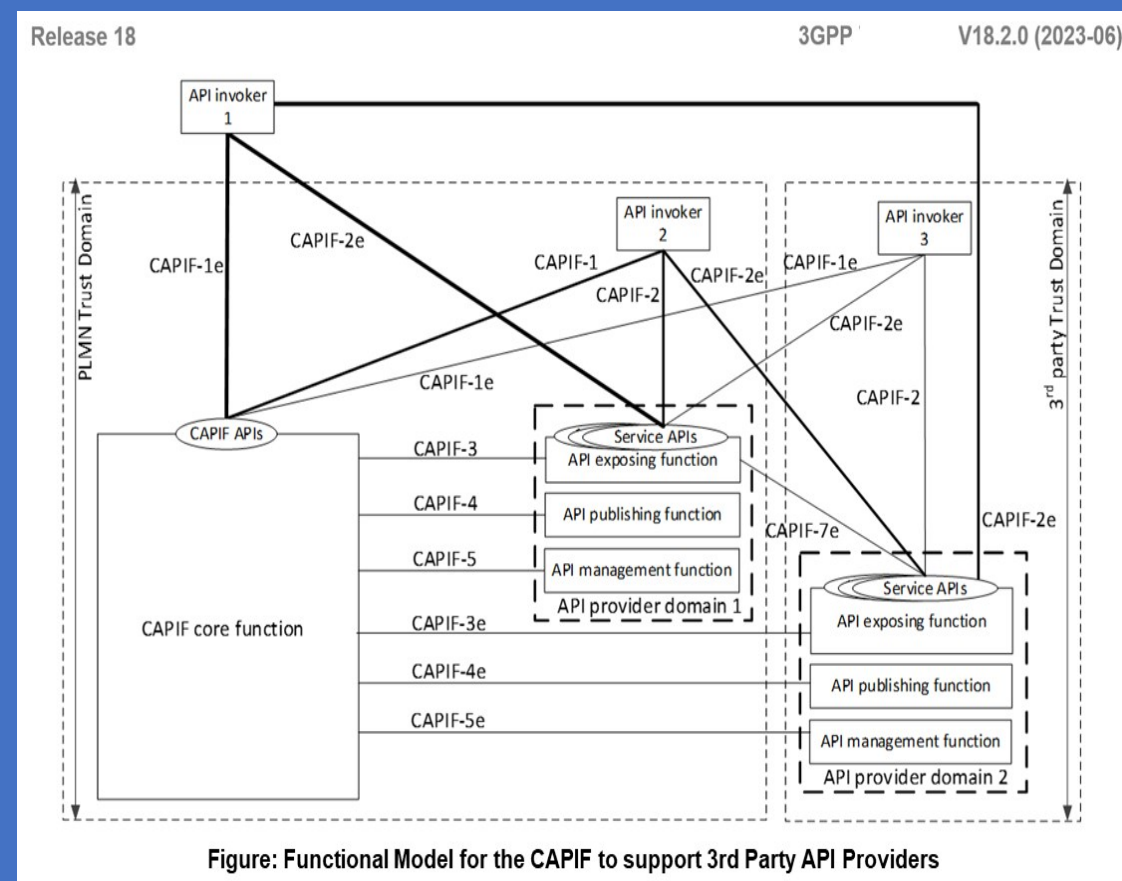


Figure: Functional Model for the CAPIF to support 3rd Party API Providers

1. 3GPP Changing: Subscriber-aware Northbound API access (SNA) to Resource-owner aware Northbound APIs access (RNAA)

1.9 Deployment Options of API Providers

Deployment of the 5G

- enhanced Common API Framework (CAPIF),
- Service APIs and
- Authorization APIs

by different Organizations within the PLMN Trust Domain

The **5G Common API Framework (CAPIF) Provider** and **API Provider** can be different organizations (e.g. PLMN Operator can be a *5G Common API Framework (CAPIF) Provider* and an **MVNO** can be the **API Provider**) within the **PLMN Trust Domain**.

The Figure illustrates the Deployment where the **5G CAPIF Entities** are deployed by different organizations.

Nodes (marked in "Red boxes") identify one (1) example of deployment.

