5G and 5G Advanced selected Capabilities
to
LF Edge Akraino Technical Summit

Ike Alisson

2022 - 09- 22 Rev P10

Table of Contents (ToC)

PNI - NPN/SNPN (5G Private Networks)

NPN/SNPN Mapping Solutions to Key Issues - 3GPP Rel. 17

	Key Issues					
Nr Solutions	#1 Enhancements to Support SNPN along with Credentials owned by an Entity separate from the SNPN	#2: NPN support for Video, Imaging and Audio for Professional Applications (VIAPA)	#3 Support of IMS Voice and Emergency Services for SNPN	#4 UE Onboarding and Remote Provisioning	#5 Support for Equivalent SNPNs	#6 Support of Non 3GPP Access for NPN Services
1	X	X				
2	X	X				
3	X					
4	X					
5				X		
6				X		
7				X		
8	X					
9	X					
10	X					
11	X					
12	X					
13		X				
14		X				
15		X				
16		X				
17		X				
18		X				
19			X			
20			X			
21			X			
22			X			
23			X			
24			X			
25			X			
26			X			
27				X		
28				X		
29				X		
30				X		
31				X		
32				X		
33				X		
34				X		
35				X		
36				X		
37				X		
38				X		
39				X		
40				X		
41	X					
42	X					
43	X					
44	X					
45	X					
46		X				
47		X				
48		X				
49		X				
50		X				
51		X				
52		X				
53			X			
54			X			

1. 3GPP Definition of PNI - NPN/SNPN with Diagrams- 1

A Non-Public Network (NPN) is a 5GS deployed for Non-Public Use

1. An NPN is either:

1. a Stand-alone Non-Public Network (SNPN), i.e. operated by an NPN Operator and not relying on Network Functions provided by a PLMN,

or

2. a Public Network Integrated NPN (PNI-NPN), i.e. a Non-Public Network deployed with the support of a PLMN.

NOTE: An NPN and a PLMN can share NG-RAN

2. Stand-alone Non-Public Networks (SNPNs)

SNPN 5GS deployments are based on the Architecture for:

- *5GC with Un-trusted Non-3GPP Access (Fig. 1-1) for access to SNPN Services via a PLMN (and vice versa)*

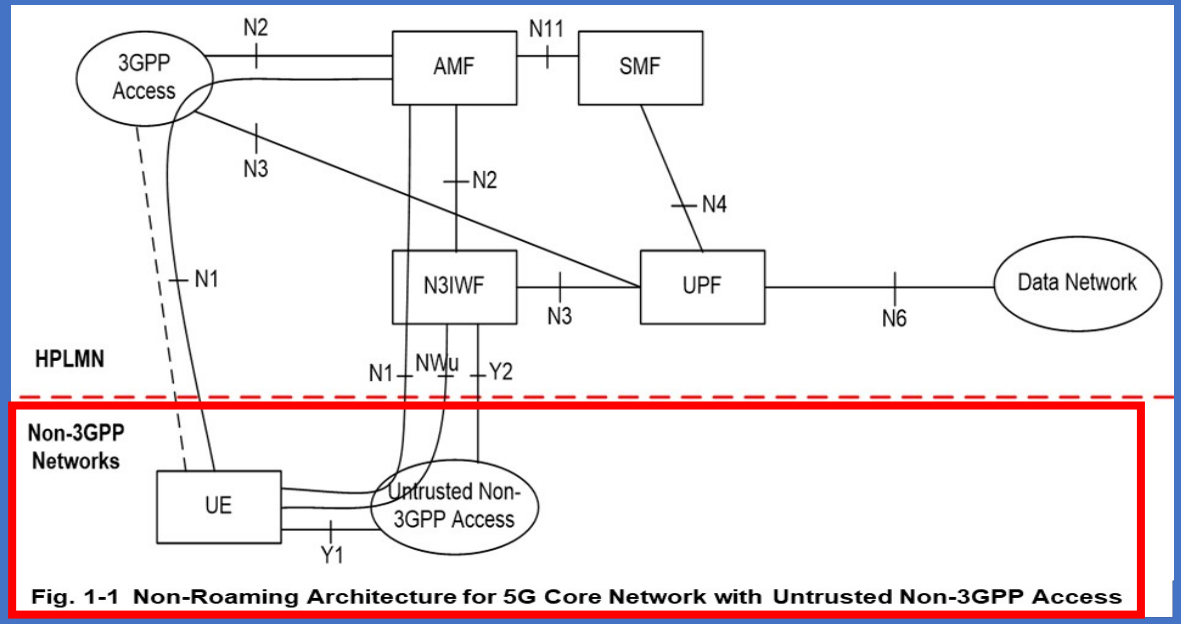


Fig. 1-1 Non-Roaming Architecture for 5G Core Network with Untrusted Non-3GPP Access

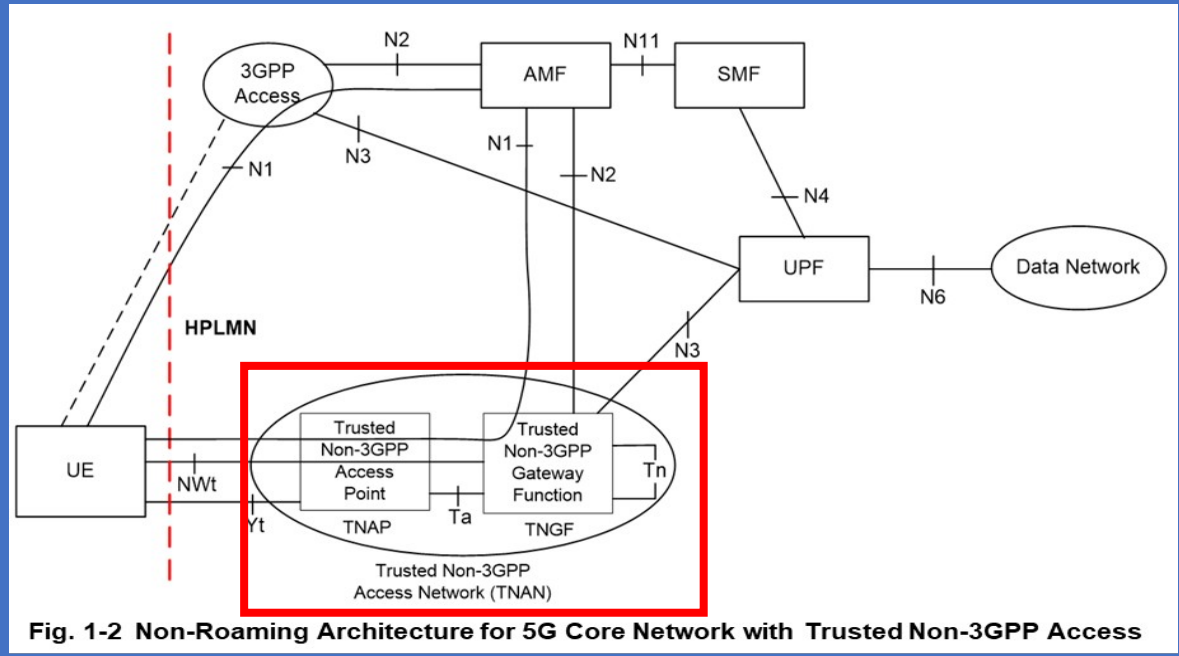


Fig. 1-2 Non-Roaming Architecture for 5G Core Network with Trusted Non-3GPP Access

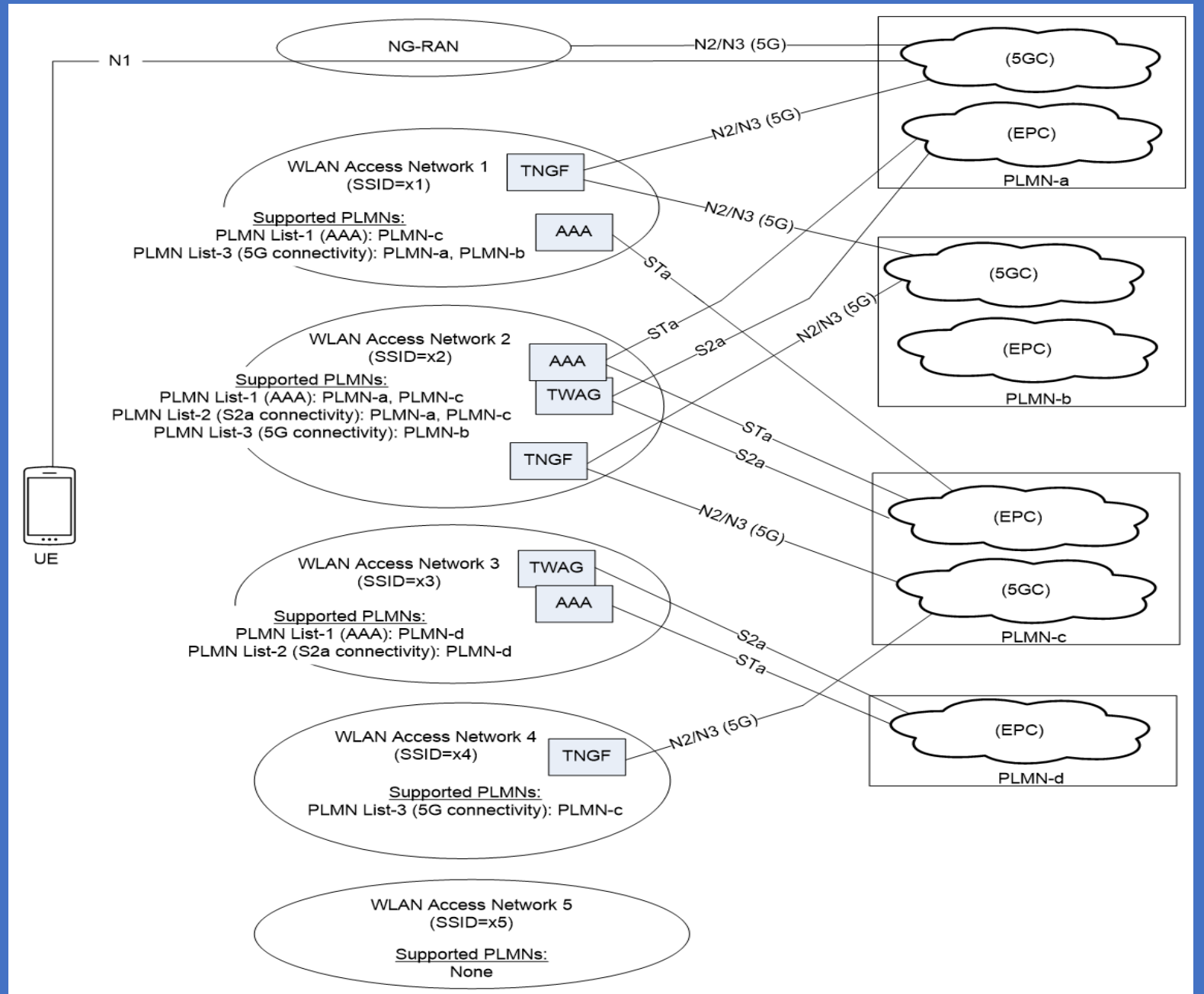


Figure **Example deployment scenario for trusted Non-3GPP access network selection**

1. 3GPP Definition of PNI - NPN/SNPN with Diagrams - 4

As of 3GPP Rel. 17, **the following 5GS features and functionalities are not supported for SNPNs:**

1. **Interworking with EPS** is not supported for SNPN.

2. **Emergency Services** are not supported for SNPN when the UE accesses the SNPN
   over NWu via a PLMN.

3. While **Roaming is not supported for SNPN**, e.g. Roaming between SNPNs, it is possible for a UE to access an SNPN with credentials from a CH

4. **Hand-over between SNPNs**, between SNPN and PLMN or PNI-NPN are **not supported.**

5. **CIoT 5GS Optimizations are not supported in SNPNs.**

6. **CAG (Closed Access Group) is not supported in SNPNs**.

- A UE with two (2) or more Network Subscriptions, where one (1) or more Network Subscriptions may be for a subscribed SNPN, can apply procedures specified for Multi-USIM UEs.

- The UE shall use a separate PEI for each network subscription when it registers to the network.

NOTE: The number of preconfigured PEIs for a UE is limited.

If the Number of Network Subscriptions for a UE is greater than the Pre-configured Number of PEIs, the Number of Network Subscriptions that can be registered with the Network simultaneously is restricted by the Number of Pre-Configured Number of PEIs.

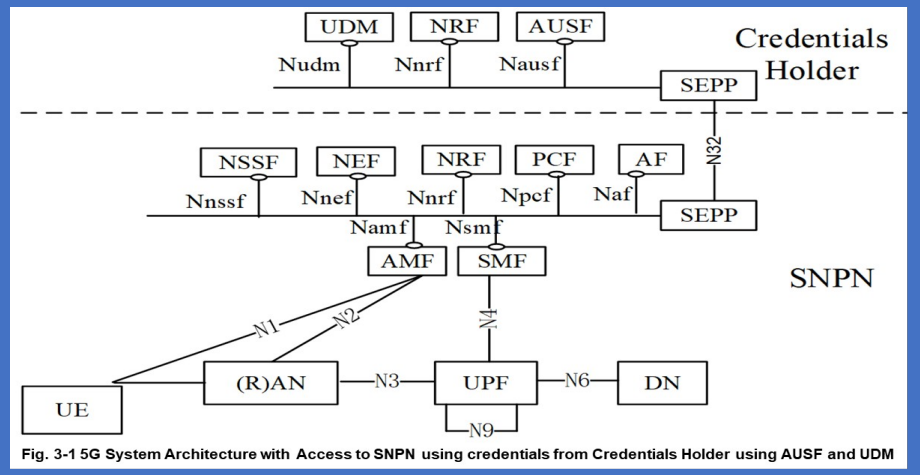


Fig. 3-1 5G System Architecture with Access to SNPN using credentials from Credentials Holder using AUSF and UDM

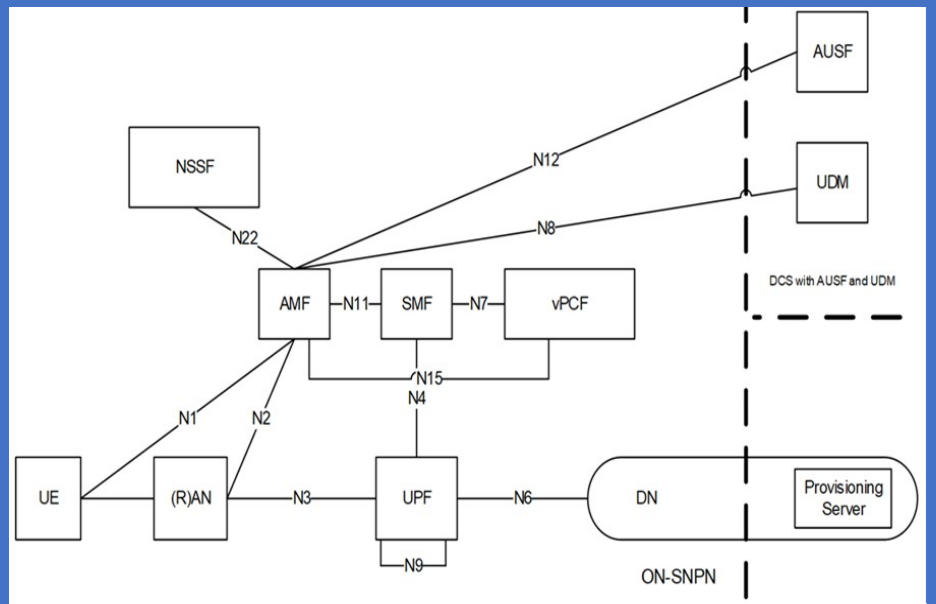


Fig.: Architecture for UE Onboarding in ON-SNPN when DCS includes AUSF and a UDM

Identifiers

The combination of a PLMN ID and Network identifier (NID) identifies an SNPN.

NOTE 1: The PLMN ID used for SNPNs is not required to be unique. PLMN IDs reserved for use by private networks can be used for non-public networks, e.g. based on mobile country code (MCC) 999 as assigned by ITU. Alternatively, a PLMN operator can use its own PLMN IDs for SNPN(s) along with NID(s), but registration in a PLMN and mobility between a PLMN and an SNPN are not supported using an SNPN subscription given that the SNPNs are not relying on network functions provided by the PLMN.

The NID shall support two assignment models:

- Self-assignment: NIDs are chosen individually by SNPNs at deployment time (and may therefore not be unique) but use a different numbering space than the coordinated assignment NIDs.

- Coordinated assignment: NIDs are assigned using one of the following two options:

  1. The NID is assigned such that it is globally unique independent of the PLMN ID used;

     or

  2. The NID is assigned such that the combination of the NID and the PLMN ID is globally unique.

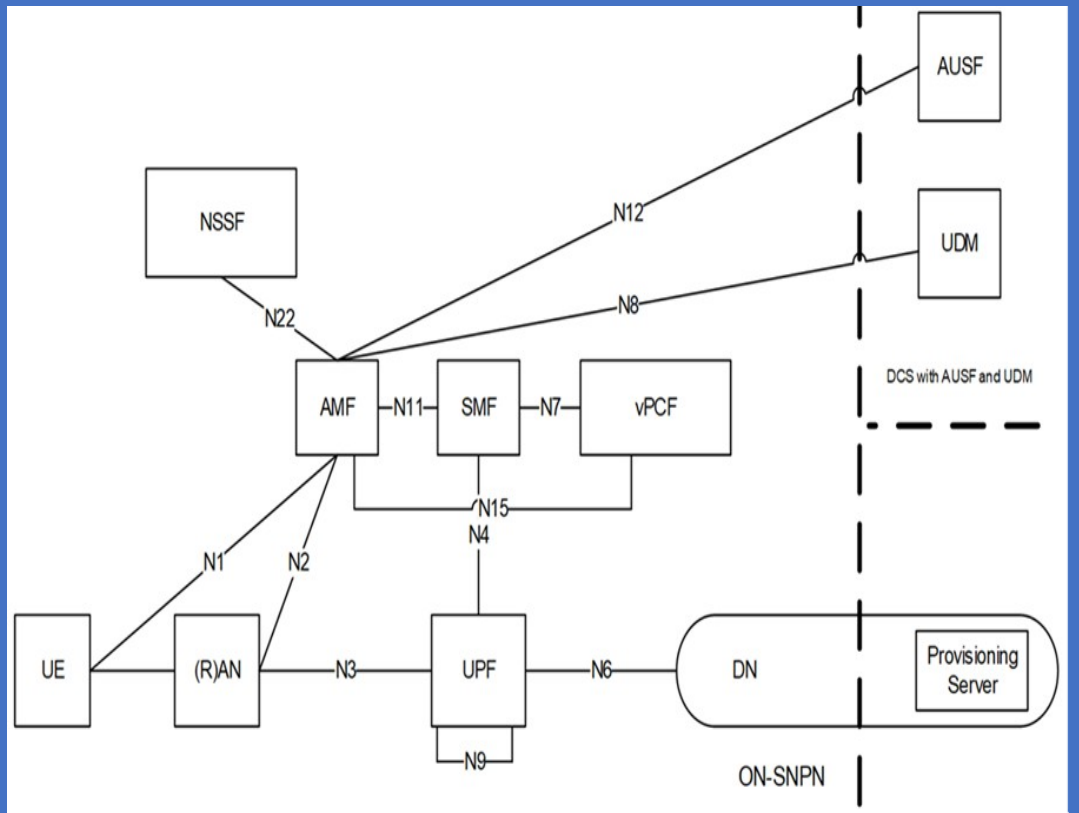


Fig.: Architecture for UE Onboarding in ON-SNPN when DCS includes AUSF and a UDM

Alternatively, **a Credentials Holder (CH)** may Authenticate and Authorize access to an SNPN.

In this Rel. 17, Direct Access to SNPN is specified for 3GPP Access only.

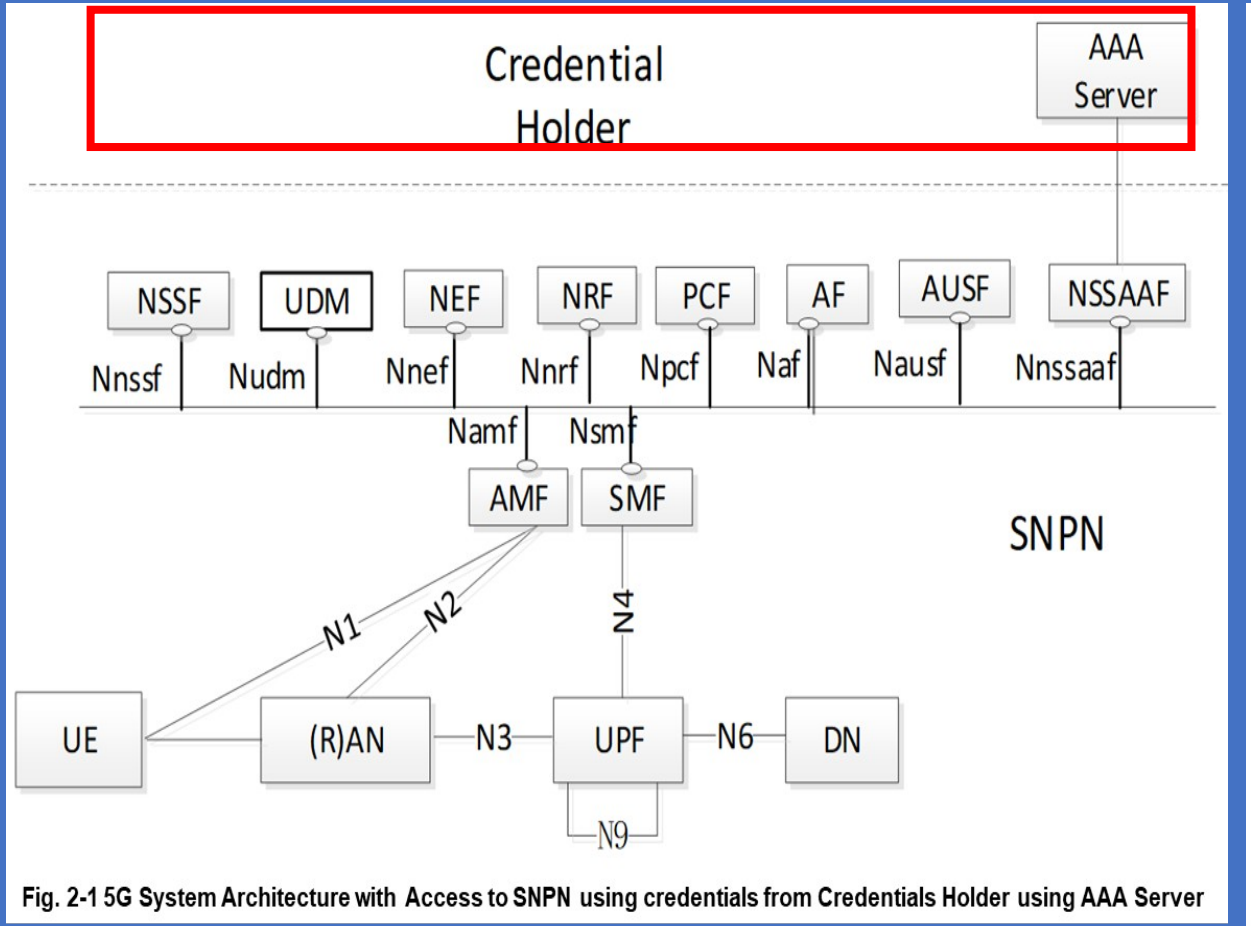


Fig. 2-1 5G System Architecture with Access to SNPN using credentials from Credentials Holder using AAA Server

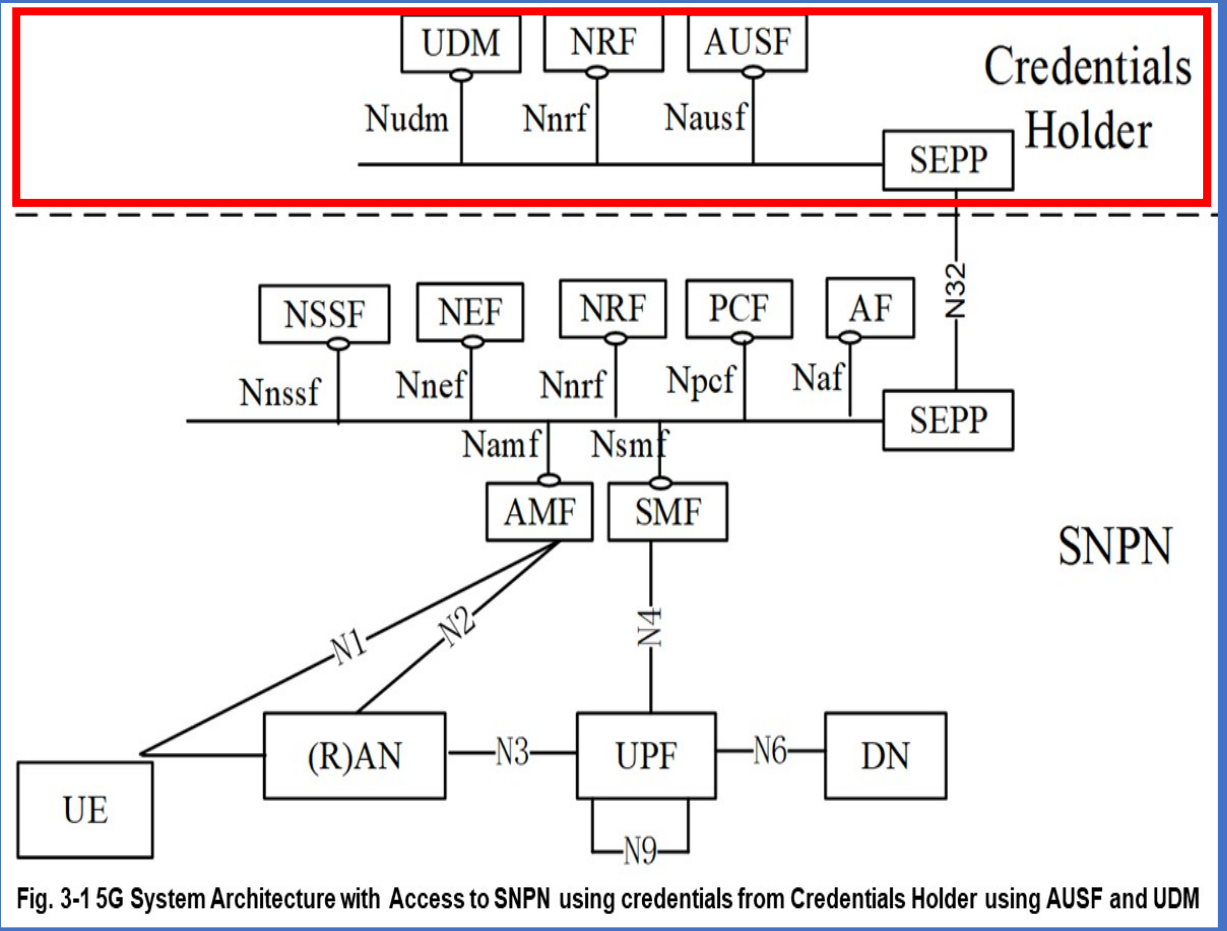


Fig. 3-1 5G System Architecture with Access to SNPN using credentials from Credentials Holder using AUSF and UDM

Ref.3GPP TS 23 501 5G System Architect., Rel., 17, Dec 2021: 337 - 338, 344

2. Market Definition and Deployments of "Private 5G" PNI - NPN/NSPN - 6

5G World in London (September 22, 2021) brought some perspective.

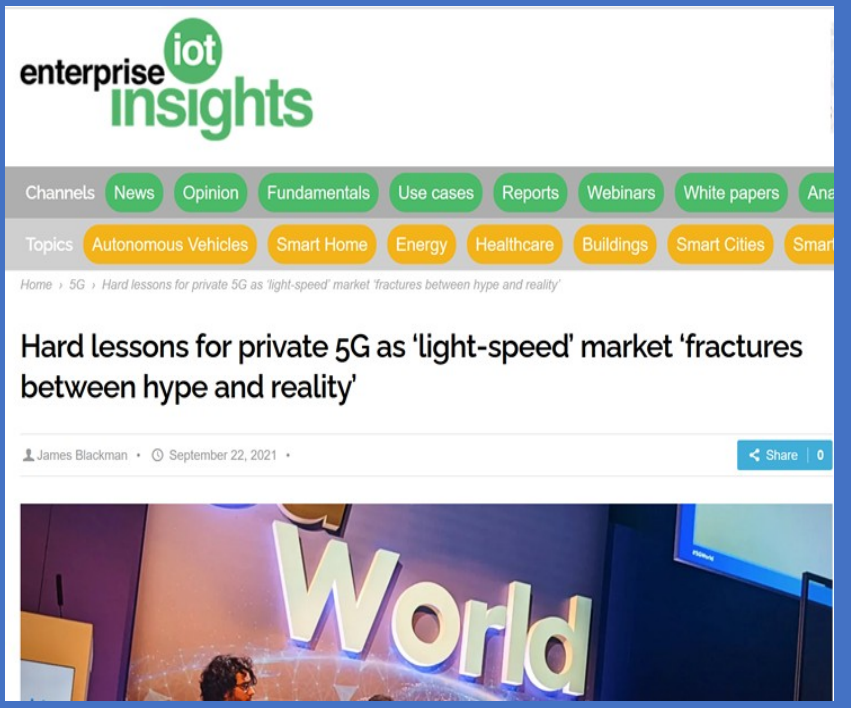
There is a Learning Curve for Enterprises, and a Learning Curve for Everyone selling Private Network Services.

So the Market is moving slower, from Tests and Proofs;

It is not even a 5G Market, yet (of course).

"The Majority is on LTE, so at moment it is an LTE Market, and LTE is currently delivering what most Use Cases want."

It looks clearer through the lens of each player in the Market, only because their views of it are all different, and all of them are feasible on their own terms.



https://enterpriseiotinsights.com/20210922/channels/news/hard-lessons-for-private-5g-as-lightspeed-market-is-fractured-between-hype-and-reality?utm_campaign=Enterprise%20IoT%20Newsletter&utm_medium=email&_hsmi=162862354&_hsenc=p2ANqtz-_rkpszzAFyrYTATSTBWE88VSKQCqdUyAdfuNgJFBs7nlbwnCmskZSPs6Nl4Ftg77p8boVhFiPUCc-0Oklff37DT2D3cQ&utm_content=162862354&utm_source=hs_email

The 'Failure' of Private 5G – another Telco bungle, or just Industrial Inertia? (Is the Window really Closing?) ***August 31, 2021***

Most "Vertical' Licences", so far, remain attached to PoCs.

So the early interest is from 'Industrial Leaders', often with vested interests in Selling solutions Over-the-Top, to kick the tyres on Private 5G.

And the Number of fully-fledged deployments are limited,

if you look at the Names of the Licensees, more than half (50%) of them are strictly speaking Non-Commercial.

Either,

1. **they are Research and / or Proofs, as you rightly mention, or [else]**

2. **they are System-Integrator (SI) Deployments – [all of which] want to Test and Showcase 5G Solutions they are looking to provide to clients.**

The question then becomes what level of PNI-NPN will emerge as the most successful."

https://enterpriseiotinsights.com/20210831/channels/news/the-failure-of-private-5g-another-telco-bungle-or-just-industrial-inertia-is-the-window-really-closing

NPN/SNPN

NPN/SNPN Mapping Solutions to Key Issues - 3GPP Rel. 17

	Key Issues					
Nr Solutions	#1 Enhancements to Support SNPN along with Credentials owned by an Entity separate from the SNPN	#2: NPN support for Video, Imaging and Audio for Professional Applications (VIAPA)	#3 Support of IMS Voice and Emergency Services for SNPN	#4 UE Onboarding and Remote Provisioning	#5 Support for Equivalent SNPNs	#6 Support of Non 3GPP Access for NPN Services
1	X	X				
2	X	X				
3	X					
4	X					
5				X		
6				X		
7				X		
8	X					
9	X					
10	X					
11	X					
12	X					
13		X				
14		X				
15		X				
16		X				
17		X				
18		X				
19			X			
20			X			
21			X			
22			X			
23			X			
24			X			
25			X			
26			X			
27				X		
28				X		
29				X		
30				X		
31				X		
32				X		
33				X		
34				X		
35				X		
36				X		
37				X		
38				X		
39				X		
40				X		
41	X					
42	X					
43	X					
44	X					
45	X					
46		X				
47		X				
48		X				
49		X				
50		X				
51		X				
52		X				
53			X			
54			X			

1. Key Issue #1: Enabling support for idle and Connected mode Mobility between SNPNs without New Network selection

2. Key Issue #2: Support of Non-3GPP Access for SNPN

3. Key Issue #3: Enabling NPN as hosting network for providing Access to Localized Services

4. Key Issue #4: Enabling UE to Discover, Select and Access NPNs as Hosting Network and receive Localized Services

5. Key Issue #5: Enabling Access to Localized Services via a Specific Hosting Network

6. Key Issue #6: Support for returning to Home Network

Mapping Solutions to Key Issues

Table Mapping Solutions to Key Issues

	Key Issues					
Solutions	1	2	3	4	5	6
1	X					
2		X				
3		X				
4		X				
5		X				
6		X				
7			X	X	X	X
8						X
9						X
10				X		X
11					X	
12				X		
13				X	X	
14				X		
15				X	X	
16		X				
17						X
18					X	

Ref. 3GPP, Rel. 18, April., 2022)

1. Key Issue #1: Enabling support for idle and Connected mode Mobility between SNPNs without New Network selection

2. Key Issue #2: Support of Non-3GPP Access for SNPN

3. Key Issue #3: Enabling NPN as hosting network for providing Access to Localized Services

4. Key Issue #4: Enabling UE to Discover, Select and Access NPNs as Hosting Network and receive Localized Services

5. Key Issue #5: Enabling Access to Localized Services via a Specific Hosting Network

6. Key Issue #6: Support for returning to Home Network

Mapping Solutions to Key Issues

Table : Mapping Solutions to Key Issues

Solutions	Key Issues 1	2	3	4	5	6
1	X					
2		X				
3		X				
4		X				
5		X				
6		X				
7			X	X	X	X
8						X
9						X
10				X		X
11				X	X	
12			X	X		
13				X	X	
14				X		
15				X	X	
16		X				
17						X
18					X	
19		X				
20		X				
21		X				
22			X			
23				X		
24				X		
25				X		
26				X		
27				X	X	
28				X	X	
29				X		
30				X		
31				X		
32				X		
33				X		
34				X		
35					X	
36					X	
37					X	
38						X
39						X

Ref. 3GPP, Rel. 18, May., 2022)

1. Key Issue #1: Enabling support for idle and Connected mode Mobility between SNPNs without New Network selection

2. Key Issue #2: Support of Non-3GPP Access for SNPN

3. Key Issue #3: Enabling NPN as hosting network for providing Access to Localized Services

4. Key Issue #4: Enabling UE to Discover, Select and Access NPNs as Hosting Network and receive Localized Services

5. Key Issue #5: Enabling Access to Localized Services via a Specific Hosting Network

6. Key Issue #6: Support for returning to Home Network

Mapping Solutions to Key Issues

Table : Mapping Solutions to Key Issues

	Key Issues					
Solutions	1	2	3	4	5	6
1	X					
2		X				
3		X				
4		X				
5		X				
6		X				
7			X	X	X	X
8						X
9						X
10				X		X
11				X	X	
12			X	X		
13				X	X	
14				X		
15				X	X	
16		X				
17						X
18					X	
19		X				
20		X				
21		X				
22			X			
23				X		
24				X		
25				X		X
26				X		
27				X	X	
28				X	X	
29				X		
30				X		
31				X		
32				X		
33				X		
34				X		
35				X	X	
36					X	
37					X	
38						X
39						X
40				X	X	
41			X	X		
42				X		
43				X		
44				X		
45				X	X	
46					X	
47						X

Ref. 3GPP, Rel. 18, Aug., 2022)

Solution #1: Enable efficient Mobility via Equivalent SNPNs

The solution addresses Key Issue (KI) #1 "Enhanced Mobility between SNPNs without new network selection".

The solution utilizes a List of SNPN Identities (i.e. a List of combinations of PLMN ID and NID) to ***enable UE with one (1) Single SNPN Subscription*** to efficiently access different SNPNs ***without performing new network selection.***

The list is implemented by the similar logic as the List of Equivalent PLMNs, as specified in TS 5G System Architecture Rel. 17, clause 5.18.2a.

The Solution also re-use existing Function as specified in clause 5.18.1 of TS 5G System Architecture, Rel. 17, where different combination of PLMN ID and NID can point to the same 5GC.

