

5G System Architecture selected Exposure Capabilities enhancements

for

5G Services

Ike Alisson

2023 - 08- 10

Rev PA06



Table of Contents

1. **5G System Network Capability External Exposure**
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**
- 3.

Annex

1. **Shift from 2G/3G/4G "Best-effort Services" to 5G User Experience & Performance Services**
2. **The main difference(s) between the standard DevOps SaaS (SW-as-a-Service) & the Telecom aaP (as- a-Platform) Models**



1. 5G System Network Capability External Exposure

The 5G Network Exposure Function supports external exposure of Capabilities of Network Functions (NFs).

External exposure can be categorized as:

1. Monitoring Capability,
2. Provisioning Capability,
3. Policy/Charging Capability,
4. Analytics Reporting Capability and
5. Member UE Selection Capability.

1. **The Monitoring Capability** is for monitoring of specific event for UE in 5G System and making such monitoring events information available for external exposure via the 5G Network Exposure Function

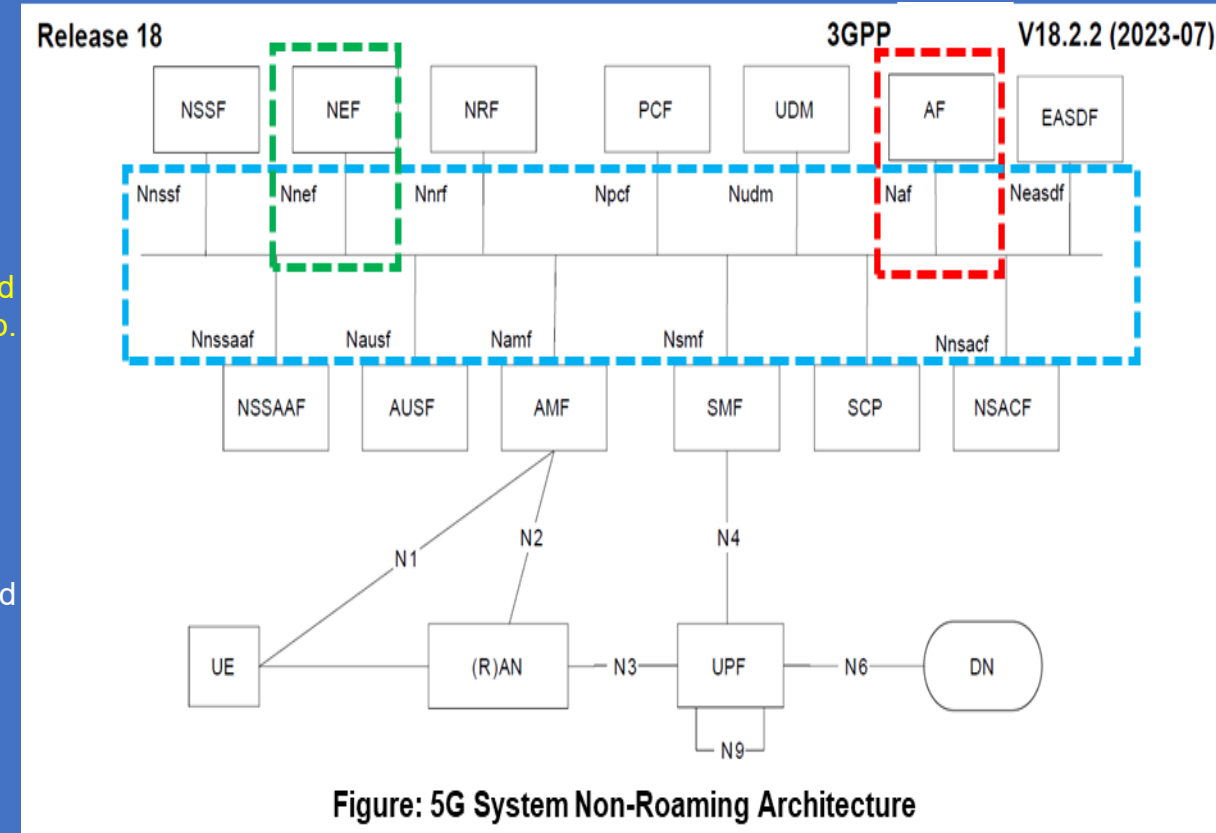
The Monitoring Capability also allows AF to subscribe to the Group Status changes for a Group, either a 5G VN Group or a Group configured by OA&M. In this case the AF is notified if the Group Member list is updated or a Group Member is no longer subscribed to the group.

2. **The Provisioning Capability** is for allowing external party to provision of information which can be used for the UE in 5G System.

3. The **Policy/Charging Capability** is for handling Access and Mobility Management, QoS and Charging Policies for the UE based on the request from external party.

4. The **Analytics Reporting Capability** is for allowing an external party to fetch or subscribe/unsubscribe to Analytics information generated by 5G System.

5. **The Member UE Selection Capability** is for allowing an external party to acquire one or more list(s) of Candidate UE(s) (**among the List of Target member UE(s) provided by the AF**) and additional information that is based on the assistance information generated by 5G System based on some defined filtering criteria.



1. 5G System Network Capability External Exposure

The 5G Network Exposure Function supports external exposure of Capabilities of Network Functions (NFs).

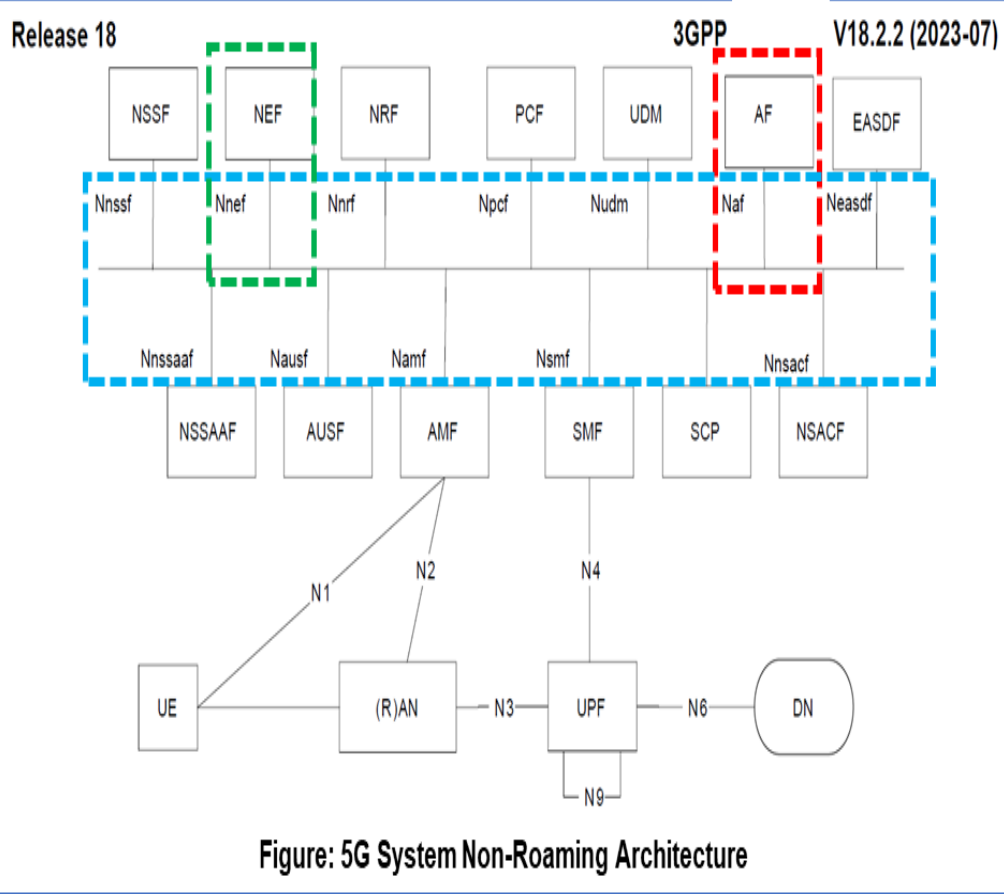
5. The Member UE Selection Capability is for allowing an external party to acquire one (1) or more list(s) of Candidate UE(s) (**among the List of Target member UE(s) provided by the AF**) and additional information that is based on the assistance information generated by 5G System based on some defined filtering criteria.

An AF may only be able to identify the target UE of an AF Request for External Exposure of 5G Core Capabilities (**e.g. Data Provisioning or for Event Exposure for a specific UE**) by providing the **UE's Address information**.

In this case, there is first needed to **retrieve the Permanent Identifier of the UE** before trying to fulfil the AF request.

The 5GC may determine the **Permanent identifier of the UE**, as described based on:

- The **Address of the UE as provided by the AF**; this may be an **IP Address or a MAC Address**;
- **The Corresponding DNN and/or S-NSSAI information**: this may have been provided by the AF or determined by the NEF based on the requesting AF; this is needed if the UE address is an IP address.



1. 5G System Network Capability External Exposure

The 5G Network Exposure Function supports external exposure of Capabilities of Network Functions (NFs).

The 5GC exposure may provide an AF specific UE Identifier to the AF:

- that has explicitly requested a translation from the address of the UE to a unique UE identifier (via Nnef_UEId service); or
- that has implicitly requested a translation from the Address of the UE to a AF specific UE Identifier by requesting external exposure about an individual UE identified by its address.

The AF may have its own means to maintain the AF specific UE Identifier through, e.g. an AF session.

After the retrieval of an AF specific UE Identifier the AF shall not keep maintaining a mapping between this identifier and the UE IP address as this mapping may change.

The AF specific UE Identifier shall not correspond to a MSISDN; it is represented as a GPSI in the form of an External Identifier.

When used as an AF specific UE identifier, the External Identifier provided by the 5G CN shall be different for different AF.

NOTE 1: This is to protect User Privacy.