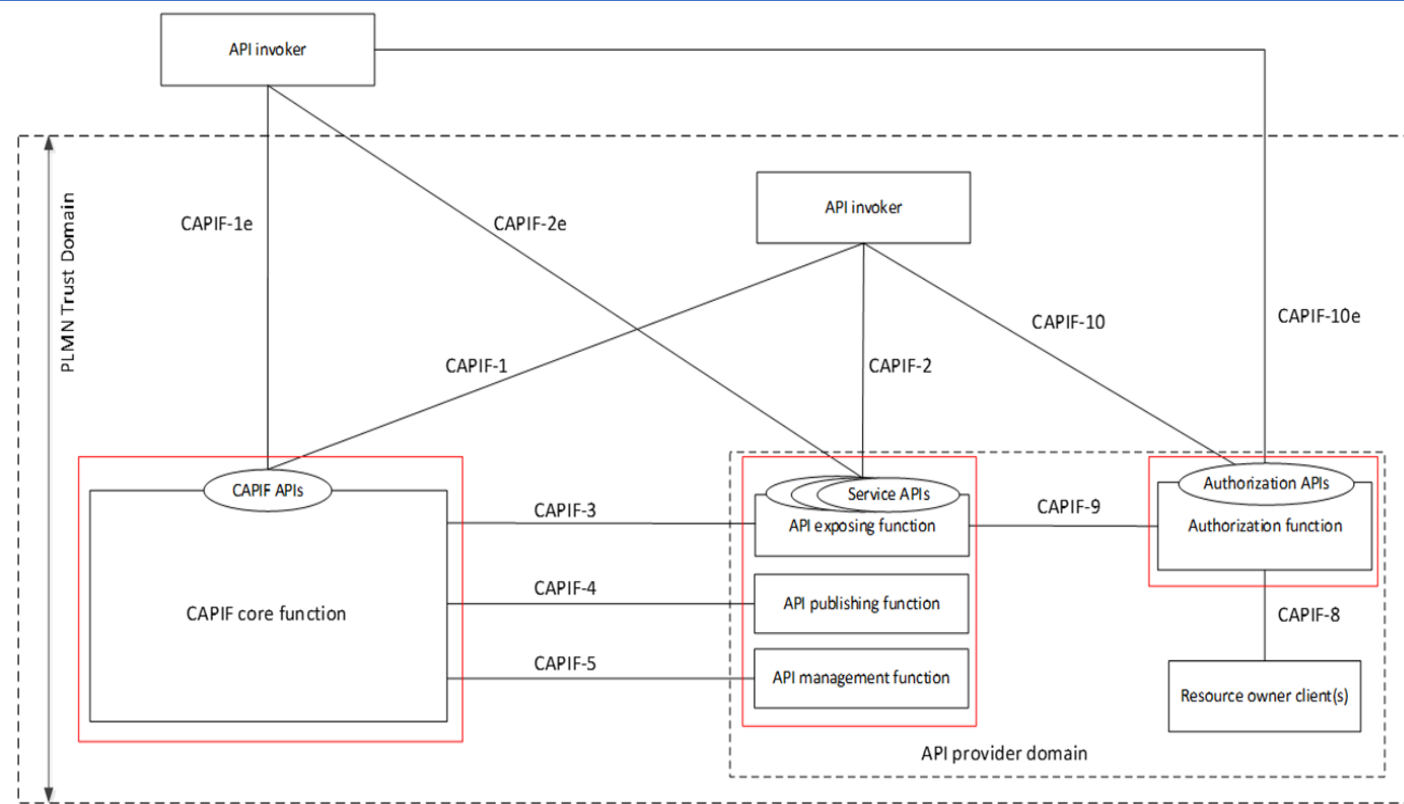
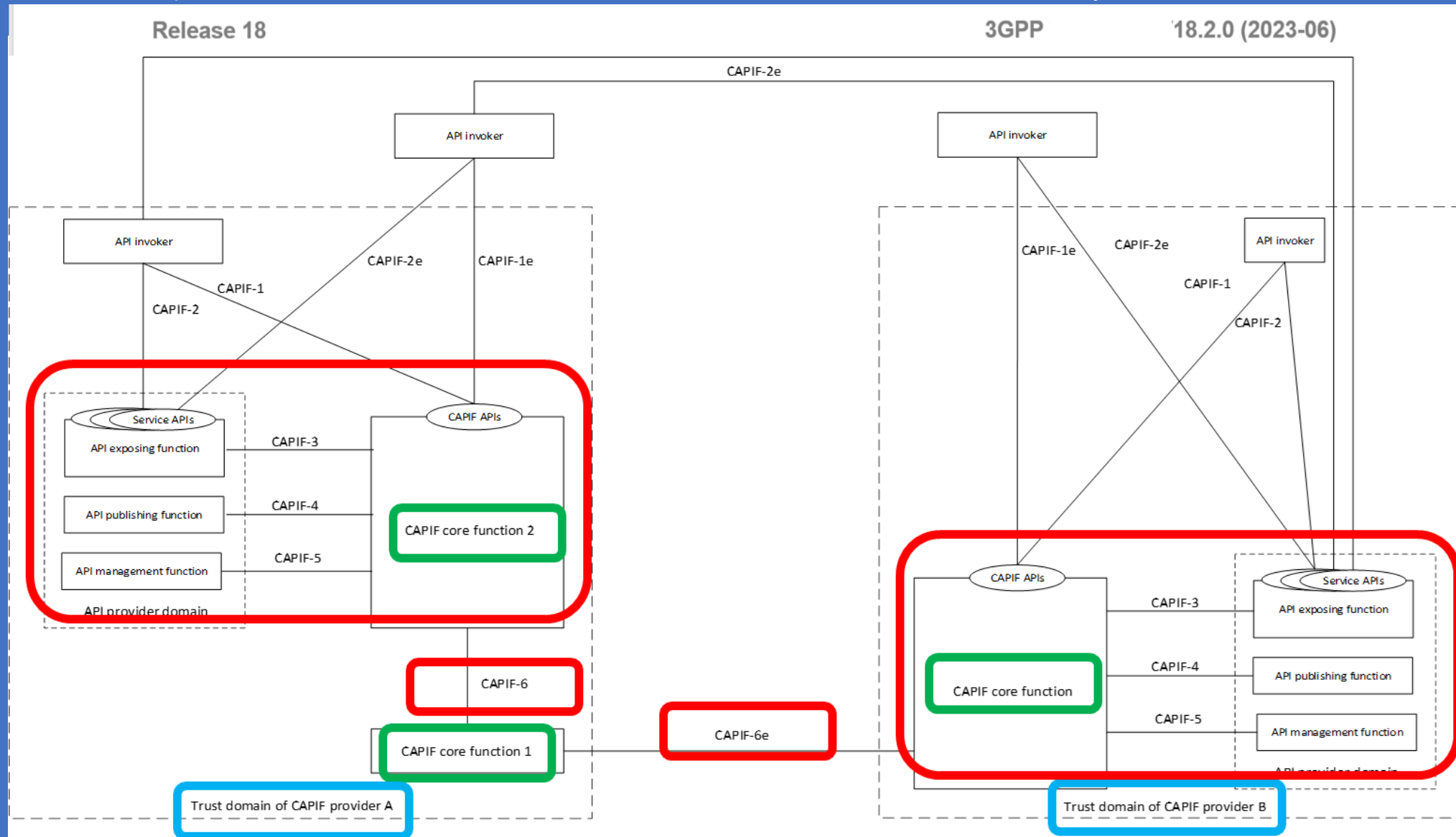


Figure: Deployment of the 5G enhanced Common API Framework (CAPIF), Service APIs and Authorization APIs by different Organizations within the PLMN Trust Domain

CAPIF-6 and CAPIF-6e Reference Points connect two 5G Common API Framework Core Functions (CCFs) located in the same or different PLMN Trust Domains, respectively. The reference points allows API invokers of a CAPIF Provider to utilize the Service APIs from the 3rd Party CAPIF Provider or another CAPIF Provider within trust domain.



The API Invoker supports several Capabilities as:

- the Authentication and obtaining Authorization and Discovering using CAPIF-1/CAPIF-1e Reference Point
- invoking the Service APIs using CAPIF-2/CAPIF-2e Reference Point

Figure: 5G Common API Framework Core Function (CCF) Interconnection Functional Model

5G CAPIF Interconnection Model

The Figure shows the 5G Architectural Model for the CAPIF interconnection within the same CAPIF Provider Domain, which allows API Invokers of CAPIF Core Function (CCF) 1 to utilize the Service APIs from CAPIF Core Function (CCF) 2, where both CAPIF Core Function 1 and CAPIF core Function (CCF) 2 are hosted within the Trust Domain of the CAPIF Provider A.

The CAPIF provider A & CAPIF provider B host the CAPIF in their Trust Domains. A Business Relationship exists between the CAPIF Providers. The CAPIF Providers in their respective Trust Domain hosts multiple CAPIF instances where each CAPIF instance consists of the CCF (local), the API Provider Domain and the API Invokers. All interactions within the CAPIF instance is according to the Functional Model as specified by 3GPP.