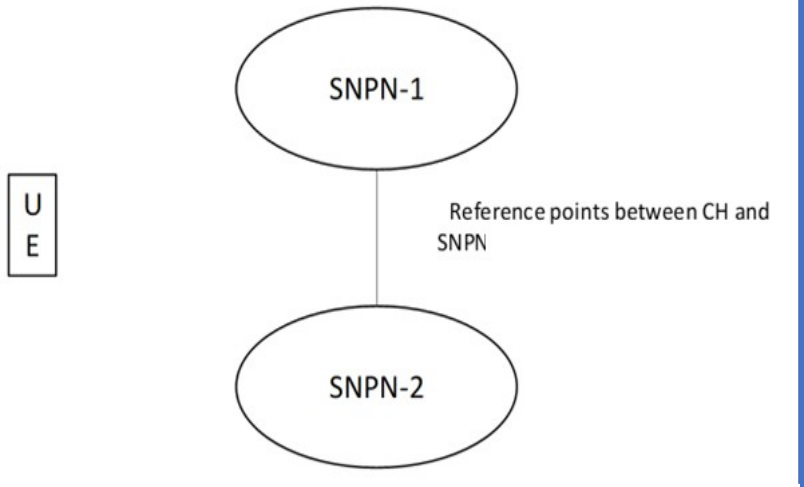


Figure: 5G UE accesses multiple SNPNs using CH

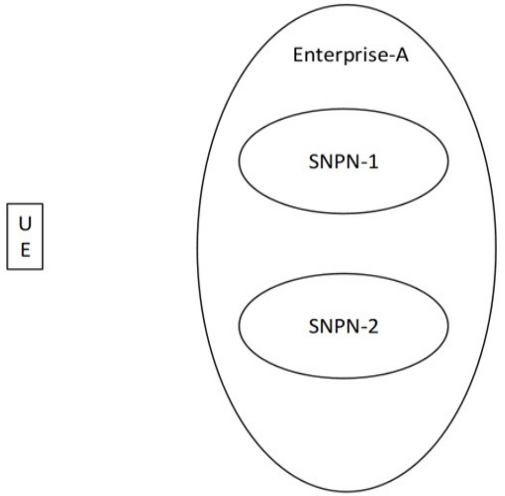


Figure: 5G UE accesses multiple SNPNs belonging to the same Administrative Entity

3GPP TS

V17.5.0 (2022-06)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
System architecture for the 5G System (5GS);
Stage 2
(Release 17)

1. List of Equivalent PLMNs, as specified in TS 5G System Architecture Rel. 17, clause 5.18.2a.

5.18.2a PLMN list handling for network sharing

The AMF prepares lists of PLMN IDs suitable as target PLMNs for use at idle mode cell (re)selection and for use at handover and RRC Connection Release with redirection. The AMF:

- provides the UE with the list of PLMNs that the UE shall consider as Equivalent to the serving PLMN

and

- provides the NG-RAN with a prioritised list of permitted PLMNs When prioritising these PLMNs, the AMF may consider the following information: HPLMN of the UE, the serving PLMN, a preferred target PLMN (e.g. based on last used EPS PLMN), or the policies of the operator(s).

For a UE registered in an SNPN, the AMF shall not provide a list of equivalent PLMNs to the UE and shall not provide a list of permitted PLMNs to NG-RAN.

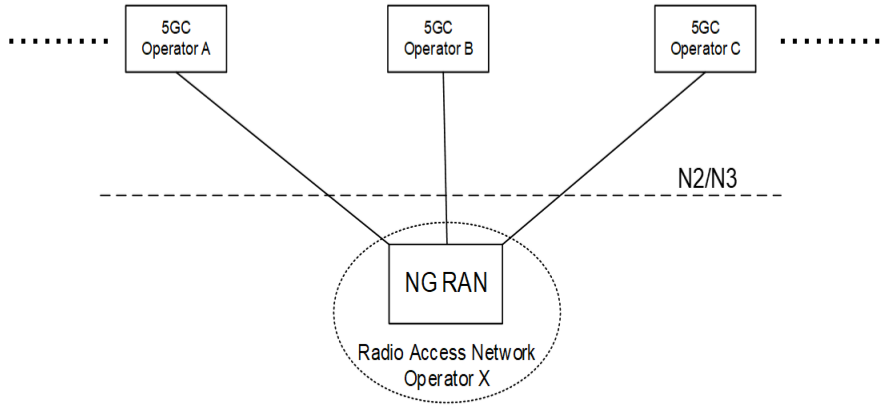


Figure : A 5G Multi-Operator Core Network (5G MOCN) in which multiple CNs are connected to the same NG-RAN

2. The Solution re-use existing Function as specified in clause 5.18.1 of TS System Architecture, Rel. 17, where different combination of PLMN ID a can point to the same 5GC.

5.18 Network Sharing 5.18.1 General concepts

A network sharing architecture shall allow multiple participating operators to share resources of a single shared network according to agreed allocation schemes. The shared network includes a radio access network. The shared resources include radio resources.

The shared network operator allocates shared resources to the participating operators based on their planned and current needs and according to service level agreements.

In this Release of the specification, only the 5G Multi-Operator Core Network (5G MOCN) network sharing architecture, in which only the RAN is shared in 5G System, is supported. 5G MOCN for 5G System, including UE, RAN and AMF, shall support operators' ability to use more than one PLMN ID (i.e. with same or different country code (MCC) some of which is specified in TS NAS for UE in Idle mode and different network codes (MNC)) or combinations of PLMN ID and NID. 5G MOCN supports NG-RAN Sharing with or without multiple Cell Identity broadcast as described in TS NG RAN.

5G MOCN also supports the following sharing scenarios involving non-public networks, i.e.NG-RAN can be shared by any combination of PLMNs, PNI-NPNs (with CAG), and SNPNs (each identified by PLMN ID and NID).

NOTE 1: PNI-NPNs (without CAG) are not explicitly listed above as it does not require additional NG-RAN sharing functionality compared to sharing by one or multiple PLMNs.

In all Non-Public Network sharing scenarios, each Cell Identity … is associated with one (1) of the following Configuration options:
- one or multiple SNPNs;
- one or multiple PNI-NPNs (with CAG); or
- one or multiple PLMNs only.

NOTE 2: This allows the assignment of Multiple Cell Identities to a Cell and also allows the cell identities to be independently assigned, i.e. without need for coordination, by the network sharing partners, between PLMNs and/or non-public networks.

NOTE 3: Different PLMN IDs (or combinations of PLMN ID and NID) can also point to the same 5GC. When same 5GC supports multiple SNPNs (identified by PLMN ID and NID), then they are not used as equivalent SNPNs for a UE.

NOTE 4: There is no standardized mechanism to avoid paging collisions if the same 5G-S-TMSI is allocated to different UEs by different PLMNs or SNPNs of the shared network, as the risk of paging collision is assumed to be very low. If such risk is to be eliminated then PLMNs and SNPNs of the shared network needs to coordinate the value space of the 5G-S-TMSI to differentiate the PLMNs and SNPNs of the shared network.

Solution #1 to Key Issue #1: Enabling support for Idle and Connected mode Mobility between SNPNs without New Network Selection through Solution #1:

The key issue #1 is addressed for supporting the **Equivalent SNPNs:**

- Solution#1 considers the UE has either a Subscription of Source **or** Target SNPN while the Subscription can be used to access both, or the UE has the credential from a Credentials Holder (CH) that can be used to access both Source and Target SNPNs (e.g. the UE has Subscription of Source SNPN and Access the Target using the Credentials from Source SNPN being a CH, or UE Access Source and Target SNPNs using the Credentials from another CH.

1. Idle Mode Mobility:

- **Solution#1** addresses this by:
- Providing the UE with a list of SNPN Identities to the UE that the UE consider as "**Equivalent**" to the registered SNPN during Cell (re)selection avoiding the need to perform Network Selection at Inter-SNPN change.

2. Connected Mode Mobility:

- **Solution#1** addresses this by:
- **Allowing equivalent SNPNs** belonging to the same administrative entity being included in the MRL (Mobility Restriction List) sent to NG-RAN.

- **PDU Session Continuity is enabled for the case when the equivalent SNPNs** belong to the same Administrative Entity.

The Use Case (UC) for supporting **equivalent SNPNs within an RA** would result into two (2) or more SNPNs that are Geographically overlapping or adjacent to each other and the UEs are moving between the two (2) or more SNPNs such that the UEs would create frequent Mobility Registration Updates unless the two (2) or more SNPNs are added to the same RA.

The Support of equivalent SNPNs impacts UE, AMF and NG-RAN.

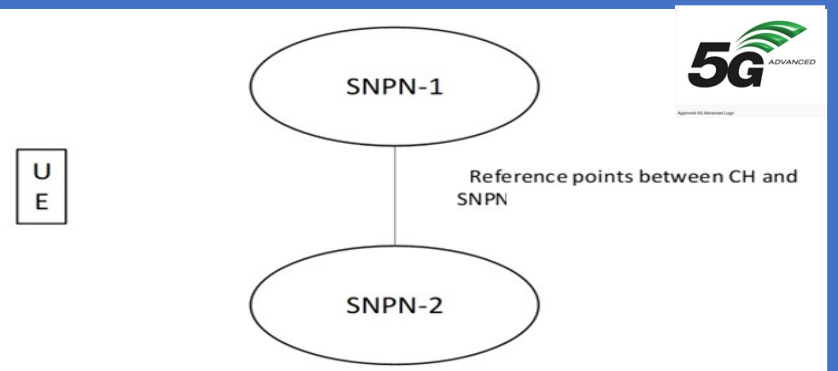


Figure: 5G UE accesses multiple SNPNs using CH

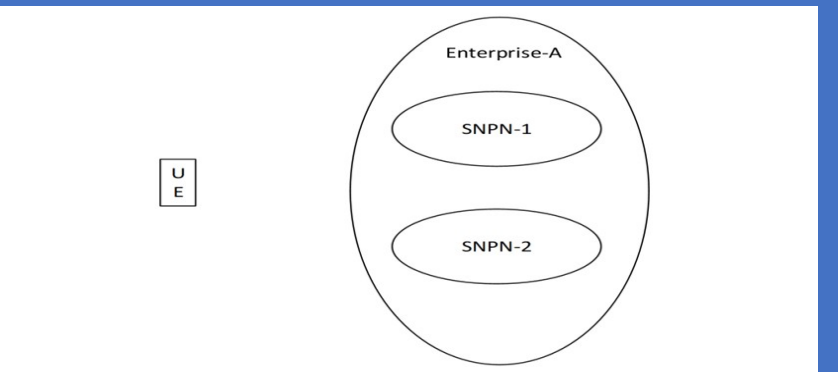


Figure: 5G UE accesses multiple SNPNs belonging to the same Administrative Entity

If equivalent SNPNs within an RA is to be supported, then NAS can be extended with a new Partial tracking area identity list – type of list that includes also the NID (together with the MCC and MNC), and NGAP can be extended allowing the TAI list to be associated to different SNPNs e.g. by adding a new TAI encoding for SNPNs.

NOTE 3: For ensuring TAI list to work with Equivalent SNPNs, the NID must be defined to be unique, i.e. the UE will by default assume it is unique. The NID included in the new Partial tracking area must be configured such that NID is unique at least across the Registration Areas.

Ref: 3GPP, NPNs/SNPNs, Rel. 18, Aug., 2022

Solution #20: Access SNPN via 3GPP and N3GPP AN using same Credentials and Credential Holder (CH)

and

Solution #21: Support for NSWOF in SNPN

This solution addresses KI#2: Support of Non-3GPP Access for SNPN

Many Enterprise Networks have existing deployments with Non-3GPP Network Infrastructure (**WLAN or Wireline Access**) using the AAA Server to Authenticate the End-Devices.

The addition of SNPN deployments could leverage the already provisioned identities and credentials to authenticate devices accessing SNPN via 3GPP and non-3GPP Access Networks, both connecting to 5GC via a CH (AAA server) external to the SNPN.

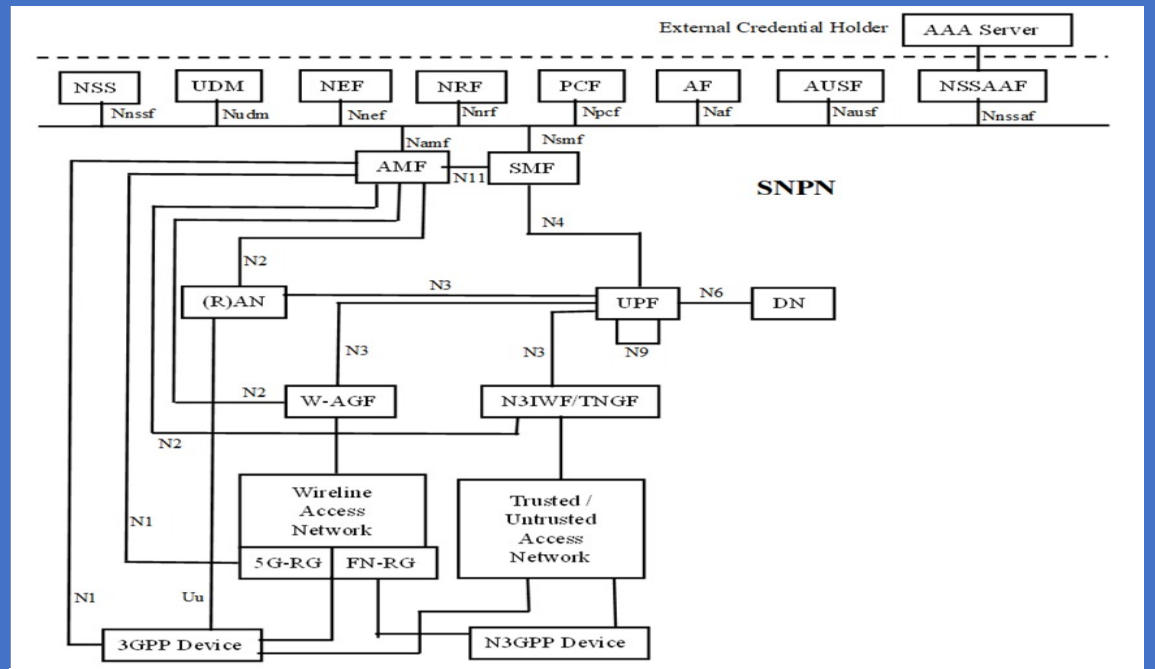


Figure: Access to SNPN via 3GPP and non-3GPP Access Networks (both connected to 5GC) using the same Credentials from an External Credential Holder)

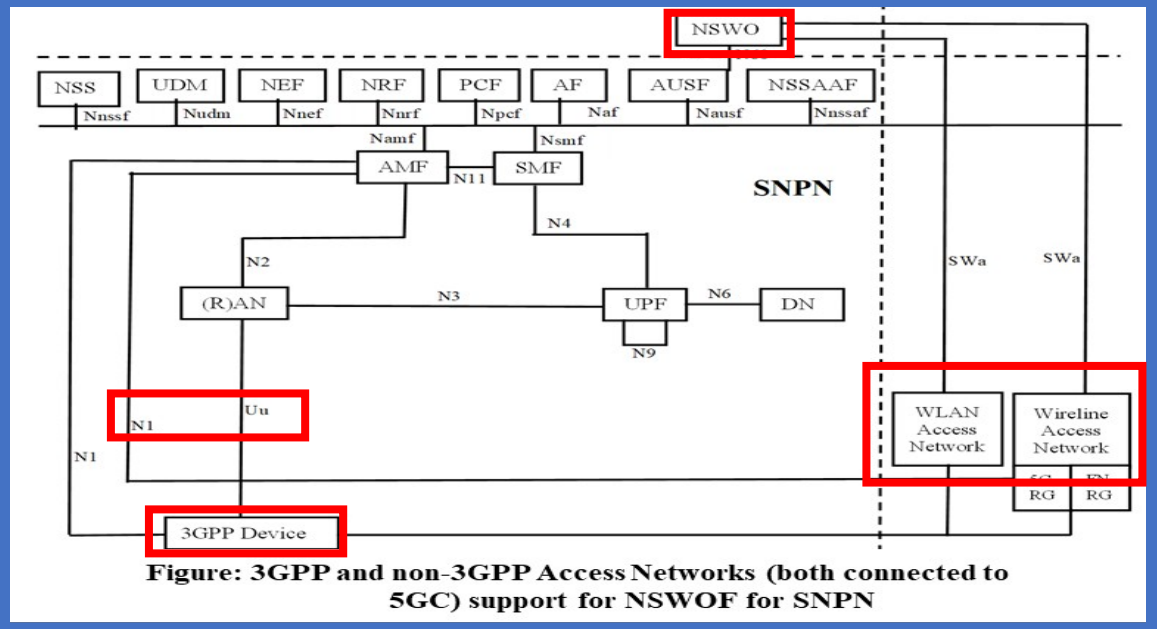


Figure: 3GPP and non-3GPP Access Networks (both connected to 5GC) support for NSWOF for SNPN

Ref: 3GPP, NPNs/SNPNs, Rel. 18, Aug., 2022

Summary: Access SNPN via 3GPP and N3GPP AN using same Credentials and Credential Holder (CH)

Solutions on KI#2: Support of Non-3GPP Access for SNPN

Many Enterprise Networks have existing deployments with Non-3GPP Network Infrastructure (**WLAN or Wireline Access**) using the AAA Server to Authenticate the End-Devices.

The addition of SNPN deployments could leverage the already provisioned identities and credentials to authenticate devices accessing SNPN via 3GPP and non-3GPP Access Networks, both connecting to 5GC via a CH (AAA server) external to the SNPN.

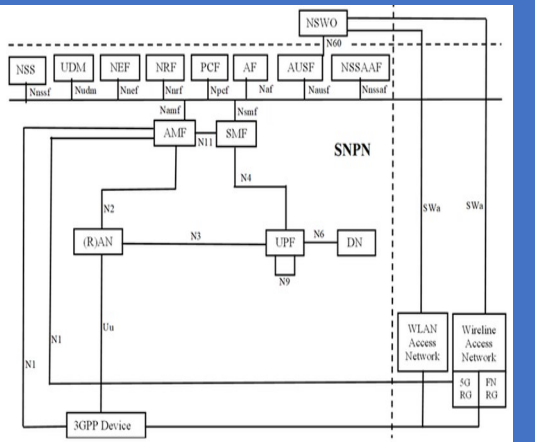


Figure: 3GPP and non-3GPP Access Networks (both connected to 5GC) support for NSWOF for SNPN

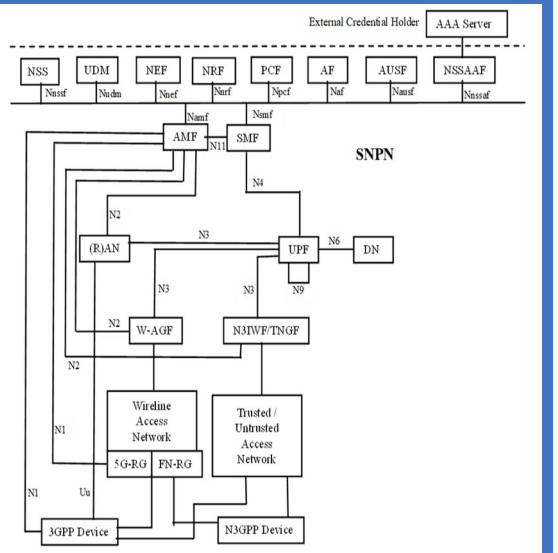


Figure: Access to SNPN via 3GPP and non-3GPP Access Networks (both connected to 5GC) using the same Credentials from an External Credential Holder)

Table 7.2-1: Evaluation of solutions for Key Issue 2

Solution #2 Access to SNPN services via Untrusted non-3GPP access network	In this solution, UE that has successfully obtained IP connectivity via an Untrusted non-3GPP access network may select the N3IWF of an SNPN and register with that SNPN (using the credentials of that SNPN) following the same N3IWF selection procedure as specified for access to stand-alone non-public network services via PLMN. For support of Emergency services the UE either relies on a configured N3IWF FQDN for N3IWF selection (when non-roaming) or follows the existing procedure for Emergency services for UE not equipped with UICC (when roaming). The solution makes no special provisions for UE onboarding assuming that, either the PVS is reachable over the public Internet that the UE accesses via the untrusted non-3GPP access network, or the UE relies on an ON-SNPN with 3GPP access. The solution has UE impact and N3IWF impact (inclusion of "selected NID" in the [NGAP] INITIAL UE MESSAGE, which is up to RAN3 to define).
Solution #3 Access to SNPN services via Trusted non-3GPP access network	The solution assumes that the non-3GPP access network advertises (e.g. with ANQP) the SNPNs with which 5G connectivity is supported, as well as the indications defined in clause 5.30.2.2 of TS 23.501 [3]. The UE is configured with one or more prioritized SNPN/GIN lists as defined in clause 5.30.2.3 of TS 23.501 [3]. For support of Emergency services the non-3GPP access network advertises the support of Emergency service (e.g. via ANQP). For support of UE onboarding the non-3GPP access network advertises the Onboarding enabled indication (e.g. via ANQP). The solution has UE impact, non-3GPP access network impact (additional parameters in ANQP messages) and TNGF impact (inclusion of "selected NID" in the [NGAP] INITIAL UE MESSAGE, which is up to RAN3 to define). The solution has impacts if UE constructs a prioritized list of WLAN access networks by using the WLAN Selection Policy (WLANSP) rules from ANSDP (currently supported only for PLMN in). Alternatively, the solution can rely on local configuration in the UE.
Solution #4 Support of onboarding over untrusted non-3GPP access in SNPN	This solution builds on top of Solution #2 and aims to add support for the following scenarios: - access to PVS is restricted inside the ON-SNPN and the PVS is not accessible from the public internet directly over the "untrusted non-3GPP access network". - UE accesses to SNPN via indirect non-3GPP access or direct non-3GPP access for Onboarding. The additional UE impact (compared to Solution #2) includes the ability to construct a GIN-based FQDN for selection of the N3IWF/SNPN that will be used for UE onboarding, as well as inclusion of Onboarding indication in the AN parameter sent to the N3IWF during registration procedure. The solution has several unresolved Editor's notes.
Solution #5 Support of Credentials Holder scenarios over untrusted non-3GPP access in SNPN	This solution builds on top of Solution #2 and aims to add support for accessing SNPN using credentials owned by Credentials Holder separate from the SNPN. The additional UE impact (compared to Solution #2) includes the ability to construct a GIN-based FQDN for selection of the N3IWF/SNPN where UE accesses by using credentials owned by the Credentials Holder belonging to a group identified by the GIN. The solution has several unresolved Editor's notes.
Solution #6 Access to SNPN services via wireline access network	The solution defines how the 5G-RG, FN-RG, and devices behind the RG (UE or N5GC devices behind an FN-RG or 5G-RG) can access SNPN services via a wireline access network. It is based on clause 4.2.1 of TS 23.316, where the SNPN is implicitly selected by wired physical connectivity between 5G-RG or FN-RG and W-AGF. The only additional requirement is that the NID is included as part of the registration procedure for wireline access system. The solution has 5G-RG and W-AGF impact (ability to formulate the SUCI that includes the SUPI type as "IMSI" and the home network domain which includes a NID in addition to PLMN ID).
Solution #16 Access to SNPN with NG-RAN and to WLAN Access Network using the same credentials	The solution describes how UE can access an SNPN with NG-RAN on one hand and a WLAN Access Network on the other hand using the same credentials. UE uses the same permanent identity (SUCI) and credentials for primary authentication in SNPN and for WLAN access authentication in a WLAN Access Network. For access network selection the solution assumes that either mechanisms standardised by 3GPP (e.g. using ANDSP) need to be enhanced for Non-Seamless WLAN Offload or rely on local UE configuration. Seamless mobility is not in scope of this solution. The solution has UE impacts. The solution has TS 23.402 [9] impacts if WLAN Selection Policy (WLANSP) rules from ANDSP are used for Non-Seamless WiFi Offload (currently supported only for PLMN . Alternatively, the solution can rely on local configuration in the UE. The solution requires new authentication procedure and needs to be evaluated by SA3.
Solution #19 Access to SNPN services via Untrusted non-3GPP access network with underlay/overlay determination	This solution builds on top of Solution #2 and aims to add a new RAT Type to discriminate between direct access to SNPN services via N3GPP access (as in Solution #2) and indirect access to SNPN services via PLMN as defined in TS 23.501 [3] clause 5.30.2.8 and clause D.3. The RAT Type for these two cases would be set to "Untrusted N3GPP" or "Untrusted Non-3GPP over underlay PLMN", respectively. The underlying assumption is that in some scenarios the access to the SNPN's 5GC may need to be restricted for one of the RAT Types, but not for the other. The solution has UE, N3IWF and AMF impact related to the determination of the RAT Type. The solution has an unresolved Editor's notes related to how the N3IWF determines the access network information.
Solution #20 Access SNPN via 3GPP and N3GPP AN using same credentials and credential holder	The solution defines how the same credentials from a credential holder external to the SNPN can be leveraged for devices accessing SNPN via 3GPP and non-3GPP access network (both connected to 5GC). The solution has no normative impacts beyond the impact of Solution #5 (support of Credentials Holder over untrusted non-3GPP access in SNPN) and Solution #3 (support of Credentials Holder over trusted non-3GPP access in SNPN). The scenario of UE and N3GPP device connected to 5GC via 5G-RG/FN-RG, is FFS. This scenario shall take into account the conclusion of the FS_5WWC_Ph2 study on the support of the device behind an RG.
Solution #21 Support for NSWOF in SNPN	The solution proposes to extend the NSWO authentication so that UE can access a non-3GPP network (e.g. WLAN or Wireline access network) using the same permanent identity and credentials as for primary authentication in SNPN via NG-RAN and 5GC. The solution has UE and 5G-RG impacts for support of NSWO authentication using SNPN credentials i.e. credentials with user identity whose "realm" part enables routing of SWa requests from the WLAN AN to the NSWO in the SNPN's 5GC (applies both to SIM-based and non-SIM based credentials). The 5G-RG impacts have dependency on the FS_5WWC_Ph2 study (e.g. Solution #22

Ref: 3GPP, NPNs/SNPNs, Rel. 18, Aug., 2022

1. Key Issue #1: Enabling support for idle and Connected mode Mobility between SNPNs without New Network selection

2. Key Issue #2: Support of Non-3GPP Access for SNPN

3. Key Issue #3: Enabling NPN as hosting network for providing Access to Localized Services

4. Key Issue #4: Enabling UE to Discover, Select and Access NPNs as Hosting Network and receive Localized Services

5. Key Issue #5: Enabling Access to Localized Services via a Specific Hosting Network

6. Key Issue #6: Support for returning to Home Network

Mapping Solutions to Key Issues

Table : Mapping Solutions to Key Issues

	Key Issues					
Solutions	1	2	3	4	5	6
1	X					
2		X				
3		X				
4		X				
5		X				
6		X				
7			X	X	X	X
8						X
9						X
10				X		X
11				X	X	
12			X	X		
13				X	X	
14				X		
15				X	X	
16		X				
17						X
18					X	
19		X				
20		X				
21		X				
22			X			
23				X		
24				X		
25				X		X
26				X		
27				X	X	
28				X	X	
29				X		
30				X		
31				X		
32				X		
33				X		
34				X		
35				X	X	
36					X	
37					X	
38						X
39						X
40				X	X	
41			X	X		
42				X		
43				X		
44				X		
45				X	X	
46					X	
47						X

Ref. 3GPP, Rel. 18, Aug., 2022)

3GPP V18.2.0 (2021-12)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on 5G Networks Providing Access to Localized Services; Stage 1 (Release 18)

PALS Consolidated Potential Requirements (CPR)

Table - Configuration of Localized Services in Hosting Network Consolidated Requirements

CPR #	Consolidated Potential Requirement	Original PR #	Comment
CPR 6.1-001	The 5G network shall support suitable mechanisms to allow automatically establishing localized service agreements for a specific occasion (time and location) and building temporary relationship among hosting network operator and other service operators including network operators or 3rd party service providers.	PR.5.3.6-1	
CPR 6.1-002	The 5G system shall support means for the service operator to request the hosting network via standard mechanisms to provide access to 3rd party services at a specific period of time and location. This period of time shall be flexible, so that a change in service provision can be decided at any time (e.g., to cancel or prolong local services in the locality of service delivery) based on localized services agreements.	PR.5.5.6-1	
CPR 6.1-003	Based on localized services agreements, the 5G system shall provide suitable means to allow the service operator to request and provision various localized service requirements, including QoS, expected/maximum number of users, event information for discovery, network slicing, required IP connectivity etc, and routing policies for the application of the localized services via the hosting network.	PR.5.5.6-2 and PR.5.4.6-1	
CPR 6.1-004	The 5G system shall support means for a hosting network to create policies and configure resources for the requested time and location for the 3rd party services based on the received request.	PR.5.5.6-3	
CPR 6.1-005	The 5G system shall support means for a hosting network to notify the service operator of the accepted service parameters and routing policies.	PR.5.5.6-4	
CPR 6.1-006	Subject to regulatory requirements and localized service agreements, the 5G network shall allow a home network operator to automatically negotiate policies with the hosting network for allowing the home network's subscribers to connect at a specific occasion, e.g., time and location, for their home network services.	PR.5.3.6-2	
CPR 6.1-007	Subject to the automatic localized services agreements between the hosting network operator and home network operator, for UE with only home network subscription and with authorization to access hosting networks the 5G system shall support: - access to the hosting network and use home network services or selected localized services via the hosting network. - seamless service continuity for home network services or selected localized services when moving between two hosting networks or a host network and the home network.	PR.5.3.6-5	
CPR 6.1-008	The 5G System shall support a mechanism to enable configuration of a network that provides access to localized services such that the services can be limited in terms of their spatial extent (in terms of a particular topology, for example a single cell), as specified by a 3rd party.	PR.5.10.6-1	
CPR 6.1-009	The 5G System shall support a mechanism to enable configuration of a network that provides access to localized services such that the services can be limited in terms of the resources or capacity available, to correspond to requirements that apply only to the locality of service delivery, as specified by a 3rd party.	PR.5.10.6-2	
CPR 6.1-010	The 5G system shall support means for a hosting network to provide a 3rd party service provider with information for automatic discovery of the hosting network by the UEs to allow access to specific 3rd party services.	PR.5.6.6-1	
CPR 6.1-011	The 5G system shall support secure mechanisms to allow a home network to coordinate with a hosting network for a subscriber to temporarily access the hosting network (e.g., based on temporary credentials) at a given time (start time and duration) and location.	PR.5.8.6-1	

NOTE 1: **Both the Home and the Hosting Network can be a PLMN or NPN.**

NOTE 2: **Only Subscribers of a Public Network can roam into a PLMN.**

PALS Consolidated Potential Requirements (CPR) -

NOTE 1: **Both the Home and the Hosting Network can be a PLMN or NPN.**

NOTE 2: Only Subscribers of a Public Network can roam into a PLMN.

User Manual Selection of Localized Services via Hosting Network

Table - User Manual Selection of Localized Services via Hosting Network Consolidated Requirements

CPR #	Consolidated Potential Requirement	Original PR #	Comment
CPR 6.2-001	The hosting network shall allow a UE to manually select temporary localized services which are provided via local breakout at the hosting network. NOTE : localized services are provided via local breakout at the hosting network based on interworking scenarios for hosting network owned/collaborative services as indicated in Annex A.	PR.5.4.6-2	

UE Configuration, Provisioning, Authentication & Authorization

Table - UE Configuration, Provisioning, Authentication and Authorization Consolidated Requirements

CPR #	Consolidated Potential Requirement	Original PR #	Comment
CPR 6.3-001	Subject to localized services agreements, the 5G network shall enable a home network operator to authorize a UE for using its home network services via a hosting network for a certain period of time and/or location.	PR.5.3.6-3	
CPR 6.3-002	The 5G network shall allow a trusted 3rd party to provide UEs with localized service policy (e.g., QoS, network slice in the hosting or home network, service restriction such as time and location) via the hosting network or the UE's home network.	PR.5.4.6-1A	
CPR 6.3-003	The 5G system shall enable a UE to use credentials provided by the hosting network with or without coordination with the home network of the UE, to make use of localized services via the hosting network with a certain time (including starting time and the duration) and location validity.	PR.5.4.6-7	
CPR 6.3-004	The 5G network shall be able to allow the home network to steer its UE(s) to a hosting network with the consideration of the location, times, coverage of the hosting network and services offered by the home network and hosting network.	PR.5.11.6-1	
CPR 6.3-005	The 5G system shall provide support to enable secure means to authenticate and authorize a user of a UE accessing a hosting network, including cases in which a UE has no subscription to the hosting network and still needs to get authorized to use localized services via the hosting network. NOTE : It can be assumed that a network provider deploying a hosting network has access to respective identification information about the user, e.g., through a separate registration process outside the scope of 3GPP.	PR.5.15.6-2	
CPR 6.3-006	The 5G system shall be able to authenticate and authorize the UE of a user authenticated to a hosting network to access the hosting network and its localized services on request of a service provider.	PR.5.15.6-3 and PR.5.2.6-2	

PALS Consolidated Potential Requirements (CPR) -

NOTE 1: **Both the Home and the Hosting Network can be a PLMN or NPN.**
NOTE 2: Only Subscribers of a Public Network can roam into a PLMN.

Hosting Network Localized Services and Home Operator Services

Table - Hosting Network Localized Services and Home Operator Services Consolidated Requirements

CPR #	Consolidated Potential Requirement	Original PR #	Comment
CPR 6.5-001	The 5G network shall enable the home network operator to indicate to the UE what services are preferred to be used from the home network when the UE connects to a hosting network and the requested services are available from both the hosting and the home network.	PR.5.3.6-4	
CPR 6.5-002	Based on localized service agreements, the hosting network shall be able to provide required connectivity and QoS for a UE simultaneously connected to the hosting network for localized services and its home network for home network services.	PR.5.4.6-3	
CPR 6.5-003	A UE shall be able to connect to its home network via the hosting network, if supported by the hosting network and the home network based on localized service agreements.	PR.5.4.6-4	

Returning to Home Network

Table - Returning to Home Network Consolidated Requirements

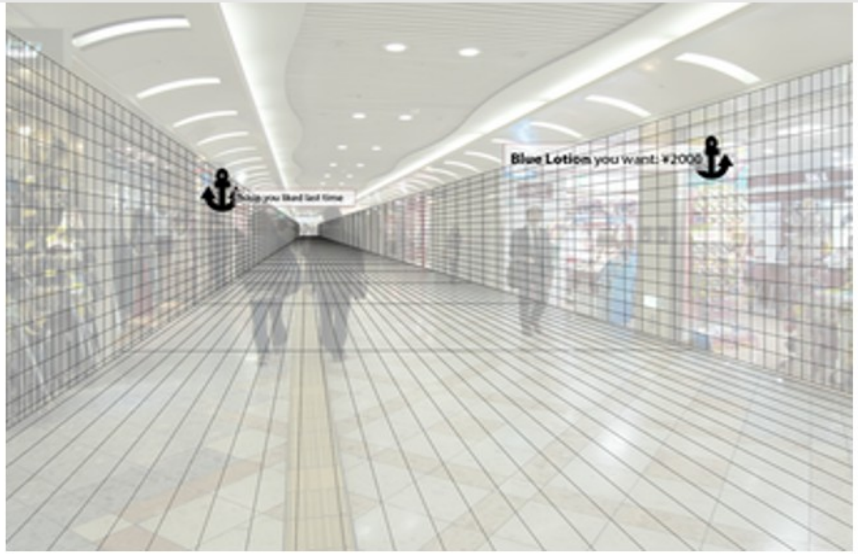
CPR #	Consolidated Potential Requirement	Original PR #	Comment
CPR 6.6-001	The 5G system shall provide mechanisms to mitigate user plane and control plane overload caused by a high number of UEs returning from a temporary local access of a hosting network to their home network in a very short period of time.	PR.5.14.6-1	
CPR 6.6-002	The 5G system shall provide mechanisms to minimize the impact on the UEs communication e.g., to prevent user plane and control plane outages when returning to a home network together with other high number of UEs in a very short period of time, after terminating their temporary local access to a hosting network.	PR.5.14.6-2	

3GPP

V0.1.0 (2022-05)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group TSG SA;
Feasibility Study on Localized Mobile Metaverse Services (Release 19)



Use Cases

1. Localized Mobile Metaverse Service Use Cases
2. Mobile Metaverse for 5G-enabled Traffic Flow Simulation and Situational Awareness

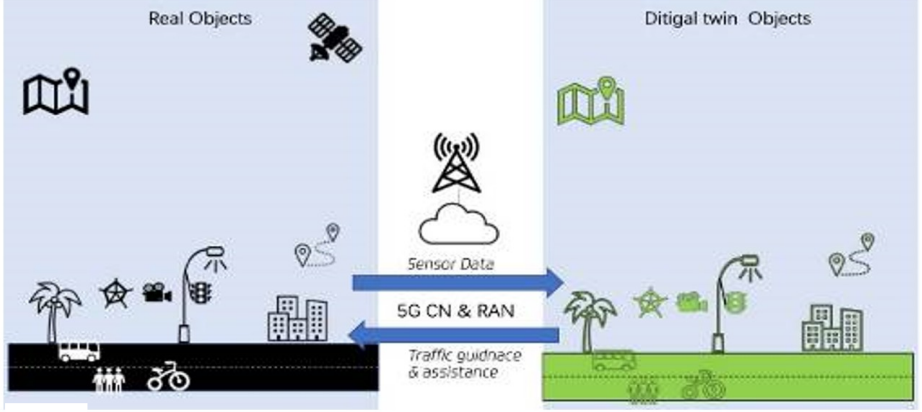


Figure Scenario of 5G-enabled Traffic Flow Simulation and Situational Awareness

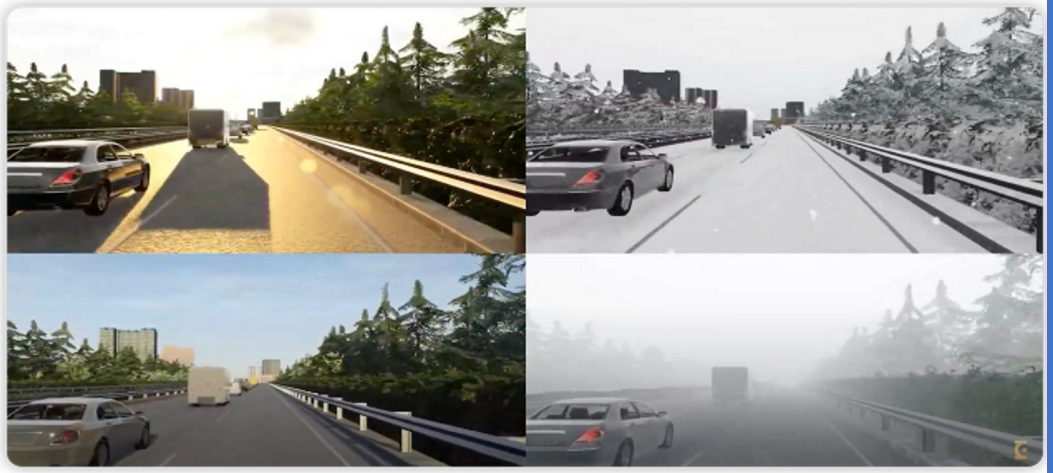


Figure Example of Smart Transport Metaverse

Figure Localized Mobile Metaverse Services offering relevant information

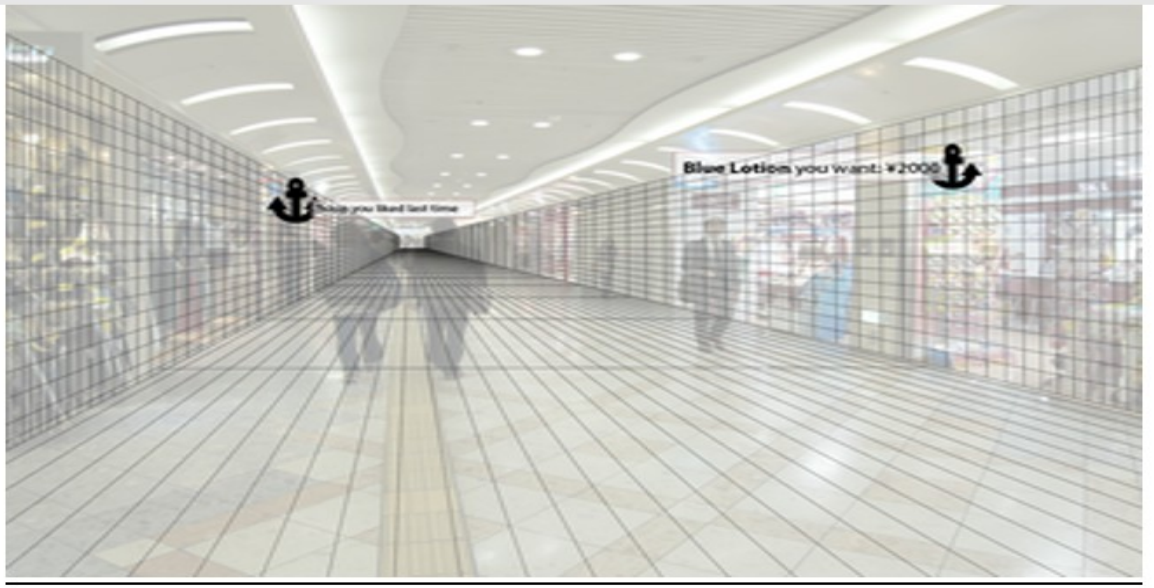


Figure: Service offering relevant information are anchored in Space

Use Cases: 3 Collaborative and Concurrent Engineering in Product Design using Metaverse Services