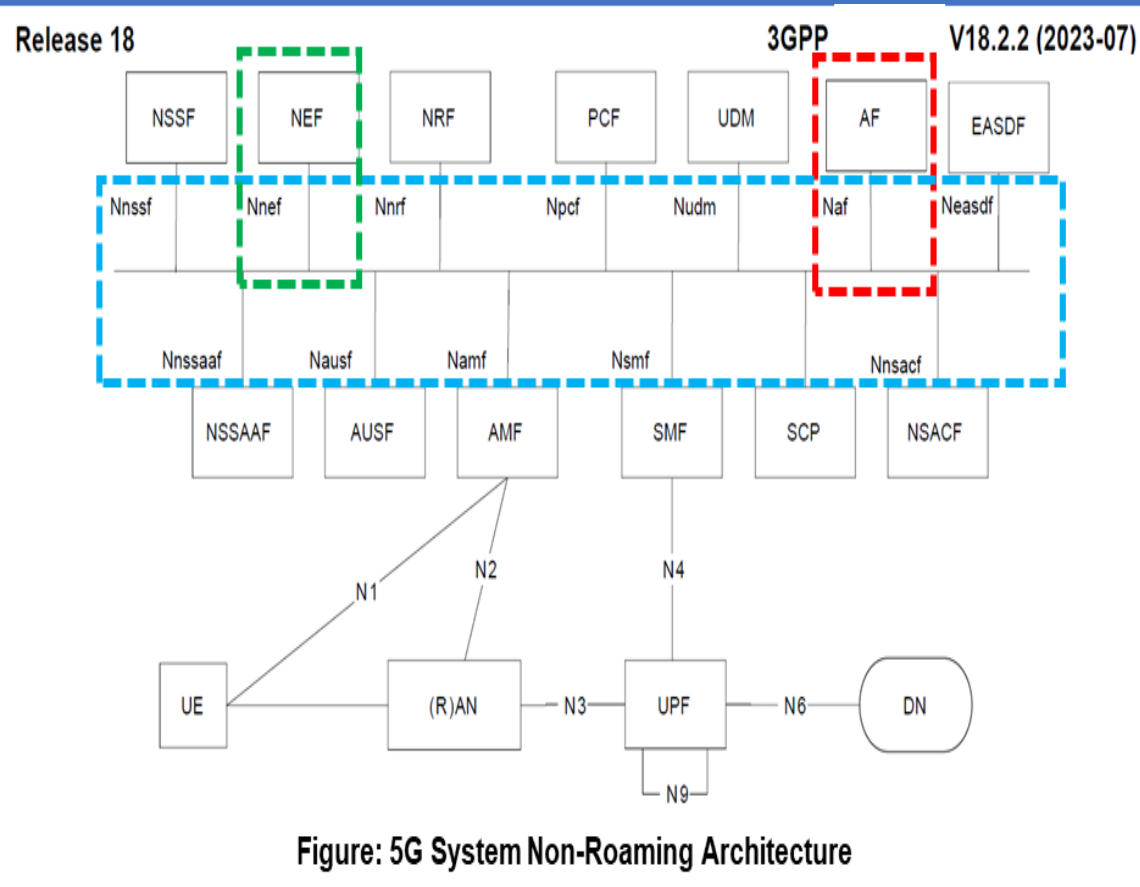
NOTE 2: The AF specific UE identifier is ensured to be unique across different AFs

NOTE 3: Based on Policies, the 5GS Exposed Functionality can be configured to enforce restriction on the usage of AF specific UE Identifier (e.g. rejection of a Service Request from AF not authorized to use the UE Identifier).

5G System Data Collection from an AF

An NF that needs to collect Data from an AF may subscribe/unsubscribe to notifications regarding Data Collected from an AF, either "directly from the AF" or via 5GC.

The Data Collected from an AF is used as input for Analytics.



Group Attribute Provisioning

A Group may be a 5G VN Group managed as defined in 5G System Architecture, as well as a Group configured by OA&M.

An AF may provision attributes for a Group:

- **LADN Service Area**, the LADN Service Area is consisted of Tracking Area (TA) Identities or Geographical Information, it is applicable to each UE member within the Group and for a specific DNN and S-NSSAI.
 - The AF request additionally contains the LADN Service Area as part of DNN & S-NSSAI specific Group Parameters, & the LADN Service Area is stored in UDR as Subscription Data & delivered to AMF. If the AMF receives the LADN Service Area for a Group, **the AMF configures the DNN of the group as LADN DNN.**
 - If the AF provides the LADN Service Area in the form of Geographical Information, the NEF maps the Geographical Information to a List of TAs before sending the Service Area to the UDM. LADN per DNN and S-NSSAI as defined in clause 5.6.5a is applicable for enforcement of LADN service area.
- **QoS**, the QoS refers to 5QI, ARP & 5QI Priority Level as defined in 5G System Architecture and it is applicable to each UE Member within the Group & for a specific DNN and S-NSSAI.
 - The AF request additionally contains the QoS for the Group, and the UDM stores such QoS in the UDR & uses such QoS to set 5GS Subscribed QoS Profile in Session Management Subscription data for each UE within the Group.
 - When a UE belongs to Multiple Groups simultaneously, the strictest QoS Profile among Groups the Group Member belongs to is selected.

NOTE: In the case that the strictest QoS profile can not be fulfilled, the next strictest QoS Profile is selected. Mechanisms as defined, are used to enforce the 5GS Subscribed QoS profile for each UE within a Group, thus to support enforcement of QoS for a Group.

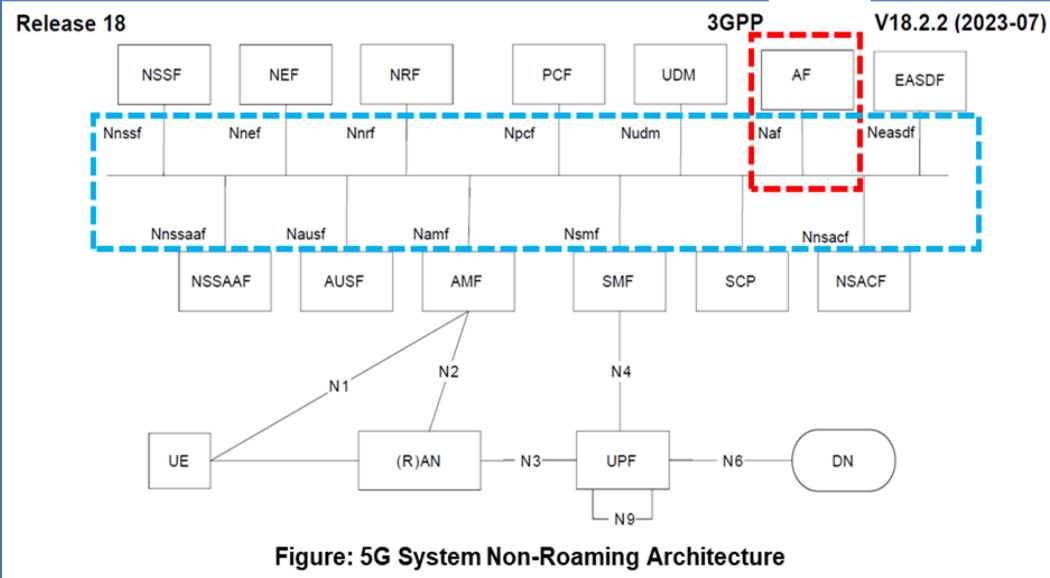


Figure: 5G System Non-Roaming Architecture

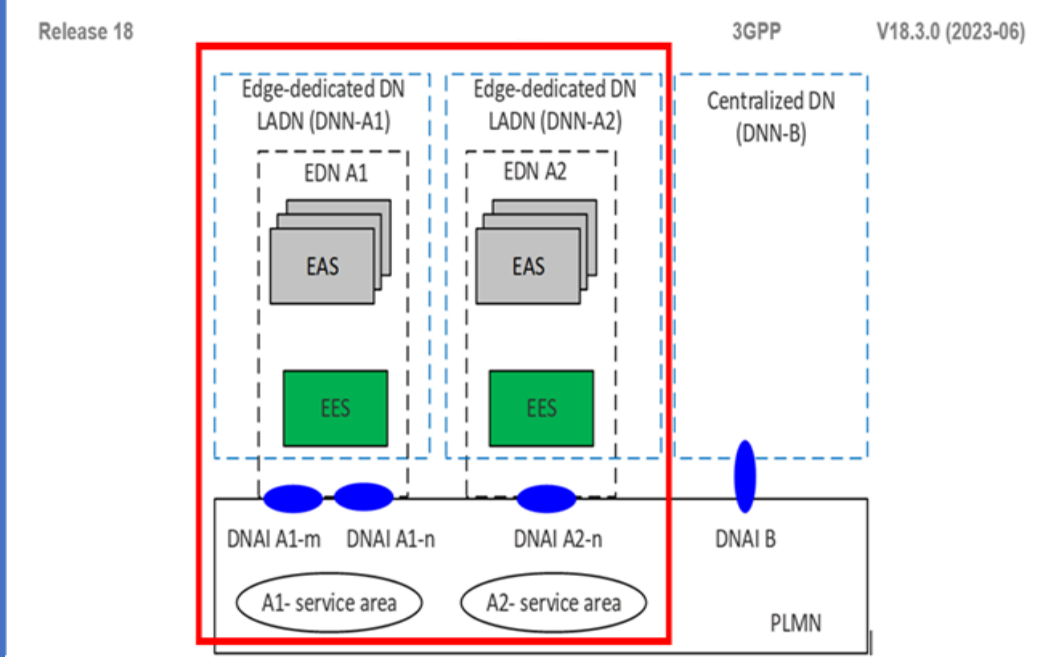


Figure: 5G Architecture for enabling Edge Applications Data Network (DN) Deployment Model for use of Local Area Data Network (LADN)

1. 5G System Network Capability External Exposure support of DNN and S-NSSAI specific Group Parameters