When multiple CAPIF instances are deployed by a CAPIF Provider there may be a hierarchy associated with the multiple CCF deployed which allows:

- the designated CCF of the CAPIF Provider A to interconnect with the designated CCF of the CAPIF provider B; and
- within CAPIF Provider A, one or more CCF interacts with the designated CCF 1

Release 18

3GPP

V18.2.0 (2023-06)

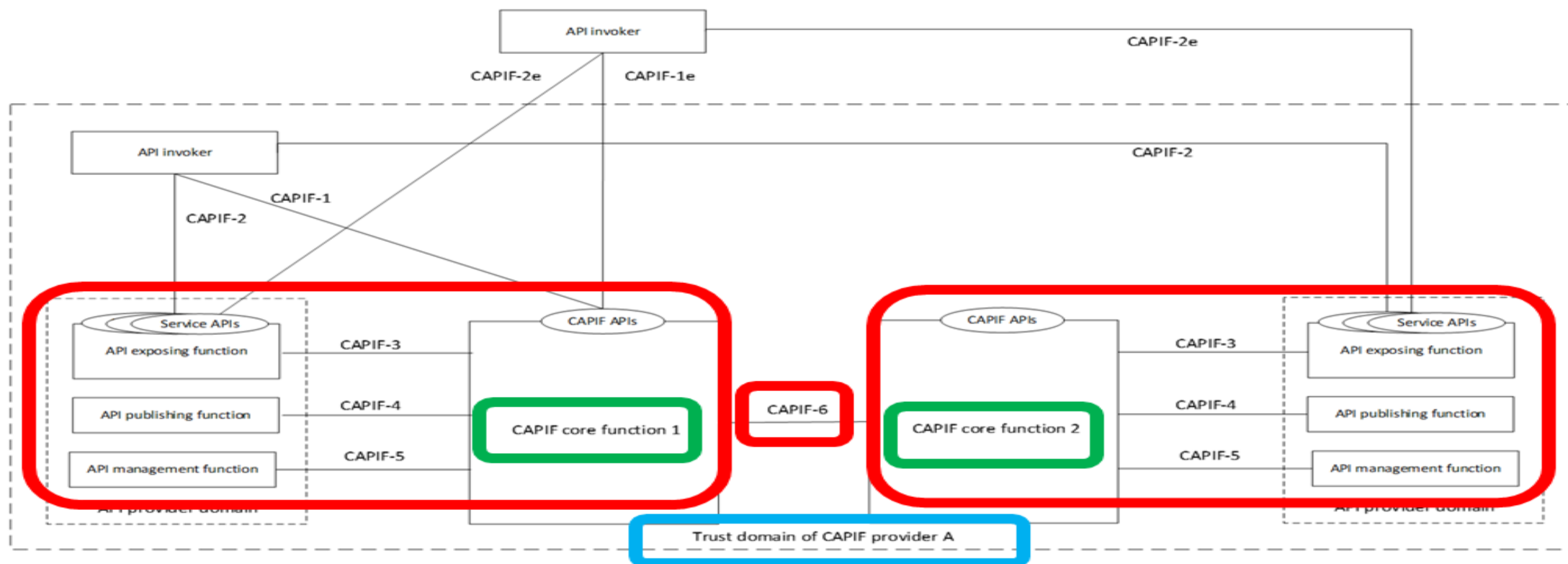


Figure: 5G Functional Architecture high-level for Common API Framework (CAPIF) Interconnection within a CAPIF Provider

1.10 5G Architecture for enabling Edge Applications deployments in relation with 5G Common API Framework

Distributed CAPIF Core Functions (CCFs)

The **EES** can support **EAS's** access to **Northbound APIs** exposed by **4G/5G CN Nodes**, **SCEF/NEF** by providing distributed **CAPIF Core Functions (CCFs)** as shown in the Figure.

The EDNs reside outside the PLMN Trust Domain as shown in the Figure.

In **EDN 2**, the **EAS** and **EES** are within the same **ECSP Trust Domain**. While in **EDN 1**, the **EES** and the **EAS** are in the **different ECSP Trust Domain**.

The **EES** of an **EDN** provides the following Functions for Network Capability Exposure:

- the CAPIF Core Function (CCF) as specified in 5G Common API Framework to support onboarding of **EASs (API invokers)**, Publish of Service APIs, Discovery of Service APIs and Charging of Service APIs invocations; and
- the API Exposing Function as specified in 5G Common API Framework to expose the **Service APIs from SCEF/NEF** to the EASs via Proxy or Gateway Function.

Centralized CAPIF Core Function (CCF)

The **EES** can support EAS (owned by **3rd Party** or by **PLMN Operator**) access to Northbound APIs exposed by **SCEF/NEF** by using centralized **CAPIF core functions (CCFs)** as shown in the Figure.

The EDNs reside outside the PLMN Trust Domain. In **EDN 2**, the **EAS** and **EES** are within the same **ECSP Ttrust Domain**. While in **EDN 1**, the **EES** and the **EAS** are in the **different ECSP Trust Domains**.

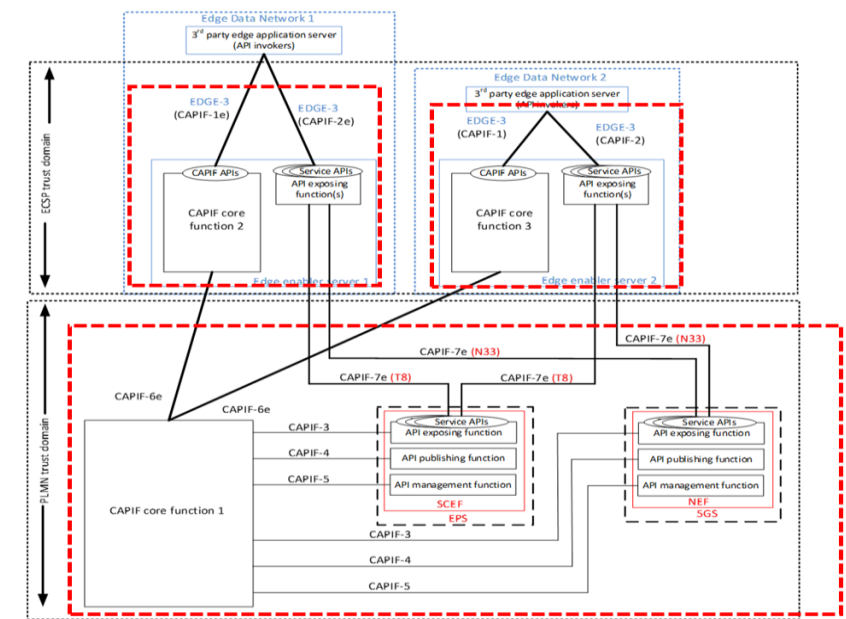


Figure: 5G Architecture enabling Edge Applications Edge Enabler Server(EES) supporting distributed 5G CommonAPI Framework Core Function (CCF)