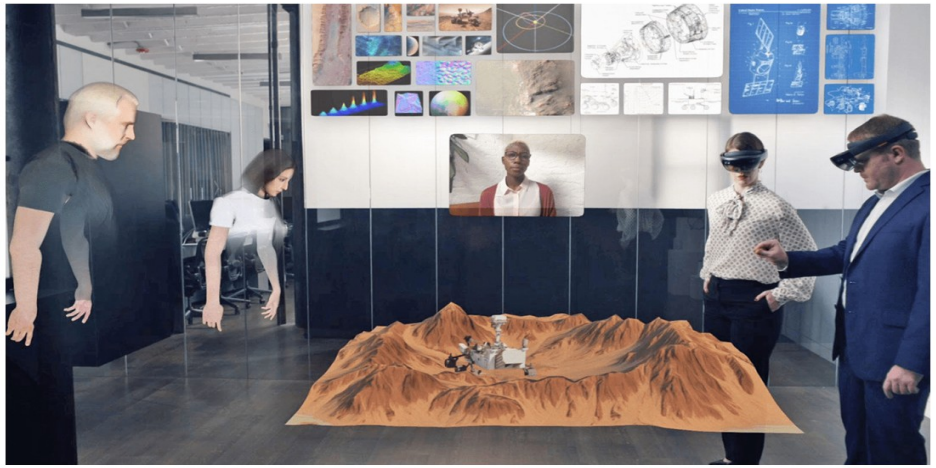


Figure XR enabled collaborative and concurrent engineering in product design

Table Typical QoS requirements for multi-modal streams [9] [10] [11] [12] [13]

	Haptics	Video	Audio
Jitter (ms)	≤ 2	≤ 30	≤ 30
Delay (ms)	≤ 50	≤ 400	≤ 150
Packet loss (%)	≤ 10	≤ 1	≤ 1
Update rate (Hz)	≥ 1000	≥ 30	≥ 50
Packet size (bytes)	64-128	≤ MTU	160-320
Throughput (kbit/s)	512-1024	2500 - 40000	64-128

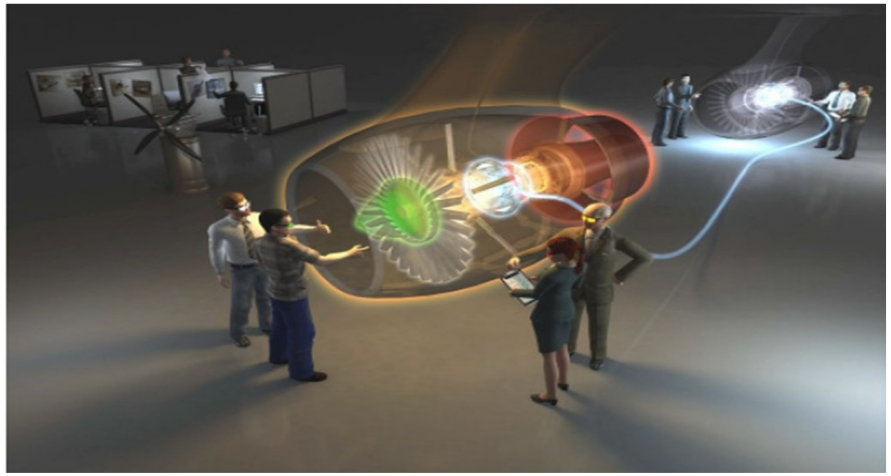


Figure : Illustration of Collaborative Workspace (Source: ESI-Icido GmbH)

Table – Potential key performance requirements for collaborative and concurrent engineering in product design

Use Cases	Characteristic parameter (KPI)				Influence quantity		
	Max allowed end-to-end latency	Service bit rate: user-experienced data rate	Reliability	Area Traffic capacity	Message size (byte)	UE Speed	Service Area
Collaborative and concurrent engineering	[10] ms(note 1)	[1-100] Mbit/s ([14])	[> 99.9%] ([14])	[3.804] Tbit/s/km^2 (note 2)	Typical haptic data: 1 DoF: 2-8 3 DoFs: 6-24 6 DoFs: 12-48 Video: 1500 Audio: 100 ([14])	Stationary or Pedestrian	typically < 100 km^2 (note 3)

NOTE 1: The network based conference focus is assumed, which receives data from all the participants, performs rendering (image synthesis), and then distributes the results to all participants. The latency refers to the transmission delay between a UE and the application server.

NOTE 2: To support at least 15 users present at the same location (e.g. in an area of 20m*20m) to actively enjoy immersive Metaverse service concurrently, the area traffic capacity is calculated considering per user consuming non-haptic XR media (e.g. for video per stream up to 40000 kbit/s) and concurrently 60 haptic sensors (per haptic sensor generates data up to 1024 kbit/s).

NOTE 3: In practice, the service area depends on the actual deployment. In some cases a local approach (e.g. the application servers are hosted at the network edge) is preferred in order to satisfy the requirements of low latency and high reliability.

5G Tactile and Multi-modal VR Communication Service

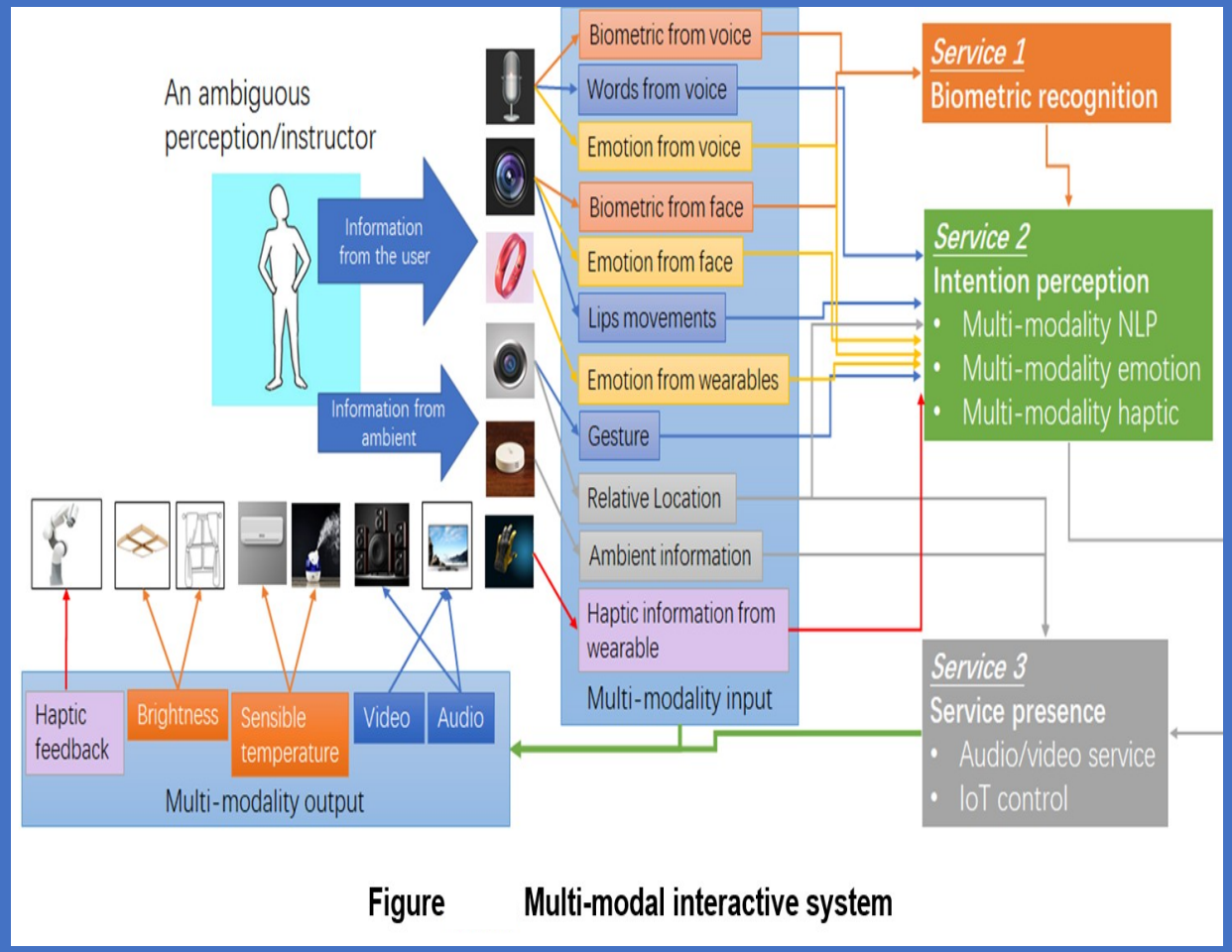


Figure Multi-modal interactive system

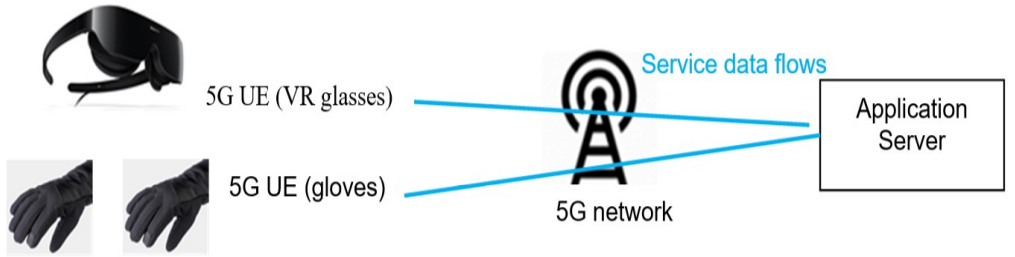


Figure . Immersive multi-modal VR application with multiple 5G UEs directly connected to 5G network

Table : Typical synchronization thresholds for immersive multi-modality VR applications

Media components	synchronization threshold (note 1)	
audio-tactile	audio delay: 50 ms	tactile delay: 25 ms
visual-tactile	visual delay: 15 ms	tactile delay: 50 ms
NOTE 1: for each media component, "delay" refers to the case where that media component is delayed compared to the other.		

Use case - 5G Immersive Multi-modal Virtual Reality (VR) Application Key Performance Requirements

Table Potential key performance requirements for immersive multi-modal VR applications

Use Cases	Characteristic parameter (KPI)			Influence quantity				Remarks
	Max allowed end-to-end latency	Service bit rate: user-experienced data rate	Reliability	Message size (byte)	# of UEs	UE Speed	Service Area	
Immersive multi-modal VR (UL: device → application sever)	5 ms (note 2)	16 kbit/s -2 Mbit/s (without haptic compression encoding); 0.8 - 200 kbit/s (with haptic compression encoding)	[99.9%] (without haptic compression encoding) [99.999%] (with haptic compression encoding)	1 DoF: 2-8 3 DoFs: 6-24 6 DoFs: 12-48 More DoFs can be supported by the haptic device	-	Stationary or Pedestrian	typically < 100 km² (note 3)	Haptic feedback
	5 ms	< 1Mbit/s	[99.99%]	MTU	-	Stationary or Pedestrian	typically < 100 km² (note 3)	Sensor information e.g. position and view information generated by the VR glasses
Immersive multi-modal VR (DL: application sever → device)	10 ms (note1)	1-100 Mbit/s	[99.9%]	1500	-	Stationary or Pedestrian	typically < 100 km² (note 3)	Video
	10 ms	5-512 kbit/s	[99.9%]	50	-	Stationary or Pedestrian	typically < 100 km² (note 3)	Audio
	5 ms (note 2)	16 kbit/s -2 Mbit/s (without haptic compression encoding); 0.8 - 200 kbit/s (with haptic compression encoding)	[99.9%] (without haptic compression encoding) [99.999%] (with haptic compression encoding)	1 DoF: 2-8 3 DoFs: 6-24 6 DoFs: 12-48	-	Stationary or Pedestrian	typically < 100 km² (note 3)	Haptic feedback

NOTE 1: Motion-to-photon delay (the time difference between the user's motion and corresponding change of the video image on display) is less than 20 ms, the communication latency for transferring the packets of one audio-visual media is less than 10 ms, e.g. the packets corresponding to one video/audio frame are transferred to the devices within 10 ms.

NOTE 2: According to IEEE 1918.1 [3] as for haptic feedback, the latency is less than 25 ms for accurately completing haptic operations. As rendering and hardware introduce some delay, the communication delay for haptic modality can be reasonably less than 5 ms, i.e. the packets related to one haptic feedback are transferred to the devices within 10 ms.

NOTE 3: In practice, the service area depends on the actual deployment. In some cases a local approach (e.g. the application servers are hosted at the network edge) is preferred in order to satisfy the requirements of low latency and high reliability.

PALS The Application Layer Approaches require 5G Network to expose Network Capabilities for Localized Services

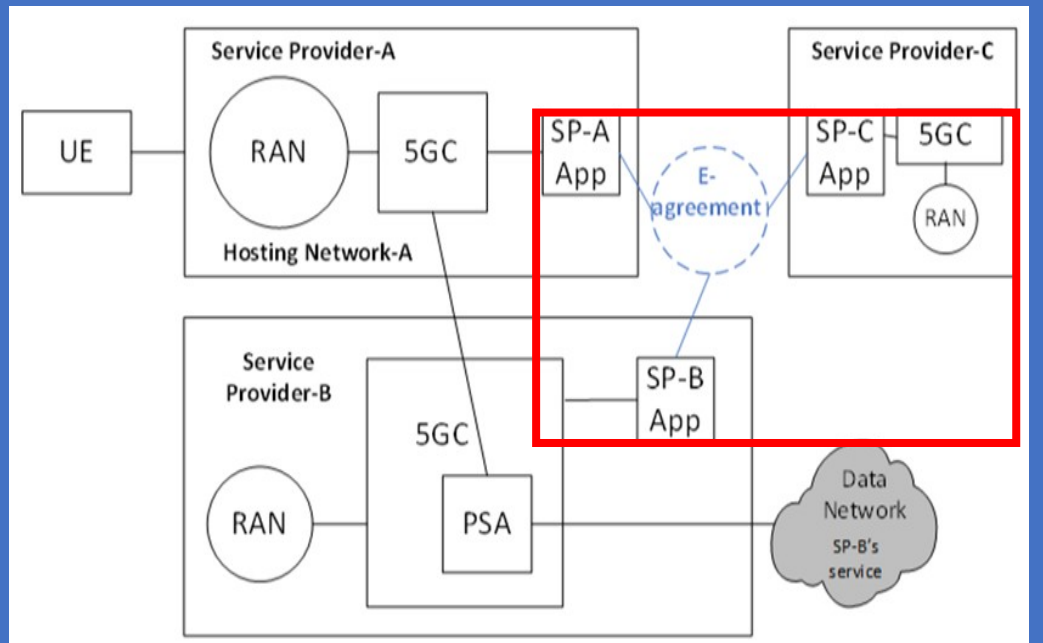
As shown in the Figure, the e-Agreement is established among Service Operators, e.g. SP-A, SP-B, and SP-C have no SLAs in place for the Services provided by SP-A's Hosting Network - A.

The SP-A Operator creates an e-Agreement which provides the Localized Service Configuration.

The SP-B and SP-C Operators can subscribe this Localized Service with required Service Policies for their UEs.

The SP-B and SP-C can then configure their UEs for Localized Service.

Based on the e-Agreement, the Hosting Network can be configured with Localized Service at a specific time & location for its subscribers (other Network Operator), e.g. Localized Service Policies of Time, Location, Network-A Access Parameters, including Spectrum, Access Technologies (3GPP or non-3GPP), Network Slice, Charging Policies, and Subscriber's Network Policies for Authentication, and Routing.



Network Operators (MNOs) Relationship using Application Layer Approach

Use Case for UEs using home network services via hosting networks

Description

Given the main objective of the study that UEs and their service providers are without previous relationship to the hosting network, automatic e-agreement mechanisms are needed to allow network operators to build short term relationship using application layer approaches. The e-agreement mechanisms allow the automation of multi-step processes in telecommunication domain to establish service level e-agreement among network operators for enabling the 5GS to facilitate the sharing of services and resources of the networks among network operators and to configure their networks and UEs accordingly at specific occasion, e.g. time and location.

The application layer approaches require 5G network to expose network capabilities. For example, as shown in Figure the e-agreement is established among service operators, e.g. SP-A, SP-B, and SP-C have no SLAs in place for the services provided by SP-A's hosting network-A.

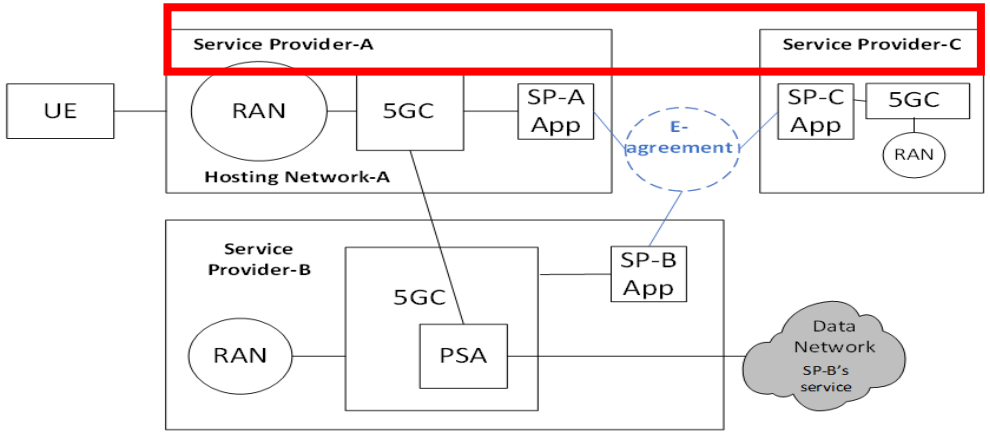


Figure : diagram for building relationship between network operators using application layer approach

3GPP TSG-SA1 Meeting #97-e
Online, , 14th Feb 2022 - 24th Feb 2022

S1-220219

CR-Form-v12.2

CHANGE REQUEST

22.261	CR	0630	rev	1	Current version:	18.5.0

*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:	Clarification of terminology for localized services
Source to WG:	Ericsson LM, Qualcomm
Source to TSG:	
Work item code:	PALS
Date:	2022-02-28
Category:	F
Release:	Rel-18

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.

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:	The chapter addressing local services (6.41) use the terms “service provider” and “service operator”, but there seems to be no clear distinction between these two terms. A service provider and a service operator seems to refer to the same entity, and if so, it is proposed to, to avoid unnecessary confusion and stick to the same term. The term ‘service provider’ is proposed
Summary of change:	Replace ‘service operator’ by ‘service provider’
Consequences if not approved:	Unnecessary risk of confusion with use of different terms for same purpose/entity

PALS Interworking between Networks Operators and Application Providers for Localized Services

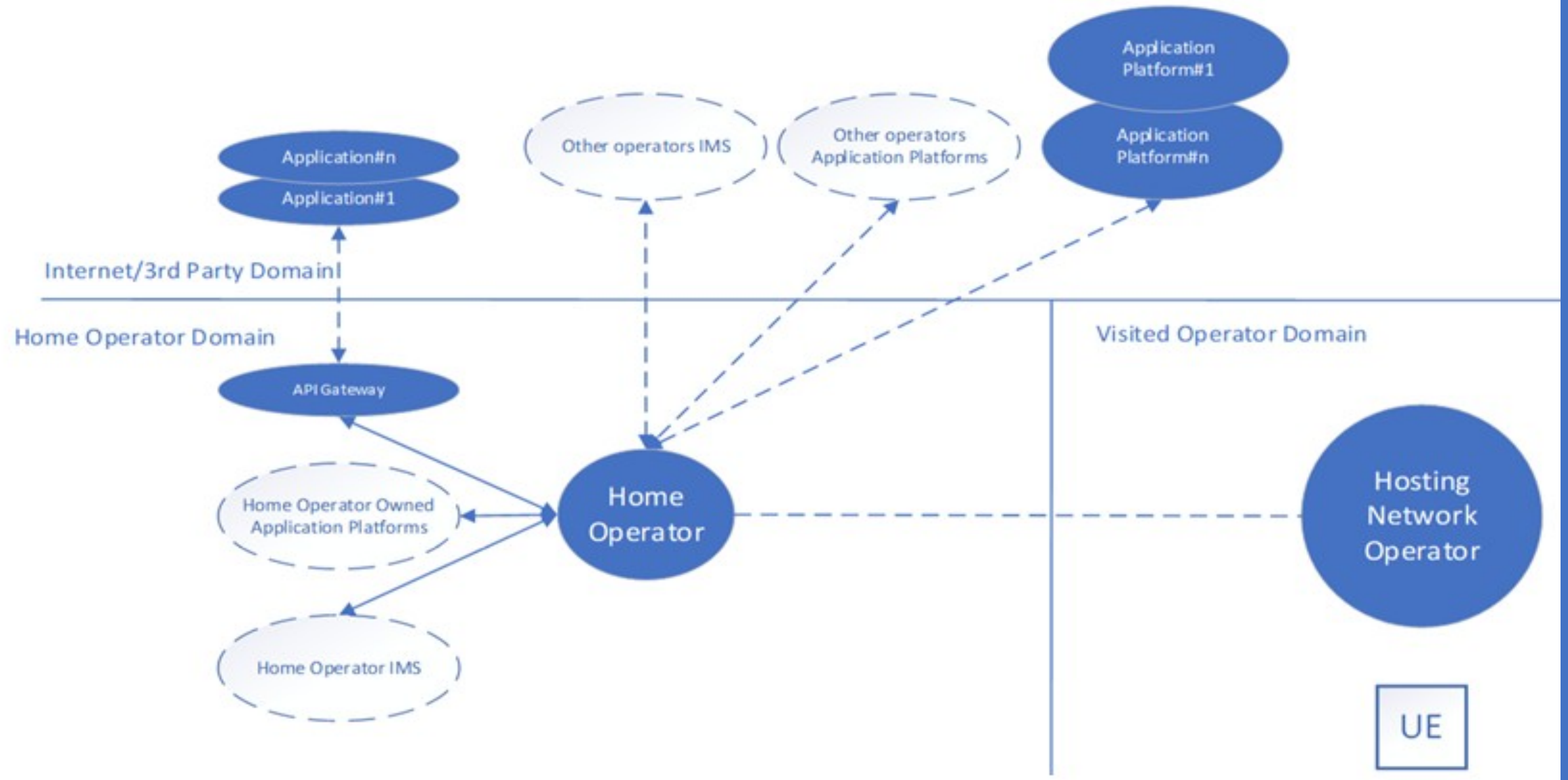


Fig.: Home Operator owned/collaborative Roaming Scenario - Home Routed

PALS Interworking between Networks Operators and Application Providers for Localized Services

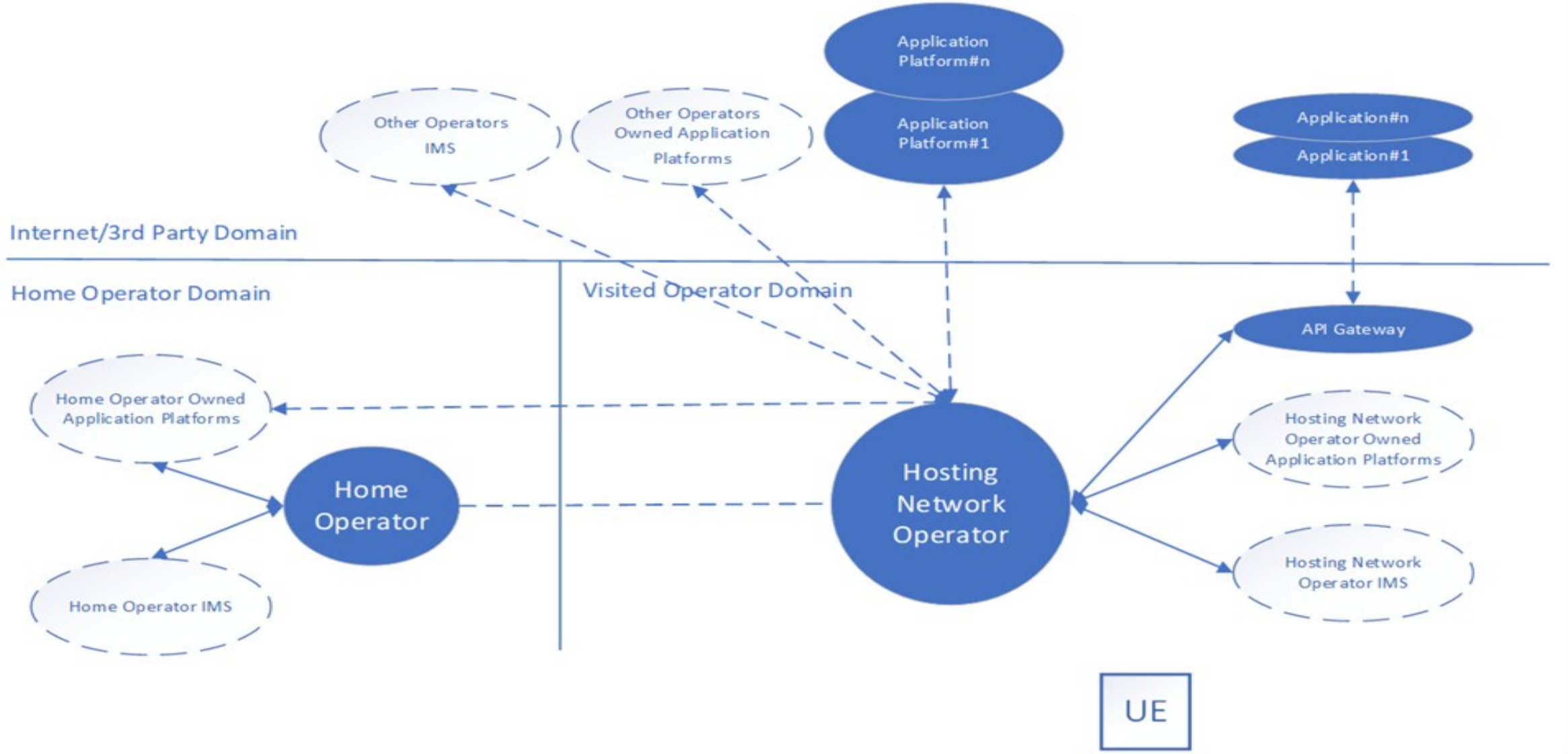


Fig.: Hosting Network Operator owned/collaborative Roaming Scenario - Local Breakout

5G NFs SFC - Service Function Chaining

Solutions shall build on the 5G System Architectural Principles including Flexibility and Modularity for newly introduced functionalities (**3GPP defined FMSS**).

- Service path (i.e. for Traffic handled by the Service Functions (SFs)) is traversed over N6 after PSA UPF(s) in 5G network.

Currently, the SMF may be configured with the Traffic Steering policy related to the mechanism enabling traffic steering to the N6-LAN, DN and/or DNAIs associated with N6 traffic routing requirements provided by the AF.

- UPF with SFC capabilities need to support flexible SFC configuration for a PDU session that requires different SFC processing for different Applications.

For allowing an AF, e.g. a 3rd Party AF, to request predefined SFC for Traffic Flow(s), etc. (when the AF belongs to a 3rd Party, this is based on Service Level Agreement (SLA) with the 3rd Party).

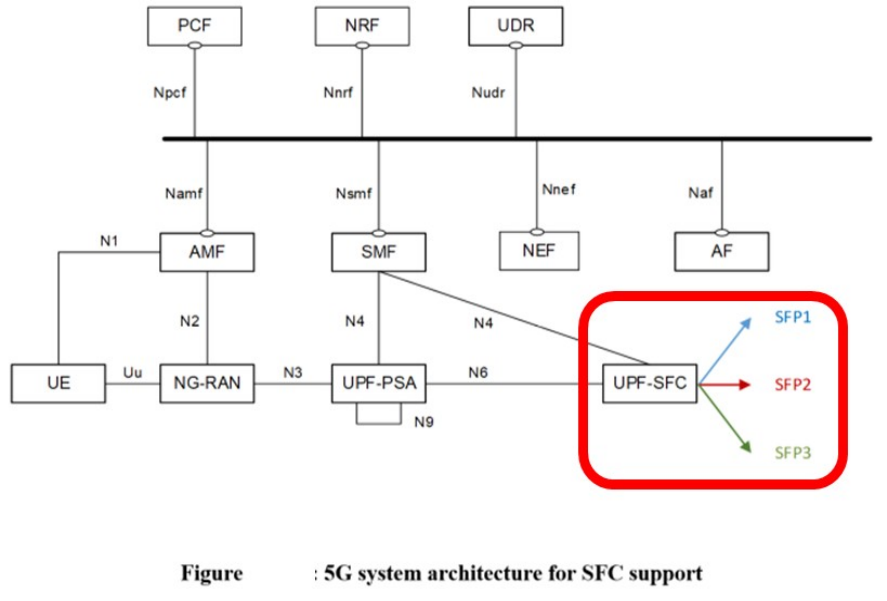


Figure : 5G system architecture for SFC support

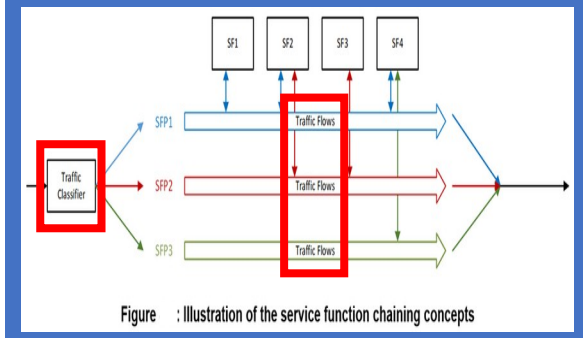
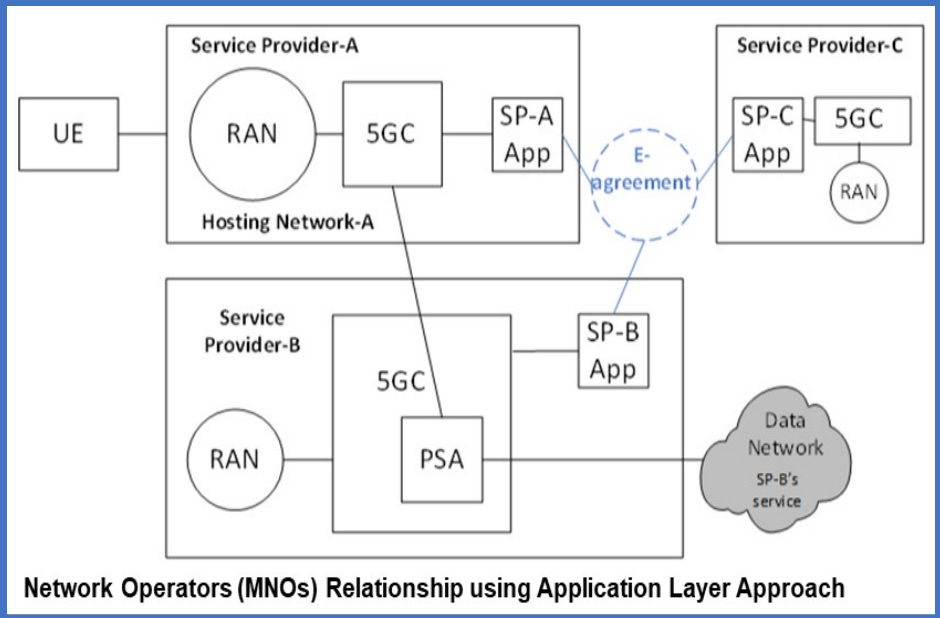


Figure : Illustration of the service function chaining concepts



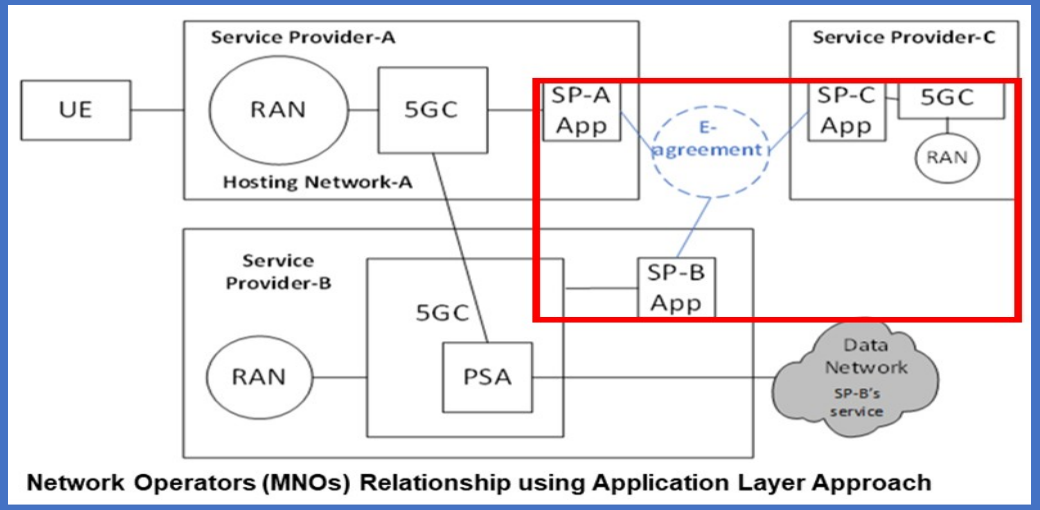
Network Operators (MNOs) Relationship using Application Layer Approach

3GPP

V18.2.0 (2021-12)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on 5G Networks Providing Access to Localized Services; Stage 1 (Release 18)



Network Operators (MNOs) Relationship using Application Layer Approach

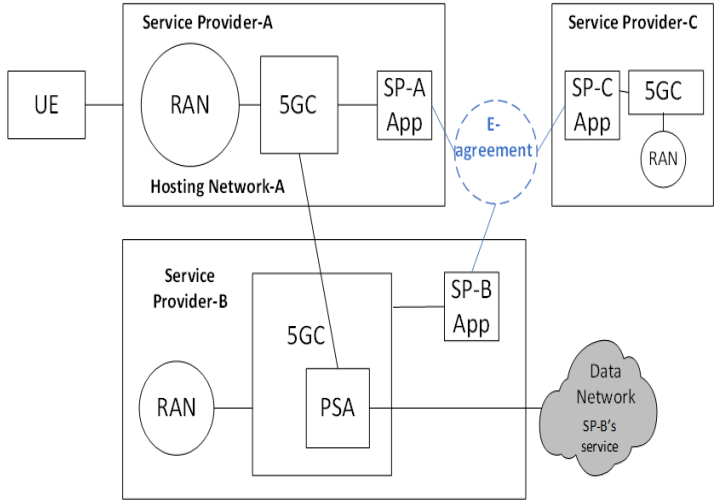


Figure : diagram for building relationship between network operators using application layer approach

The SP-A operator creates an e-agreement which provides the localized service configuration. The SP-B and SP-C operators can subscribe this localized service with required service policies for their UEs. The SP-B and SP-C can then configure their UEs for localized service.

Based on the e-agreement, the hosting network can be configured with localized service at a specific time and location for its subscribers (other network operator), e.g. localized service policies of time, location, network-A access parameters, including spectrum, access technologies (3GPP or non-3GPP), network slice, charging policies, and subscriber's network policies for authentication, and routing.

Based on the e-agreement, the hosting network configuration creation and termination can be performed by SP-A or a trusted third-party application of the subscriber representing other network operator. With the application layer approach, the localized service can be used by authorized UEs of SP-A, SP-B, and SP-C which subscribes the service.

Note: the Application approach for Automatic E-agreement is an example that provides some insights for what the suitable APIs would be required for localized service enabler in 5GS.

AEF (APIs Exposure Function) Capabilities

Potential enhancements in CAPIF and **Application Enablement Frameworks (e.g. SEAL, EDGEAPP, VAL - Vertical Application Layers)** to support the Subscriber-aware Northbound API Access (SNA), .