Group Attribute Provisioning

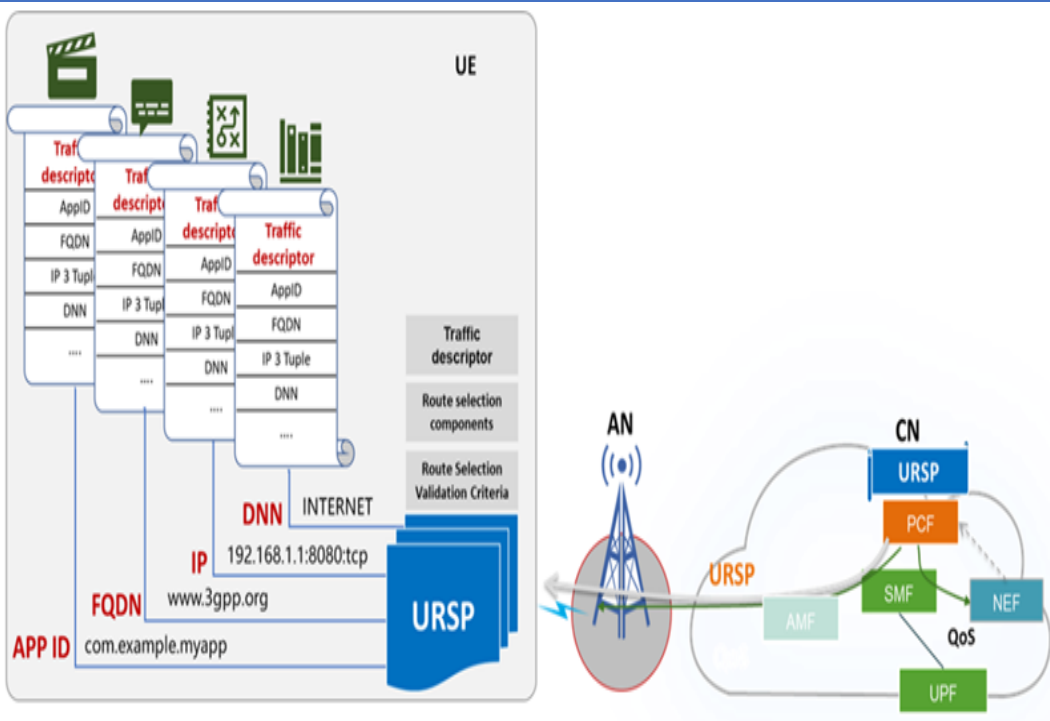
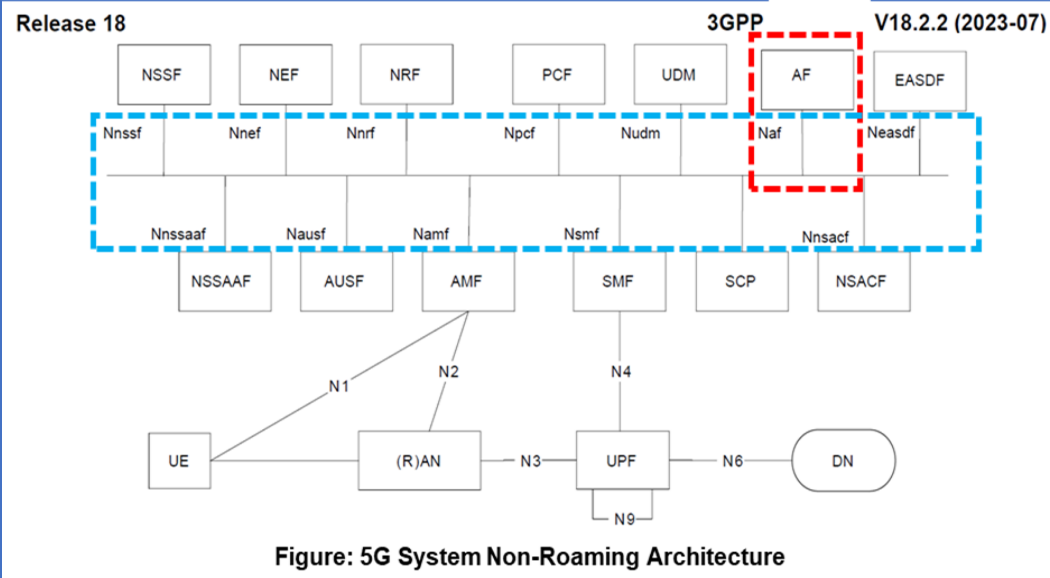
A Group may be a 5G VN Group managed as defined in 5G System Architecture, as well as a Group configured by OA&M.

An AF may provision attributes for a Group:

Support Change of PDU Session Type for a group of UEs

The Service specific Parameters Provisioning Procedure as defined in 5GS Procedures is applicable for updating of PDU Session Type of the URSP for a Group of UEs.

When the UE receives the URSP Rules, the UE re-evaluates the URSP Rules, and may release the PDU Session and re-establishes the PDU Session with the "high precedence" PDU Session type in the URSP rules.



1. 5G System Network Capability External Exposure support of User Plane (UP) Direct 5GS Information Exposure

In order to expose Network Information, the User Plane (UP) direct 5GS Information Exposure Function may be applied.

The User Plane (UP) direct 5GS Information Exposure Function allows the UPF to report the Network Information directly to Consumer based on the instructions provided by SMF.

NOTE: In the Scenario of Edge Computing as described in 5GS enhancements for Edge Computing, the "Consumer" can be the L-NEF or Local AF, when the Local AF is trusted.

When the Exposed Network Information is provided by the UPF, the PSA UPF may be instructed to report Network Information via Nupf_EventExposure service (e.g. directly to an AF, i.e. bypassing the SMF and the PCF);

or the UPF may be instructed to report the information to the Consumer via SMF/PCF/NEF, as described in 5GS Architecture specification.

When the exposed Network Information is provided by the NG-RAN, the NG-RAN may be instructed by the SMF to report the information via the GTP-U tunnel(s) between the NG RAN and PSA UPF, as defined.

The User Plane Direct 5GS Information Exposure may be used for exposing the following information:

- QoS Monitoring information
- TSC Management Information

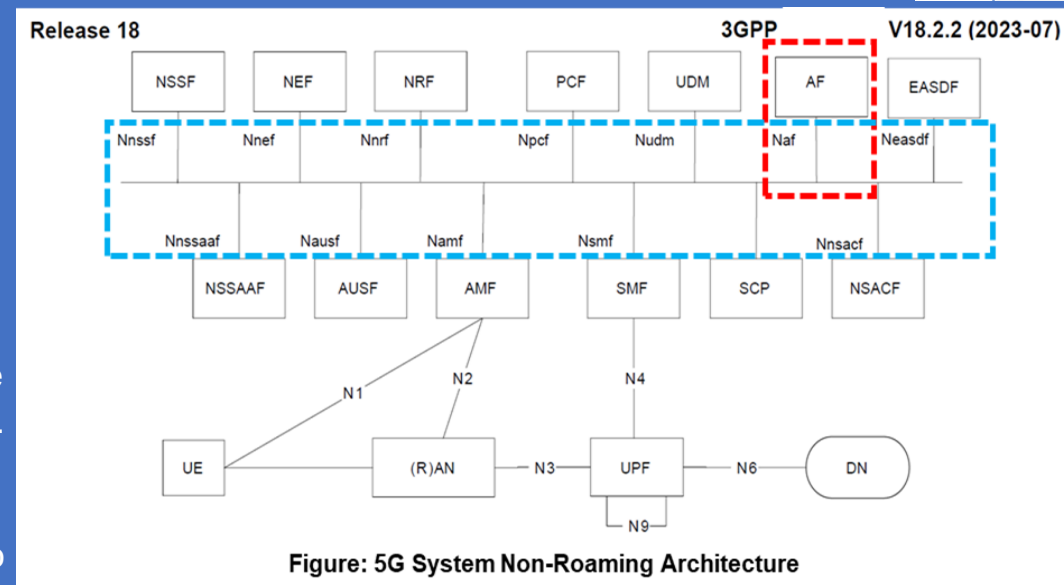


Figure: 5G System Non-Roaming Architecture

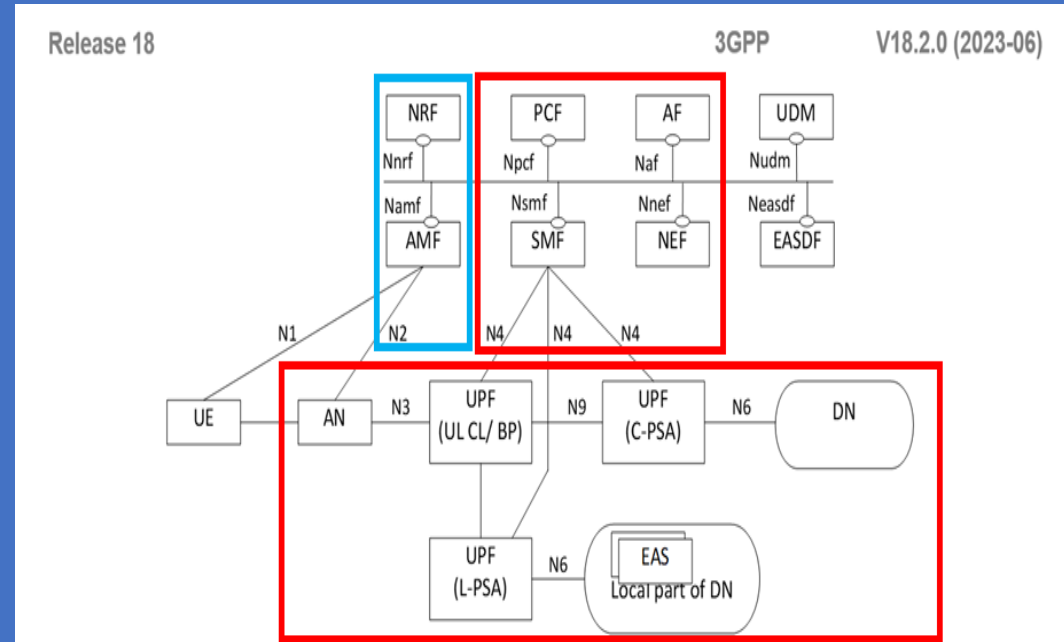


Figure: 5G System Architecture with UL CL/BP access to Edge Application Server (EAS) for Non-Roaming Scenario

1. 5G System Network Capability External Exposure Provisioning of Traffic Characteristics and Monitoring of Performance Characteristics for a Group

5G CN Provisioning Capability allows an AF to perform Provisioning of Traffic Characteristics and Monitoring of Performance Characteristics for a Group of UEs.

NOTE : The AF may use Application Layer Functionalities to handle Requests for UE-to-UE Traffic as defined by 3GPP.

The 5G CN determines whether or not to invoke the **TSCTSF** in the same way as for **AF Session with required QoS Procedure**.

In the case that the TSCTSF is used, the **TSCTSF** receives the **AF requested QoS Information from the 5G CN**.

In the case that TSCTSF is not used, the AF request is handled as described in 5GS Procedures and Policies.

When the TSCTSF receives the AF requested QoS information from 5G System exposure or the PCF(s) receive the AF requested QoS information from UDR, the TSCTSF or PCF (s) manage the AF requested QoS information for each UE Group member within the Group as follows:

-
-
-

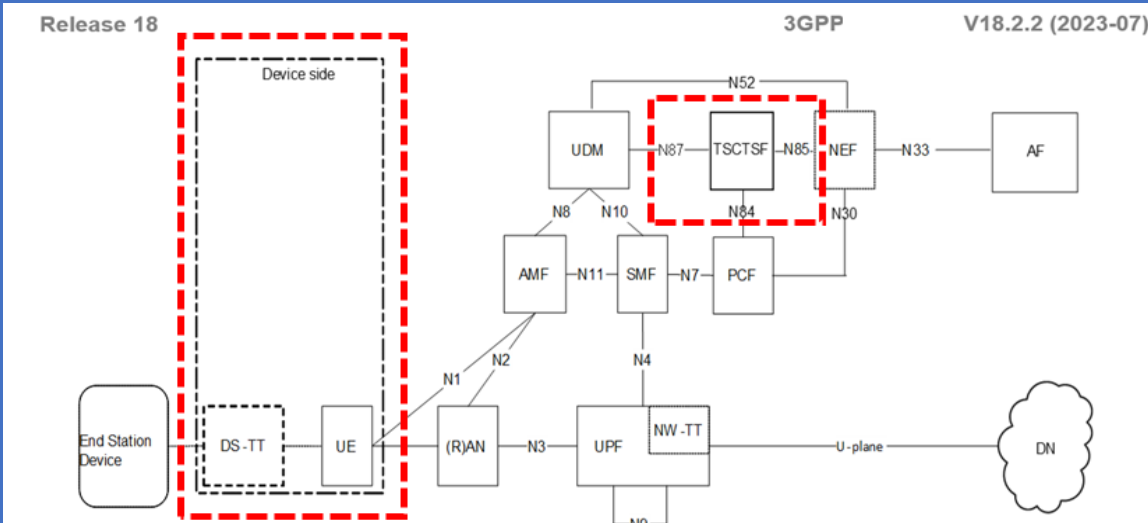


Figure: 5G System Architecture enabling Time Sensitive Communication and Time Synchronization Function (TSCTSF) Services