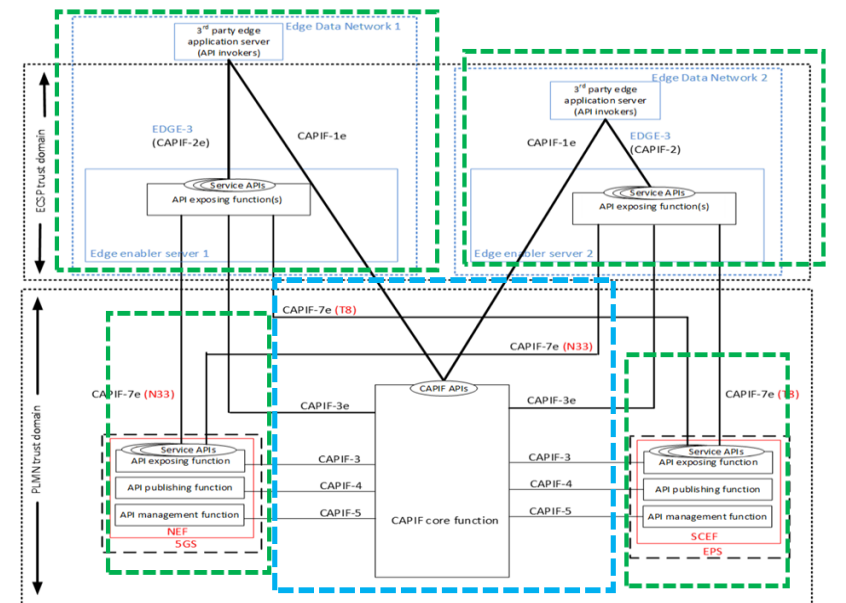


Figure: 5G Architecture enabling Edge Applications Edge Enabler Server(EES) supporting centralized 5G CommonAPI Framework Core Function (CCF)

2. Further shift of APIs Capabilities to End-Users (Subscribers) from early 5G Rel. 15 FMSS & SEES enabled APIs Capabilities shift from MNOs to 3rd Party ISPs & ICPs

5G Architecture enabling Edge Applications exposing Edge Application Server (EAS) Service APIs using 5G Common API Framework (CAPIF)

The **EES** provides support for an **EAS** to expose its **Service APIs** (i.e., *EAS Service APIs*) for consumption by the other **EASs** by providing **CAPIF Functions** as shown in the Figure.

In **EDN 1**, all the **EESs** are within the same **ECSP Trust Domain**.

The **EASs** (**EAS 1** and **EAS 2** as "**API Providers**") are within the same **ECSP Trust Domain** and **EAS 3 (API Provider)** is within the **3rd-Party Trust Domain**.

The **3rd Party EASs (API Invoker)** connected to **EES 2 (CCF 2)** are within the same **ECSP Trust Domain**, whereas the **3rd party EASs (API Invoker)** connected to **EES 1 (CCF 1)** are outside the **ECSP Trust Domain**.

The **EES** of an **EDN** provides the following functions for exposure of EAS Service APIs:

- The CCF as specified in 5G Common API Framework to support:
- On-boarding of **EASs (API invokers)**,
- Publish of EAS Service APIs,
- Discovery of EAS Service APIs,
- Charging of EAS Service APIs Invocations.

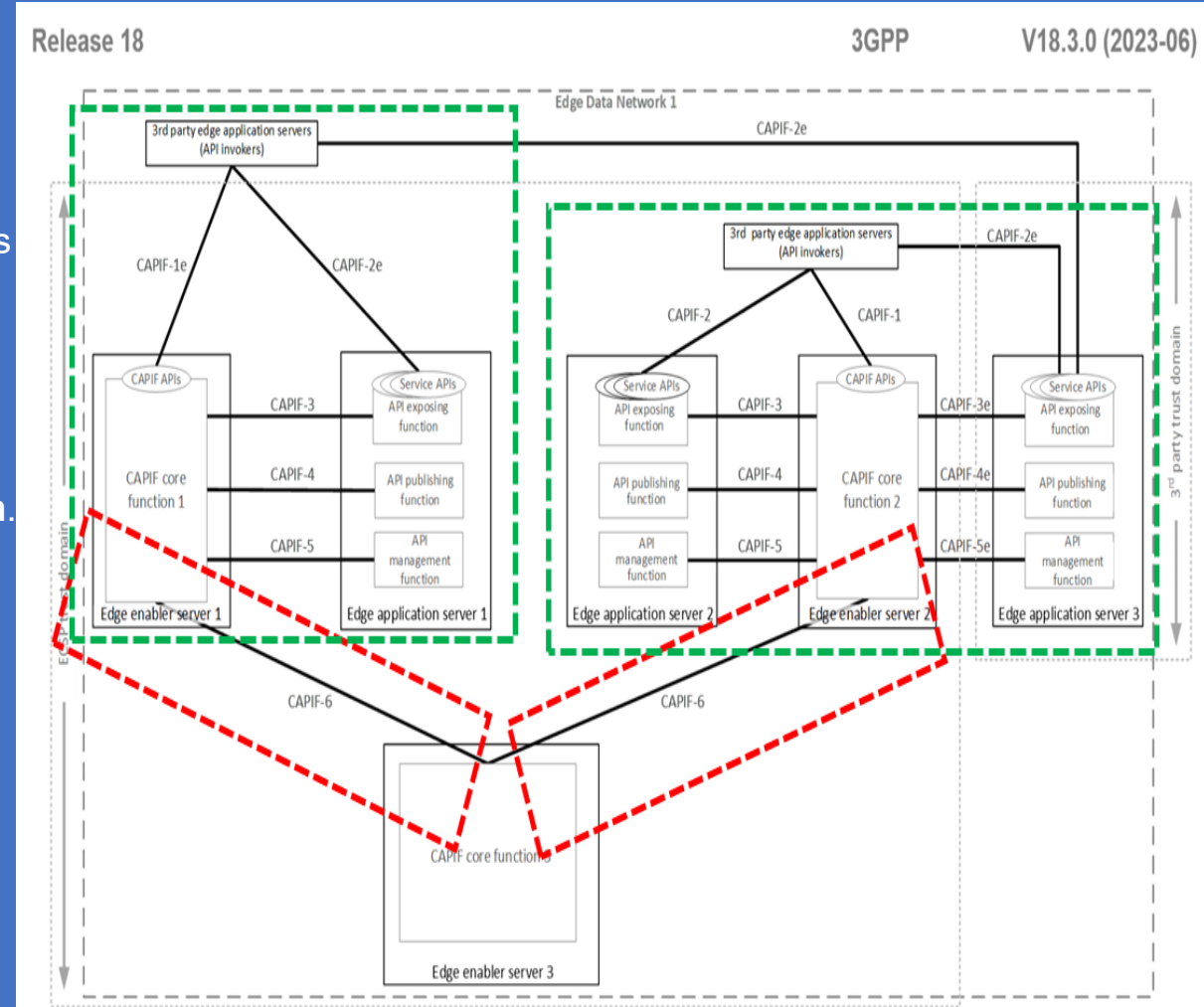


Figure: 5G Architecture enabling Edge Applications Edge Enabler Server (EES) supporting 5G Common API Framework Functions for exposure of EAS Service APIs

2. Further shift of APIs Capabilities to End-Users (Subscribers) from early 5G Rel. 15 FMSS & SEES enabled APIs Capabilities shift from MNOs to 3rd Party ISPs & ICPs

5G Architecture for enabling Edge Applications UE Identifier API

EES exposes UE Identifier API to the EAS and EEC in order to provide an Identifier uniquely identifying a UE.