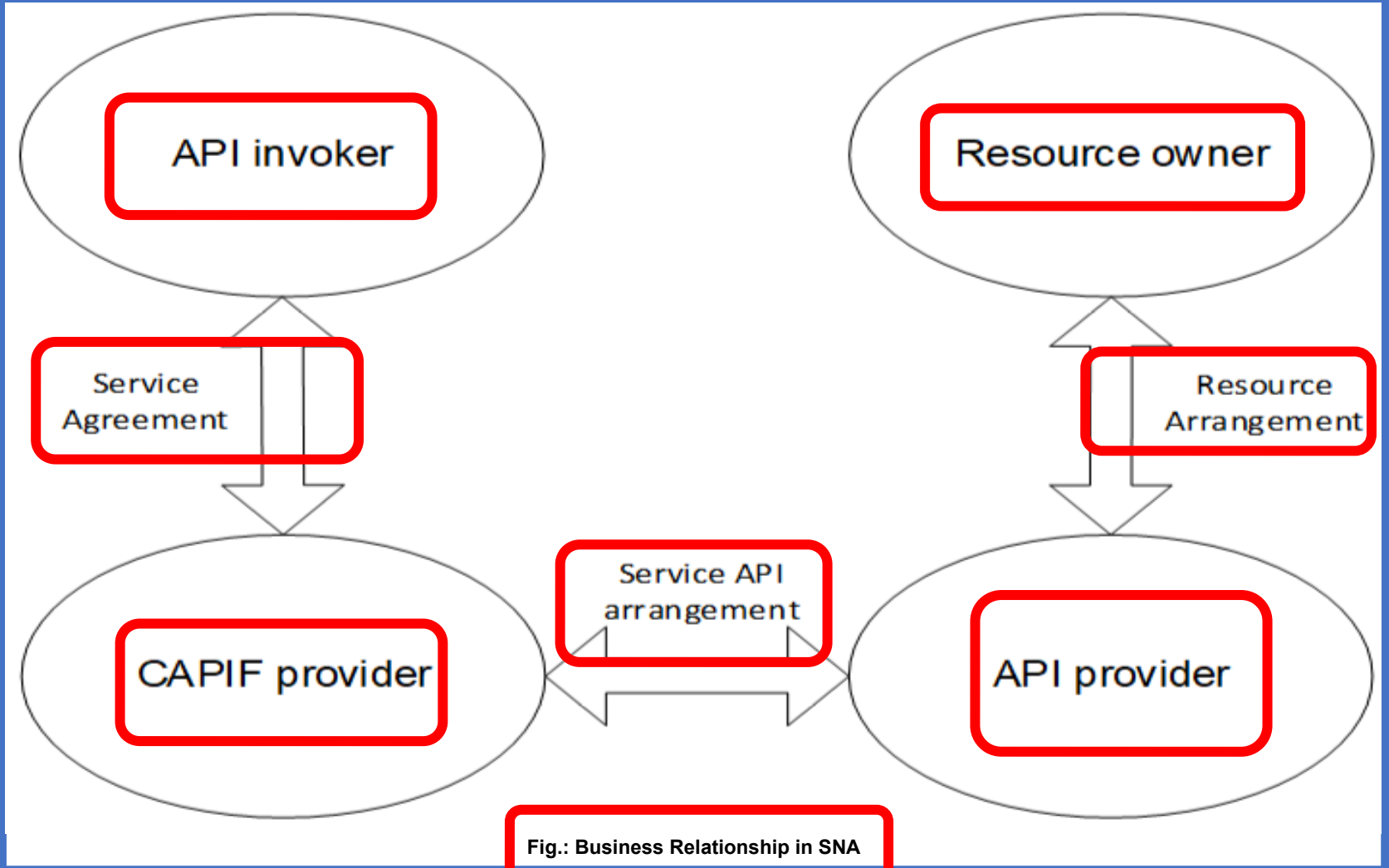


Fig.: Business Relationship in SNA

Potential enhancements in CAPIF and **Application Enablement Frameworks (e.g. SEAL, EDGEAPP, Vertical Enabler Layers**) to support the Subscriber-aware Northbound API Access (SNA), .

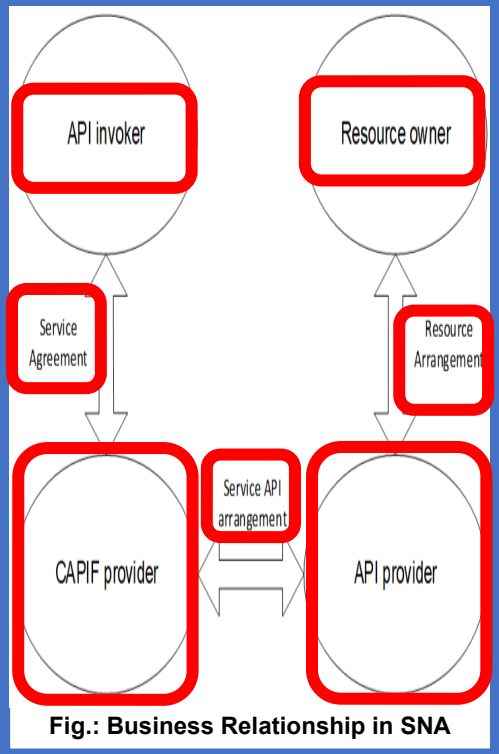


Fig.: Business Relationship in SNA

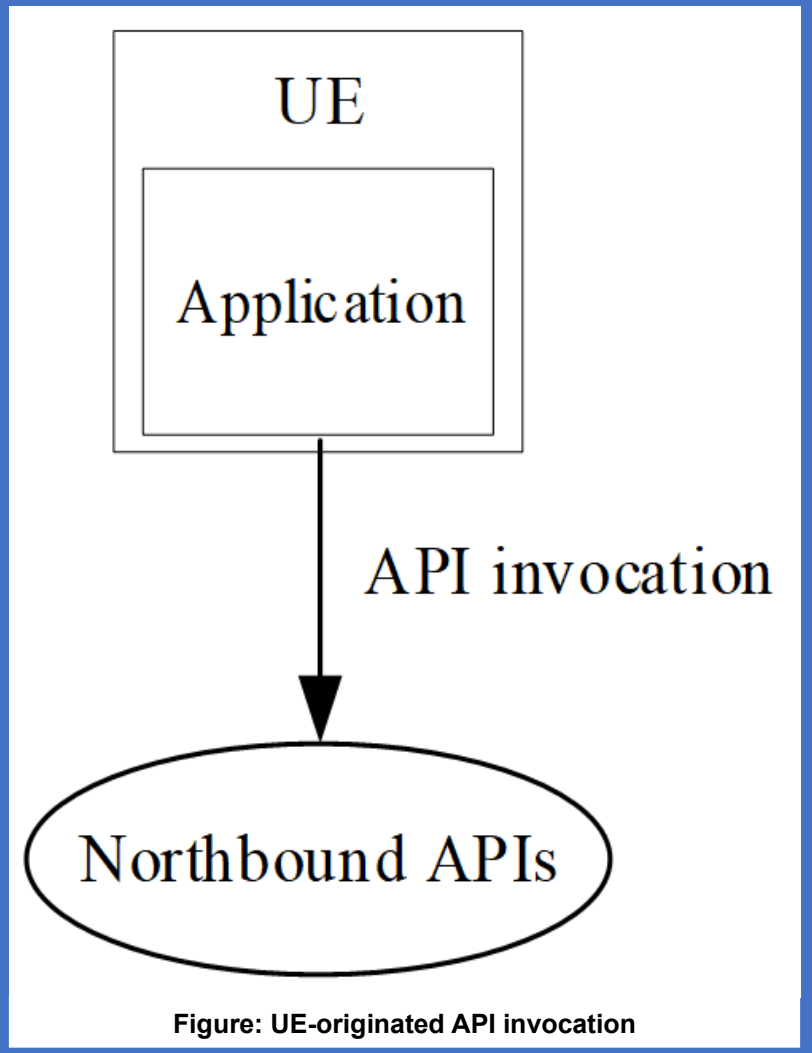


Figure: UE-originated API invocation

or

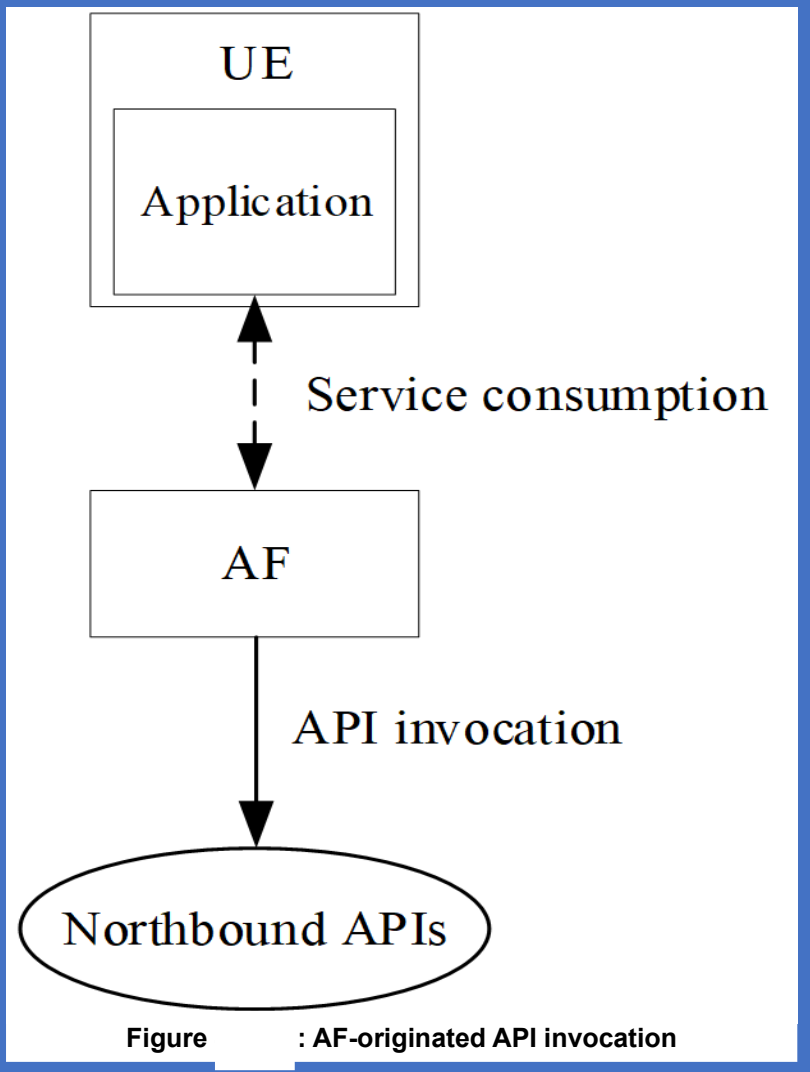


Figure : AF-originated API invocation

5G UE Service Access Identities and Service Access Categories Configurations

Table 1: 5G User Equipment (UE) Service Access Identities Configuration

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.

Table 2: 5G User Equipment (UE) Service Access Categories Configuration

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 UEto a NB-IOT cell connected to 5GC when the UE is authorized to send exception data.

P.S. "Mobility" in 5G with Rel. 15 is re-defined and classifying the UE into 4 (four) Categories of Mobility (namely UEs that are "Stationary", "Nomadic" (within a constrained area) and WAN/Mobile as well as introducing IP Anchor node and UE Relay. D.S.

1. Enabling Applications/Services Exposure Frameworks

CAPIF-6 and CAPIF-6e Reference Points connect two CAPIF Core Functions 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 such as supporting

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

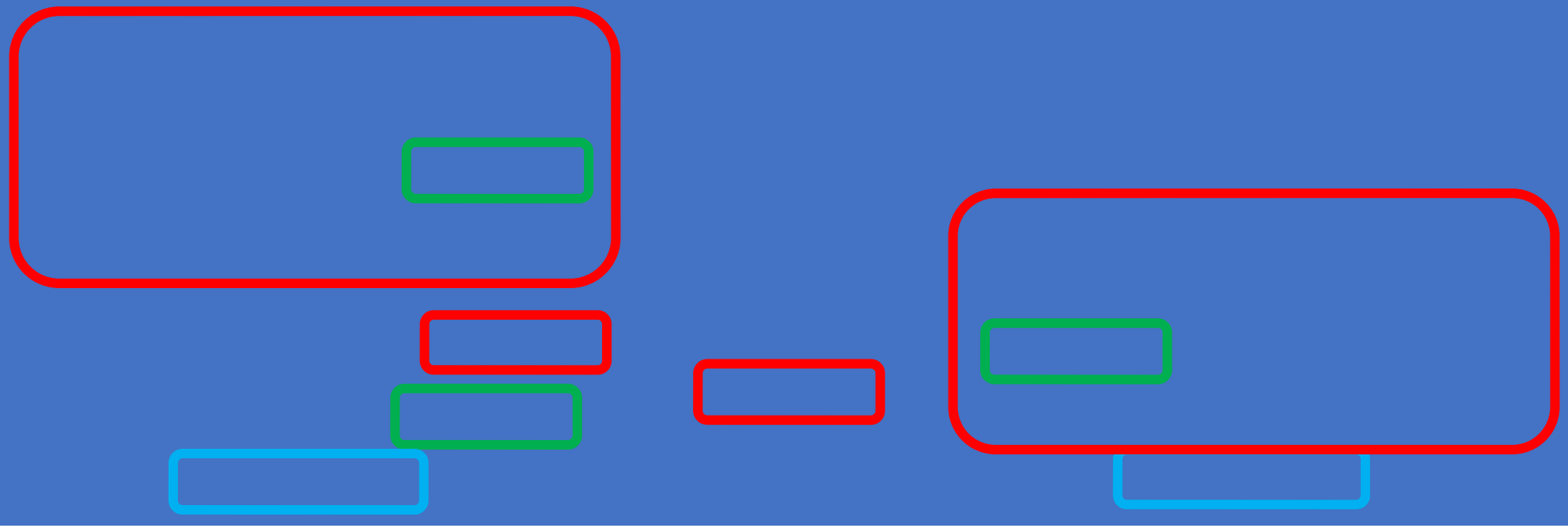


Figure: CAPIF Interconnection Functional Model

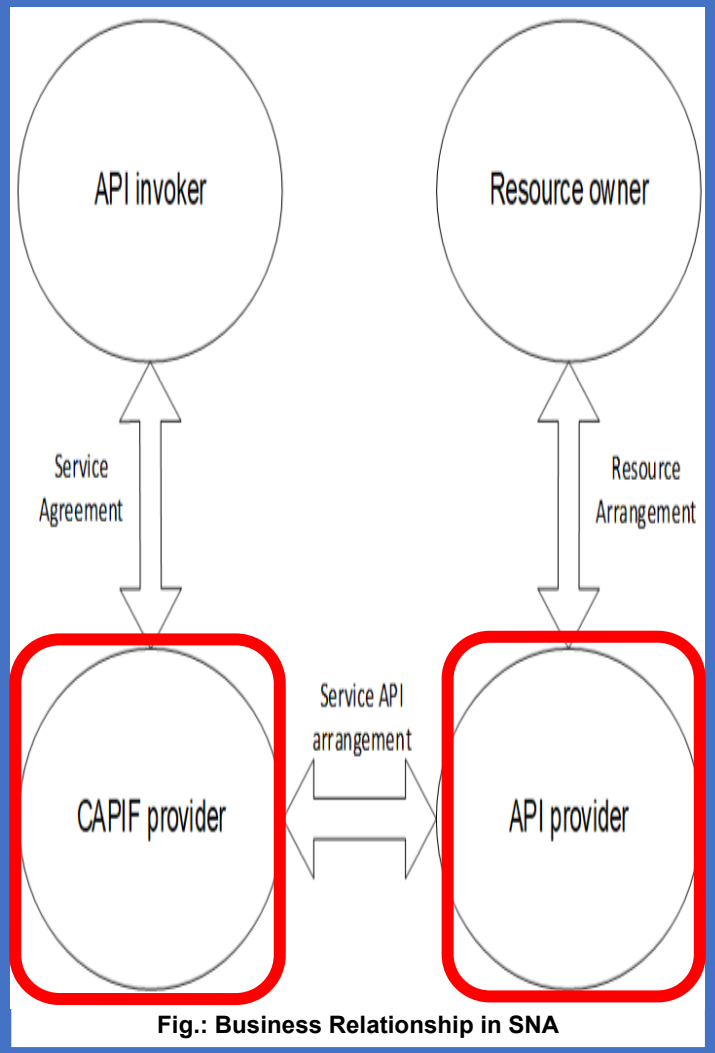


Fig.: Business Relationship in SNA

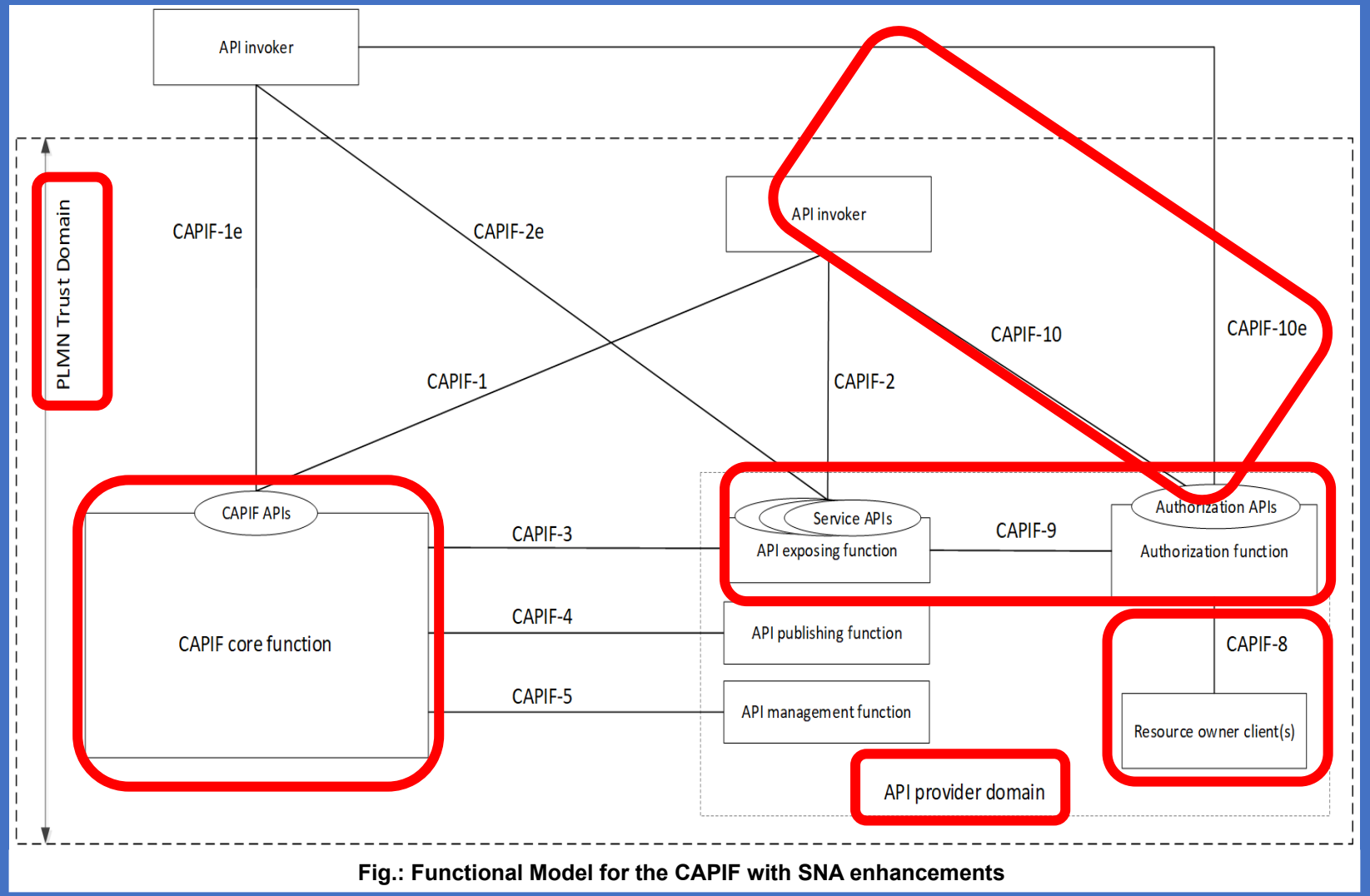


Fig.: Functional Model for the CAPIF with SNA enhancements

Ref. 3GPP Subsrciber APIs Enablem., Rel. 18, Aug. 2022

5G CAPIF Core Function and Deployment of the Authorization Function

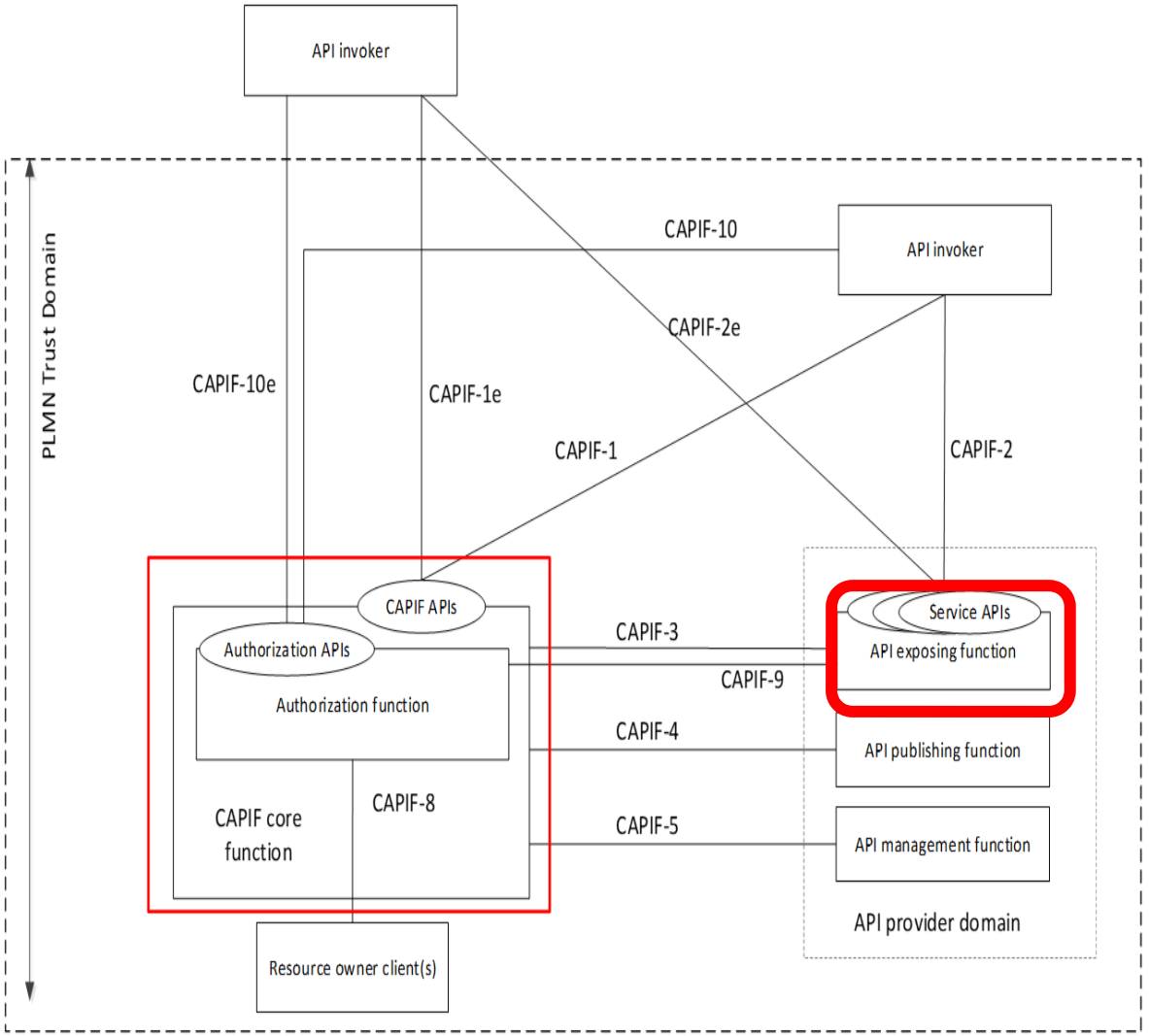


Fig.: 5G CAPIF Core Function (CF) Deployment of the Authorization Function

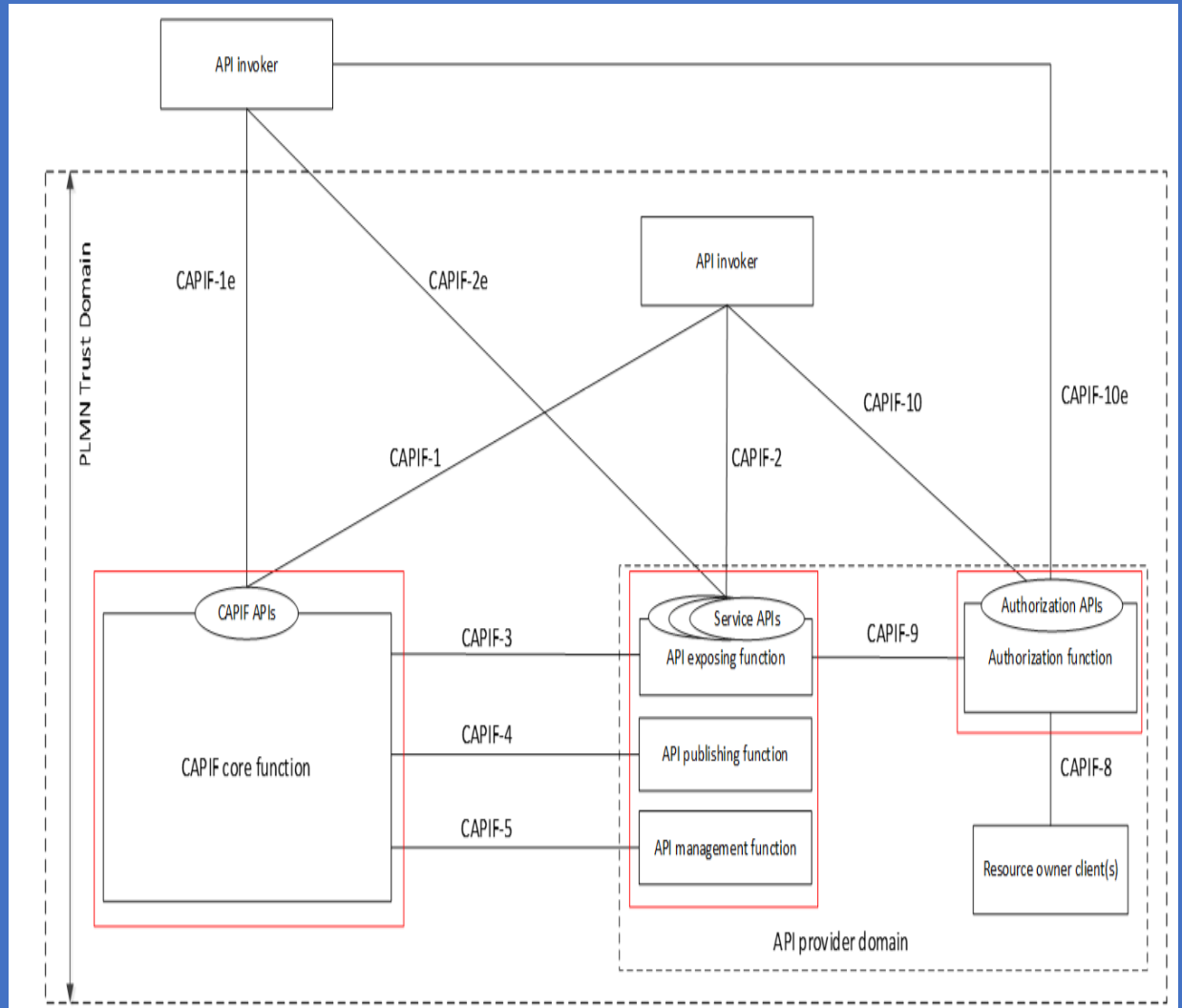


Fig.: 5G enhanced CAPIF deployment by different Organizations within the PLMN

Ref. 3GPP Subscriber APIs Enablement., Rel. 18, Aug. 2022

5G CAPIF Core Function and EDGEAPP Architecture EES

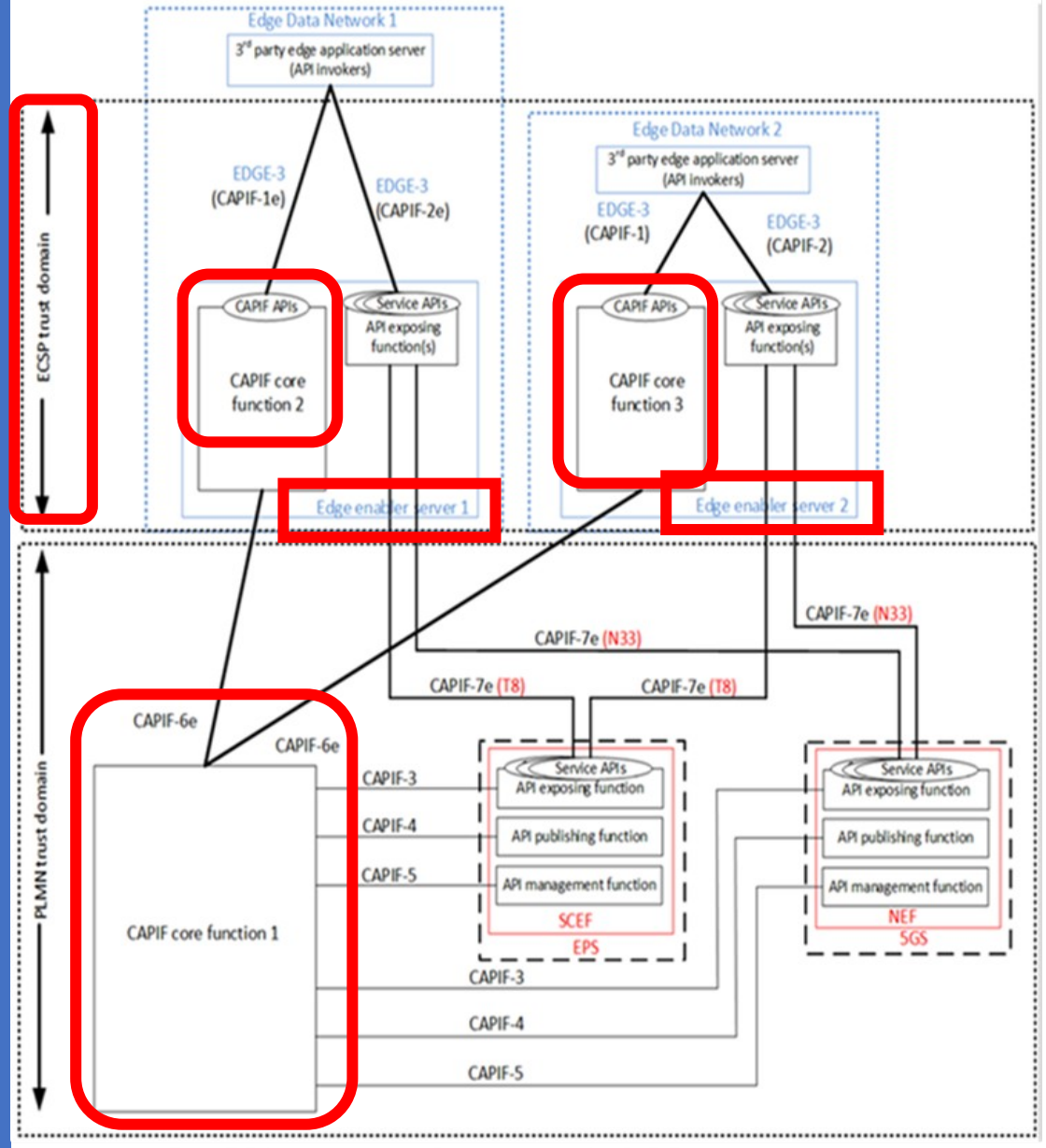


Fig. EES supporting Distributed CAPIF Functions

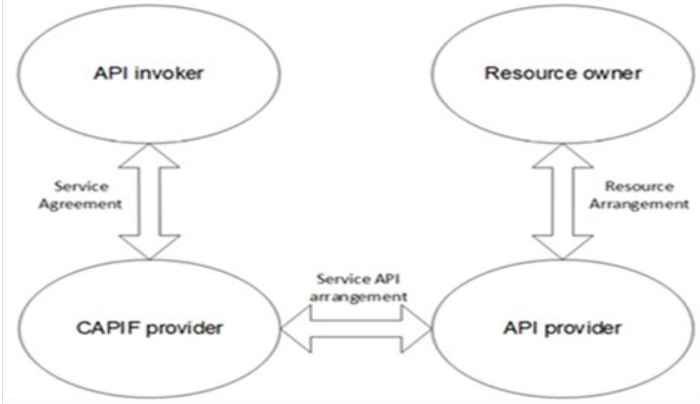


Fig. Business Relationship in SNA

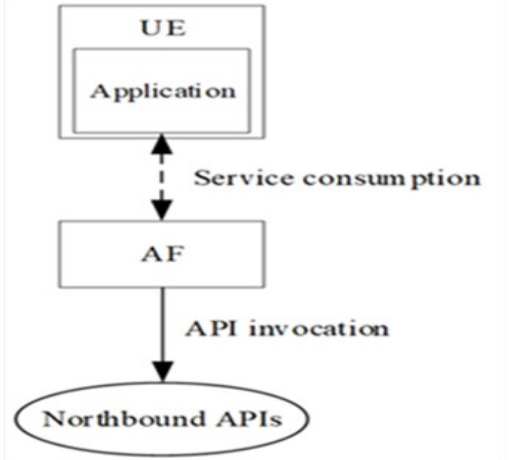


Fig. AF-originated API Invocation

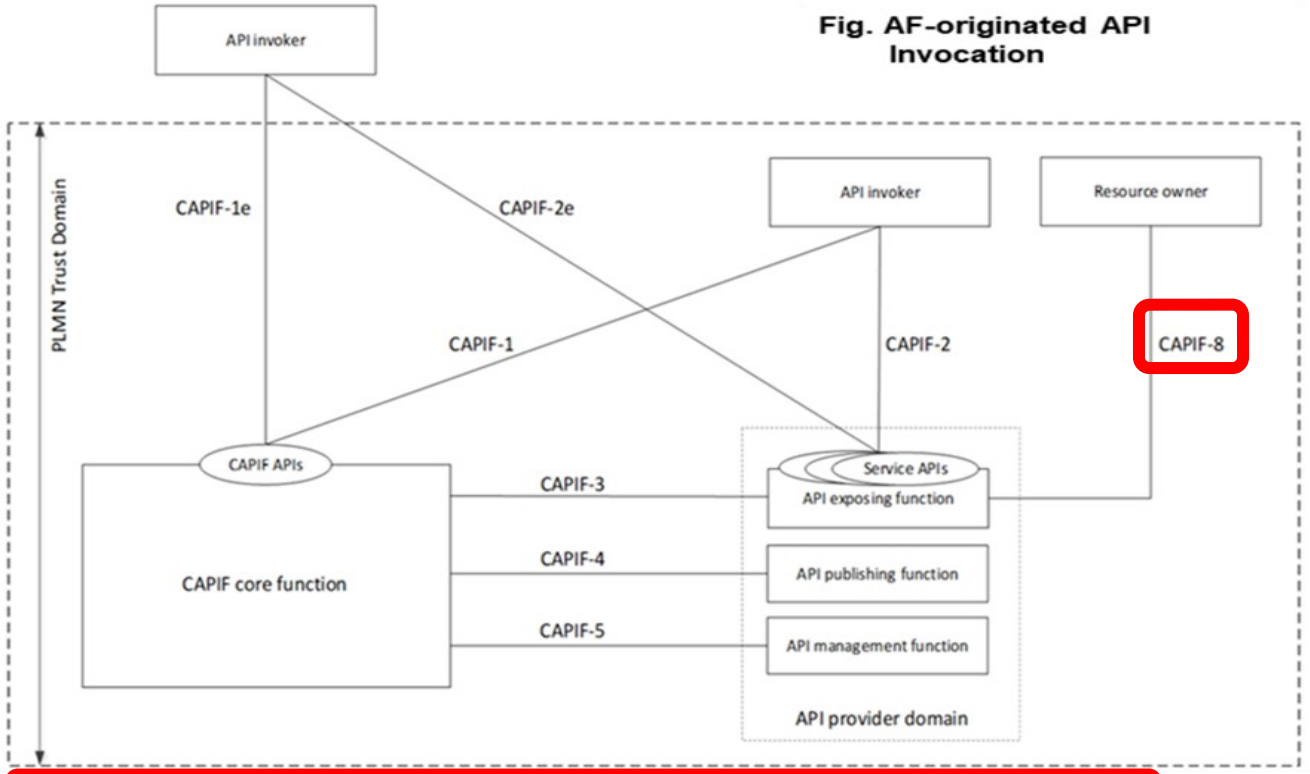


Fig. CAPIF AEF (API Expos. Funct.) for obtaining User Consent via CAPIF-8

5G EDGEAPP Architecture with Edge and Cloud Server Deployment (for ACR between EAS and CAS with CES)