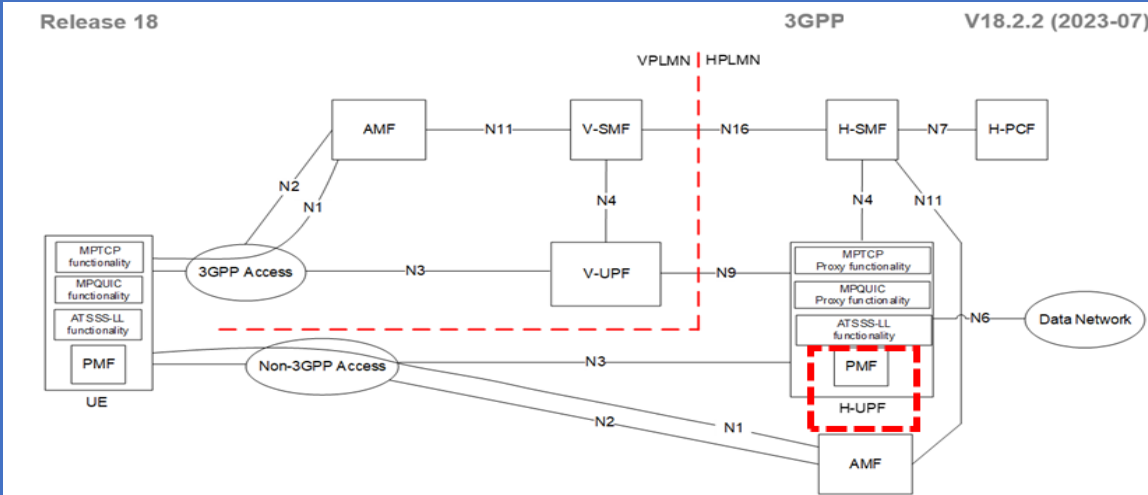


Figure: 5G System with Home-routed Architecture for ATSSS (Access Traffic Steering, Switching, Splitting) support with UE registered to different PLMNs

Note: The Figure shows the 5G System Architecture when the UE is registered to a VPLMN over 3GPP Access and to HPLMN over Non-3GPP Access (i.e. the UE is registered to different PLMNs). In this case, the MPTCP Proxy Functionality, the MPQUIC Proxy Functionality and the PMF (Performance Management Function) are located in the H-UPF.

Release 18

1. 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. 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).	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).		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 clause 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. 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:

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		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			

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

Business Relationships in 5G Common API Framework (CAPIF) applied to:
 - **Application Function (AF on UE) - originated API Invocations**
 - **UE - originated API Invocations**

Business Relationship between

- the User (UE),
- the AF and the NAPS 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 in the 5G Common API Framework (CAPIF) **Business Relationship**, thus the **Business Relationship should be updated to include the Resource Owner**.

The Figure shows the typical business relationship 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 **5G Common API Framework (CAPIF) Provider** and the **API Provider** can be part of the same organization (e.g. PLMN Operator).

When the 5G Common API Framework (CAPIF) Provider is a PLMN Operator, the "Resource Owner" may be a "Subscriber" of the PLMN.

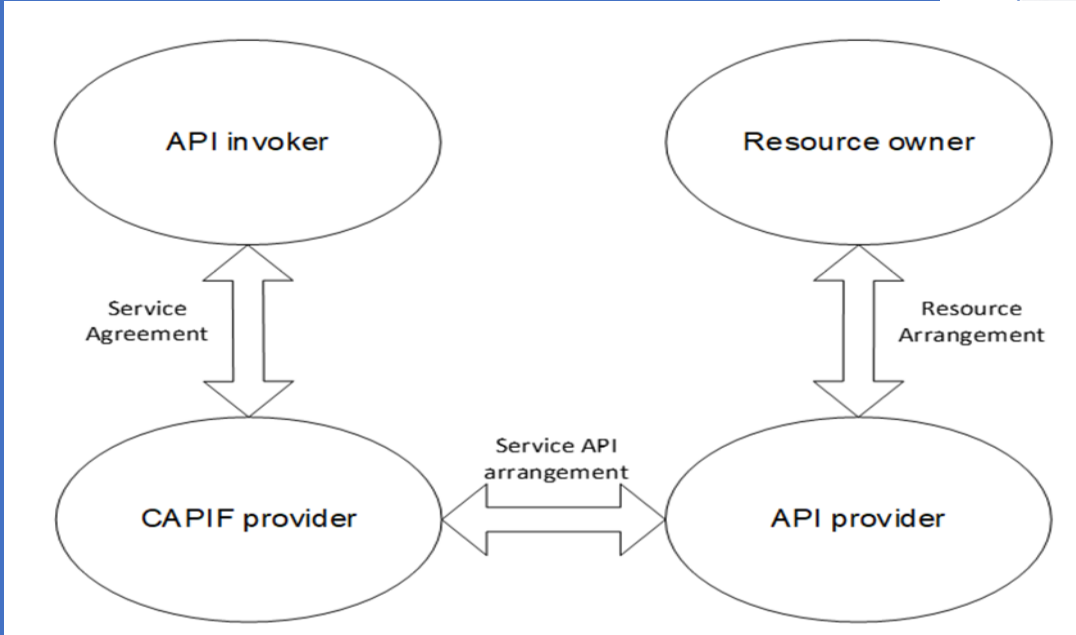


Figure: Business Relationships in 5G CAPIF applied to AF- originated and UE-originated API invocations

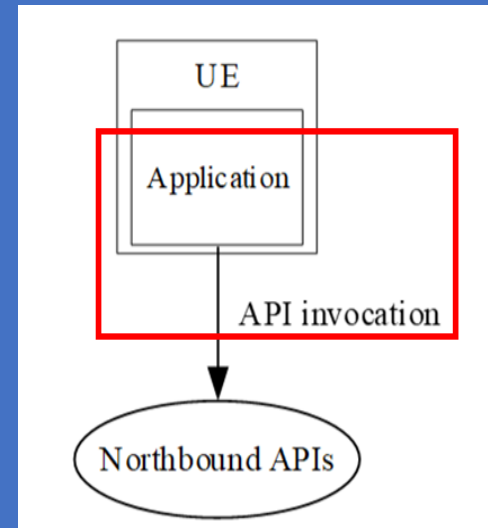


Figure: 5G UE-originated API invocation

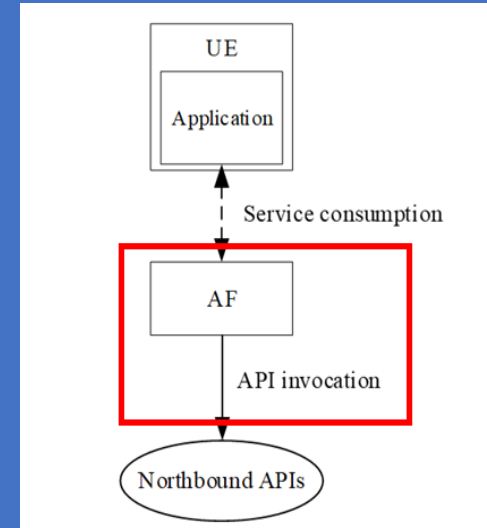


Figure: 5G AF-originated API invocation

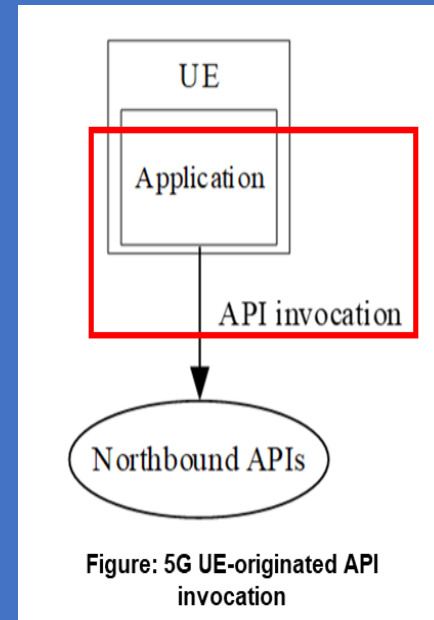
2. Further shift of APIs Capabilities to End-Users (Subscribers) from early 5G Rel. 15 FMSS & SEES enabled APIs Capabilities shift from MNOs to 3rd Party ISPs & ICPs

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.

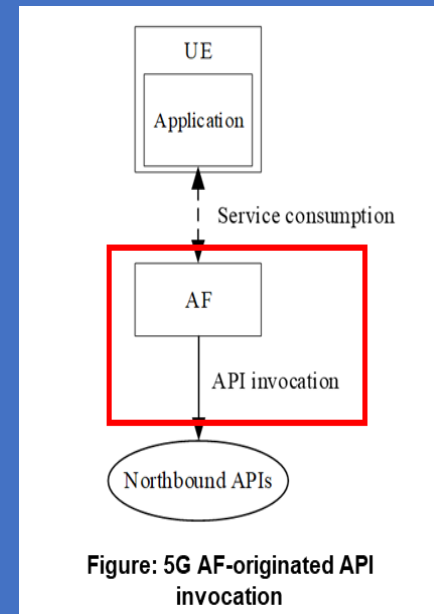
From CAPIF point of view, the Application on the UE, plays the role of the "API Invoker", as defined in 5G Common API Framework (CAPIF).



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.



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

Reference Point Representation of 5G Common API Framework (CAPIF) Functional Model with enhancements to support "Resource Owner" API Invocation (Subscriber and/or UE) as e.g.:

- "Provide"/"Revoke User Consent" (via specified CAPIF-8).

The Resource Owner Client(s) are:

- Application Clients used by End-Users or
- Subscribers of the API Provider Domain's Service Provider.

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

The Resource Owner communicates with the Authorization 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.

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** 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.