This API is used by an EAS or EEC to obtain the Identifier of the UE if the EAS or EEC does not have it (e.g. hasn't already cached).

This identifier, called UE ID is used by the EAS to invoke Capability APIs specific to UEs over EDGE-3 and/or EDGE-7 depending on the UE ID type.

The EAS's "direct invocation" of the UE Identifier API of the EES may result in UE ID not found Response (e.g. if the NATed UE's public IPv4 address can't be resolved by the Core Network).

Under such circumstances, the EAS may choose to signal its AC to trigger the UE ID query onto the EEC over EDGE-5.

In turn, the EEC would invoke the EES's UE Identifier API using the UE's CN assigned IP addresses (i.e. IPv4 and/or IPv6) which should result in return of the UE ID to the EEC and from thereon to the AC and the EAS.

NOTE 1: To overcome CN UE's assigned Private IP address reuse issue (e.g. UE's Private IPv4 reuse by 5GC), the EES would need to be pre-configured with the Public IP address range (used by the NAT function over N6) and its associated IP domain.

NOTE 2: EEC retrieval of the UE's IP address from the device is out of scope.

The Figure illustrates the interactions between the EES and the EAS or EEC.

1. The EAS or EEC is authorized to discover and to use UE Identifier API provided by the EES.
2. When the EEC is used to invoke the UE Identifier API with the UE IPv6 address as the input parameter, the UE IPv6 address may or may not be NATed. If NATed however, the IPv6 may not be reused (i.e. assigned to more than one UE simultaneously). If the EEC already has the UE ID (GPSI), and it needs the Edge UE ID to share with an AC/EAS, this procedure can still be used to retrieve Edge UE ID.
3. EAS is considered an AF behind EES (as another AF) and EES is authorized to pass EAS ID instead of its own AF ID when it needs to interact with the NEF's Nnef_UEId_Get (as per "AF specific UE ID retrieval").

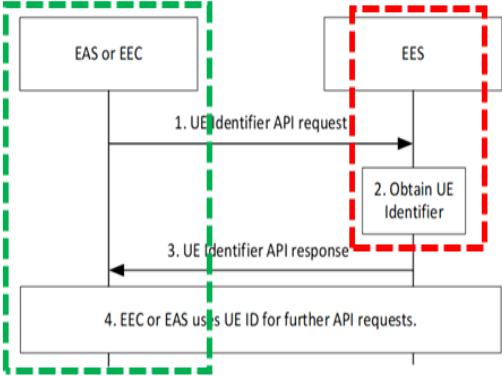


Figure: 5G Architecture for enabling Edge Applications UE Identifier API

Table UE Identifier API request

| Information element | Status | Description |
|--|--------|---|
| User information (NOTE 1) (NOTE 3) | O | Information about the User or UE available in the EAS or EEC, e.g. IP address. |
| UE ID (NOTE 2) (NOTE 3) | O | UE ID in the form of GPSI |
| EAS ID list (NOTE 4) | O | Identifier of the EAS(s) for which the UE IDs are requested for by EAS or EEC given the User information (e.g. IP address). |
| EAS Provider ID | O | Identifier of the ASP that provides the EAS. |
| Security Credentials | M | Security credentials of the EAS or EEC. |
| NOTE 1: This IE is Mandatory when EAS invoke the UE ID API. When EEC invokes the API, if available, this IE contains both UE's private IPv6 address (due to the existence of NAT66) and UE's private IPv4 address. When EAS invokes the API, it may recognize the UE IP address is a public IP address different from the actual UE IP address (private IP address), i.e., the UE is behind a NAT, and should therefore include the Port Number and associated IP address as part of the User information. | | |
| NOTE 2: This IE is used when invoked by the EEC and if the EEC have the UE ID already in a form not desired to be shared with the EAS. | | |
| NOTE 3: At least one of them shall be present. | | |
| NOTE 4: This IE is Mandatory when EAS invoke the UE ID API. | | |

Table UE Identifier API response

| Information element | Status | Description |
|---------------------|--------|--|
| Successful response | O | Indicates that the UE identifier request was successful. |
| > UE ID list | M | List of all the UE IDs Identifier uniquely identifying the UE(s). |
| >> UE ID | M | AF-specific UE ID or Edge UE ID |
| >> UE ID type | M | Indication whether the UE ID is CN assigned AF-specific UE ID or Edge UE ID. |
| >> EAS ID | O | It is present if the EAS ID was provided in the request (see EAS ID list |
| Failure response | O | Indicates that the UE identifier request failed. |
| > Cause | O | Indicates the cause of UE identifier request failure |

2. Further shift of APIs Capabilities to End-Users (Subscribers) from early 5G Rel. 15 FMSS & SEES enabled APIs Capabilities shift from MNOs to 3rd Party ISPs & ICPs

5G Architecture for enabling Edge Applications on UE AC EDGE-5 APIs

The *Edge Enabler Client* (EEC on UE) exposes **EDGE-5 APIs** corresponding to **EEC's Capabilities**, for the **AC** to request **EEC's Services** for Edge enablement. Using these **APIs**, **ACs** request the **EEC** for **EEL services**.

EDGE-5 APIs include one-time Request/Response Operations for:

- **EAS discovery**,
- **Retrieval of UE ID and**
- **ACR Operations**.

The **AC** can request for an **AC subscription**.