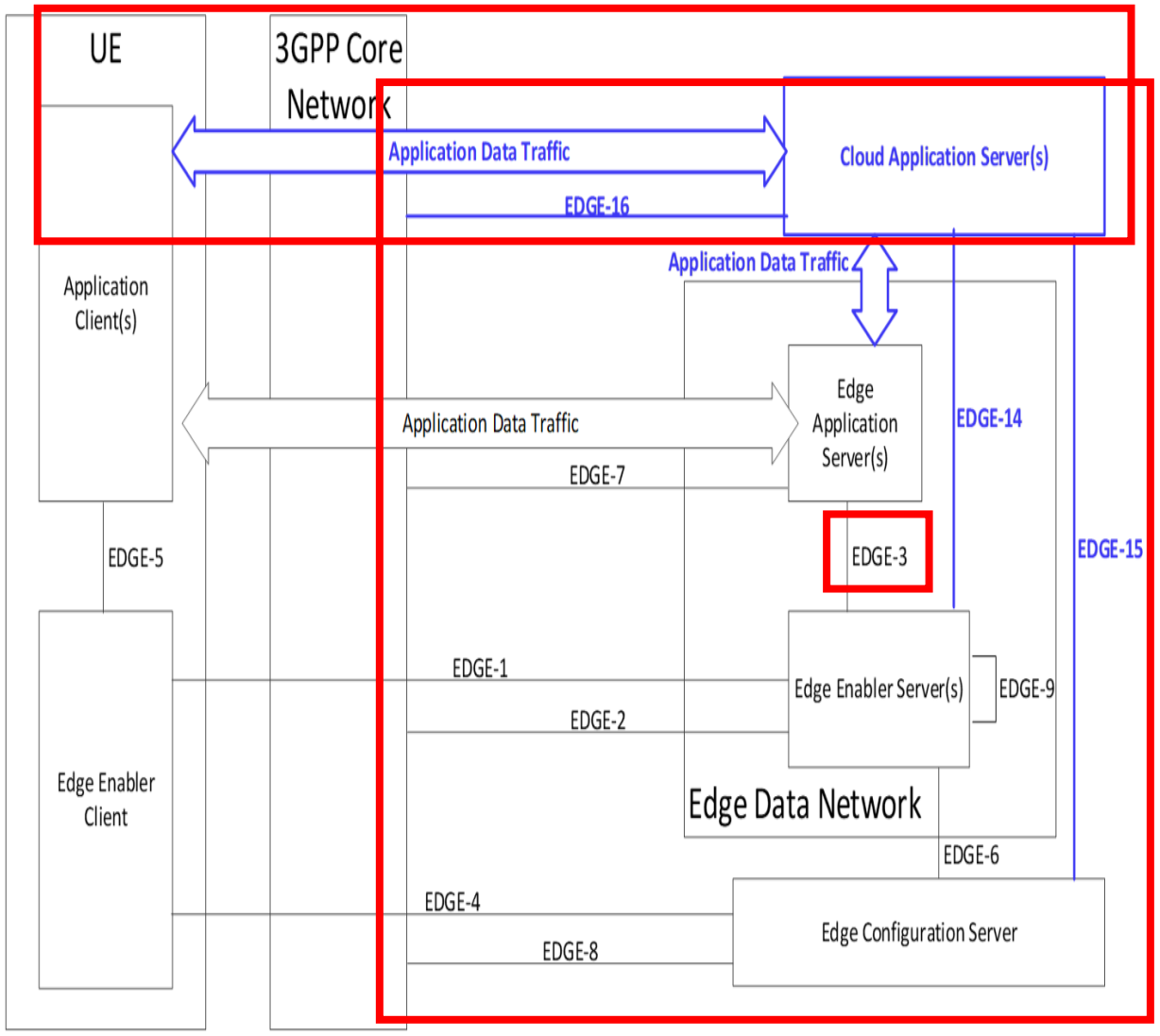


Figure: 5G Architecture with Cloud Application Server (CAS) and without Cloud Enabler Server (CES)

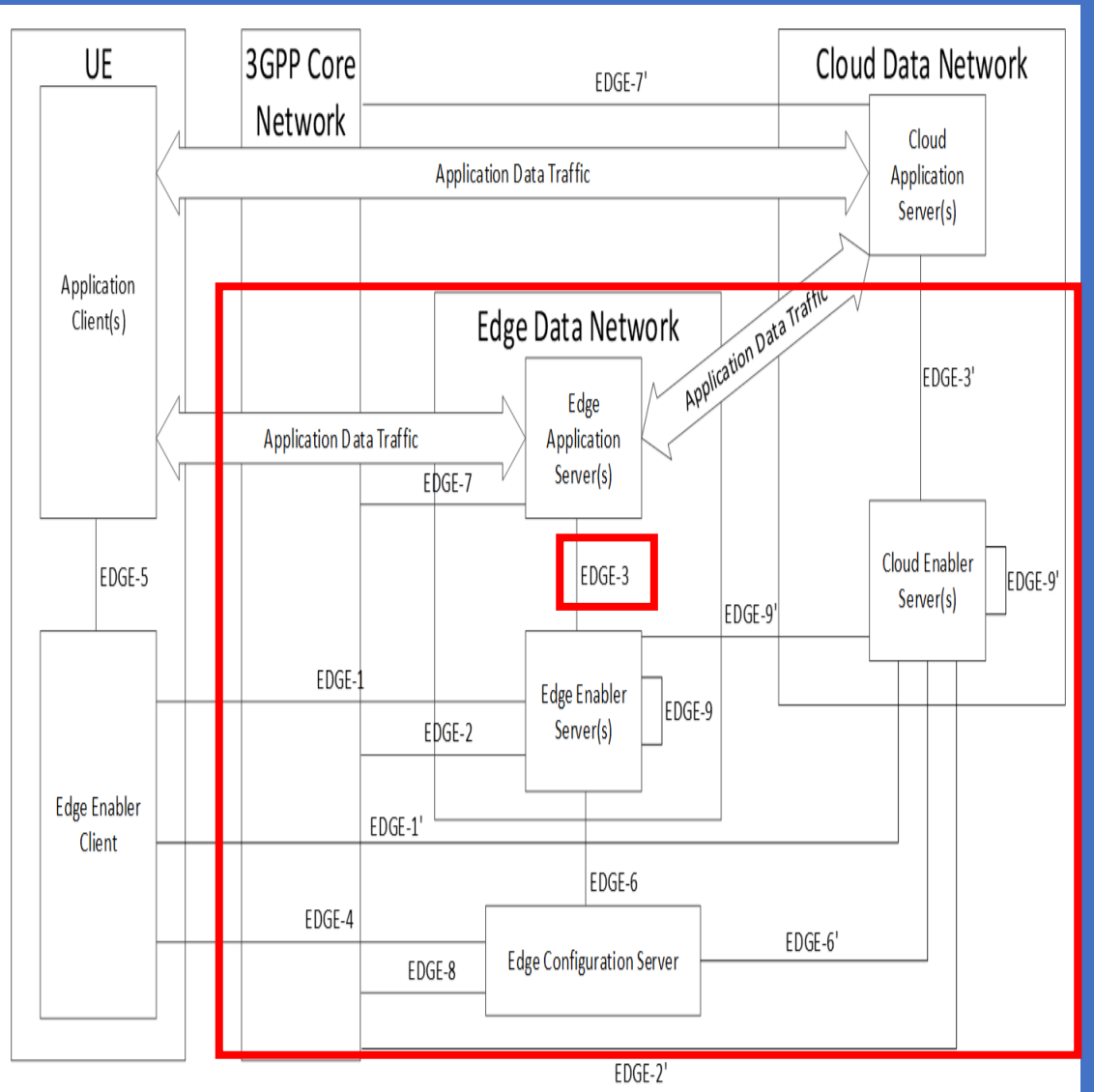


Figure: 5G Illustration of Application Architecture with Edge and Cloud Server Deployment

Ref. 3GPP Subscriber APIs Enablement., Rel. 18, Aug. 2022

Dependent on the Use Case (UC), the **EEL** (*Edge Enabling Layer*) may apply different additional criteria to determine this **common EAS.**

E.g., it could be desirable to determine the **EAS** so that the **Latency** for all the **ACs** in the session is approximately the same or that the **Latency** for a specific **AC** is minimized.

There is further utilization of Capabilities related to **EEL** (*Edge Enabling Layer*) and **AEF** (*API Exposing Function*) and **5G NDL** (*Network Data Layer)* specified and stored **NF's Application Context** (*ACR/ACT, Application Context Relocation/Application Context Transfer*) for assuring Service Continuity between **S-EAS** and **T-EAS**) as well as *Data Traffic split rendering* between **EASs** and **CAS** (*Cloud Application Server*).

Table: KPI Table for Additional High Data Rate and Low Latency Service

Use Cases	Characteristic parameter (KPI)			Influence quantity		
	Max allowed end-to-end latency	Service bit rate: user-experienced data rate	Reliability	# of UEs	UE Speed	Service Area (note 2)
Cloud/Edge/Split Rendering (note 1)	5 ms (i.e. UL+DL between UE and the interface to data network) (note 4)	0,1 to [1] Gbit/s supporting visual content (e.g. VR based or high definition video) with 4K, 8K resolution and up to120 frames per second content.	99,99 % in uplink and 99,9 % in downlink (note 4)	-	Stationary or Pedestrian	Countrywide
Gaming or Interactive Data Exchanging (note 3)	10ms (note 4)	0,1 to [1] Gbit/s supporting visual content (e.g. VR based or high definition video) with 4K, 8K resolution and up to120 frames per second content.	99,99 % (note 4)	≤ [10]	Stationary or Pedestrian	20 m x 10 m; in one vehicle (up to 120 km/h) and in one train (up to 500 km/h)
Consumption of VR content via tethered VR headset (note 6)	[5 to 10] ms (note 5)	0,1 to [10] Gbit/s (note 5)	[99,99 %]	-	Stationary or Pedestrian	-

NOTE 1: Unless otherwise specified, all communication via wireless link is between UEs and network node (UE to network node and/or network node to UE) rather than direct wireless links (UE to UE).
NOTE 2: Length x width (x height).
NOTE 3: Communication includes direct wireless links (UE to UE).
NOTE 4: Latency and reliability KPIs can vary based on specific use case/architecture, e.g. for cloud/edge/split rendering, and may be represented by a range of values.
NOTE 5: The decoding capability in the VR headset and the encoding/decoding complexity/time of the stream will set the required bit rate and latency over the direct wireless link between the tethered VR headset and its connected UE, bit rate from 100 Mbit/s to [10] Gbit/s and latency from 5 ms to 10 ms.
NOTE 6: The performance requirement is valid for the direct wireless link between the tethered VR headset and its connected UE.

5G ACT & ACR (Application Context Transfer & Application Context relocation

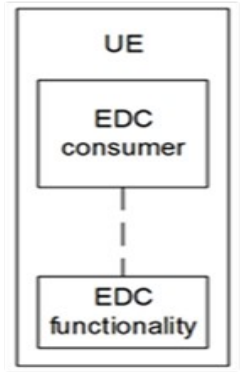


Fig. EDC Funct. in the UE

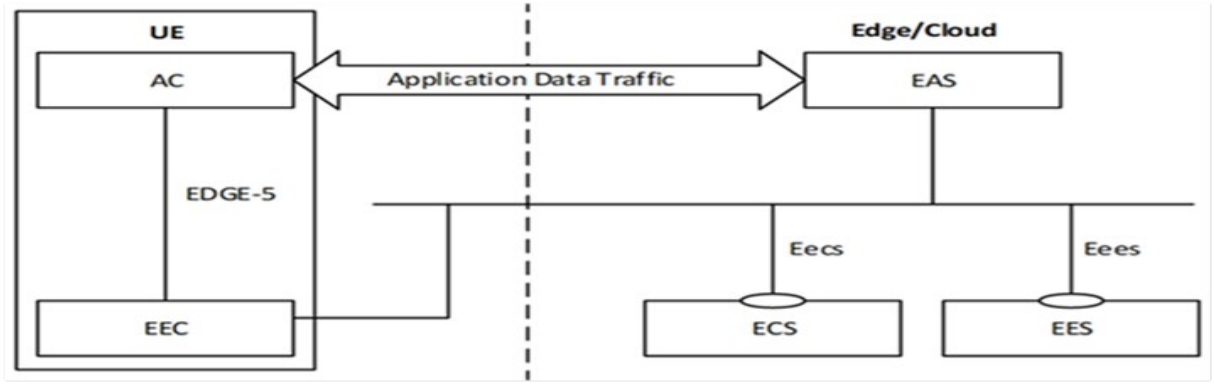


Fig. Archit. For Enabling Edge Applic. - Service-based Represent

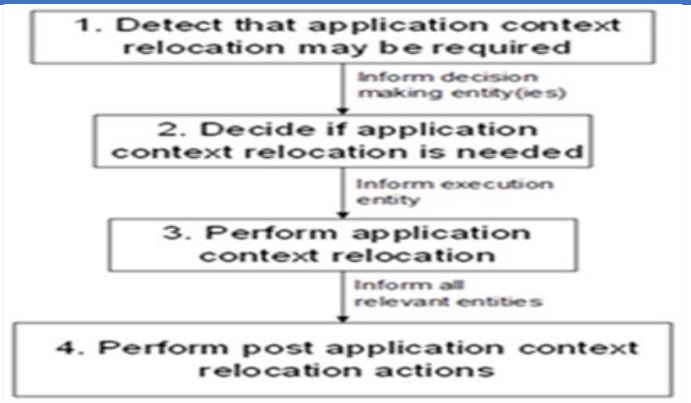


Fig. High level overview of ACR (Application Context Relocation)

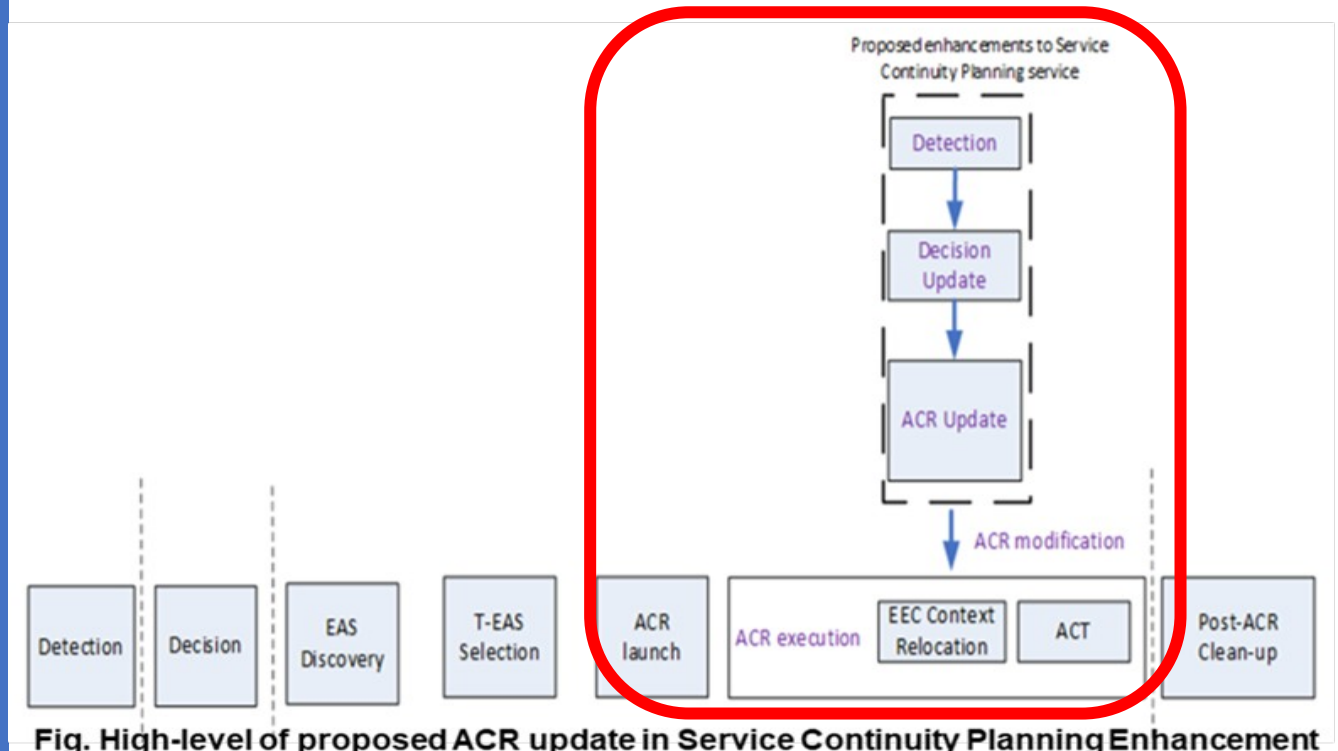


Fig. High-level of proposed ACR update in Service Continuity Planning Enhancement

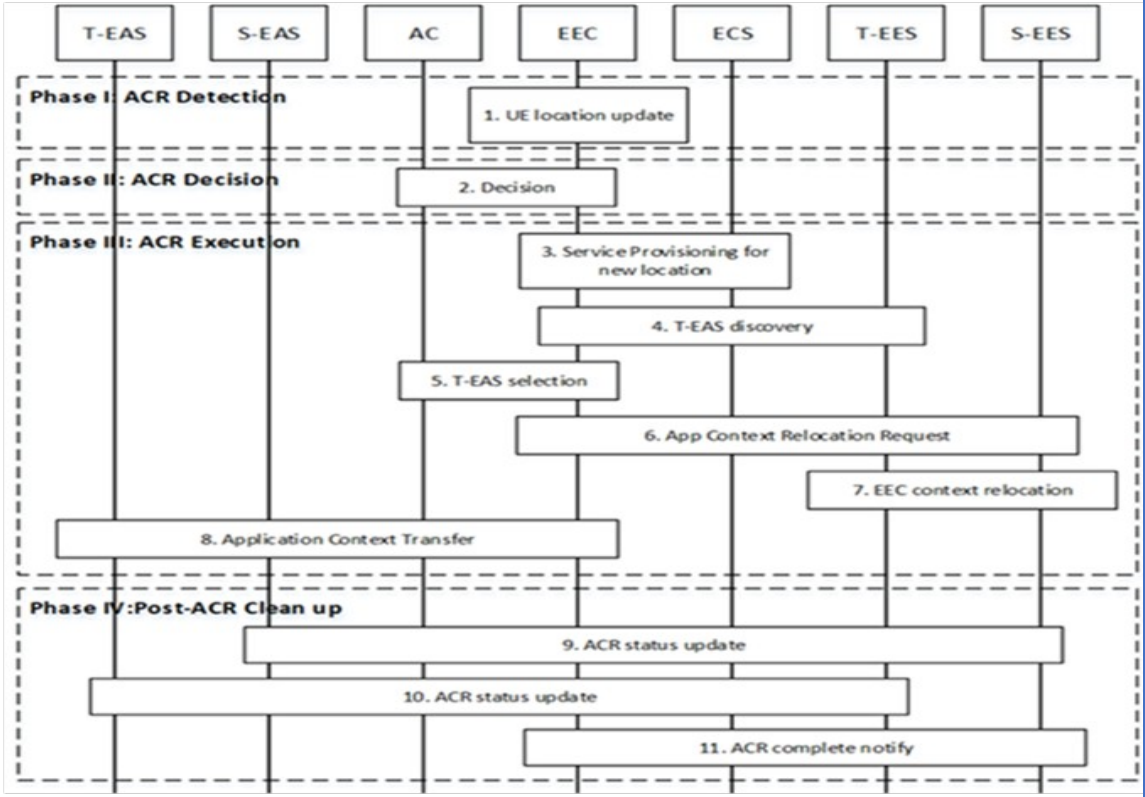


Fig. ACR initiated by the EEC & AC

3GPP 5G UE New Services Enablement Clients (UAC - Unified Access Control for Access Identities & Access Categories

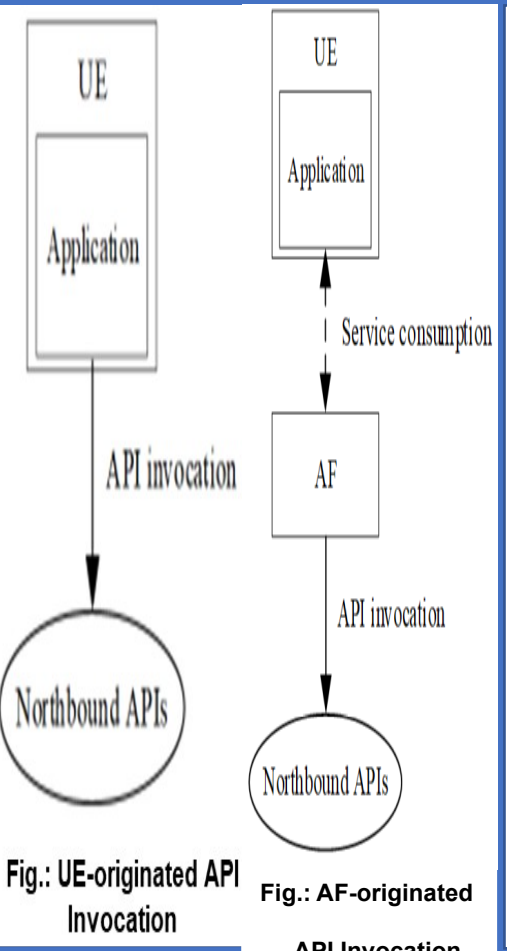


Fig.: UE-originated API Invocation

Fig.: AF-originated API Invocation

+

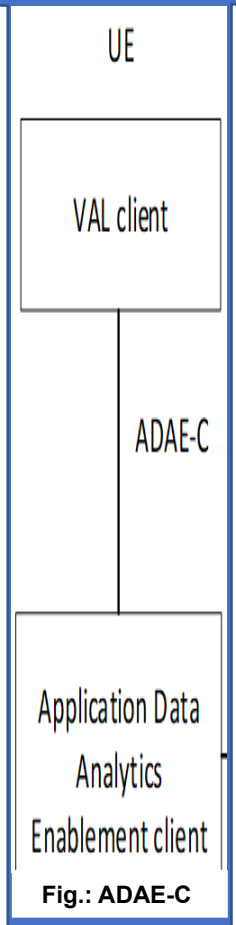


Fig.: ADAE-C

+

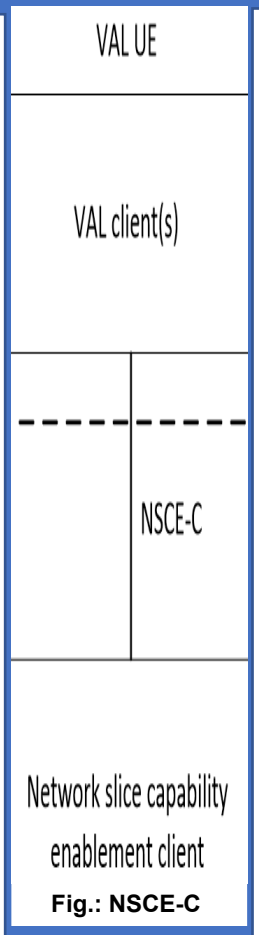


Fig.: NSCE-C

+

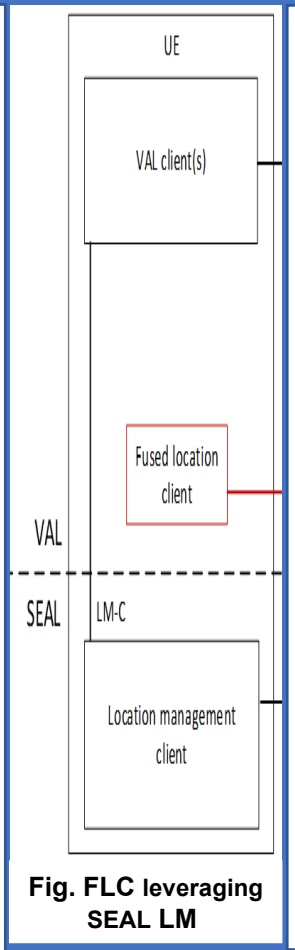
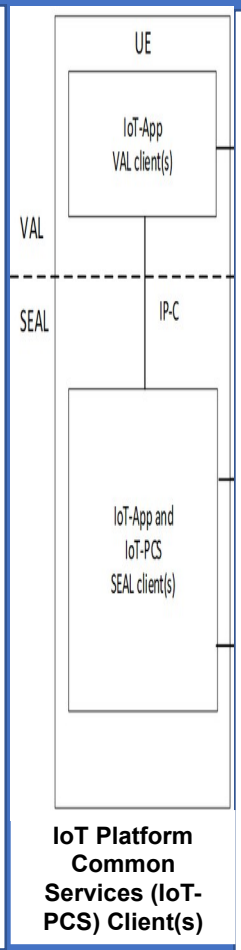


Fig. FLC leveraging SEAL LM

+



IoT Platform Common Services (IoT-PCS) Client(s)

+

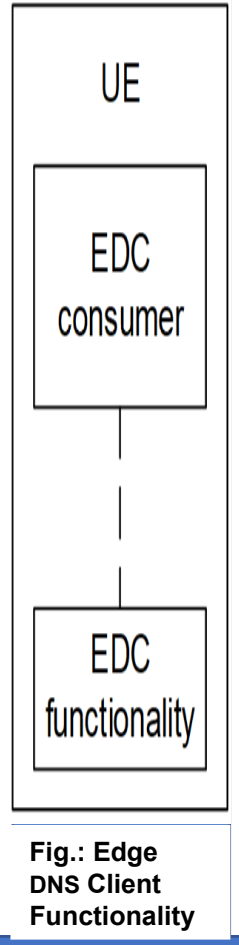


Fig.: Edge DNS Client Functionality

+

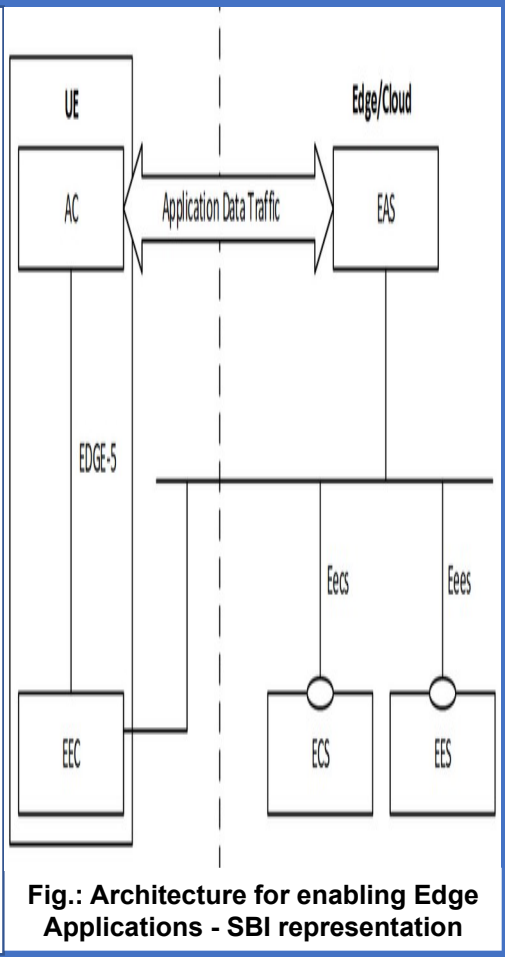


Fig.: Architecture for enabling Edge Applications - SBI representation

URSP - UE Route Selection Policy URSP

The URSP is defined and is a set of one or more URSP rules, where a URSP rule is composed of:

a) A precedence value of the URSP rule identifying the precedence of the URSP rule among all the existing URSP rules;

b) A traffic descriptor, including either:

1) match-all traffic descriptor; or

2) at least one of the following components:

- A) one or more application identifiers;
- B) one or more IP 3 tuples: Destination/ 1. IP Address 2. Port nr, & 3. the Protocol
- C) one or more non-IP descriptors, i.e. destination information of non-IP traffic;
- D) one or more DNNs;
- E) one or more connection capabilities; and
- F) one or more domain descriptors, i.e. destination FQDN(s) or a regular expression as a Domain Name matching criteria; and

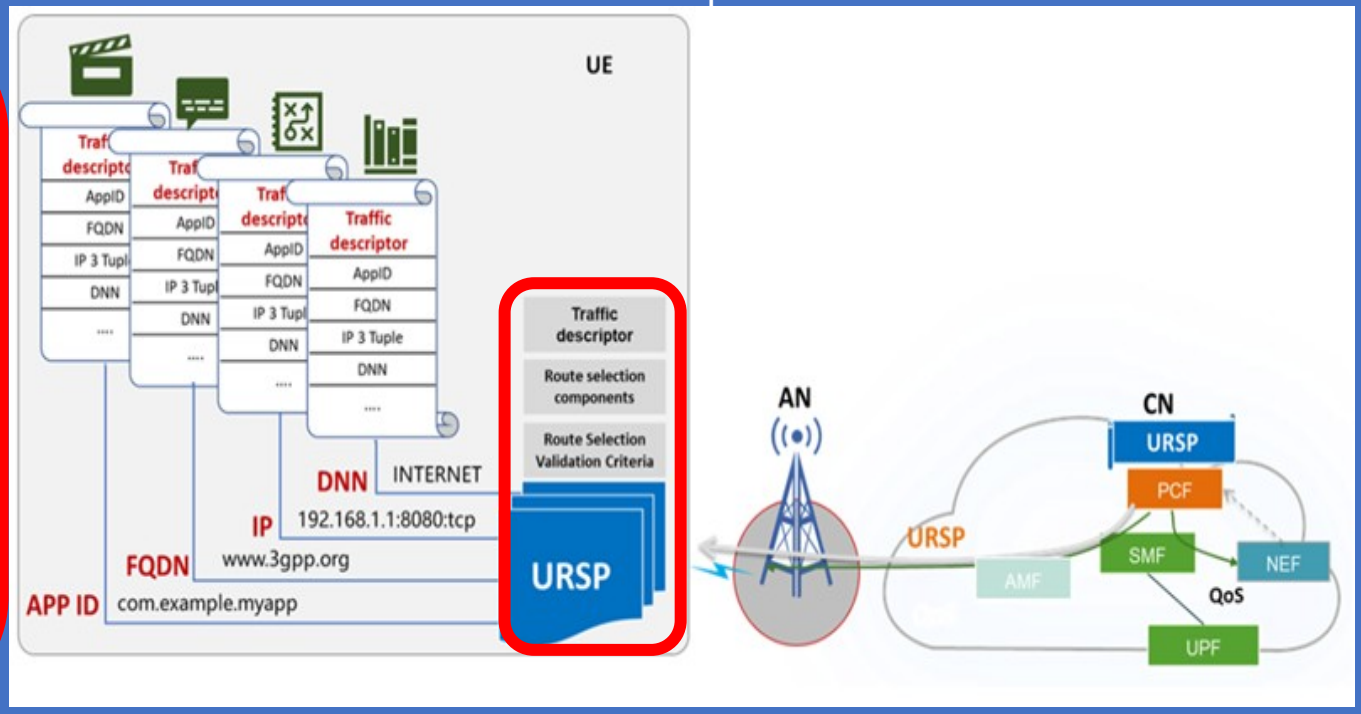
c) one or more route selection descriptors each consisting of a precedence value of the route selection descriptor and either

1) one PDU session type and, optionally, one or more of the followings:

- A) SSC mode;
- B) 1 or more S-NSSAIs;
- C) 1 or more DNNs;
- D) Void;
- E) preferred Access Type;
- F) Multi-Access Preference;
- G) a Time Window; and
- H) Location Criteria;

2) non-seamless non-3GPP offload indication; or

3) 5G ProSe Layer-3 UE-to-network relay offload indication.



EASDF - Edge Application Server Discovery Function

Functional Description

The Edge Application Server Discovery Function (EASDF) includes one (1) or more of the following Functionalities:

- Registering to NRF for EASDF Discovery and Selection.
- Handling the **DNS messages** according to the **instruction from the SMF**, including:
  - Receiving DNS message handling Rules and/or **BaselineDNSPattern from the SMF.**
  - Exchanging **DNS messages from the UE**.
  - **Forwarding DNS messages to C-DNS or L-DNS for DNS Query.**
  - Adding **EDNS Client Subnet (ECS) option into DNS Query for an FQDN**.
  - Reporting to the SMF the information related to the received DNS messages.
  - Buffering/Discarding **DNS response messages from the UE or DNS Server**.
- Terminates the **DNS security**, if used.

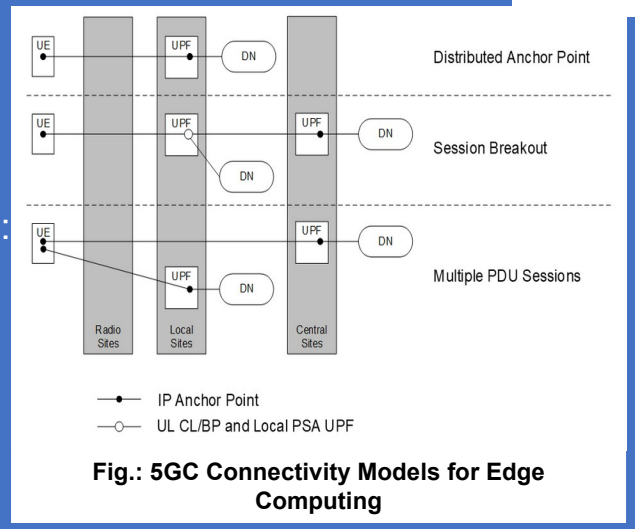


Fig.: 5GC Connectivity Models for Edge Computing

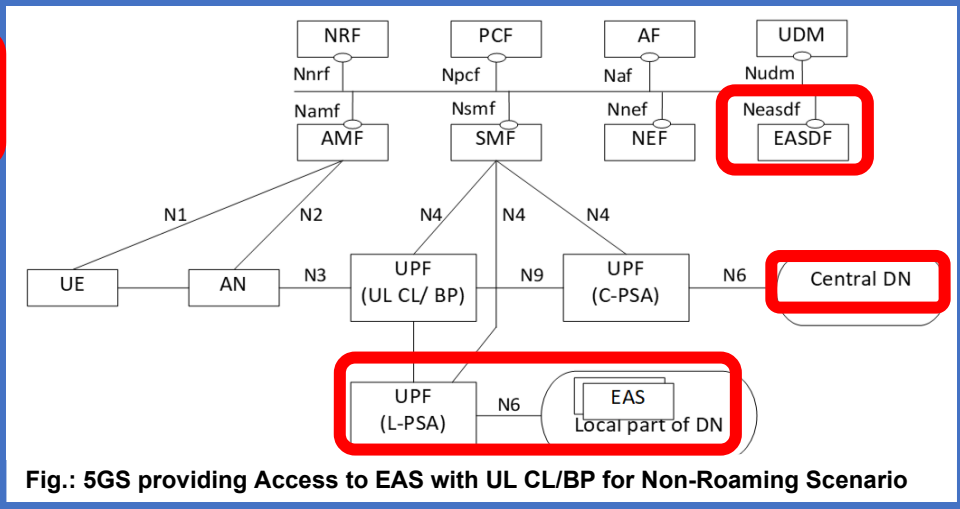


Fig.: 5GS providing Access to EAS with UL CL/BP for Non-Roaming Scenario

The **EASDF has direct User Plane Connectivity** (i.e. without any NAT) with the **PSA UPF over N6** for the transmission of **DNS signalling** exchanged with the UE. **The deployment of a NAT between EASDF and PSA UPF is not supported**.

Multiple EASDF instances may be deployed within a PLMN.

The interactions between 5GC NF(s) and the EASDF take place within a PLMN.

5G UPF Enhancements for Service Exposure and SBA support (UPEAS) & Group Management for Communication Enhancements

Improving 5CN Capabilities for the 5G specified 4 Service enablement Architectures for New Services

1) **Avoiding Duplicate Data Transfer & Reducing Transmission Path** enabling the 5CN Services directly "Subscribe/Unsubscribe" on UPF Services for QoS Monitoring Latency Report,

2) Retrieving the UPF original status or Real-Time Service Flow Information in NWDAF, e.g., to facilitate Data Collection & Analysis considering efficient sampling intervals for the different Services.

3) UPF Event Exposure e.g. for 5G IoT Solutions require interfacing of UPF to NEF/Local NEF for Network Information Exposure to an Application Server (e.g. in **IoT-PCS** (*IoT Platform Common Services*) servers enabling a set of Applications deployed using corresponding Servers (IoT-App), which may belong to different verticals & further insights into Scenarios in which an IoT Platform interfaces with the 5G CN to request future Background Data Transfer (BDT) Policies on behalf of IoT Servers.

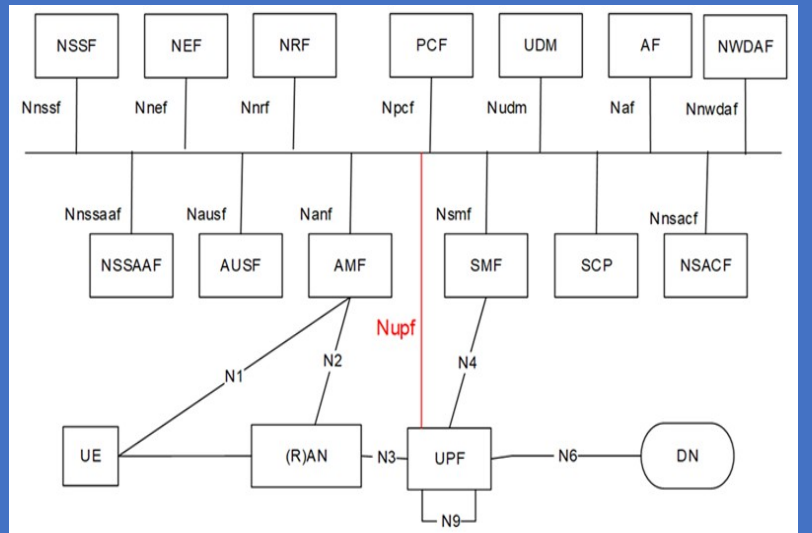


Figure: 5G System Architecture with Service-based UPF

While the UPF is in the role of "Consumer" of the 5G CN Services, i.e. the UPF can register its NF Profile in the 5G CN with related ***Nupf Service Information*** & does not describe Services provided by the UPF itself.

The 5GC potential enhancements on *Generic Group Management, Exposure & Communication enhancements* (that can be specifically utilized in Slicing & equivalent NPN/SNPNs inter-operability & **roaming, etc.), aim to enhance Group Attribute Management & Group Status Event Reporting, Set/Modify the Group Attributes as Provisioning of Service Area or QoS Applicable to each UE of a given group;** Subscribe to Group Status Event Reporting for the Event "Newly Registered or (De)-Registered Group Member", Whether & How to enhance NEF Exposure Framework to enable Capability Exposure for Provisioning of Traffic Characteristics & Monitoring of Performance Characteristics Applicable to each UE of a given group, Support Group Communication for a 5G VN, which supports multiple SMFs, including support of SMF redundancy for reliability of the 5G VN Group Communication.