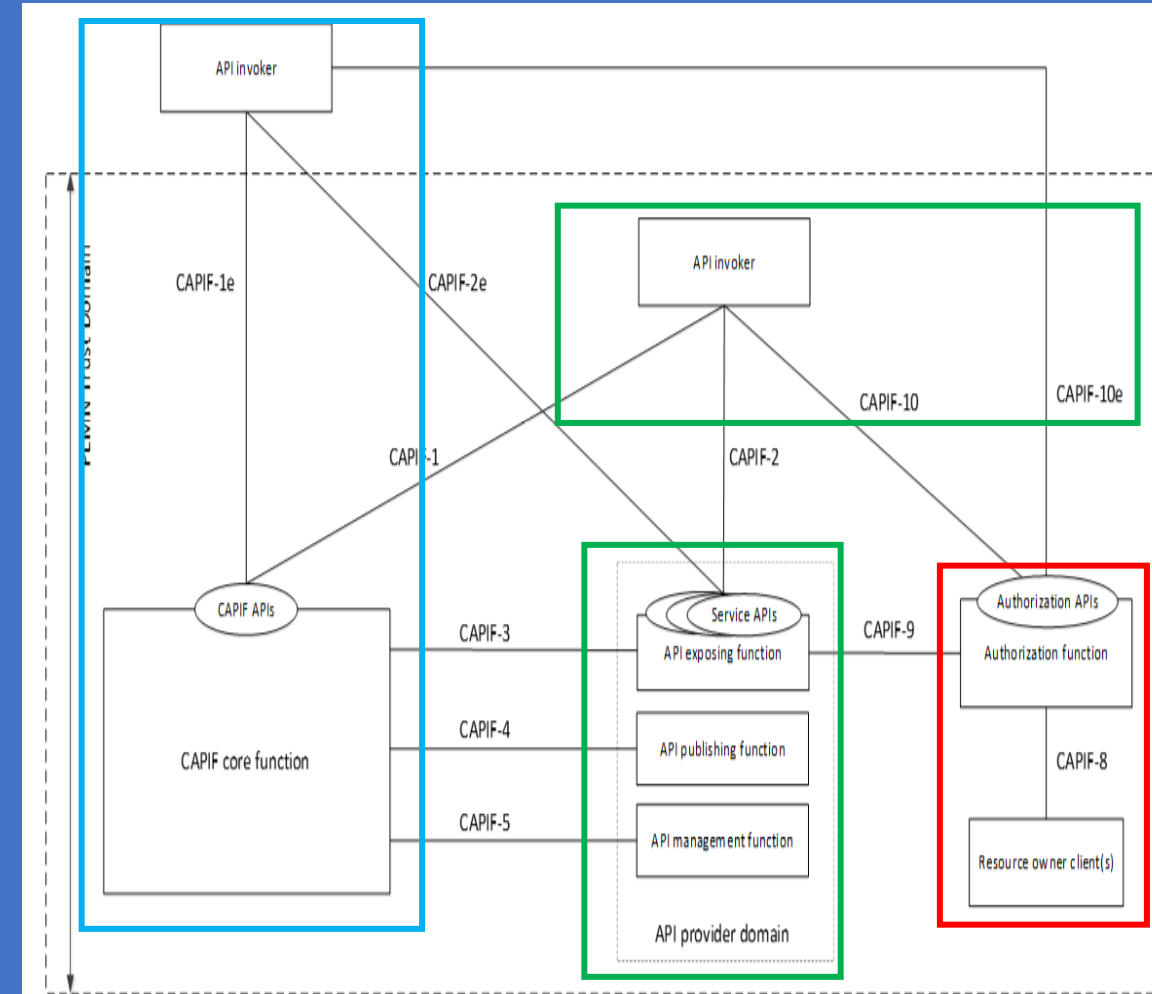


Figure: 5G Common API Framework (CAPIF) Functional Model with enhancements for Resource Owner (Subscriber or UE) Authorization enabling "Providing"/"Revoking" User Consent via CAPIF-8

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

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.

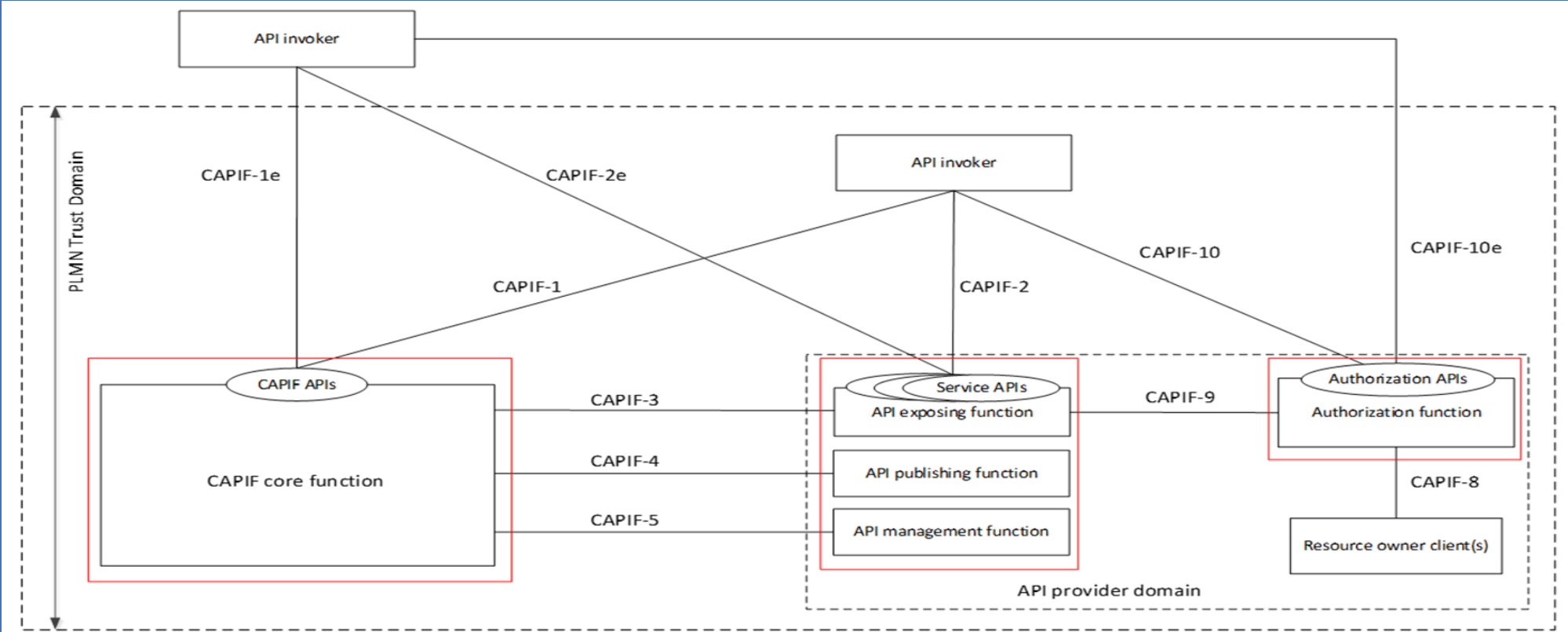
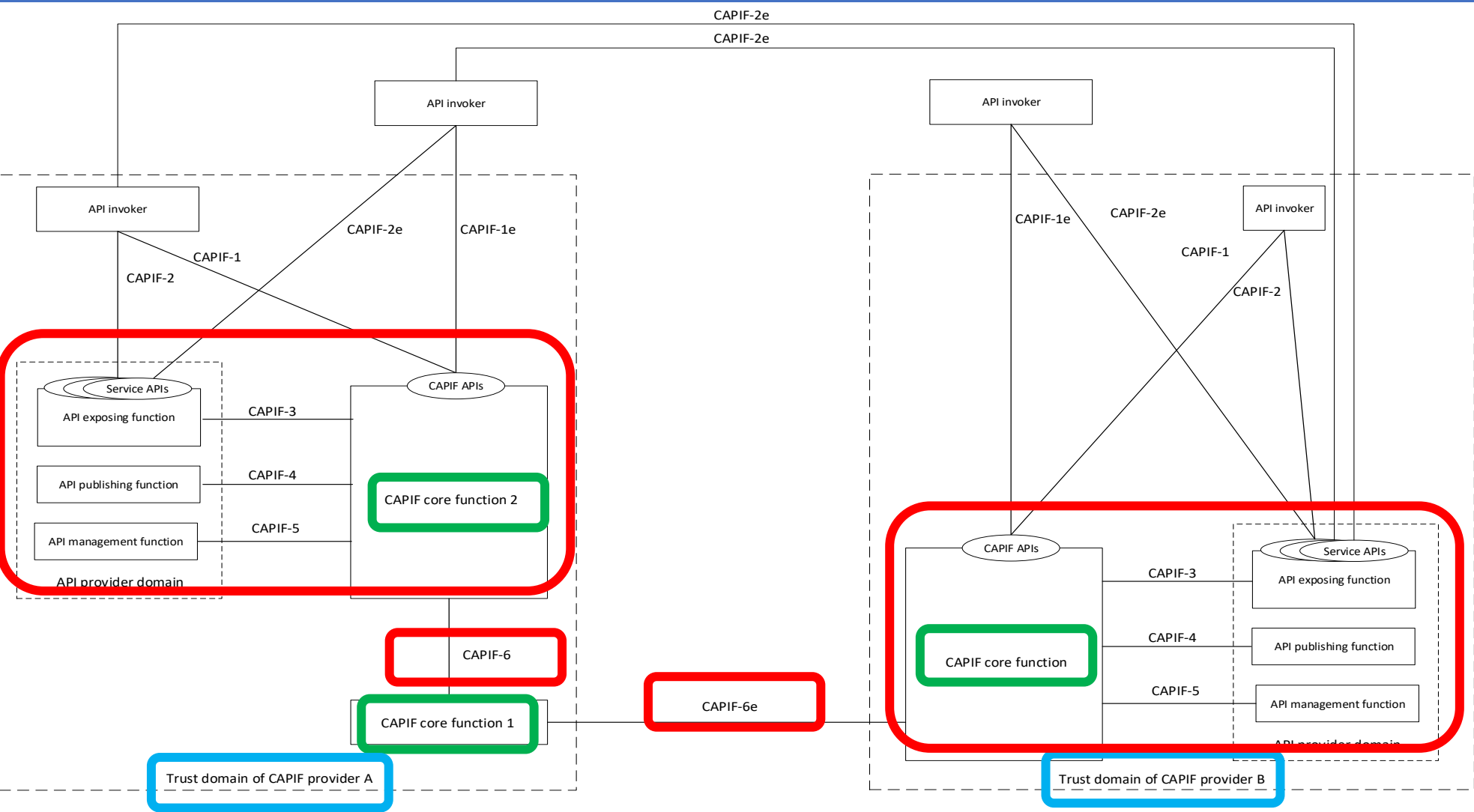


Figure: Deployment of the 5G enhanced Common API Framework (CAPIF), Service APIs and Authorization APIs by different Organizations within the PLMN Trust Domain

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



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

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 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**.