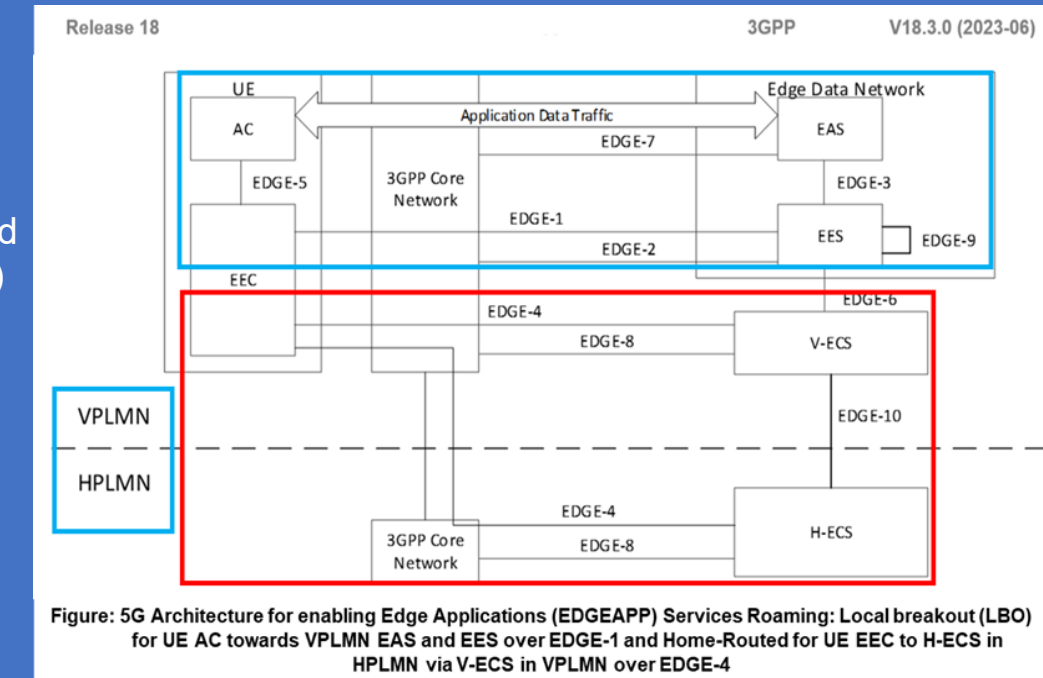
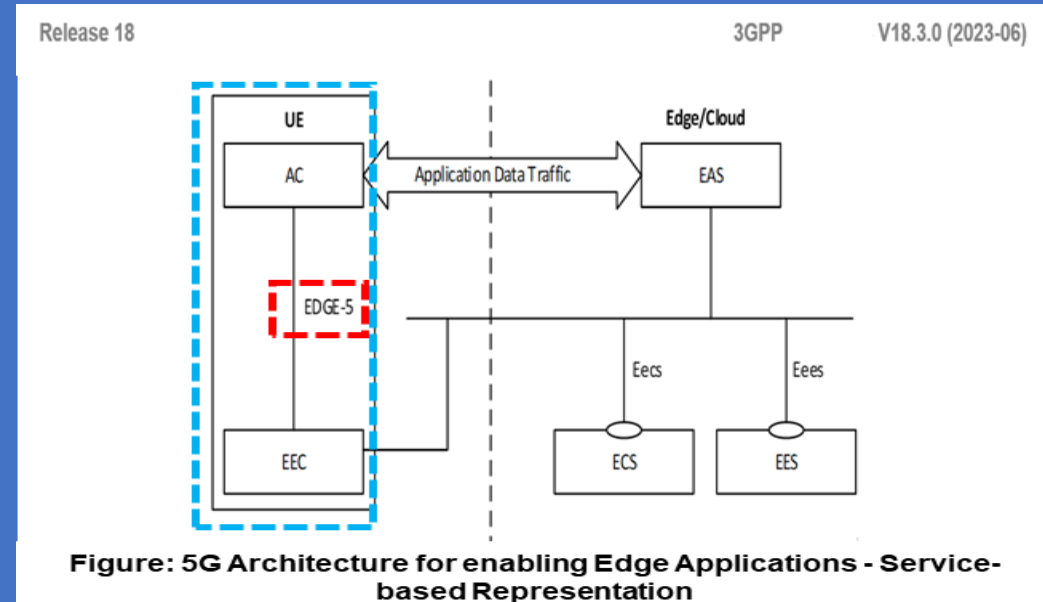
The **EEC** creates the Subscription and when required, performs necessary Operations such as **EAS discovery**, **ACR** etc., delivering notifications to the **AC** as required.

NOTE: **EEC** can initiate any **EDGE-1** or **EDGE-4** Operation without receiving a Request or without receiving **AC** related information from the **AC**.

User's Authorization/Consent as well as **AC's** Authorization in invoking Functions exposed by **EEC (to AC)** which in turn relies on Functions exposed by the Network (e.g. Location) via **EES/NEF** is specified.

EDGE-5 specified Procedures are:

- Registration;
- EAS discovery;
- ACR trigger request;
- EEC services subscription;
- UE ID request;



2. Further shift of APIs Capabilities to End-Users (Subscribers) from early 5G Rel. 15 FMSS & SEES enabled APIs Capabilities shift from MNOs to 3rd Party ISPs & ICPs

5G Architecture for enabling Edge Applications Capability exposure APIs for enabling Edge Applications

The Figure shows the Capability Exposure for enabling Edge Applications.

The Capability Exposure for enabling Edge Applications includes:

- 3GPP Core Network (i.e. 5GC, EPC),
- 5G Architecture for enabling Edge Applications (EDGEAPP)
 - Edge Configuration Server (ECS)
 - Edge Enabler Server (EES)

Capabilities Exposure, to fulfil the needs of the Edge Service Operations.

The Capability Exposure Functionality is utilized by the Functional Entities (i.e. EES, EAS and ECS) depicted in the Figure showing the Architecture for enabling the Edge Applications Capability Exposure APIs.

NOTE: The Edge Enabling Layer (EEL) also supports the exposure of EAS Service APIs using 5G Common API Framework (CAPIF), which is not explicitly depicted in the Figure.

Table : APIs provided by the ECS

| API Name | Known Consumers |
|--------------------------|-----------------|
| Eecs_ServiceProvisioning | EEC |
| Eecs_EESRegistration | EES |
| Eecs_TargetEESDiscovery | EES |

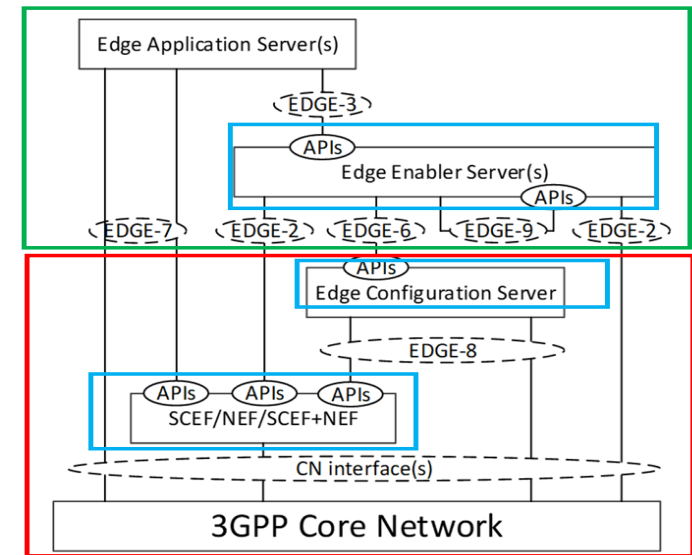


Figure: 5G Architecture Capability Exposure APIs for enabling Edge Applications

Table : APIs provided by the EES

| API Name | Known Consumers |
|---------------------------|-----------------|
| Eees_EECRegistration | EEC |
| Eees_EASRegistration | EAS |
| Eees_EASDiscovery | EEC |
| Eees_ULocation | EAS |
| Eees_ACRManagementEvent | EAS |
| Eees_AppClientInformation | EAS |
| Eees_ULIdentifier | EEC, EAS |
| Eees_SessionWithQoS | EAS |
| Eees_TargetEASDiscovery | EAS, EES |
| Eees_AppContextRelocation | EEC, EAS |
| Eees_ACREvents | EEC |
| Eees_EELManagedACR | EAS |
| Eees_EECContextPull | EES |
| Eees_EECContextPush | EES |
| Eees_SelectedTargetEAS | EAS |
| Eees_ACRStatusUpdate | EAS |

NOTE: The event exposure related APIs (e.g. Eees_EASDiscovery and Eees_ACREvents) can be realized as single event subscription API.