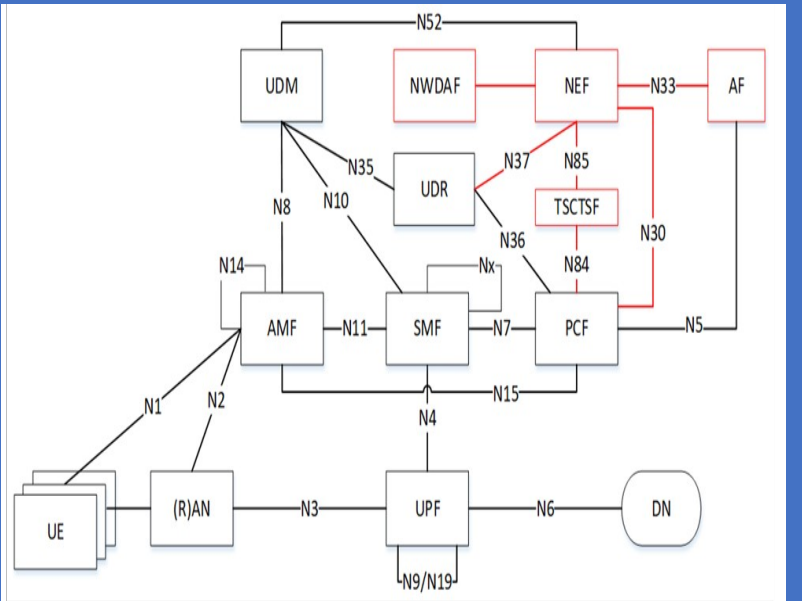


Figure: 5G System Architecture to support Connection Management for a Group

Architecture for enabling E2E Edge Services

The OPG believes that, for Operators to develop a Federated Edge Computing Platform such as the OP, *Requirements must be enforceable in Contracts by a Published Set of Standards.*

To this end, the OPG proposes selecting ETSI ISG MEC and 3GPP to provide a Standard Reference for an Edge Service End to End (E2E) definition.

We note that 3GPP EDGEAPP Architecture and ETSI ISG MEC Architecture could complement each other in a way that is acceptable to OPG.

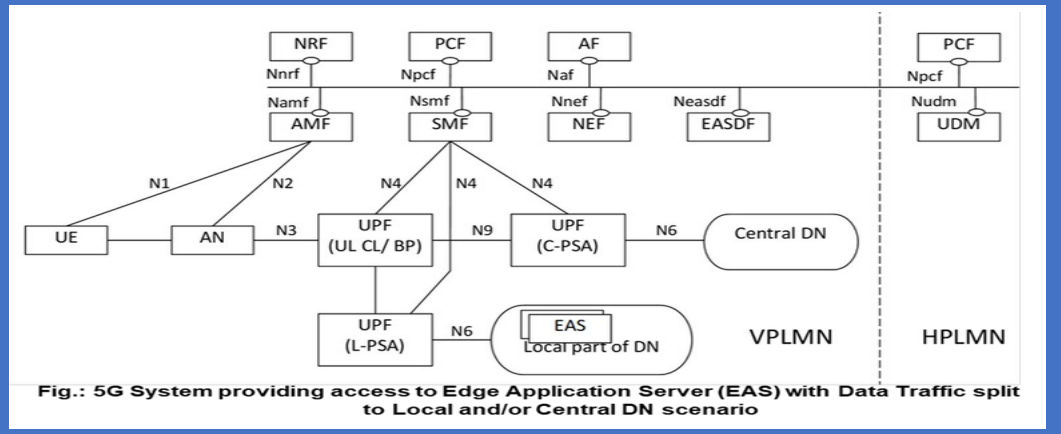


Fig.: 5G System providing access to Edge Application Server (EAS) with Data Traffic split to Local and/or Central DN scenario

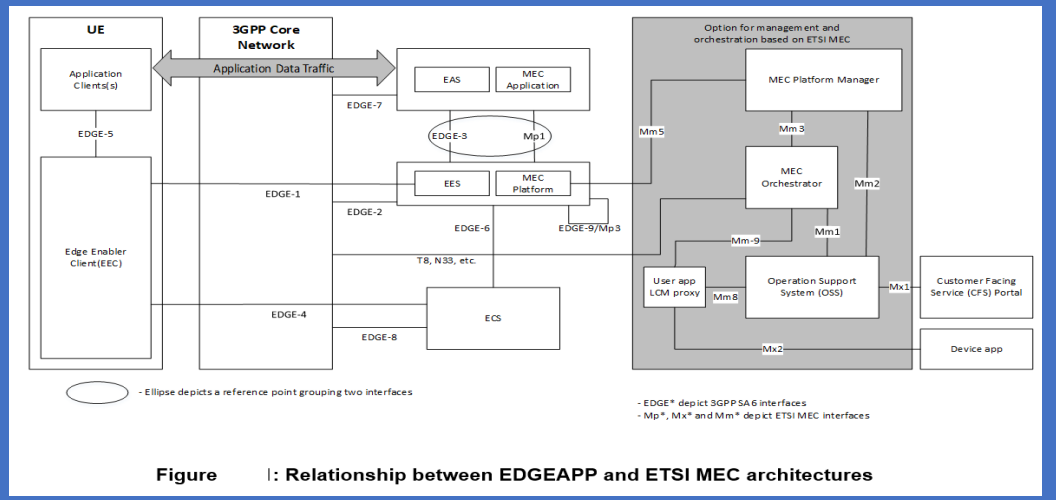


Figure I: Relationship between EDGEAPP and ETSI MEC architectures

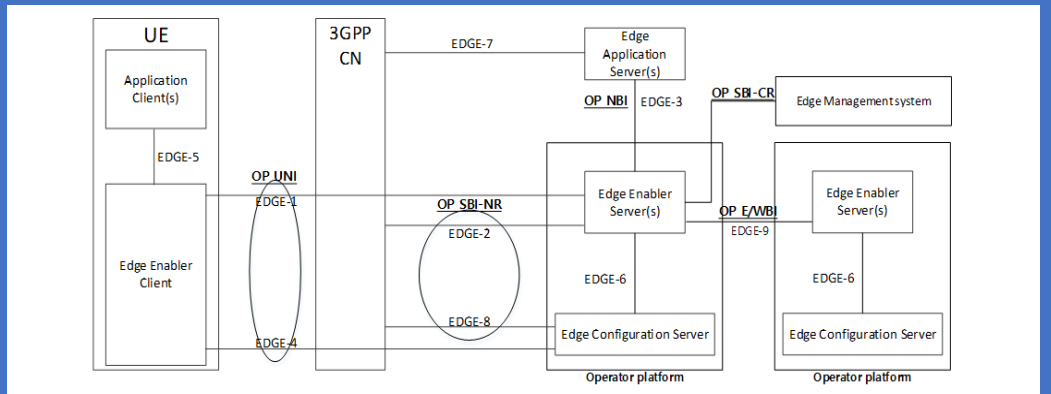


Figure : Relationship between EDGEAPP architecture and GSMA OPG reference architecture

Alignment/Comparison of 3GPP 5G EDGEAPP EAS Profile/Registration and ETSI MEC Application (MEA appInfo)

IE in EAS profile	Status	IE in appInfo [14]	Status [14]	Remarks
EASID	M	appName	M	**3GPP specification [2]:** The EASID identifies a particular application for e.g. SA6Video, SA6Game etc. For example, all Edge SA6Video Servers will share the same EASID. NOTE: The definition of the EASID is out of scope of this specification. **ETSI MEC specification [14]:** Name of the application. It shall be consistent with the appName in the AppD, if an AppD is available. In AppD, it is defined as: Name to identify the MEC application. In both specifications, the IE is used to identify a particular application. The purpose of the IE is the same in both specifications, and can be considered equivalent.
EAS Endpoint	M	endpoint	O	**3GPP specification [2]:** Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the EAS. **ETSI MEC specification [14]:** Endpoint information (e.g. URI, FQDN, IP address) of the application server, which is part of the application functionalities. The purpose of the IE is the same in both specifications, and can be considered equivalent.
ACID(s)	O			The IE is not applicable in application registration in ETSI MEC.
EAS Provider Identifier	O	App Provider	M	**3GPP specification [2]:** The identifier of the ASP that provides the EAS. **ETSI MEC specification [14]:** Provider of the application. It shall be consistent with the appProvider in the AppD, if an AppD is available. The purpose of the IE is the same in both specifications, and can be considered equivalent.
EAS Type	O	appCategory	O	**3GPP specification [2]:** The category or type of EAS (e.g. V2X) **ETSI MEC specification [14]:** Category of the application. The purpose of the IE is the same in both specifications, and can be considered equivalent.
EAS description	O	AppD > appDescription	O	**3GPP specification [2]:** Human-readable description of the EAS. **ETSI MEC specification [14]:** Human readable description of the MEC application. The purpose of the IE is the same in both specifications, and can be considered equivalent.
EAS Schedule	O			The IE is not applicable in application registration in ETSI MEC.
EAS Geographical Service Area	O			The IE is not applicable in application registration in ETSI MEC.
EAS Topological Service Area	O			The IE is not applicable in application registration in ETSI MEC.
EAS Service KPIs	O			The IE is not applicable in application registration in ETSI MEC.
EAS service permission level	O			The IE is not applicable in application registration in ETSI MEC.
EAS Feature(s)	O			The IE is not applicable in application registration in ETSI MEC.
EAS Service continuity support	O			The IE is not applicable in application registration in ETSI MEC.
List of EAS DNAI(s)	O			The IE is not applicable in application registration in ETSI MEC.
List of N6 Traffic Routing requirements	O			The IE is not applicable in application registration in ETSI MEC.
EAS Availability Reporting Period	O			The IE is not applicable in application registration in ETSI MEC.
EAS Status	O			The IE is not applicable in application registration in ETSI MEC.
		appDId	O	**ETSI MEC specification [14]:** The application descriptor identifier. It is managed by the application provider to identify the application descriptor in a globally unique way. Shall be present if the application instance is instantiated by the MEC Management.
		appInstanceId	O	**ETSI MEC specification [14]:** Identifier of the application instance. Shall be present if the application instance is instantiated by the MEC Management.
		appServiceRequired	O	**ETSI MEC specification [14]:** Describes services a MEC application requires to run. ServiceDependency is defined in ETSI GS MEC 010-2 [13]. It shall shall not be provided if an AppD is available.
		appServiceOptional	O	**ETSI MEC specification [14]:** Describes services a MEC application may use if available. ServiceDependency is defined in ETSI GS MEC 010-2 [13]. It shall shall not be provided if an AppD is available.
		appFeatureRequired	O	**ETSI MEC specification [14]:** Describes features a MEC application requires to run. FeatureDependency is defined in ETSI GS MEC 010-2 [13]. It shall shall not be provided if an AppD is available.
		appFeatureOptional	O	**ETSI MEC specification [14]:** Describes features a MEC application may use if available. FeatureDependency is defined in ETSI GS MEC 010-2 [13]. It shall shall not be provided if an AppD is available.

Deployment and Evolution options of EDGEAPP and ETSI MEC Platforms (Informative):

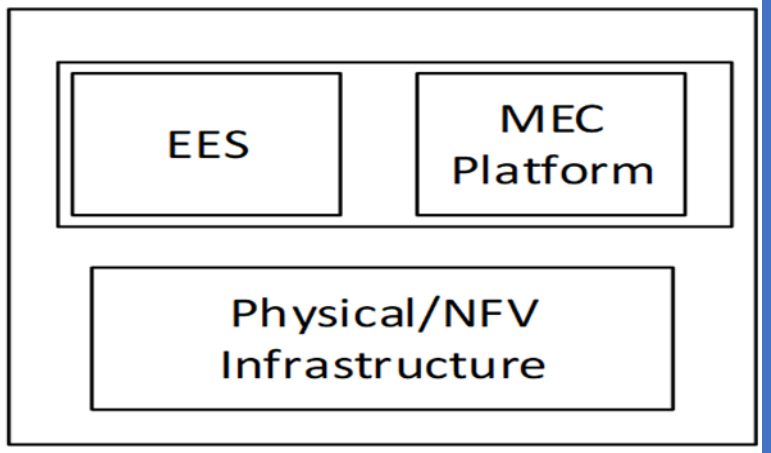


Figure.: EES and MEC Platform as two different AFs on a single Physical//NFV Infrastructure

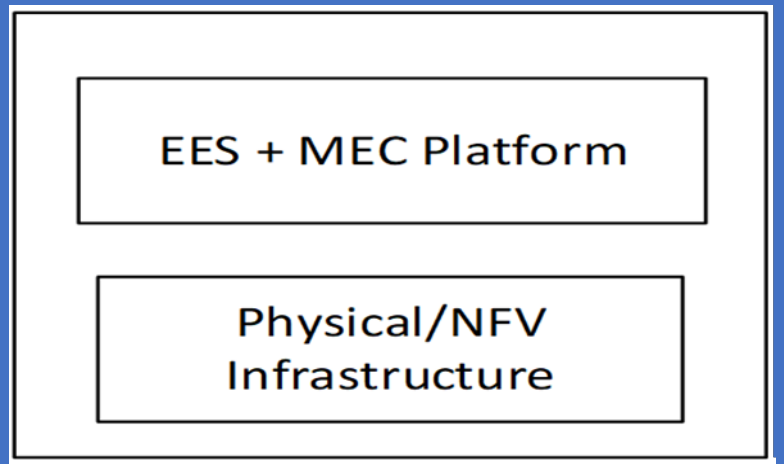


Fig.: EES and MEC Platform as a single AF on a single NFV Infrastructure

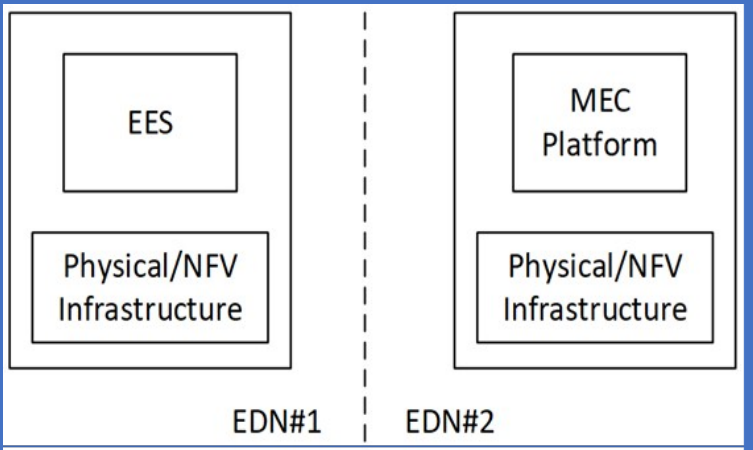


Fig.: EES and MEC Platform as two different AFs on two different EDNs

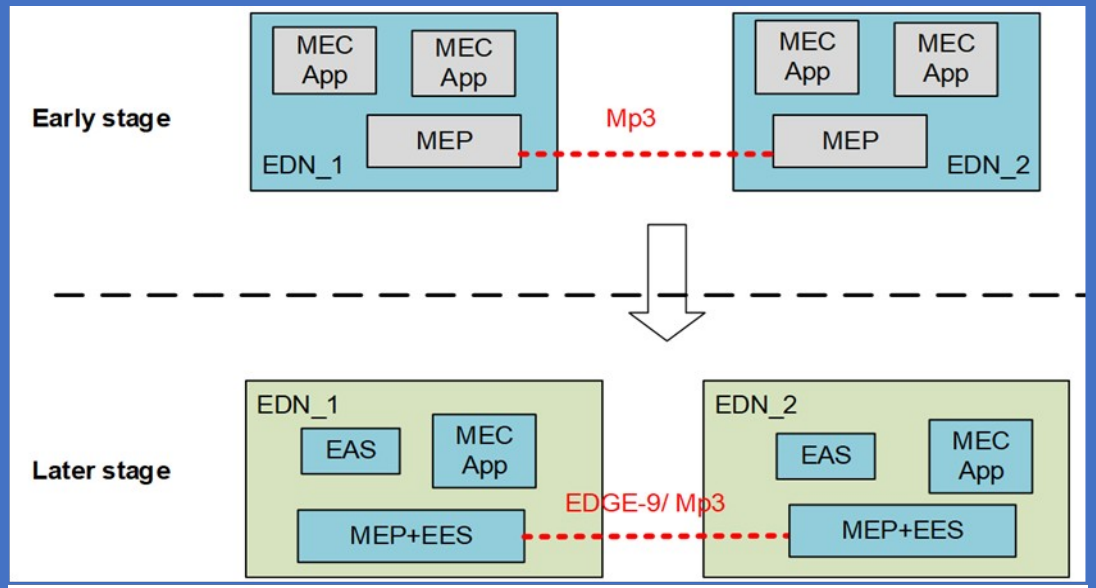


Fig.: Evolution Option #1 - An early stage deployed MEP is enhanced to support the functionality of EES in a later stage

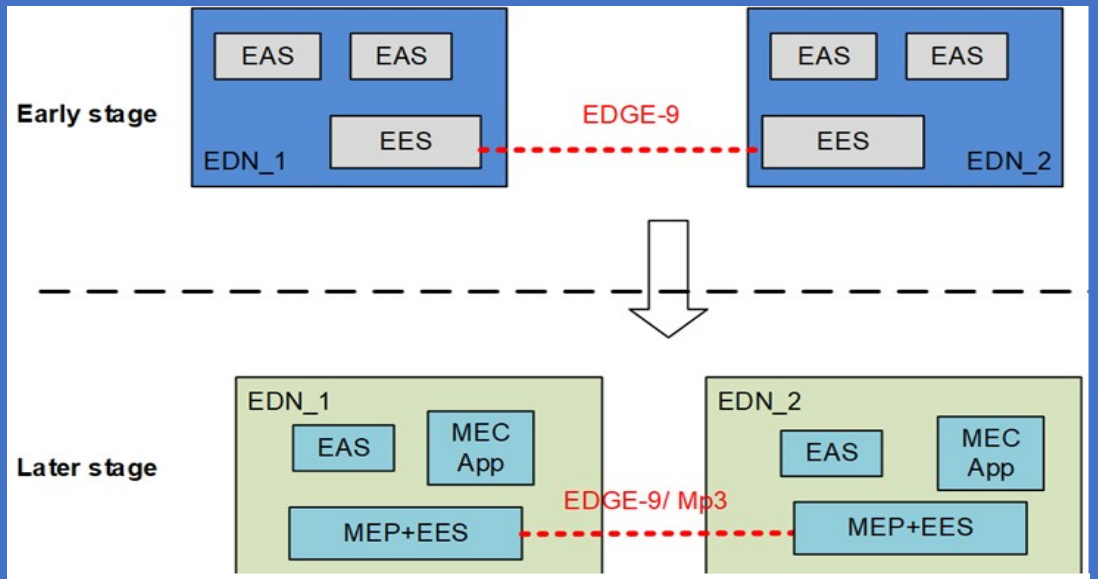


Fig.: Evolution Option #2 - Enhancement of a deployed EES to support functionality of MEP

Annex B (informative): Relationship with 3GPP SA6 EDGEAPP architecture

B.1 Introduction

The architecture for enabling edge applications (also known as EDGEAPP architecture) is, as defined in 3GPP an application layer architecture for enabling edge applications over 3GPP networks. Edge Application Servers (EASs) and the Edge Enabler Server (EES) are contained within the Edge Data Network (EDN). The Edge Configuration Server (ECS) provides configurations related to the EES, including details of the EDN hosting the EES. The UE contains Application Clients (ACs) and the Edge Enabler Client (EEC). The EAS(s), the EES and the ECS may interact with the 3GPP Core Network. An example for how the 3GPP SA6 (EDGEAPP) architecture and ETSI MEC architecture can complement each other is illustrated in Figure B.1-1, per the informative Annex C of 3GPP

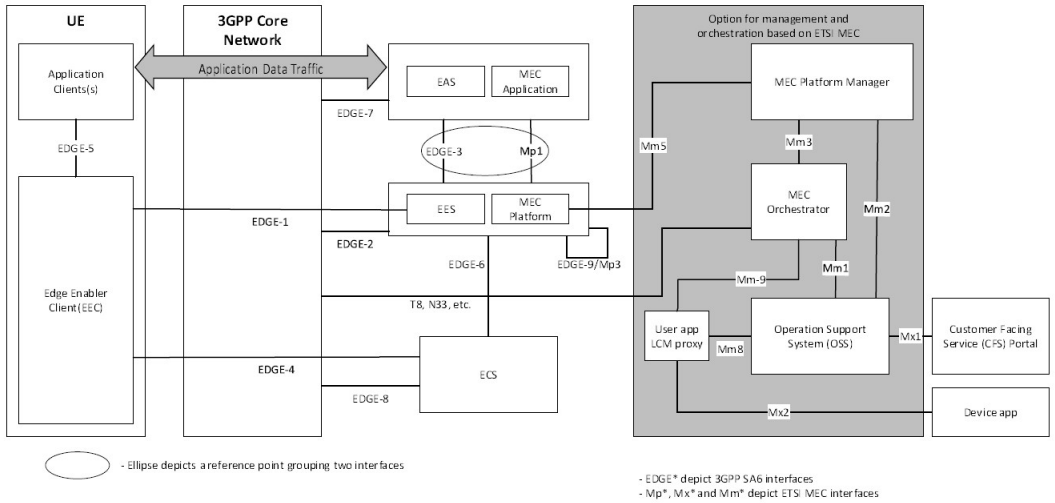


Figure B.1-1: Relationship between 3GPP SA6 (EDGEAPP) architecture and ETSI MEC architecture,

Type: AppInfo

This type represents the information provided by the MEC application instance as part of the "application registration request" and "application registration update" messages.

The attributes of the AppInfo shall follow the indications provided in table

Table Attributes of AppInfo

Attribute name	Data type	Cardinality	Description
appName	String	1	Name of the application. It shall be consistent with the appName in the AppD, if an AppD is available.
appProvider	String	0..1	Provider of the application. It shall be consistent with the appProvider in the AppD, if an AppD is available. See note 1.
appCategory	CategoryRef	0..1	Category of the application.
appDId	String	0..1	The application descriptor identifier. It is managed by the application provider to identify the application descriptor in a globally unique way. Shall be present if the application instance is instantiated by the MEC Management.
appInstanceId	String	0..1	Identifier of the application instance. Shall be present if the application instance is instantiated by the MEC Management.
endpoint	EndPointInfo	0..1	Endpoint information (e.g. URI, FQDN, IP address) of the application server, which is part of the application functionalities. Shall be present when isInsByMec is FALSE. See note 2.
appServiceRequired	ServiceDependency	0..N	Describes services a MEC application requires to run. ServiceDependency is defined in ETSI GS MEC 010-2 [4]. It shall not be provided if an AppD is available.
appServiceOptional	ServiceDependency	0..N	Describes services a MEC application may use if available. ServiceDependency is defined in ETSI GS MEC 010-2 [4]. It shall not be provided if an AppD is available.
appFeatureRequired	FeatureDependency	0..N	Describes features a MEC application requires to run. FeatureDependency is defined in ETSI GS MEC 010-2 [4]. It shall not be provided if an AppD is available.
appFeatureOptional	FeatureDependency	0..N	Describes features a MEC application may use if available. FeatureDependency is defined in ETSI GS MEC 010-2 [4]. It shall not be provided if an AppD is available.
isInsByMec	Boolean	0..1	Indicate whether the application instance is instantiated by the MEC Management. Default to FALSE if absent.
appProfile	AppProfile	0..1	Can be mapped to EAS profile More information can be found in the informative Annex C. See note 1 and note 2.

NOTE 1: If appProfile is present, appProvider shall be consistent with provid provided in EAS profile data type, i.e. the same.
NOTE 2: If appProfile is present, endpoint shall refer to the same end point as endPt provided in EAS profile data type.

Relationship of Edge Computing Service Players taking into account Federation, Service and Roaming Agreements between

Edge Communication Service Providers (ECSPs)

PLMN Operators,

Application Service Providers (ASPs) and

End Users

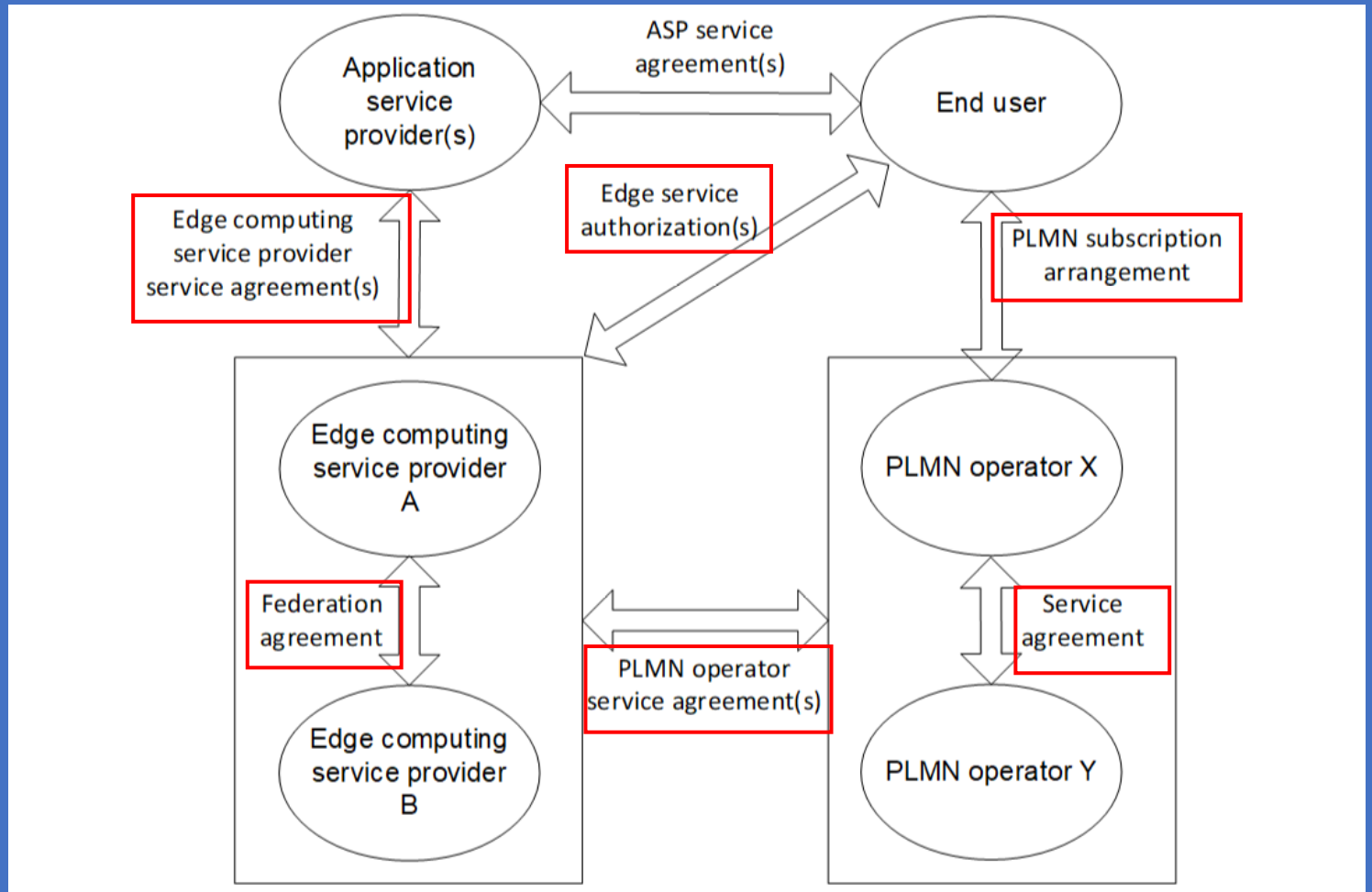


Figure : Relationships involved in edge computing service – federation and roaming

5G System Enhancements for Edge Computing in 5G Advanced"

KI#1: Accessing EHE (Edge Hosting Environment) in a VPLMN when Roaming

KI#2: Fast and efficient Network Exposure Improvements

KI#3: Policies for Finer Granular Sets of UEs

KI#4: Influencing UPF and EAS (re)location for Collections of UEs

KI#5: GSMA OPG Impacts and Improvements for EHE Operated by Separate Party

KI#6: Avoiding UE to switch away from EC PDU Session

KI#7: Obtain and Maintain Mapping Table between IP Address/IP Range with DNAI

Solution		Key issues						
Title	(page)	KI#1	KI#2	KI#3	KI#4	KI#5	KI#6	KI#7
01: <solution title>	10	X						

Table : Solution-Key issue matrix

3GPP, 5G System Enhancements for Edge Computing, Rel. 18, Feb., 2022

5G System Enhancements for Edge Computing in 5G Advanced"

KI#1: Accessing EHE in a VPLMN when Roaming

KI#2: Fast and efficient Network Exposure Improvements

KI#3: Policies for Finer Granular Sets of UEs

KI#4: Influencing UPF and EAS (re)location for Collections of UEs

KI#5: GSMA OPG Impacts and Improvements for EHE Operated by Separate Party

KI#6: Avoiding UE to switch away from EC PDU Session

KI#7: Obtain and Maintain Mapping Table between IP Address/IP Range with DNAI

Table : Solution-Key Issue Matrix

Solution Title	Key issues						
	KI#1	KI#2	KI#3	KI#4	KI#5	KI#6	KI#7
01: EAS discovery in Home Routed roaming scenario	X						
02: Session Breakout in Visited PLMN	X						
03: EAS (re)discovery procedure in roaming scenario	X						
04: Support EAS (re-)discovery in VPLMN via HR PDU Session	X						
05: Accessing V-EHE via HR PDU Session	X						
06: URSP solution to support roamers access to EHE in a VPLMN	X						
07: Using URSP Rules to Establish an LBO PDU Session	X						
08: V-ECS Discovery during Steering of Roaming	X						
09: PDU Session configuration from EASDF	X						
10: LBO PDU Session establishment using PLMN criteria in RSD	X						
11: Exposure of Network Congestion		X					
12: Efficient exposure of RAN information		X					
13: Fast and efficient network exposure improvements		X					
14: Group Management				X			
15: Selection of common DNAI				X			
16: Selecting the same EAS/DNAI for collection of UEs				X			
17: Application layer EAS selection for collections of UEs				X			
18: Discovery of the same EAS for collections of UEs				X			
19: Influencing UPF and EAS (re)location for collections of UEs				X			
20: Global EASDF					X		
21: EAS Deployment information differentiated by PLMN ID					X		
22: EAS discovery for federated OPs					X		
23: Improvements for EHE operated by separate party					X		
24: Reuse Option D after UL-CL insertion	X						
25: EAS discovery in VPLMN via V-EASDF for a HR PDU Session	X						
26: SM Policy for HR Session Breakout in VPLMN	X						
27: EAS discovery with dynamic setup of a LBO PDU Session	X						
28: Support edge computing in Roaming	X						
29: Use of Internal Group ID and constraints in EDI			X				
30: Policies referring to "Allowed services" and/or "Subscriber categories"			X				
31: Providing traffic offload policy for a set of UEs with service information			X				
32: Offload policy for finer granular set of UEs			X				
33: AF requests offload policy for sets of UEs			X				
34: Selecting the same EAS/DNAI for collection of UEs				X			
35: Providing dedicated (re)location information as traffic routing information				X			
36: Providing dedicated (re)location information as EAS Deployment information				X			
37: (Re)location of same EAS and coordination across UEs				X			
38: EAS Discovery for EHE shared with other PLMN					X		
39: Support EAS relocation of inter-PLMN	X				X		
40: EAS discovery for shared EHE					X		
41: Controlling non-3GPP access of EC traffic via URSP and ATSSS						X	
42: Network-guided EC traffic switching						X	
43: Network-based solution for keeping EC traffic on 3GPP Access						X	
44: EAS traffic switching avoidance						X	
45: Application selected PDU Session	X					X	
46: Avoid UE switching on-going EC traffic away from 3GPP access						X	
47: Avoiding Switch Away Based on an SMF Indication						X	
48: Avoiding Switch Away Based on an Indication in the URSP						X	
49: URSP based solution to avoid UE to switch away from Edge PDU Session						X	
50: Obtain and maintain mapping table between IP address/IP range with DNAI							X
51: EDI holding the IP address to DNAI mapping							X
52: AF obtaining target DNAI provided by NEF							X

3GPP, 5G System Enhancements for Edge Computing, Rel. 18, May, 2022

5G System Enhancements for Edge Computing in 5G Advanced"

KI#1: Accessing EHE in a VPLMN when Roaming

KI#2: Fast and efficient Network Exposure Improvements

KI#3: Policies for Finer Granular Sets of UEs

KI#4: Influencing UPF and EAS (re)location for Collections of UEs

KI#5: GSMA OPG Impacts and Improvements for EHE Operated by Separate Party

KI#6: Avoiding UE to switch away from EC PDU Session

KI#7: Obtain and Maintain Mapping Table between IP Address/IP Range with DNAI

Table : Solution-Key Issue Matrix

Solution	Title	Key issues						
		KI#1	KI#2	KI#3	KI#4	KI#5	KI#6	KI#7
01	EAS discovery in Home Routed roaming scenario	X						
02	Session Breakout in Visited PLMN	X						
03	EAS (re)discovery procedure in roaming scenario	X						
04	Support EAS (re-)discovery in VPLMN via HR PDU Session	X						
05	Accessing V-EHE via HR PDU Session	X						
06	URSP solution to support roamers access to EHE in a VPLMN	X						
07	Using URSP Rules to Establish an LBO PDU Session	X						
08	V-ECS Discovery during Steering of Roaming	X						
09	PDU Session configuration from EASDF	X						
10	LBO PDU Session establishment using PLMN criteria in RSD	X						
11	Exposure of Network Congestion		X					
12	Efficient exposure of RAN information		X					
13	Fast and efficient network exposure improvements		X					
14	Group Management				X			
15	Selection of common DNAI				X			
16	Selecting the same EAS/DNAI for collection of UEs				X			
17	Application layer EAS selection for collections of UEs				X			
18	Discovery of the same EAS for collections of UEs				X			
19	Influencing UPF and EAS (re)location for collections of UEs				X			
20	Global EASDF					X		
21	EAS Deployment information differentiated by PLMN ID					X		
22	EAS discovery Edge Node Sharing					X		
23	Improvements for EHE operated by separate party					X		
24	Reuse Option D after UL-CL insertion	X						
25	EAS discovery in VPLMN via V-EASDF for a HR PDU Session	X						
26	SM Policy for HR Session Breakout in VPLMN	X						
27	EAS discovery with dynamic setup of a LBO PDU Session	X						
28	Support edge computing in Roaming	X						
29	Use of Internal Group ID and constraints in EDI			X				
30	Policies referring to "Allowed services" and/or "Subscriber categories"			X				
31	Providing traffic offload policy for a set of UEs with service information			X				
32	Offload policy for finer granular set of UEs			X				
33	AF requests offload policy for sets of UEs			X				
34	Selecting the same EAS/DNAI for collection of UEs				X			
35	Providing dedicated (re)location information as traffic routing information				X			
36	Providing dedicated (re)location information as EAS Deployment information				X			
37	(Re)location of same EAS and coordination across UEs				X			
38	EAS Discovery for EHE shared with other PLMN					X		
39	Support EAS relocation of inter-PLMN	X				X		
40	EAS discovery for shared EHE					X		
41	Controlling non-3GPP access of EC traffic via URSP and ATSSS						X	
42	Network-guided EC traffic switching						X	
43	Network-based solution for keeping EC traffic on 3GPP Access						X	
44	EAS traffic switching avoidance						X	
45	Application selected PDU Session	X					X	
46	Avoid UE switching on-going EC traffic away from 3GPP access						X	
47	Avoiding Switch Away Based on an SMF Indication						X	
48	Avoiding Switch Away Based on an Indication in the URSP						X	
49	URSP based solution to avoid UE to switch away from Edge PDU Session						X	
50	Obtain and maintain mapping table between IP address/IP range with DNAI							X
51	EDI holding the IP address to DNAI mapping							X
52	AF obtaining target DNAI provided by NEF							X
53	EDC-based EAS discovery for HR PDU Session with Session Breakout	X						
54	PCF controlling common DNAI				X			
55	Access the shared EAS via N9 tunnel					X		

3GPP, 5G System Enhancements for Edge Computing, Rel. 18, Sept, 2022

5G System Enhancments - EAS Deployment Information Management

EAS Deployment Information Management refers to the capability to
- Create,
- Update or
- Remove EAS Deployment Information from AF and the distribution to the SMF.

The NEF is in charge of the Management of EAS Deployment Information which may be stored in UDR.

The EAS Deployment Information indicates how Edge Services are deployed in each Local part of the DN, the description of EAS Deployment Information is shown in **Table**

The EAS Deployment Information Management procedures are described in this clause, the procedures are independent of any PDU Session, including:

- *The procedure for EAS Deployment Information management from AF via the NEF.*
- *The procedure for EAS Deployment Information management in the SMF.*
- *The procedure for BaselineDNSPattern Management in the EASDF.*

Table Description of EAS Deployment Information

Parameters	Description
DNN	DNN for the EAS Deployment Information. [optional]
S-NSSAI	S-NSSAI for the EAS Deployment Information. [optional]
External Group Identifier/Internal Group Identifier	Group ID for the EAS Deployment information. [optional] NOTE: The AF may provide External Group Identifier, and NEF can map the External Group Identifier into Internal Group Identifier according to information received from UDM.
Application ID	Identifies the application for which the EAS Deployment Information corresponds to. [optional]
FQDN(s)	Supported FQDN(s) for application(s) deployed in the Local part of the DN.
DNAI(s)	DNAI(s) for the EAS Deployment information. [optional]
DNS Server Information	list of DNS server identifier (consisting of IP address and port) for each DNAI. [optional]
EAS IP address range Information	IP address(es) of the EASs in the Local part of the DN or the IP address ranges (IPv4 subnetwork(s) and/or IPv6 prefix(es) of the Local part of the DN where the EAS is deployed for each DNAI. [optional]

Solution 29 (KI#3): **Use of Internal Group ID and Constraints in EDI (EAS Deployment Information)**

To identify a finer granularity of UEs, Internal Group ID is to be used.

There is no practical limit for how many Internal group IDs that can be assigned in a 5GS.

The structure of an Internal Group ID is as follows:

A UE can be associated with a number of Internal Group IDs as per 5G System Architecture.

Stage 3 has not specified any limit for how many internal groups a UE can be associated with.