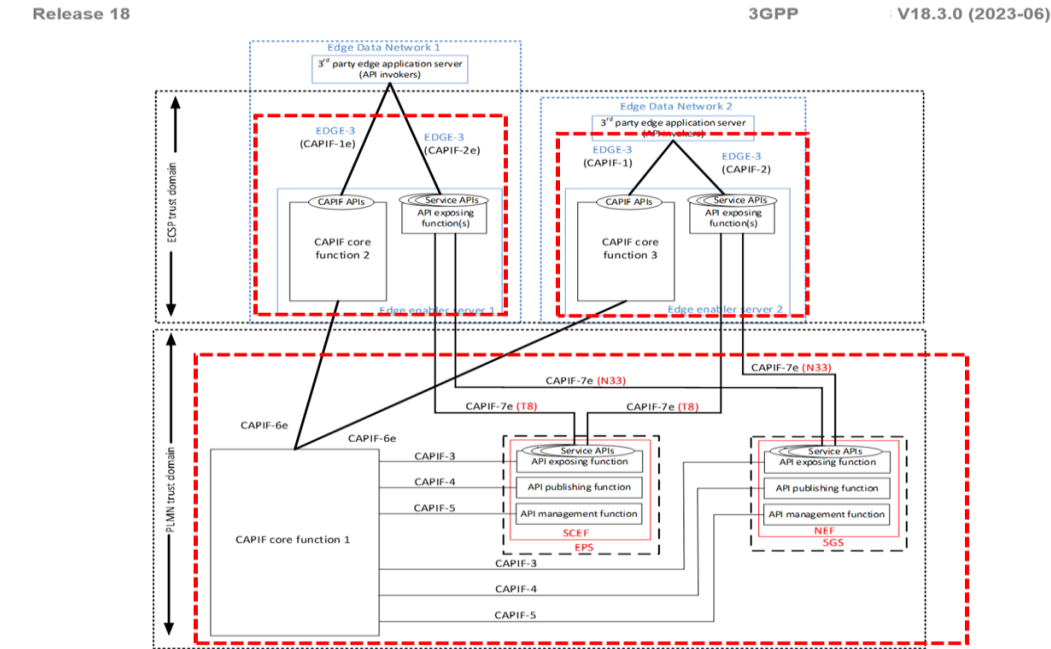


Figure: 5G Architecture enabling Edge Applications Edge Enabler Server(EES) supporting distributed 5G Common API Framework Core Function (CCF)

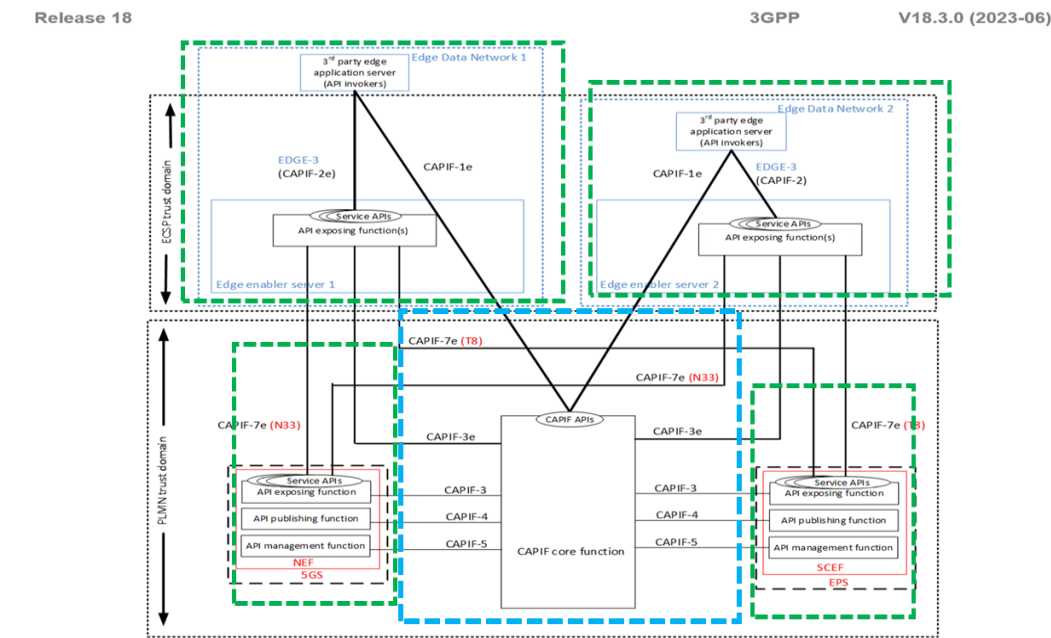


Figure: 5G Architecture enabling Edge Applications Edge Enabler Server(EES) supporting centralized 5G Common API Framework Core Function (CCF)

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.

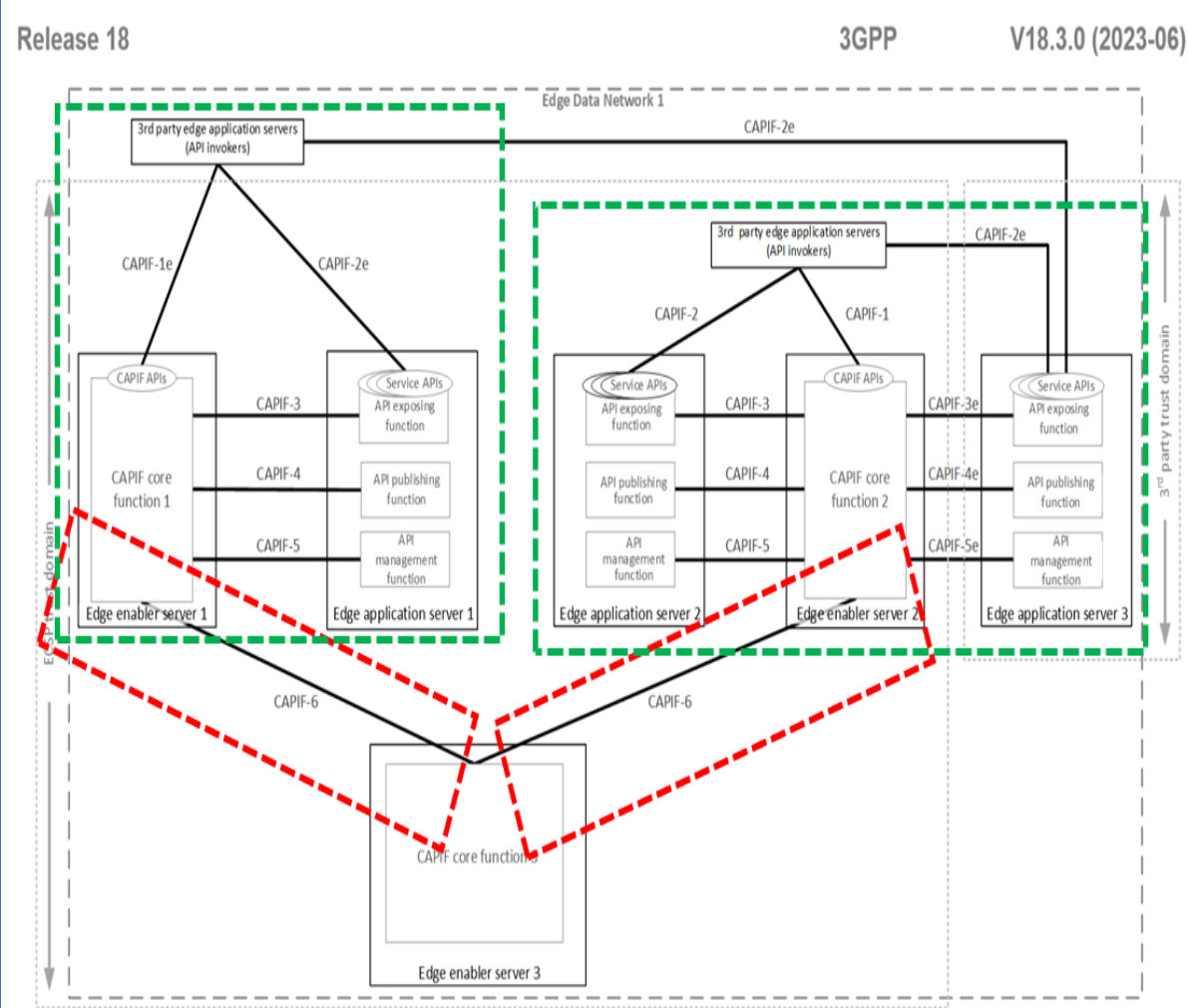


Figure: 5G Architecture enabling Edge Applications Edge Enabler Server (EES) supporting 5G Common API Framework Functions for exposure of EAS Service APIs

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").

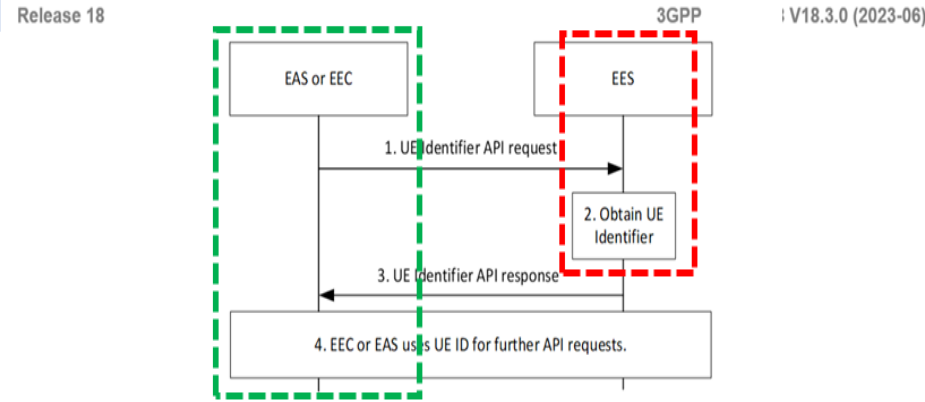


Figure: 5G Architecture for enabling Edge Applications UE Identifier API

Release 18 3GPP TS V18.3.0 (2023-06)

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

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**.

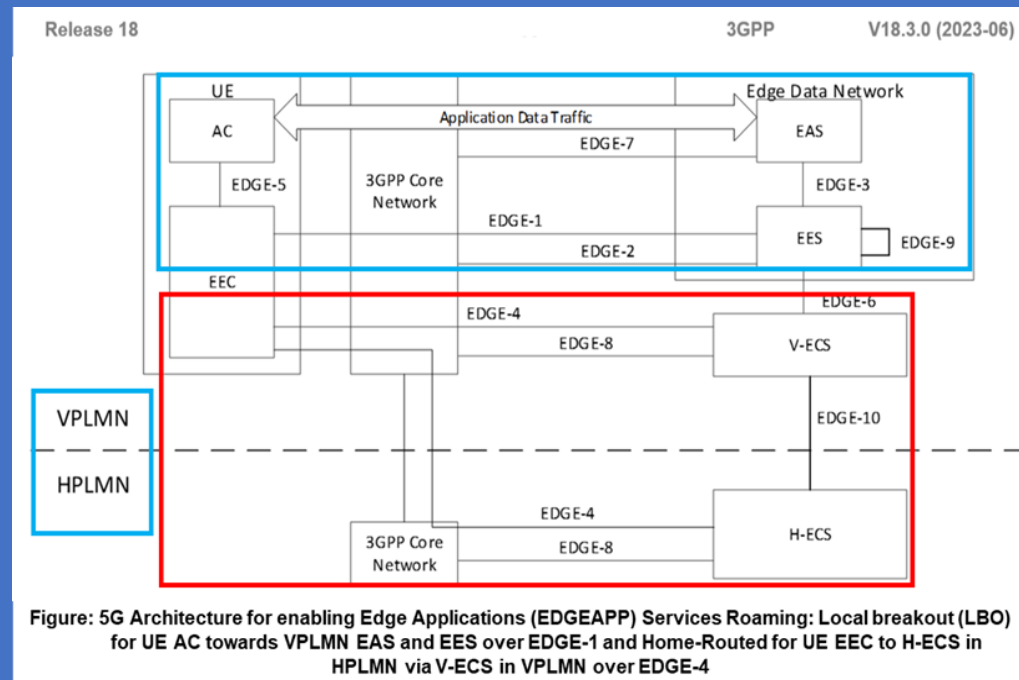
The EEC creates the Subscription and when required, performs necessary Operations such as **EAS discovery, ACR etc.**, delivering notifications to the **AC** as required.