Annex-1 Mobile Networks to evolve from:

a Design that offers "Best-effort Services

to

a Design that offers Performance and User Experience Guarantees

Capabilities related to e.g.:

When a **Multi-access (MA) PDU Session** is established, the Network may provide the UE with **Measurement Assistance Information** to enable the UE in determining which measurements shall be performed over both Accesses, as well as whether measurement reports need to be sent to the Network.

- Measurement Assistance Information shall include the addressing information of **a Performance Measurement Function (PMF)** in the UPF, the UE can send PMF protocol messages incl.:
- Messages to allow for **Round Trip Time (RTT)** Measurements: the "**Smallest Delay**" steering mode is used or when either "**Priority-based**", "**Load-Balancing**" or "**Redundant**" steering mode is used with RTT threshold value being applied;
 - Messages to allow for **Packet Loss Rate (PLR)** measurements, i.e. when steering mode is used either "**Priority-based**", "**Load-Balancing**" or "**Redundant**" steering mode is used with **PLR** threshold value being applied;
 - Messages for reporting Access Availability/Un-availability by the UE to the UPF.
 - Messages for sending **UE-assistance Data** to **UPF**.
 - Messages for sending "**Suspend Traffic Duplication**" and "**Resume Traffic Duplication**" from **UPF** to **UE** to "**suspend**" or "**resume**" traffic duplication as defined in **5GS Architecture**.

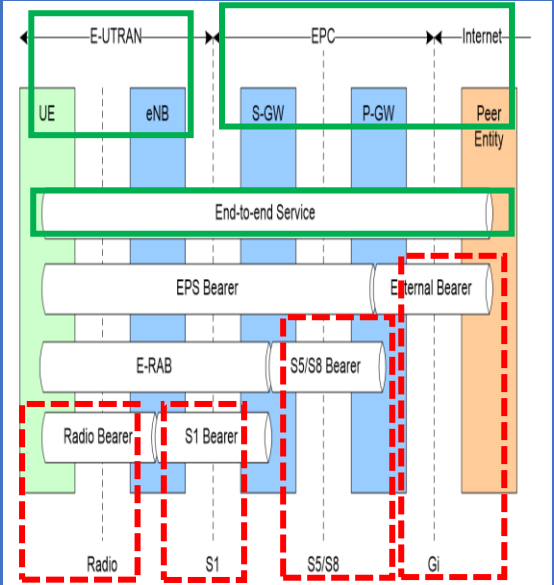
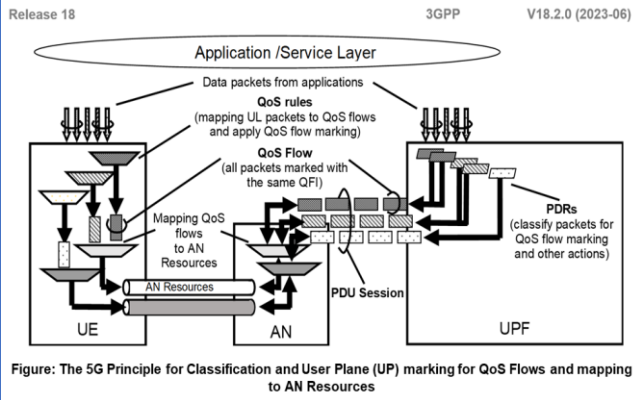