To support different constraints related to EC, the solution uses EDI, which is enhanced with a constraints field that tells under which constraints the EDI record applies.

The EDI can be provisioned by an operator though OAM to UDR (or via NEF) or the EDI can be provided by an AF.

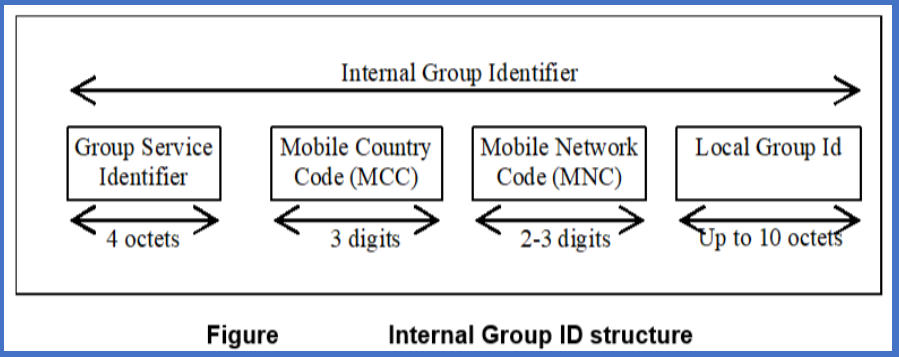


Figure Internal Group ID structure

Table Description of EAS Deployment Information

Parameters	Description
DNN	DNN for the EAS Deployment Information. [optional]
S-NSSAI	S-NSSAI for the EAS Deployment Information. [optional]
External Group Identifier/Internal Group Identifier	Group ID for the EAS Deployment information. [optional] NOTE: The AF may provide External Group Identifier, and NEF can map the External Group Identifier into Internal Group Identifier according to information received from UDM.
Application ID	Identifies the application for which the EAS Deployment Information corresponds to. [optional]
FQDN(s)	Supported FQDN(s) for application(s) deployed in the Local part of the DN.
DNAI(s)	DNAI(s) for the EAS Deployment information. [optional]
DNS Server Information	list of DNS server identifier (consisting of IP address and port) for each DNAI. [optional]
EAS IP address range Information	IP address(es) of the EASs in the Local part of the DN or the IP address ranges (IPv4 subnetwork(s) and/or IPv6 prefix(es) of the Local part of the DN where the EAS is deployed for each DNAI. [optional]

Table EDI parameters

Parameters	Description
DNN	DNN for the EAS Deployment Information. [optional]
S-NSSAI	S-NSSAI for the EAS Deployment Information. [optional]
External Group Identifier/Internal Group Identifier	Group ID for the EAS Deployment information. [optional] NOTE: The AF may provide External Group Identifier, and NEF can map the External Group Identifier into Internal Group Identifier according to information received from UDM.
Application ID	Identifies the application for which the EAS Deployment Information corresponds to. [optional]
Constraints	**When and where this EDI applies´ Example: Time: 08:00-17:00 Place: TAI-list**
FQDN(s)	Supported FQDN(s) for application(s) deployed in the Local part of the DN.
DNS Server Information	list of DNS server identifier (consisting of IP address and port) for each DNAI. [optional]
EAS IP address range Information	IP address(s) of the EASs in the local DN for each DNAI. [optional]

5G Enhanced Architecture (EDGEAPP) for enabling Edge Applications in 5G Advanced"

Key issue #1: Enhanced notification service to the EEC
Key issue #2: Enablement of Service APIs exposed by EAS
Key issue #3: Enhancements to Service Continuity Planning
Key issue #4: EDGE-5
Key issue #6: Edge Services support across ECSPs
Key issue #7: Application traffic filter exposure
Key issue #8: EAS selection synchronization
Key issue #9: Enhancement of dynamic EAS instantiation triggering
Key issue #10: Support for Roaming UEs
Key issue #11: ACR between EAS and Cloud Application Server (CAS)
Key issue #12: EEL service differentiation
Key issue #13: Edge Enabler Layer (EEL) support for EAS Synchronization
Key issue #14: Application traffic influence for initially selected EAS
Key issue #15: Support of constrained devices for Edge
Key issue #16: Support of NAT (Network Address Translation) deployed within the Edge Data Network
Key issue #17: Discovery of a common EAS
Key issue #18: Linkage between EASs
Key issue #19: ACR scenario combination
Key issue #20: Method of supporting Federated EAS Service

Table Mapping of solutions to key issues

	KI # 1	KI # 2	KI # 3	KI # 4	KI # 5	KI # 6	KI # 7	KI # 8	KI # 9	KI # 10	KI # 11	KI # 12	KI # 13	KI # 14	KI # 15	KI # 16	KI # 17	KI # 18	KI # 19	KI # 20
Sol #1	x																			
Sol #2							x													
Sol #4						x				x										
Sol #5						x				x										
Sol #6			x																	
Sol #7			x																	
Sol #8		x																		
Sol #9														x						
Sol #10															x					
Sol #11		x			x															
Sol #12			x									x								
Sol #13						x				x										
Sol #14										x										
Sol #15								x						x						
Sol #16												x								
Sol #17														x						
Sol #18															x					
Sol #19																			x	
Sol #20	x																			
…																				

5G Enhanced Architecture (EDGEAPP) for enabling Edge Applications in 5G Advanced"

Key issue #1: Enhanced notification service to the EEC
Key issue #2: Enablement of Service APIs exposed by EAS
Key issue #3: Enhancements to Service Continuity Planning
Key issue #4: EDGE-5
Key issue #6: Edge Services support across ECSPs
Key issue #7: Application traffic filter exposure
Key issue #8: EAS selection synchronization
Key issue #9: Enhancement of dynamic EAS instantiation triggering
Key issue #10: Support for roaming Ues
Key issue #11: ACR between EAS and Cloud Application Server (CAS)
Key issue #12: EEL service differentiation
Key issue #13: Edge Enabler Layer (EEL) support for EAS Synchronization
Key issue #14: Application traffic influence for initially selected EAS
Key issue #15: Support of constrained devices for Edge
Key issue #16: Support of NAT (Network Address Translation) deployed within the Edge Data Network
Key issue #17: Discovery of a common EAS
Key issue #18: Linkage between EASs
Key issue #19: ACR scenario combination
Key issue #20: Method of supporting Federated EAS Service

Key issue #21: Simultaneously EAS connectivity in ACR
Key issue #22: EAS discovery in Edge Node sharing scenario

Table ... Mapping of solutions to key issues

	KI #1	KI #2	KI #3	KI #4	KI #5	KI #6	KI #7	KI #8	KI #9	KI #10	KI #11	KI #12	KI #13	KI #14	KI #15	KI #16	KI #17	KI #18	KI #19	KI #20	KI #21	KI #22
Sol #1	X																					
Sol #2							X															
Sol #3	X																					

	KI #1	KI #2	KI #3	KI #4	KI #5	KI #6	KI #7	KI #8	KI #9	KI #10	KI #11	KI #12	KI #13	KI #14	KI #15	KI #16	KI #17	KI #18	KI #19	KI #20	KI #21	KI #22
Sol #4						X				X												
Sol #5						X				X												
Sol #6			X																			
Sol #7			X																			
Sol #8		X																				
Sol #9																	X					
Sol #10																		X				
Sol #11		X			X																	
Sol #12			X									X										
Sol #13						X				X												
Sol #14										X												
Sol #15								X									X					
Sol #16												X										
Sol #17																	X					
Sol #18																		X				
Sol #19																					X	
Sol #20	X																					
Sol #21			X																			
Sol #22				X																		X
Sol #23																			X			
Sol #24													X									
Sol #25													X									
Sol #26																					X	
Sol #27																				X		
Sol #28																				X		
Sol #29																				X		
Sol #30																				X		
Sol #31																				X		
Sol #32									X													
Sol #33									X													
Sol #34				X																		
Sol #35																					X	
Sol #36					X																	
...																						

5G Enhanced EDGEAPP Architecture for enabling Edge Applications in "5G Advanced"

Key issue #1: Enhanced notification service to the EEC
Key issue #2: Enablement of Service APIs exposed by EAS
Key issue #3: Enhancements to Service Continuity Planning
Key issue #4: EDGE-5
Key issue #6: Edge Services support across ECSPs
Key issue #7: Application traffic filter exposure
Key issue #8: EAS selection synchronization
Key issue #9: Enhancement of dynamic EAS instantiation triggering
Key issue #10: Support for roaming Ues
Key issue #11: ACR between EAS and Cloud Application Server (CAS)
Key issue #12: EEL service differentiation
Key issue #13: Edge Enabler Layer (EEL) support for EAS Synchronization
Key issue #14: Application traffic influence for initially selected EAS
Key issue #15: Support of constrained devices for Edge
Key issue #16: Support of NAT (Network Address Translation) deployed within the Edge Data Network
Key issue #17: Discovery of a common EAS
Key issue #18: Linkage between EASs
Key issue #19: ACR scenario combination
Key issue #20: Method of supporting Federated EAS Service
Key issue #21: Simultaneously EAS connectivity in ACR
Key issue #22: EAS discovery in Edge Node sharing scenario

Key issue #23: Reliable Edge Service
Key issue #24: SEAL Capability Access for EEL Support

Table Mapping of solutions to key issues

	KI #1	KI #2	KI #3	KI #4	KI #5	KI #6	KI #7	KI #8	KI #9	KI #10	KI #11	KI #12	KI #13	KI #14	KI #15	KI #16	KI #17	KI #18	KI #19	KI #20	KI #21	KI #22	KI #23	KI #24
Sol #1	X																							
Sol #2							X																	
Sol #3	X																							
Sol #4						X				X														
Sol #5						X				X														
Sol #6			X																					

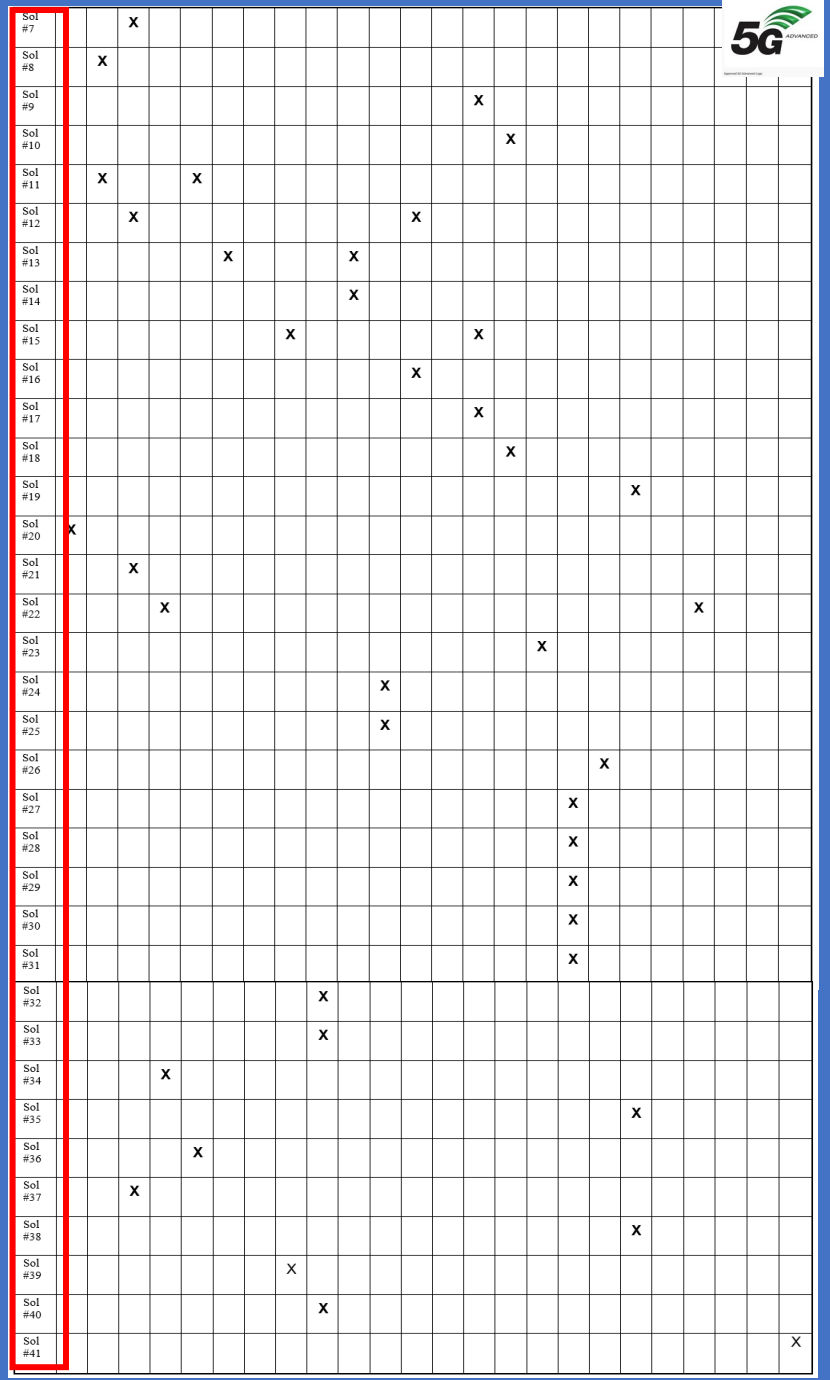
Sol #7			X																					
Sol #8		X																						
Sol #9														X										
Sol #10															X									
Sol #11		X			X																			
Sol #12			X									X												
Sol #13					X				X															
Sol #14									X															
Sol #15							X							X										
Sol #16												X												
Sol #17														X										
Sol #18															X									
Sol #19																					X			
Sol #20	X																							
Sol #21			X																					
Sol #22				X																		X		
Sol #23																X								
Sol #24											X													
Sol #25											X													
Sol #26																			X					
Sol #27																	X							
Sol #28																	X							
Sol #29																	X							
Sol #30																	X							
Sol #31																	X							
Sol #32									X															
Sol #33									X															
Sol #34				X																				
Sol #35																					X			
Sol #36					X																			
Sol #37			X																					
Sol #38																					X			

5G Enhanced EDGEAPP Architecture for enabling Edge Applications in "5G Advanced"

Key issue #1: Enhanced notification service to the EEC
Key issue #2: Enablement of Service APIs exposed by EAS
Key issue #3: Enhancements to Service Continuity Planning
Key issue #4: EDGE-5
Key issue #6: Edge Services support across ECSPs
Key issue #7: Application traffic filter exposure
Key issue #8: EAS selection synchronization
Key issue #9: Enhancement of dynamic EAS instantiation triggering
Key issue #10: Support for roaming Ues
Key issue #11: ACR between EAS and Cloud Application Server (CAS)
Key issue #12: EEL service differentiation
Key issue #13: Edge Enabler Layer (EEL) support for EAS Synchronization
Key issue #14: Application traffic influence for initially selected EAS
Key issue #15: Support of constrained devices for Edge
Key issue #16: Support of NAT (Network Address Translation) deployed within the Edge Data Network
Key issue #17: Discovery of a common EAS
Key issue #18: Linkage between EASs
Key issue #19: ACR scenario combination
Key issue #20: Method of supporting Federated EAS Service
Key issue #21: Simultaneously EAS connectivity in ACR
Key issue #22: EAS discovery in Edge Node sharing scenario
Key issue #23: Reliable Edge Service
Key issue #24: SEAL Capability Access for EEL Support

Table Mapping of solutions to key issues

	KI #1	KI #2	KI #3	KI #4	KI #5	KI #6	KI #7	KI #8	KI #9	KI #10	KI #11	KI #12	KI #13	KI #14	KI #15	KI #16	KI #17	KI #18	KI #19	KI #20	KI #21	KI #22	KI #23	KI #24
Sol #1	X																							
Sol #2							X																	
Sol #3	X																							
Sol #4						X				X														
Sol #5						X				X														
Sol #6			X																					



3GPP, 5G enhanced Architect for enabling Edge Applications., Rel. 18, , Sept. 2022

5G Enhanced Architecture for enabling Edge Applications - Summary Sept 2022

Key issues (evaluation clause reference)	Solution		Dependency on other working groups
Key issue #1: Enhanced notification service to the EEC	*Solution #1: Service provisioning via push notification*		
	Solution #3: Service provisioning triggering via SMS over NAS		
	Solution #20: Propagation of EEL notifications to EEC using Edge Notification Server		
Key issue #2: Enablement of Service APIs exposed by EAS	*Solution #8: EAS Service API enablement using CAPIF*		
	Solution #11: A deployment option for alignment with ETSI MEC using CAPIF		
Key issue #3: Enhancements to service continuity planning	*Solution #6: ACR update in service continuity planning*		
	Solution #7: EES monitors UE mobility for service continuity planning		
	Solution #12: Service continuity planning allowance		
	Solution #21: Prediction expiration time for service continuity planning enhancement		
	Solution #37: ACR request trigger timing		
Key issue #4: EDGE-5	*Solution #22: Support simultaneous EAS connectivity in ACR*		*SA3*
	Solution #34: EDGE-5 APIs		
Key issue #5: Alignment of EDGEAPP and ETSI MEC	*Solution #11: A deployment option for alignment with ETSI MEC using CAPIF*		*SA5*
	Solution #36: Alignment of EDGEAPP and ETSI MEC	*SA5*	
Key issue #6: Edge services support across ECSPs	*Solution #4: ECS discovery through serving ECS to support edge services across ECSPs*		
	Solution #5: ECS enhancement to discover EESs via other ECSs to support edge services across ECSPs		
	Solution #13: Update ECS configuration information		*SA2*
Key issue #7: Application traffic filter exposure	*Solution #2: Traffic filter support for EDGE-3 API addressing application traffic detection*		
Key issue #8: EAS selection synchronization	*Solution #15: Initial EAS selection declaration*		
Key issue #9: Enhancement of dynamic EAS instantiation triggering	*Solution #32: Dynamic EAS instantiation triggering and notification*		*SA5*

Key issues (evaluation clause reference)	Solution	Solution (clause reference)		Dependency on other working groups
	Solution #33: Support for EEC Discovery of EAS(es) before instantiation	*7.33*		*SA5*
	Solution #40: EAS instantiation status provisioned by ECS	*7.xx*		*SA5*
Key issue #10: Support for roaming UEs	*Solution #4: ECS discovery through serving ECS to support edge services across ECSPs*	*7.4*		*SA3*
	Solution #5: ECS enhancement to discover EESs via other ECSs to support edge services across ECSPs	*7.5*		*SA3*
	Solution #13: Update ECS configuration information	*7.13*		*SA2*
	Solution #14: V-ECS Discovery via the H-ECS	*7.14*		*SA3*
Key issue #11: ACR between EAS and Cloud Application Server	*Solution #24: ACR between CAS and EAS*	*7.24*		
	Solution #25: ACR between EAS and Cloud Application Server	*7.25*		
Key issue #12: EEL service differentiation	*Solution #12: Service continuity planning allowance*	*7.12*		
	Solution #16: EAS discovery for different users	*7.16*		
Key issue #13: Edge enabler layer support for EAS synchronization				
Key issue #14: Application traffic influence for initially selected EAS	*Solution #9: Application traffic influence trigger from EAS*	*7.9*		
	Solution #15: Initial EAS selection declaration	*7.15*		
	Solution #17: Traffic influence for initial EAS discovery	*7.17*		
Key issue #15: Support of constrained devices for Edge	*Solution #10: low power mode support*	*7.10*		
	Solution #18: Constraint device in EDGEAPP	*7.18*		
Key issue #16: support of NAT deployed within the edge data network	*Solution #23: UE identification with NAT*	*7.23*		*SA2, SA3*
Key issue #17: Discovery of a common EAS	*Solution #27: Enabling AC Association Aware services by selecting common EASs*	*7.27*		
	Solution #28: Common EAS discovery using EAS selection information	*7.28*		
	Solution #29: Discovery of a common EAS	*7.29*		
	Solution #30: Common EAS selection	*7.30*		
	Solution #31: Discover common EAS	*7.31*		
Key issue #18: Linkage between EASs	*Solution #26: Bundled EASs*	*7.26*		
Key issue #19: ACR scenario combination	*Solution #19: EES determines the selected ACR scenario*	*7.19*		

Key issues (evaluation clause reference)	Solution	Solution (clause reference)		Dependency on other working groups
	Solution #35: EEC selected ACR scenarios	*7.35*		
Key issue #20: Method of supporting federated EAS service				
Key issue #21: Simultaneously EAS connectivity in ACR	*Solution #22: Support simultaneous EAS connectivity in ACR*	*7.22*		
Key issue #22: EAS discovery in Edge Node sharing scenario				
Key issue #23: Reliable Edge service			*SA5*	
Key Issue #24: SEAL capability access for EEL support.	*Solution #41: Interaction with ADAES for Edge Load Analytics*			*SA6*

3GPP, 5G enhanced Architect for enabling Edge Applications., Rel. 18, , Sept. 2022

Analytics NWDAF/MDAF/MDAS + ADAES

5G Network Reference Architecture for Data Collection and Reporting

The Reference Architecture envisages a Set of high-level Procedures by which Data is collected by a Network Data Analytics Function (NWDAF) from UE Application(s) via an intermediary Application Function (AF).

The intermediary Application Function (AF) envisaged in [4] is here named the Data Collection AF.

It is intended that this Reference Architecture be instantiated in Domain-specific ways to suit the needs of different features of the 5G System.

The Reference Architecture may be instantiated separately in different Slices of a network.

The Services defined in the present Reference Architecture may be exposed to Parties outside the Trusted Domain via the NEF.

The Data Collection AF may support CAPIF [8] to provide APIs to other Applications (i.e. API invokers), as defined in clause 4.7.2.

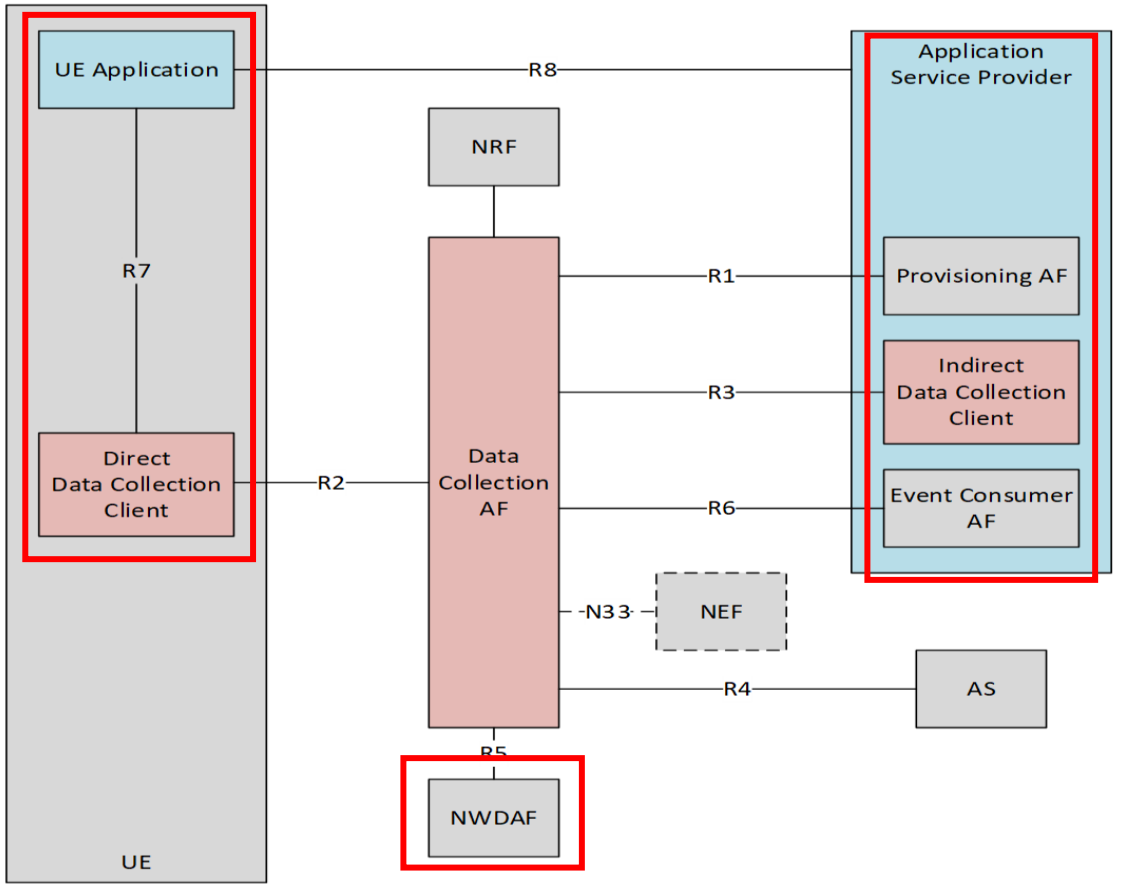


Figure: 5G Reference Architecture for Data Collection and Reporting in Reference Point

5G Network Reference Architecture for Data Collection and Reporting

Service-Based Architecture (SBA) for Data Collection and Reporting The Figure depicts the case where the Data Collection AF is deployed inside the Trusted Domain, while the Application Service Provider (ASP) and the AS may be deployed independently either Inside or Outside the Trusted Domain.

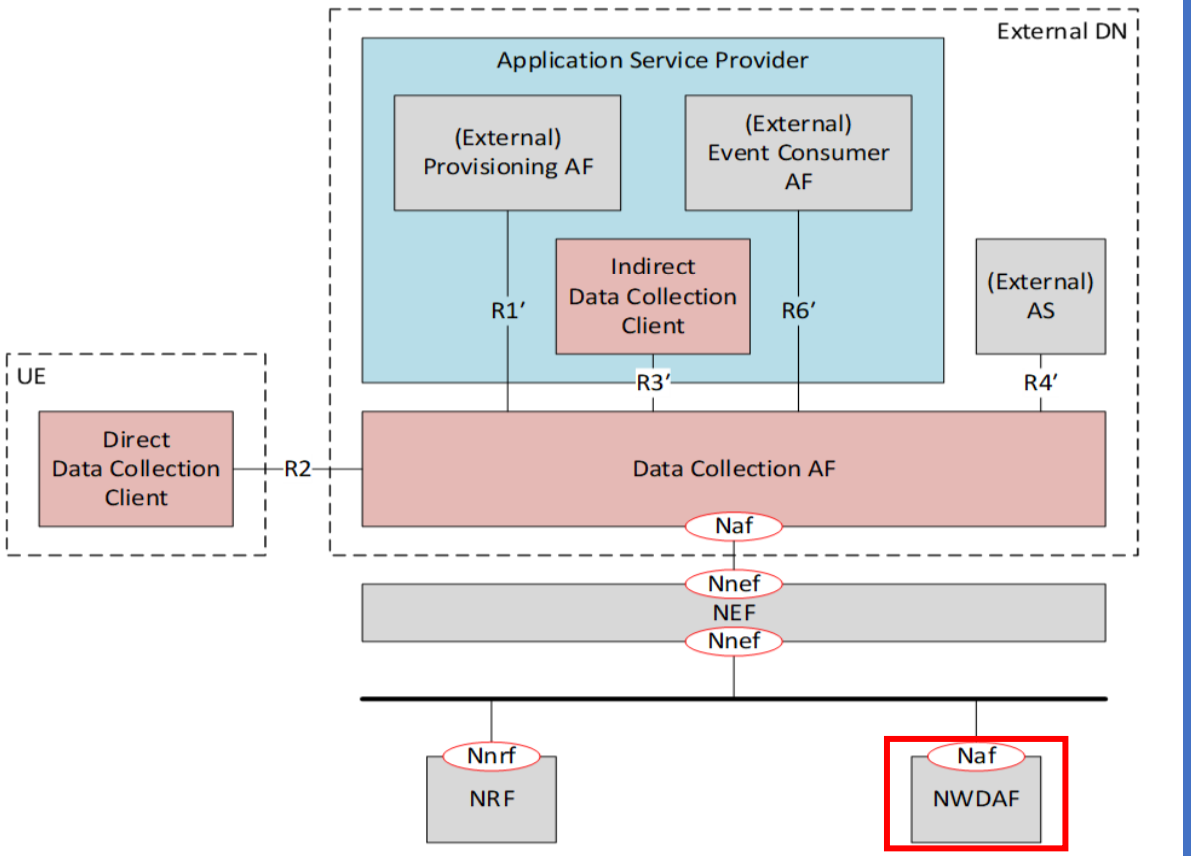


Figure: 5G Reference Architecture for Data Collection and Reporting in Service-based Architecture when the Data Collection AF is deployed outside the Trusted Domain

The Figure below shows the Reference Architecture for Data Collection and Reporting in Service-based Architecture and depicts the Case where the Data Collection AF is deployed inside the Trusted Domain, while the Application Service Provider (ASP) and the AS may be deployed independently either inside or outside the Trusted Domain.

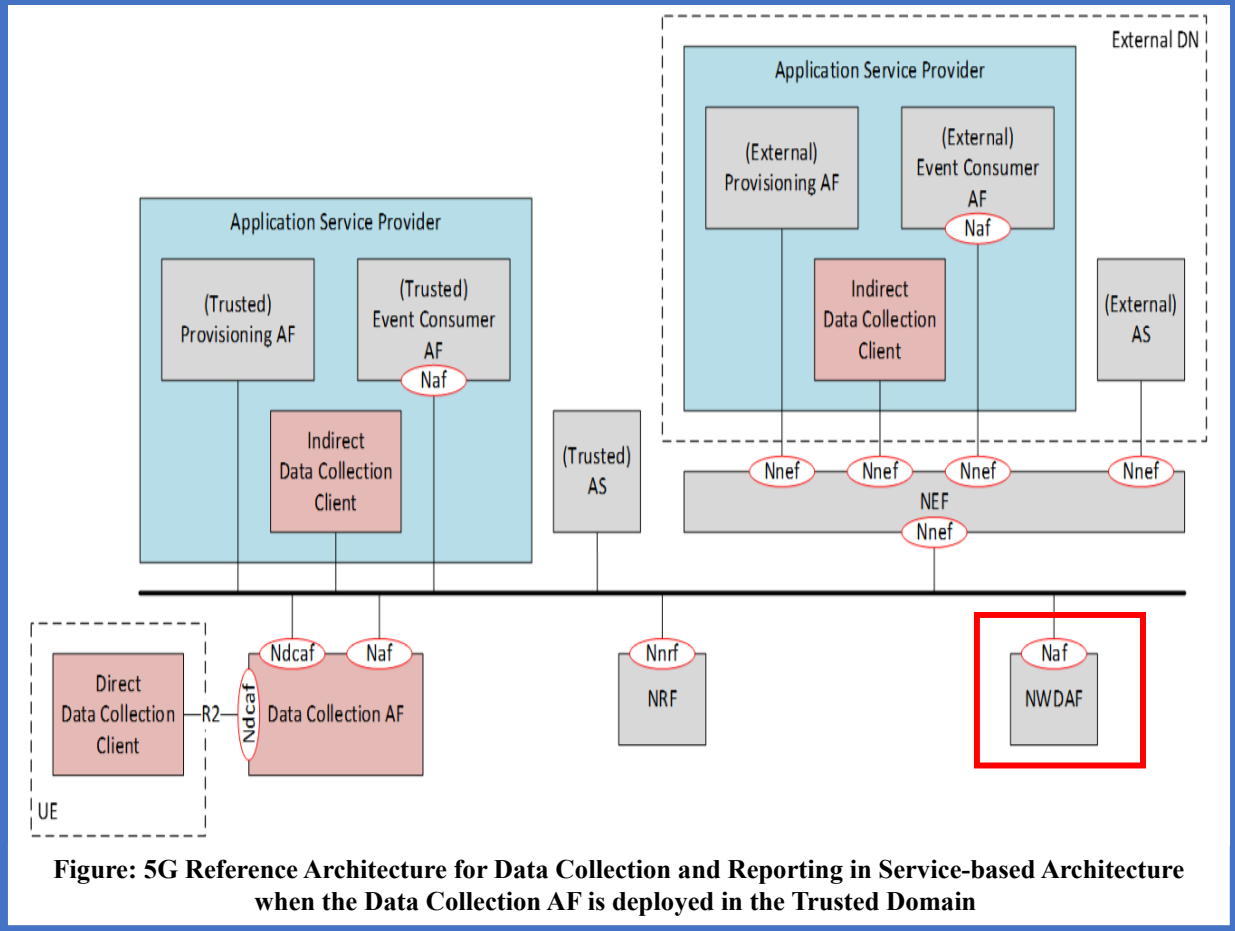


Figure: 5G Reference Architecture for Data Collection and Reporting in Service-based Architecture when the Data Collection AF is deployed in the Trusted Domain

5G Network NWDAF Enabler for Automation

Solution #4: Determining ML Model drift for improving Analytics Accuracy

The Accuracy of Analytic output from an NWDAF depends very much on the Accuracy of the ML Model provided by the MTLF (Model Training Logical Function) NWDAF.

The Training Data that are used to train an ML Model are usually Historical Data (Data stored in the ADRF).

The Validity/Accuracy of the ML Model depends on whether the Training Data used are up to Date with the Real-Time Network Configuration/Behaviour.

For example, compared to When the Training Data were collected the Network Operator may configure Additional Network Resources to a Network Slice, or the Number of Users accessing Services via the Core Network may considerably increase (e.g. Tourist season in the Summer).

Such Use Case (UC) may cause a Model Drift given that ML Model was not trained with up-to-date data.

There are many reasons that ML Model Drift can occur, but the main cause is a change of the Data with time.

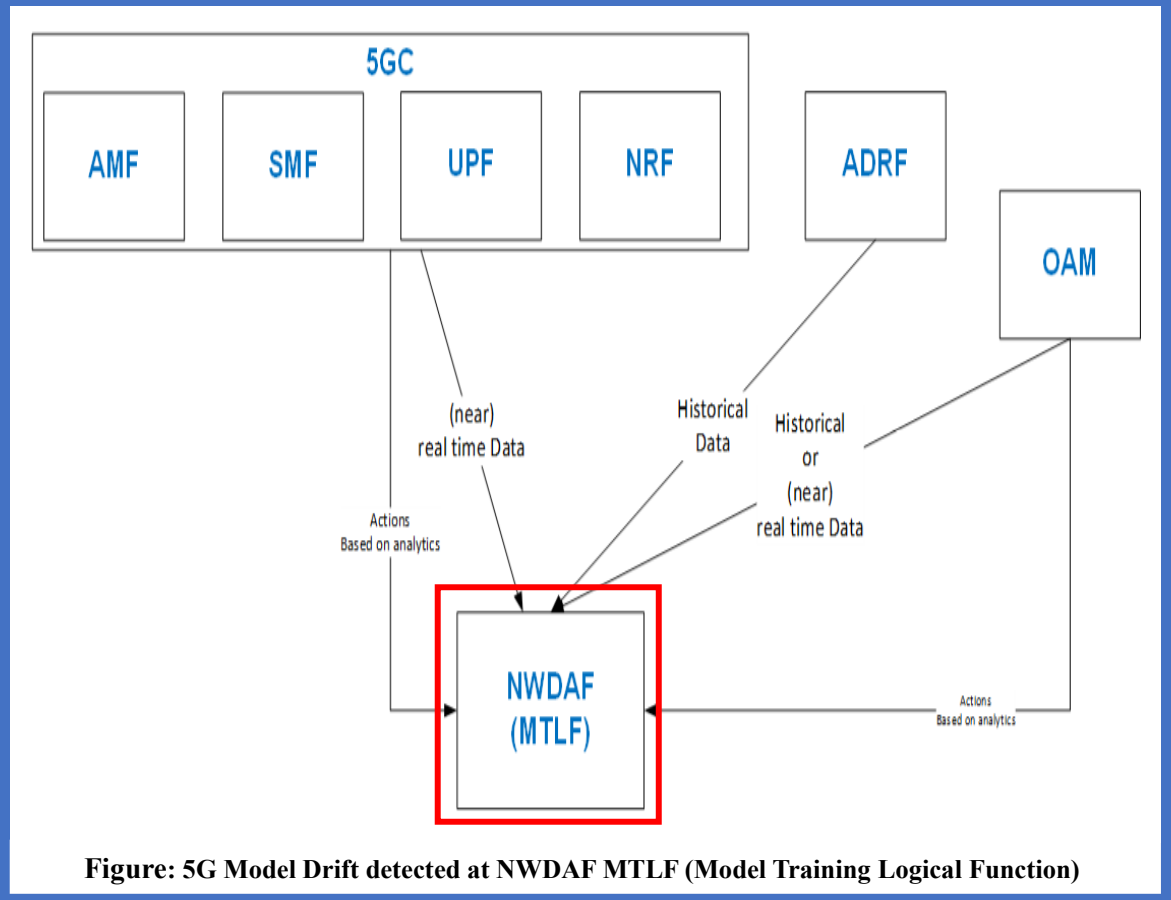


Figure: 5G Model Drift detected at NWDAF MTLF (Model Training Logical Function)

5G System NWDAF enhancements enabling automation

Key Issue #1: How to improve correctness of NWDAF Analytics

Key Issue #2: NWDAF-assisted Application Detection

Key Issue #3: Data and Analytics exchange in Roaming Case

Key Issue #4: How to Enhance Data Collection and Storage

Key Issue #5: Enhance trained ML Model sharing

Key issue #6: NWDAF-assisted URSP

Key Issue #7: Enhancements on QoS Sustainability Analytics

Key Issue #8: Supporting Federated Learning in 5GC

Key Issue #9: Enhancement of NWDAF with finer Granularity of Location Information

Key Issue #10: Interactions with MDAS/MDAF

Table: Mapping of solutions to key issues

	Key Issues									
Solutions	1	2	3	4	5	6	7	8	9	10
1	X									
2	X									
3	X									
4	X									
5	X									
6	X									
7	X									
8		X								
9		X								
10			X							
11			X							
12				X						
13					X					
14					X					
15					X					
16						X				
17			X			X				
18							X			
19							X			
20							X			
21								X		
22								X		
23								X		
24								X		
25									X	
26									X	
27									X	
28	X									
29	X									
30	X									
31	X									
32	X									
33	X									
34	X									
35	X									
36	X									
37			X							
38			X							
39			X							
40			X							
41				X						
42				X						
43				X	X					
44				X						
45				X						
46				X						
47					X					
48						X				
49						X				
50							X			
51								X		
52								X		
53								X		
54									X	
55									X	
56									X	
57									X	
58									X	
59									X	
60										X

5G ADAE internal Architecture based on 3GPP Data Analytics Framework

ADAE internal Architecture based on 3GPP Data Analytics Framework (DAF):

- 1) **NWDAF** provides Network Data Analytics Services at the 5GC
- 2) **DCCF** coordinates the Collection and Distribution of Data requested by NF/AF Consumers.