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;



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

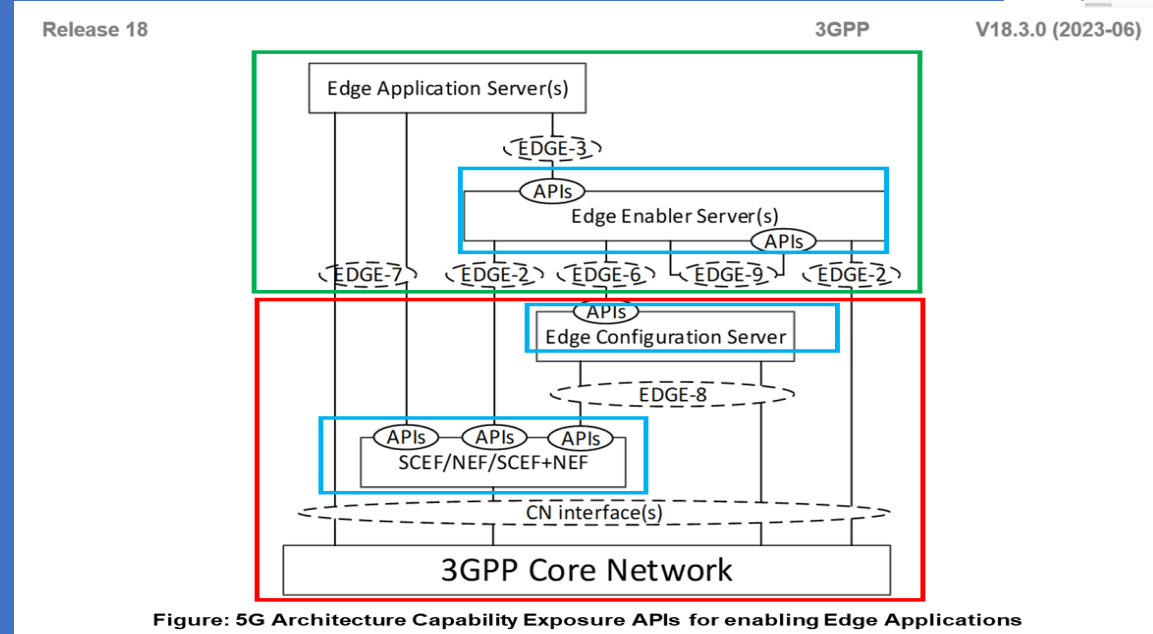


Table : APIs provided by the EES

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.

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 - UE Services Enablement Clients (UAC - Unified Access Control) for Access Identities & Access Categories - example of selected UCs Services supported as specified UE Clients

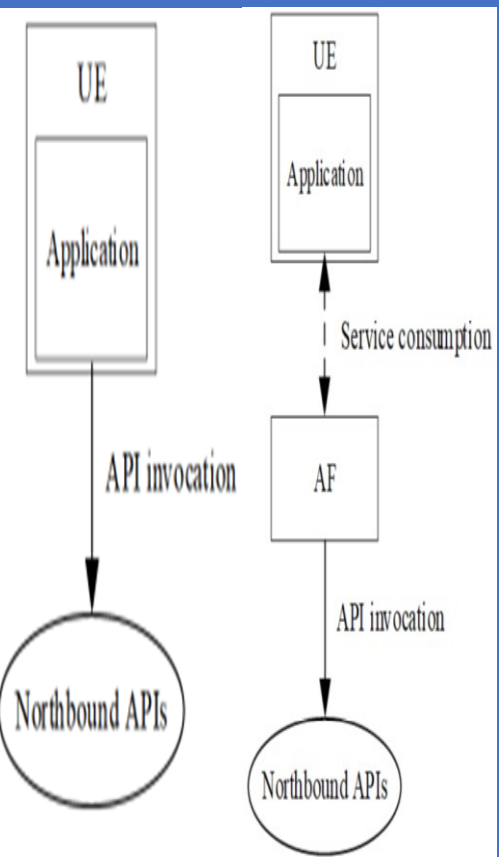
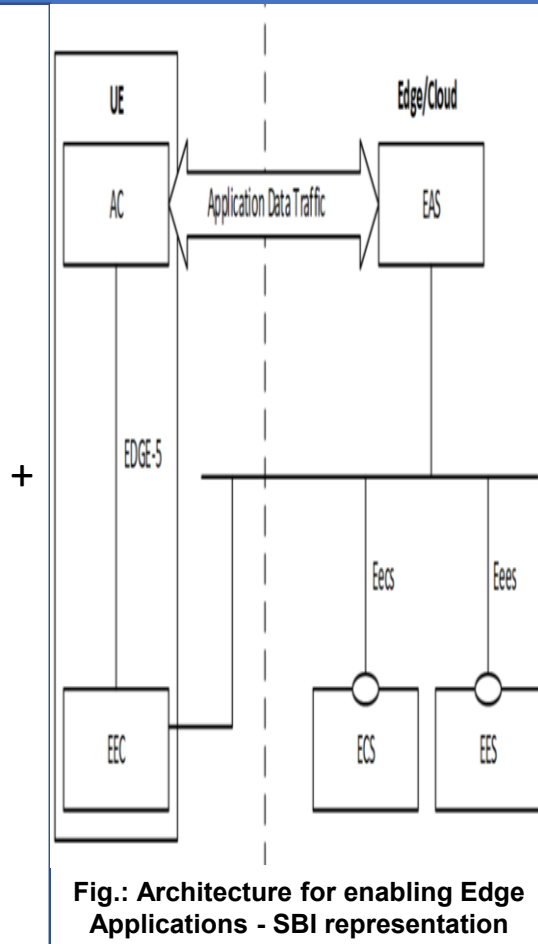
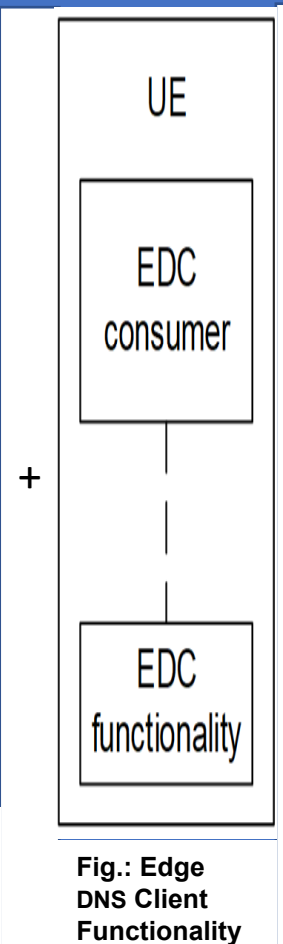
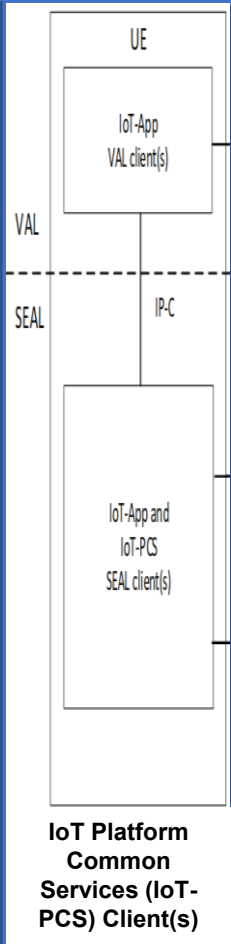
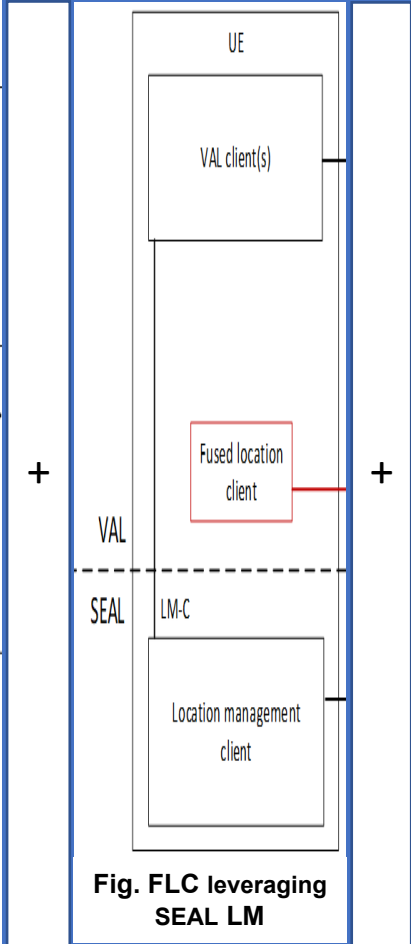
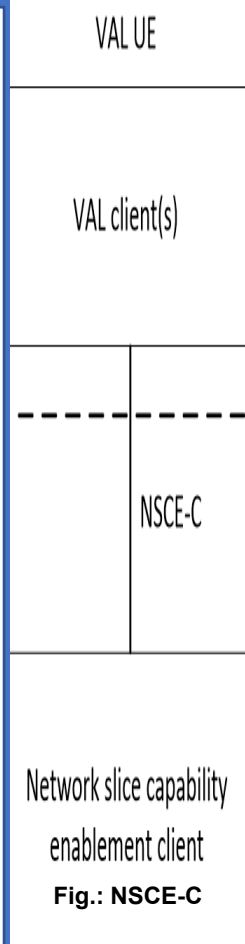
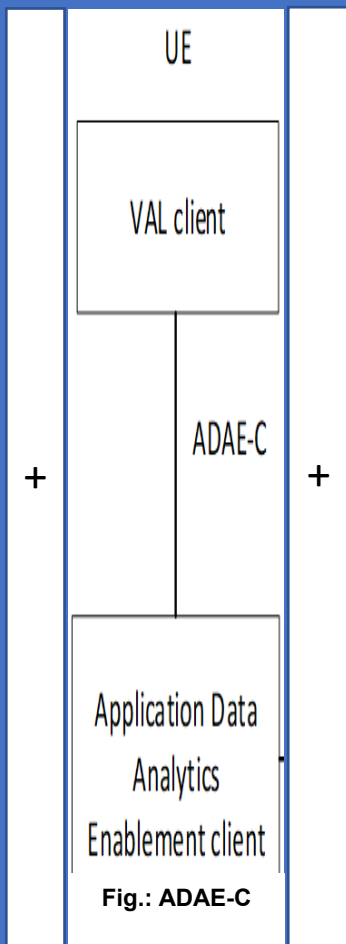


Fig.: UE-originated API Invocation

Fig.: AF-originated API Invocation





THIS IS THE END OF THE BEGINNING

Remarks & Questions?