Figure : EPS Bearer Service Architecture

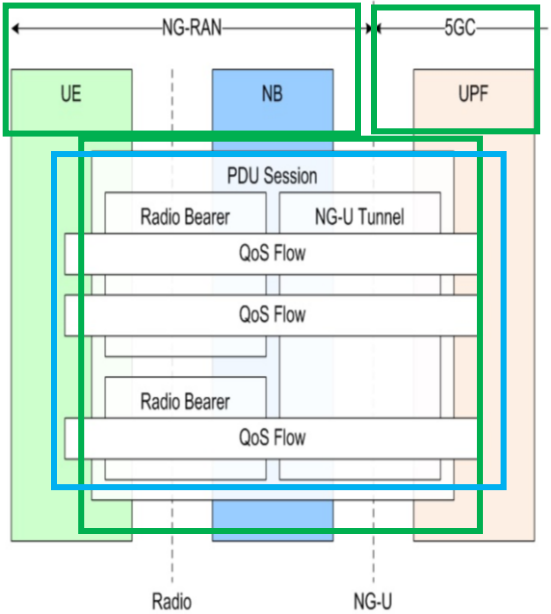
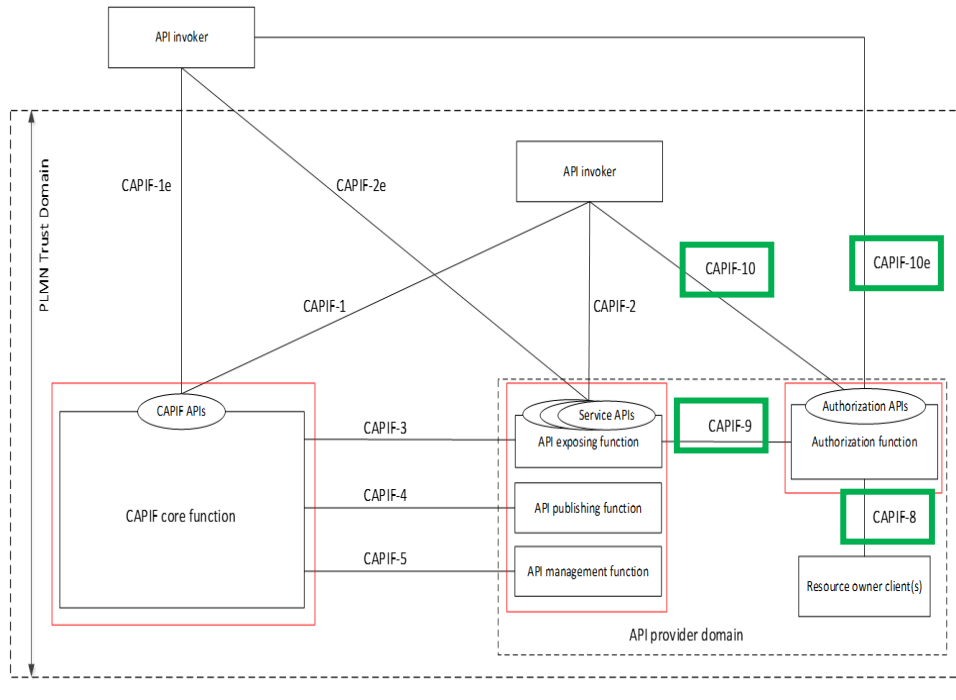
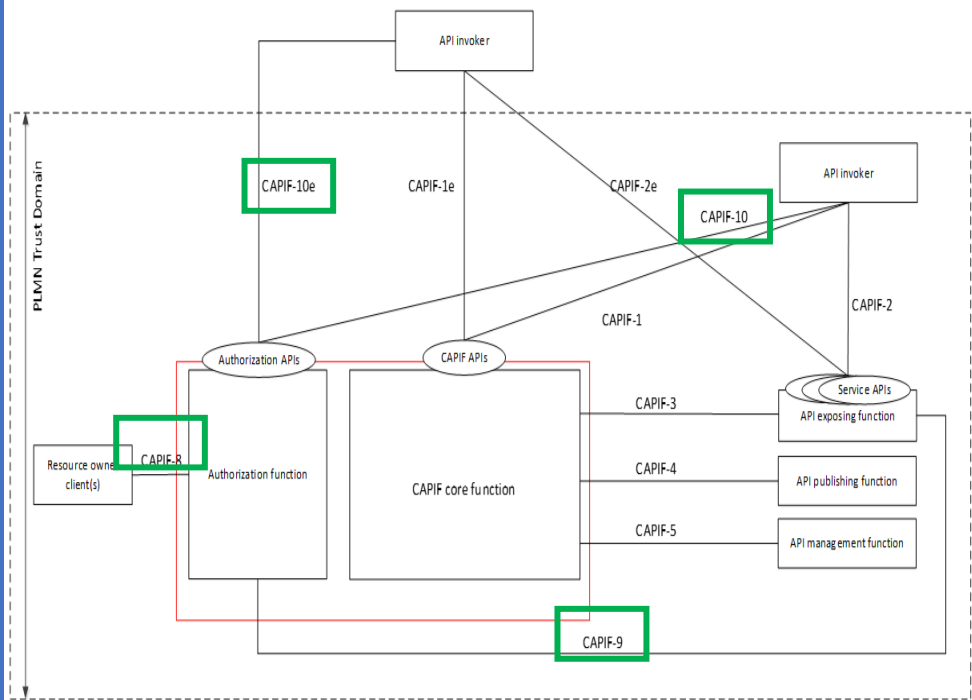
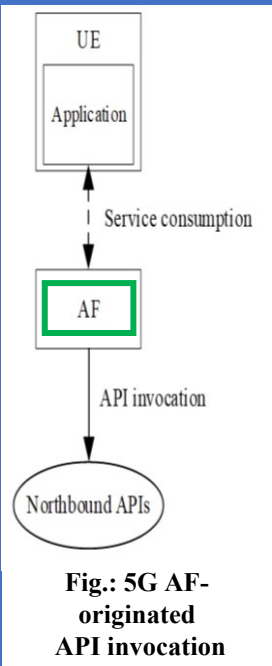
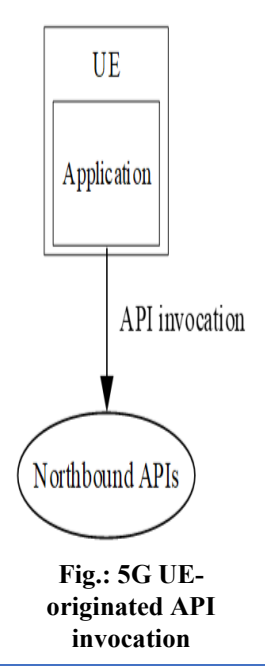


Figure: 5G CN NG-RAN Bearer Services QoS Architecture

Annex- 2: 5G Advanced enhanced API Core Function (CAPIF) Deployment Options with API Authorization Function and Service APIs

5G Advanced release presented evolved enhancements in 5G Common API Framework (CAPIF) and 5G specified Application Enablement Frameworks, e.g. Service Enabling Architecture Layer (for Vertical Layer (VAL) Applications), Architecture for developing Applications on the Edge (together with enhancement on the System for the respective enhancements for Edge Computing), VAL (Vertical Enabler Layers to support access to specified so-called "Subscriber-aware Northbound APIs, whose requirements are also specified in 3GPP 5G Advanced 5G Service Requirements (Rel. 19). As seen below, it is (standard) specified for the 5G System to be able to provide either (1) an UE with Secure Access to APIs (e.g. triggered by an Application that is not visible to the 5G System), by "authenticating" & "authorizing the UE" or (2) to use the 5G AF (so called "AF-originated API invocation), to utilize the AF ability to invoke the northbound APIs, & the Application on the UE "consumes" the Service from the AF. A Business Relationship can be applied to both AF- & UE-originated API Invocation scenarios, as the API Invoker can either be an Application on the UE or the AF. The API invoker has Service Agreement with a 5G API Core Function (CAPIF) Provider/Supplier, & the APIs Provider/Supplier provides APIs associated with the Resource Owner (Subscriber). The 5G API Core Function (CAPIF) Provider & the API Provider can be part of the same organization (e.g. PLMN Operator). When the 5G API Core Function (CAPIF) Provider is a PLMN Operator, the Resource Owner may be a Subscriber of the PLMN. In the current release, both the 5G API Core Function (CAPIF) Provider & the API Provider should belong to the same organization (e.g., PLMN operator). The Resource Owner Client(s) (ROCs) are Application Clients used by End-Users or Subscribers of the API Provider Domain's Service Provider (SP). The Resource Owner Client(s) (ROCs) interacts with the "Authorization" Function via CAPIF-8. The Resource Owner communicates with the Authorization Function to "provide & revoke" Resource Owner Consent. The Resource Owner interactions are supported via a Resource Owner Client, which is a Client-side Entity. Triggering the Resource Owner Client to provide "Authorization" is not supported via CAPIF 8. The API Exposing Function (e. g NEF) acts as a Resource Owner Consent Enforcement Point as specified in 3GPP 5G & interacts with the "Authorization" Function via CAPIF-9. The API Exposing Function can retrieve the Resource Owner Consent Parameters from the Authorization Function. The API invoker interacts with "Authorization Function via CAPIF-10/CAPIF-10e.





Remarks & Questions?