Annex 1: Mobile Networks to evolve from:

a 2G, 3G, 4G Design that offers "Best-effort" Services

to

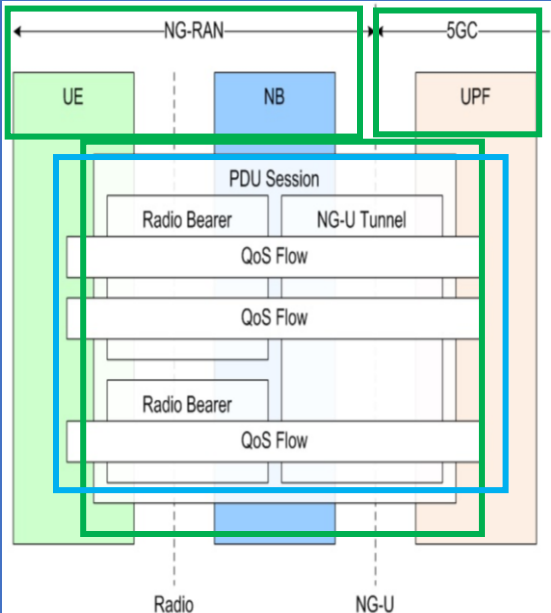
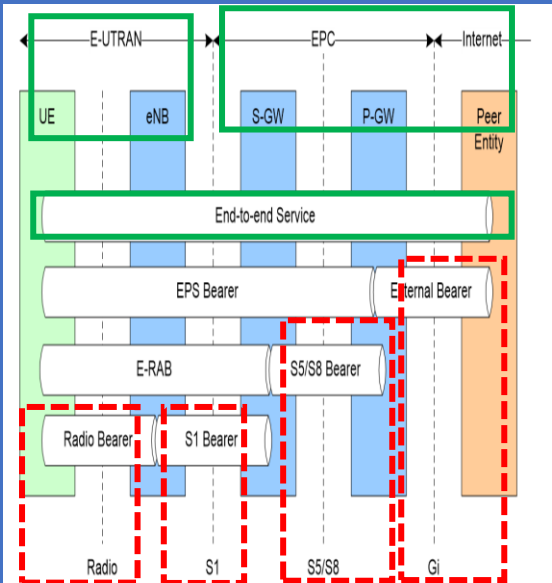
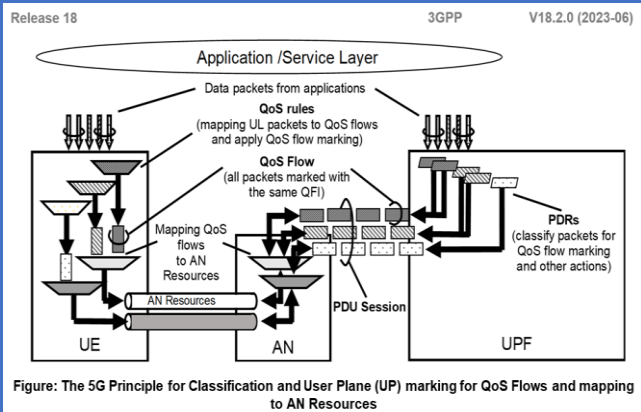
a Design that offers Performance and User Experience Guarantees

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**.



Annex 2: 5G Architecture for Hybrid and Multi-Cloud Environments

The Main Challenges to overcome in a Hybrid & Multi-Cloud Strategy are:

- 1. Maintaining Portability;
- 2. Controlling the Total Cost of Ownership (TCO);
- 3. Optimizing Productivity & Time to Market (TTM).

DevOps – a Set of Practices that brings together SW Development & IT operations with the Goal of Shortening the Development & Delivery Cycle & increasing SW Quality - is often thought of and discussed in the Context of a Single Company or Organization. The Company usually Develops the SW, Operates it & Provides it as a Service to Customers, according to the **SW-as-a-Service (SaaS) Model**. Within this context, it is easier to have Full Control over the Entire Flow, including Full Knowledge of the Target Deployment Environment.

In the **Telecom Space**, by contrast, we typically follow the **"as-a-Product (aaP) Business model**, in which **SW is developed by Network SW Vendors** e.g. as Ericsson (Nokia, Huawei, ZTE) & provided to Communication Service Providers (CSPs) that Deploy & Operate it within their Network. This **Business Model requires the consideration of additional aspects**.

The most important contrasts between the Standard DevOps SaaS Model & the Telecom aaP Model are the Multiplicity of Deployment Environments & the fact the Network SW Vendor Development Teams cannot know upfront exactly what the Target Environment looks like.

Although a SaaS Company is likely to Deploy & Manage its SW on two (2) or more different Cloud Environments, this is inevitable within Teico, as each CSP creates &/or selects its own Cloud infrastructure (Fig. 1 below).

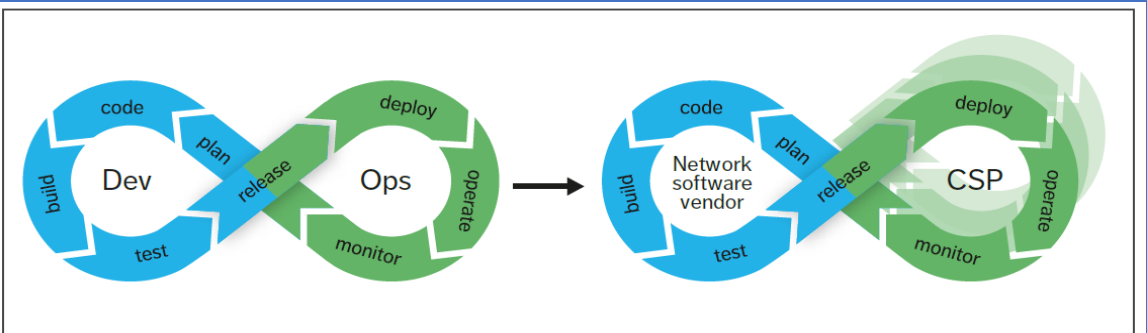


Figure 1: The DevOps and (Telecom) aaP Business Models

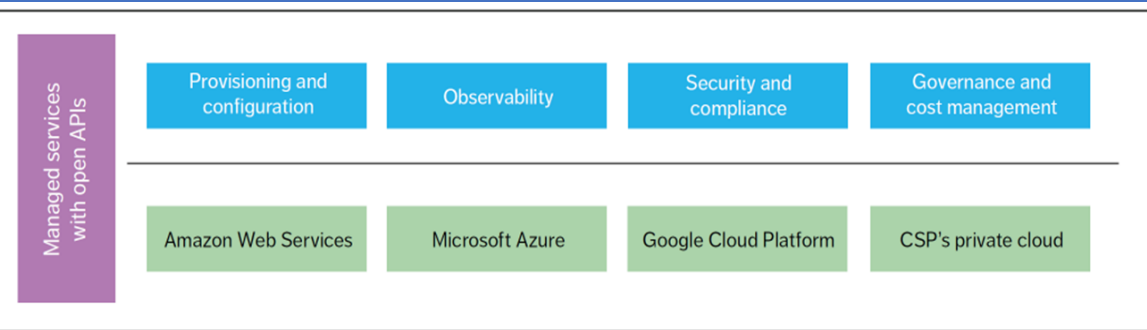


Figure 3: Key Enablers for a Multi-Cloud Native Application

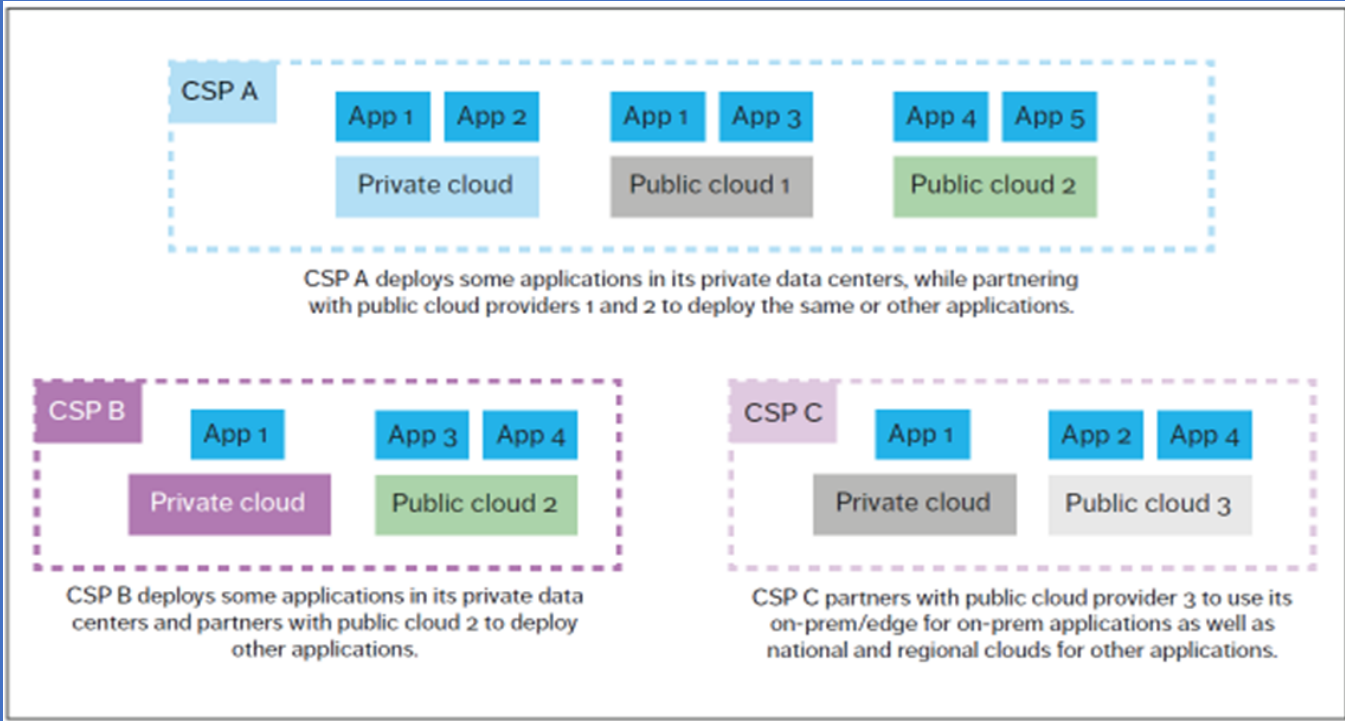


Figure 2: Examples of Hybrid and Multi-Cloud Deployment Scenarios that Applications must be able to support