Data Collection Coordination is supported by a DCCF. Data Consumers can send Requests for Data to the DCCF rather than directly to the NF/AF Data Source.

- **3) ADRF** stores Historical Data and/or Analytics, i.e., Data and/or Analytics related to past time period that has been obtained by the Consumer.

After the Consumer obtains Data and/or Analytics, Consumer may store Historical Data and/or Analytics in an ADRF. Whether the Consumer directly contacts the ADRF or goes via the DCCF or via the Messaging Framework is based on configuration.

ADAE Server can reuse the existing **3GPP Data Analytics Framework (DAF)** for the Data Collection coordination, Delivery and Storage as provided by **DCCF** and **ADRF** Functionalities.

As illustrated in **Figure A-DCCF** and **A-ADRF** can be defined as Functionalities within the internal **ADAE Architecture** and can offer similar Functionality as proposed in 5GC, but at Application Layer.

In this model, an **Application Layer - Data Collection and Coordination Function (A-DCCF)** is used to fetch Data or put Data into an Application Level entity (e.g. A-ADRF, Data Source).

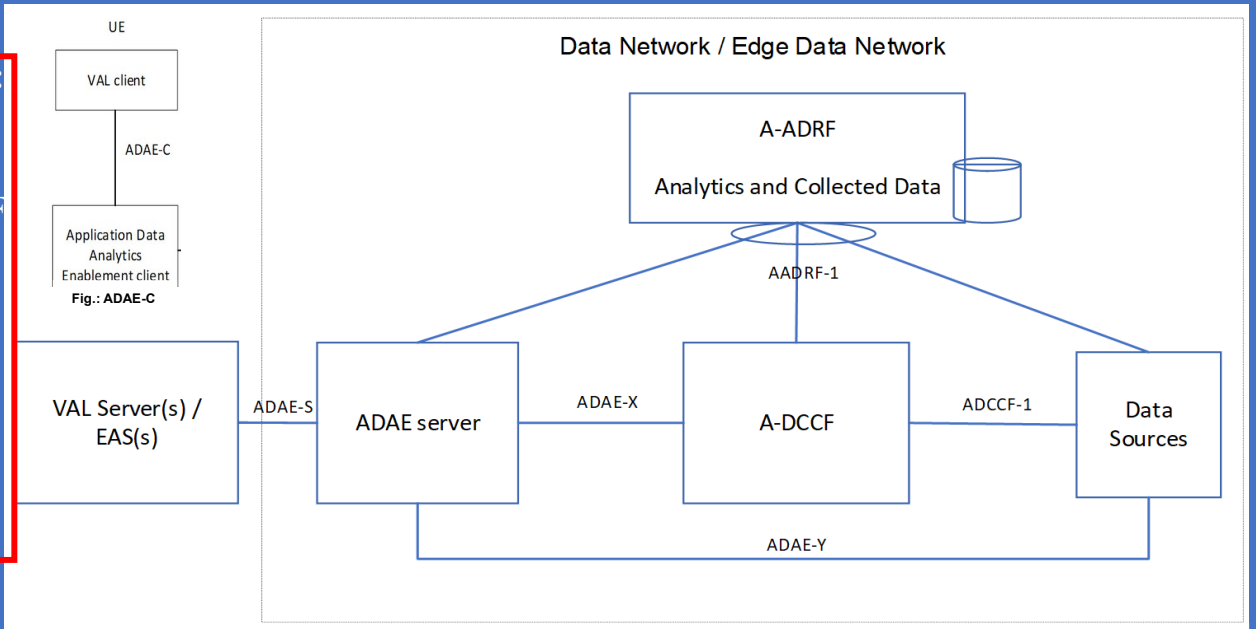


Figure: 5G Application Data Analytics Enablement (ADAE) Generic Functional Model based on 3GPP Data Analytics Framework model

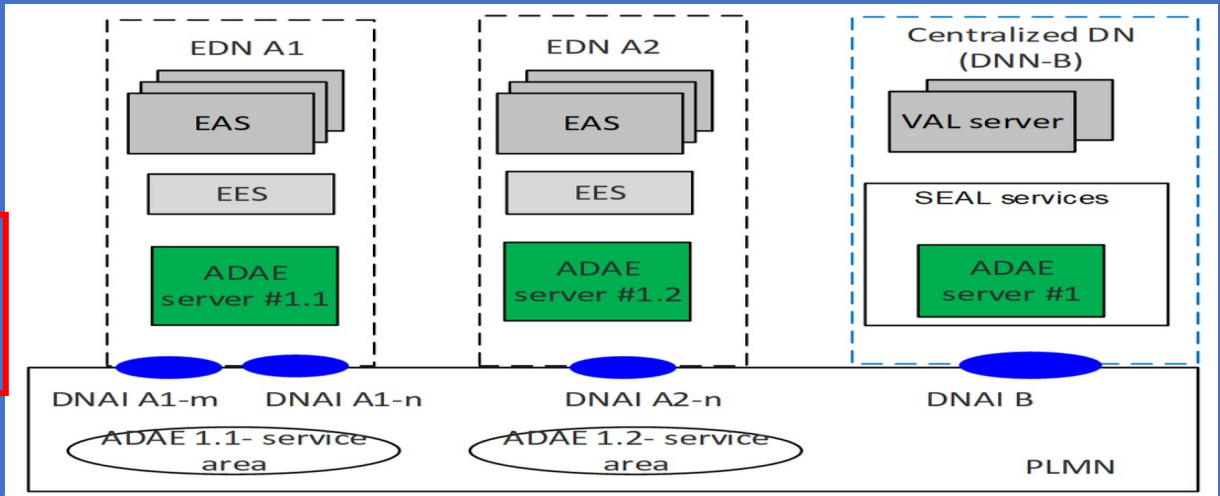


Fig.: 5G System Hierarchical (Cloud/Central and Edge/Local) deployment of ADAES

ADAE internal Architecture based on 3GPP Data Analytics Framework

Precondition: ADAE is provisioned with Data Source Profiles (Table Data Source Profile) for Data Sources in the Vertical Application Layer, Service Enablement Layer (e.g., SEAL Server/Client, EES/EEC, CAPIF entities), Core Network (e.g., OAM, DCCF, NWDAF), etc.

Alternatively, ADAE may perform a discovery for the Data Source Profiles of Data Sources of interest.

1. ADAE determines data collection sources and processing operations based on the requirements in the data analytics request. For example, ADAE may determine whether data should be collected from the application layer, the service enablement layer, the core network, or whether a data processing task should be performed using data from multiple layers/sources.

2.ADAE may collect existing data that can meet or partially meet the requirements of the data analytics request from sources with the "Data source role" IE set as "repository" in the data source profile (e.g., SEALDD storage server, Application-ADRF).

NOTE 1: ADAE Data Collection Requests/Responses may be realized via Subscriptions/Notifications.

3. ADAE collects data from other identified data sources. The request and response for data collection from a data source are defined in 6.3.1.3-4 and 6.3.1.3-5.

4. ADAE performs data processing operations as determined in step 1 and/or required by policies. For example, data samples that target the same performance metrics but originate from different sources may be normalized and validated. Such processing may remove samples that are inconsistent across different sources and keep samples that achieve consensus across all sources.

5. The collected (and optionally processed) data can be optionally stored in available repositories, such as a SEALDD storage server, Application-ADRF, etc.

The Data Source Profile includes Information about the Data Generation/Production Capability of the Data Source to support Data Collection for Data Analytics Service and the Availability/Accessibility of the Generated/Produced Data, as defined in Table 6.3.1.3-1.

Table : Data source profile

Information element	Status	Description
Source ID	M	ID of the source
Data source entity	M	Specifies the type of the entity, such as a vertical application server, a SEAL server/client, EES/EEC, EAS, etc.(NOTE 1)
Information type	M	Type of information can be provided by the data source, e.g., performance indicators, resource usage data, server load data, etc. The information types may also include those obtained from NWDAF or OAM events, or from service layer original sources such as application performance (solution #1), edge load (solution #3), (NOTE 2)
Data generation schedule	O	The schedule of data generation, e.g. when the data source is active to produce data.
Data source role	O	Role of the data source, e.g., original source, repository, logging server, etc.
Original source	O	If the data source role is not "original source, specifies the original data source of the data provided by this data source.
Data freshness	O	If the data source role is not "original source, length of time elapsed after the data is generated until is available at the data source. Alternatively, the data collection rate supported by the source is provided
Data storage capability	O	Indicates data storage capabilities, e.g. how long the data can be stored.
Anonymization capability	O	Indicates whether the data available at this data source can be anonymized before collection.
Pre-processing capabilities	O	Indicates capabilities of the data source to provide pre-processing functionality, such as aggregation, validation, etc.
Original source communication constraints	O	Constraints of the original source such as geographic constraints, access technology associated with the original data source, etc.
NOTE 1: The list of possible choices may be determined in the specification phase, based on ADAES capabilities to interact with other service layer entities NOTE 2: The values available for "information type" may be determined in the specification phase.		

Key Issue #1: Support for Application Performance Analytics

Key Issue #2: Support for Edge Analytics Enablement

Key Issue #3: Support for Data Collection for Application Layer Analytics

Key Issue #4: Key Issue on Interactions with SEAL Services

Key issue #5: Support for Slice-related Application Data Analytics

Key issue #6: Support for Slice Configuration Recommendation Enablement

Key issue #7: Support for Location Accuracy Analytics

Key issue #8: Support for Service API Capability Analytics

Table Mapping of solutions to key issues

	KI #1	KI #2	KI #3	KI #4	KI #5	KI #6	KI #7	KI #8
Sol #1	X							
Sol #2	X	X	X	X				
Sol #3		X						
Sol #4	X							
Sol #5	X							
Sol #6					X			
Sol #7						X		
Sol #8							X	
Sol #9								X

5G System Architecture with Service-based UPF enhancements and ADAES (Application Data Analytics Enablement Services)

The enhancements foresee UPF Event Exposure Framework Service(s) Registration/De-registration, & discovery via the 5G CN with support e. g. for Consumption of UPF Exposure Services by the 5G CN nodes, Trusted AF & other NFs (if needed) through the SBI (Service-based Interface) **Nupf,** introduced in the 5GS Architecture. The UPF is in the role of "Consumer" of 5G CN Services as UPF can register its NF Profile in NRF with related **Nupf** Service Information, but does not describe Services provided by the UPF itself. The existing UPF NF Profile parameters include e.g. S-NSSAI(s) & the associated NSI ID(s), DNN(s), IP range, Information about the Location of the UPF (Operator specific Information, e.g. Geographical Location, Data Centre), UPF Service Area (TAI List), DNAI. Besides, to support UPF Event Exposure Service, also Event Exposure Service Name, Supported Event ID(s) are provided with the UPF NF profile. SBI UPF Event Exposure Framework provides events related to PDU Sessions towards "Consumer" NF, allowing other NFs to subscribe & get notified of events happening on UPFs, as e.g. allow the NWDAF to collect Data indirectly for Network Data Analytics, QoS flow Bit Rate, Traffic Usage Report as e.g. UL/DL Data Rate (3GPP or WLAN Access).

The enhancements related to **ADAES** in 5G (together with 3GPP introduced Data Analytics Function, **NWDAF,** to support Network Data Analytics Services in 5G CN & Management Data Analytics Service, **MDAS**, to provide Data Analytics at the OAM), **ADAES** aims to optimize the Application Service Operation, ***Edge/Cloud Analytics Enablement,*** Data Collection aspects per identified Application Data Analytics Service, Coordination of Data Collection from multiple sources & **unified exposure of Data Analytics to the Vertical/ASP,** defining, at an overarching layer, **Value-add Application Data Analytics Services, which cover Stats/Predictions for the End-to-End (E2E) Application Services.**

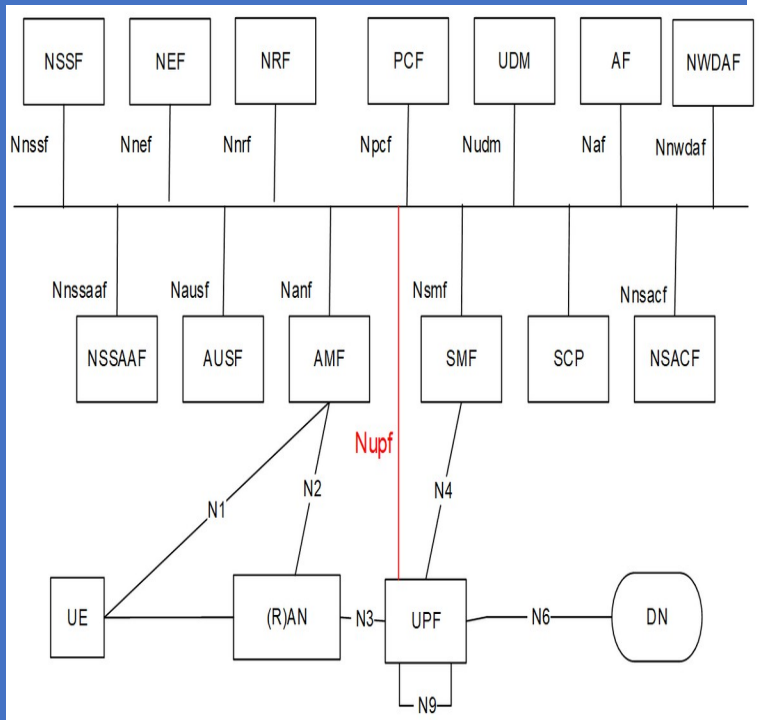


Fig.: 5G System Architecture with Service-based UPF

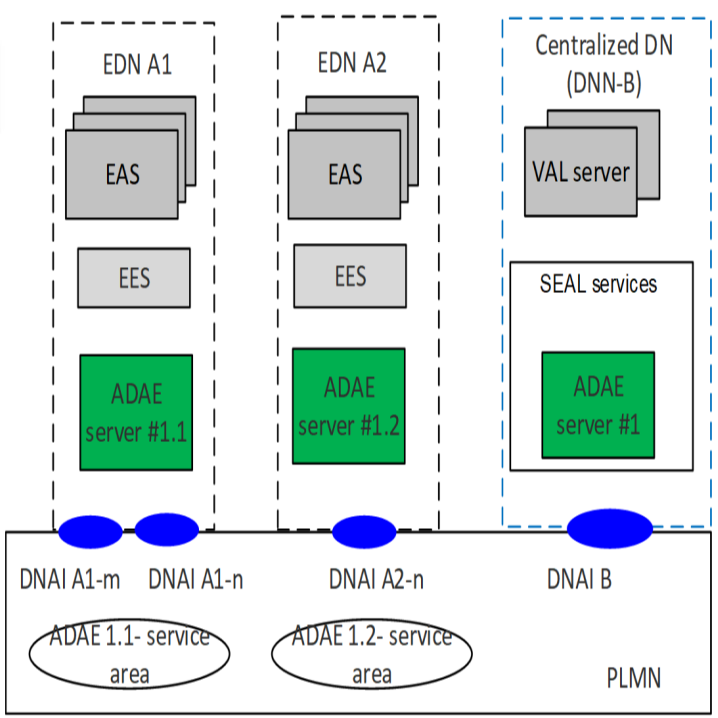


Fig.: 5G System Hierarchical (Cloud/Central and Edge/Local) deployment of ADAES

Table: 5G ADAE Services

Analytics Event	Inputs	Data Collection Sources	Analytics Outputs	Type of analytics
VAL server performance analytics	per VAL server performance measurements, historical data/stats for VAL server performance, network / KPI monitoring from 5GS	1. VAL UE 2. VAL Server 3. OAM 4. 5GC (NWDAF, NEF)	Analytics on application QoS metrics per VAL server	Prediction, statistics
VAL UE/session performance analytics	per VAL session performance measurements	1. VAL UE 2. VAL Server	Analytics on application QoS metrics per VAL session	Prediction
VAL UE-to-UE session performance analytics	per UE-to-UE session performance measurements	1. VAL UEs	Analytics on application QoS metric change for UE-to-UE session	Prediction
edge load analytics	edge platform load data, EAS/EES load data, DN performance analytics, UPF load analytics	1. OAM / MDAS 2. 5GC / NWDAF 3. SEALDD server 4. EES 5. EAS 5. MEP / RNIS	1. stats / predictions on the EDN load conditions, 2. EES or EAS load stats/predictions, 3. recommendation for pro-active EAS relocation trigger	Prediction, statistics
Slice related performance analytics	per slice measurements and analytics, application session performance analytics, historical data on slice information	1. OAM or NSCE 2. 5GC / NWDAF 3. VAL UEs	Statistics / prediction for the VAL application QoS for one or more requested S-NSSAIs/NSIs	Prediction, statistics
Location accuracy analytics	UE mobility analytics, UE location reports and achieved accuracy, historical location accuracy statistics for target VAL service area or VAL UE	1. SEAL LMS / FLS 2. 5GC / NWDAF 3. A-ADRF	a predictive location accuracy sustainability or change indication	Prediction
Service API analytics	Service API logs for requested APIs, historical data / statistics on service API availability and service level	1. CCF 2. A-ADRF	stats / predictions for service API(s)	Prediction, statistics
Slice configuration recommendation	per slice measurements and analytics, historical data on slice information	1. SEAL NSCE 2. OAM 3. NWDAF 4. A-ADRF	Statistics for the network slice configuration recommendation for one or more requested S-NSSAIs	Statistics

5G NWDAF (Network Data Analytics Function) (with focus on **AnLF** (*Analytics Logical Function*) and **MTLF** (*Model Training Logical Function*)
The 5G Reference Architecture for Data Collection & Reporting envisages a set of high-level procedures by which Data is collected by a *Network Data Analytics Function* (**NWDAF**) from *UE Application(s)* via an intermediary *Application Function* (**AF**) (aka ***Data Collection AF).*** It is intended that this Reference architecture be **instantiated in Domain-specific ways to suit the needs of different features of the 5G System** (may be instantiated separately in **different Slices of a Network**)
The Services may be exposed to parties outside the Trusted Domain. The accuracy of Analytic output from an **NWDAF** depends very much on the accuracy of the ML Model provided by the **MTLF** (*Model Training Logical Function*) **NWDAF.** The T*raining Data* that are used to train an *ML Model* are usually *Historical Data* (**Data** stored in the **ADRF**). The *Validity/Accuracy* of the ML Model depends on whether the *Training Data* used are **up to date with the Real-Time Network Configuration/behaviour**. E.g. compared to when the Training Data were collected **the Network Operator may configure additional Network Resources to a Network Slice (SST), or the Number of Users accessing Services via the Core Network may considerably *increase*** *(e.g. Tourist season in the Summer). Such* ***UCs*** *may cause a* ***Model Drift*** *given that ML Model was not trained with up-to-date data. Hence, as shown in Fig.: below,* ***NWDAF Solution Capability*** allows the Network to determine when an ML Model requires re-training.

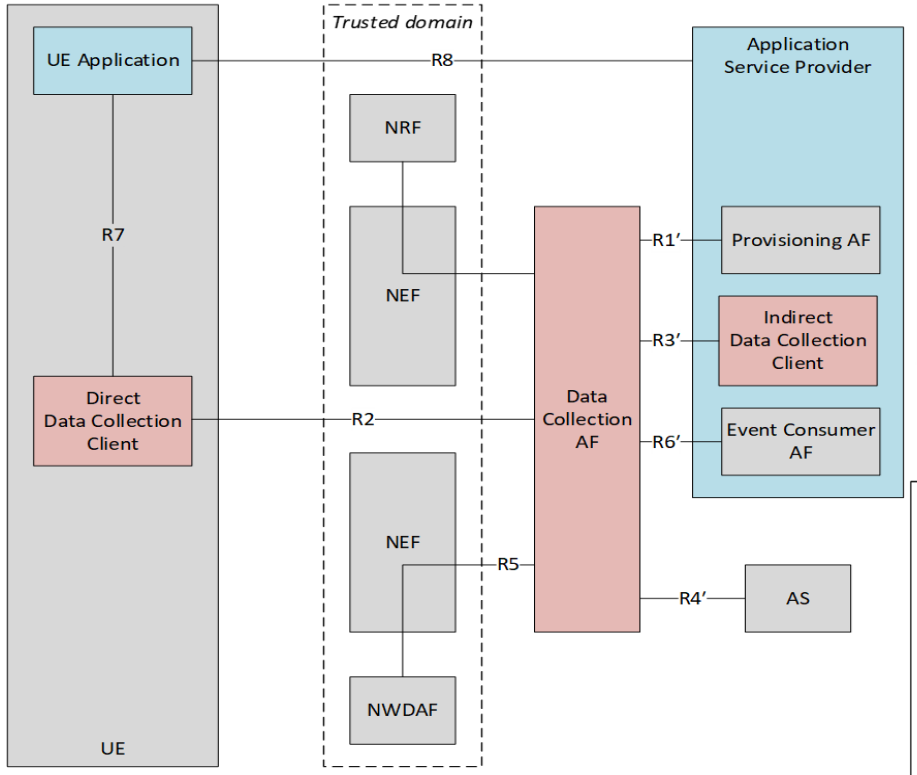


Fig.: 5G Reference Architecture for Data Collection and Reporting with Data Collection AF deployed outside the Trusted domain

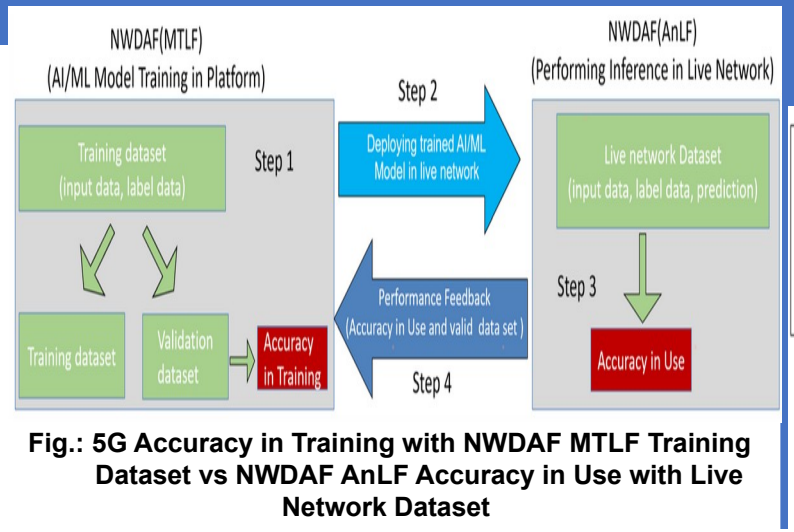


Fig.: 5G Accuracy in Training with NWDAF MTLF Training Dataset vs NWDAF AnLF Accuracy in Use with Live Network Dataset

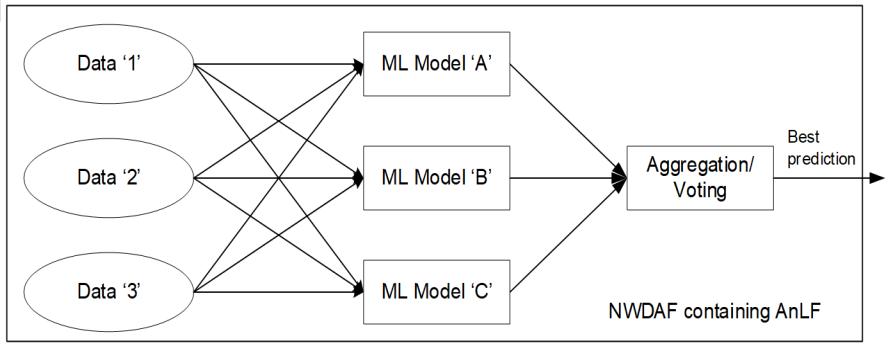


Fig.: 5G NWDAF containing AnLF Aggregation/Voting Choses the Best Prediction

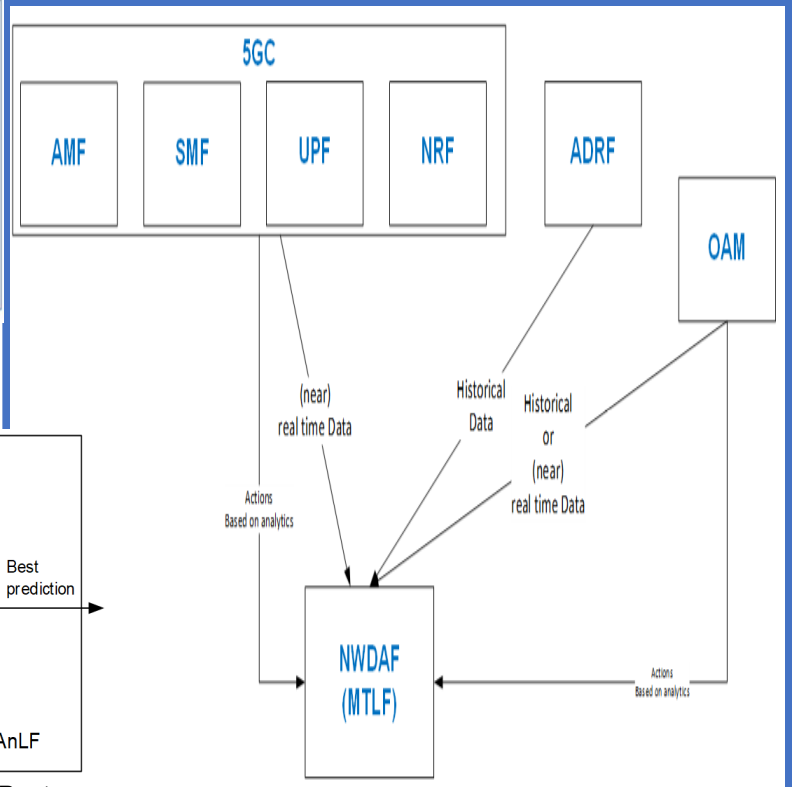


Fig.: 5G NWDAF MTLF Model drift detected

IoT-PCS SEAL

5G Application Capability for IoT Platforms

The Figure depicts the resulting deployment. Note that this deployment aligns with the distributed network exposure access model introduced by the solution in clause 5.2, while using the proposed IoT-PCS-specific instances of SEAL reference points.

The depicts a generic IoT Platform with IoT Platform Common Services (IoT-PCS) Servers enabling a Set of Applications deployed using corresponding servers (IoT-App), which may belong to different verticals.

On the Device side, corresponding IoT-PCS and IoT-App Clients enable the Client-side functionality.

For Inter-Service Communications, an IoT-App SEAL Server communicates with the IoT-PCS server over the SEAL-X3 Reference Point.

In this deployment, both SEAL Servers provide Network Exposure Access, resulting in a Distributed Network Exposure Access Deployment.

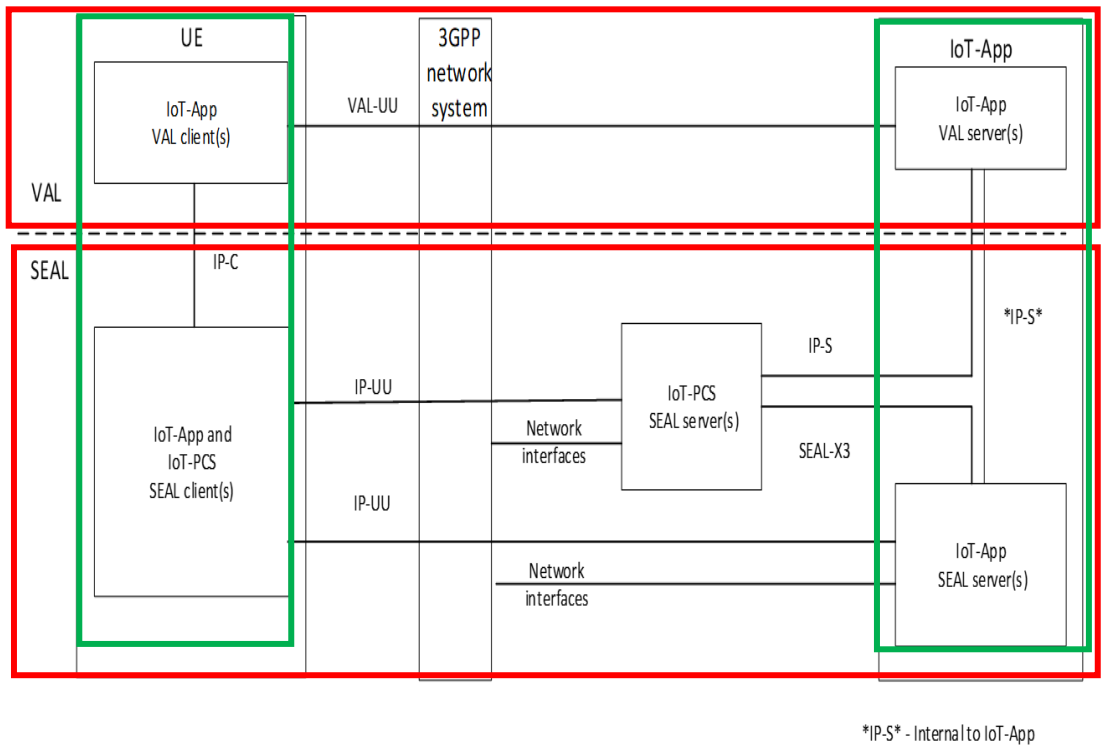


Figure: 5G Functional Model for IoT-PCS (Distributed Network Exposure Access)

5G SEAL Data Delivery (SEALDD) Enabler for Vertical Applications

Illustration of the Application Enabling Layer (AEL) Platform Architecture, Capabilities and Services to efficiently support

- Distribution,
- Storage and
- Delivery for the Application Content/Data for Vertical Applications.

It takes into consideration the Existing Stage 1 and Stage 2 work within 3GPP related to Data Delivery and 3GPP System User Plane aspects specified in 5G Service Requirements & Architectural enhancements for 5G Multicast-Broadcast Services

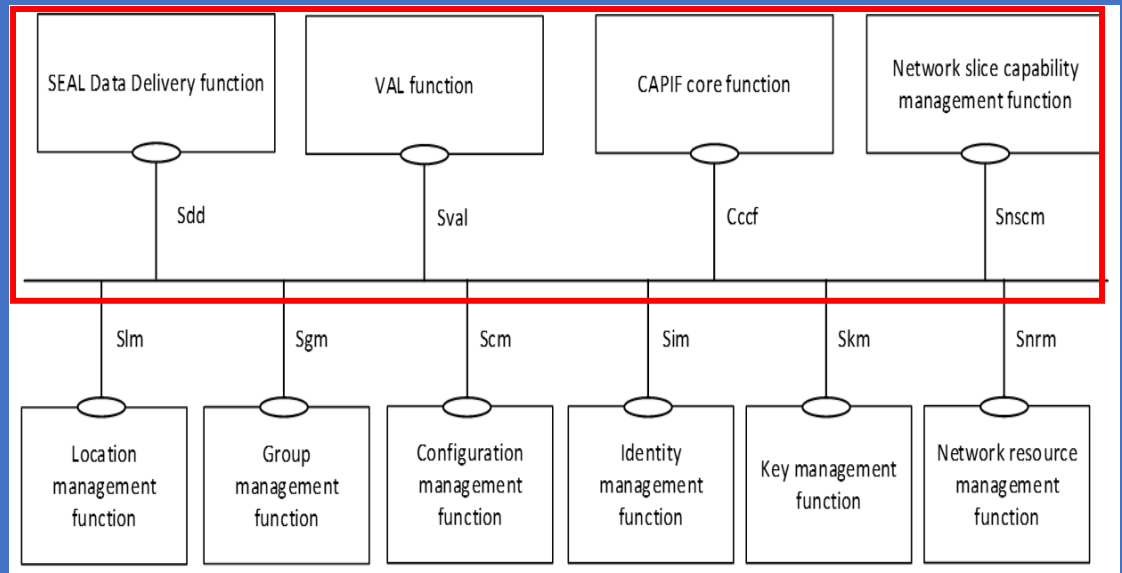


Figure: 5G SEALDD Representation in SEAL Generic Functional Model Representation using Service-based Interfaces

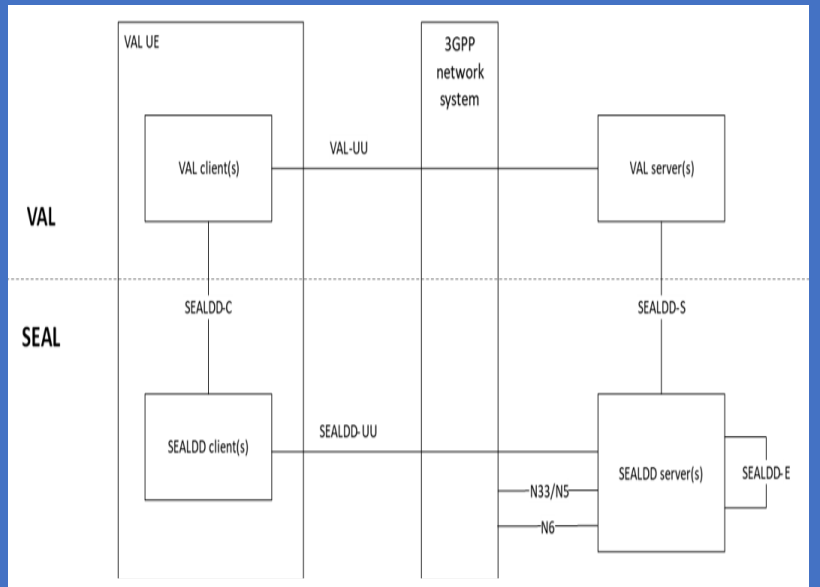


Figure: 5G Architecture for SEAL Data Delivery Service

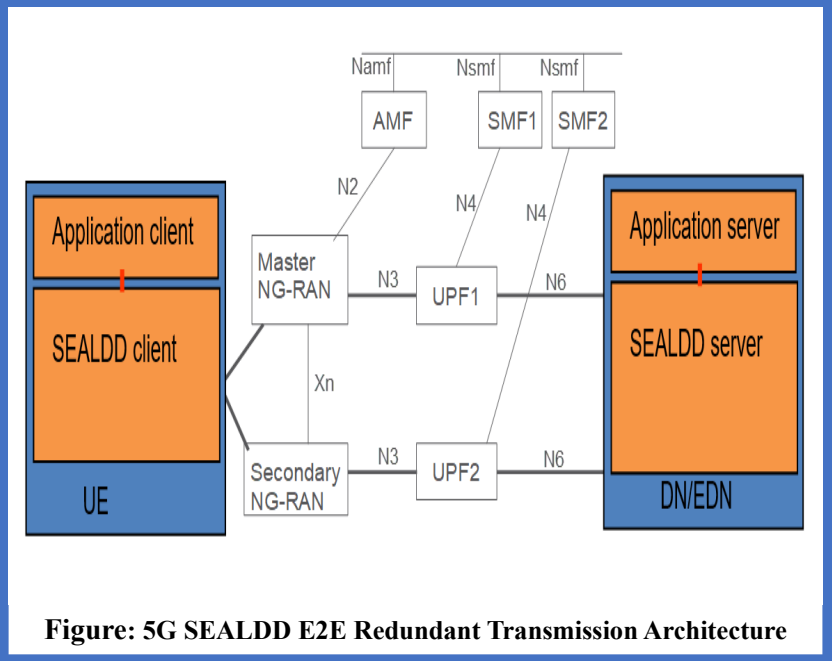


Figure: 5G SEALDD E2E Redundant Transmission Architecture

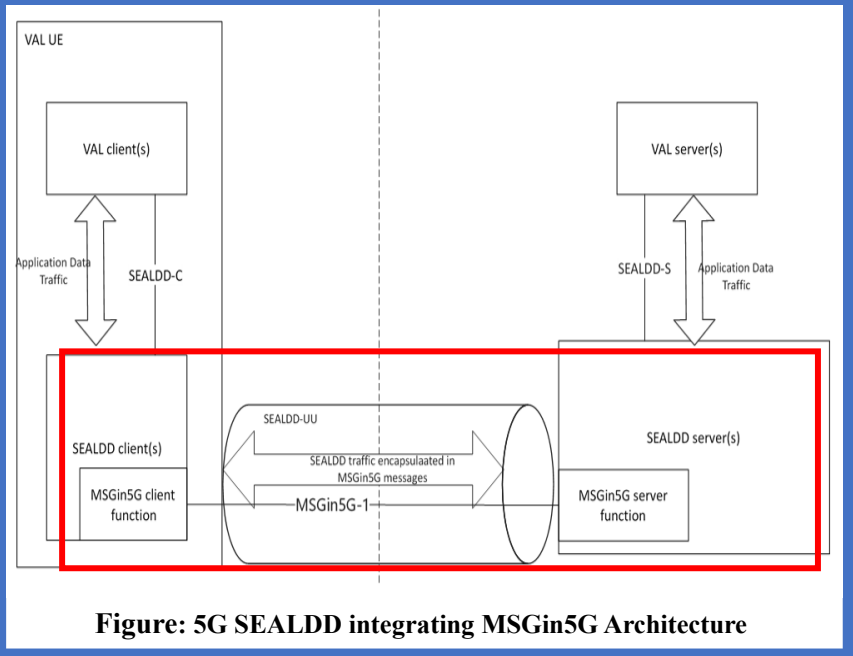


Figure: 5G SEALDD integrating MSGin5G Architecture

ADAE internal Architecture based on 3GPP Data Analytics Framework

Precondition: ADAE is provisioned with Data Source Profiles (Table Data Source Profile) for Data Sources in the Vertical Application Layer, Service Enablement Layer (e.g., SEAL Server/Client, EES/EEC, CAPIF entities), Core Network (e.g., OAM, DCCF, NWDAF), etc.

Alternatively, ADAE may perform a discovery for the Data Source Profiles of Data Sources of interest.

1. ADAE determines data collection sources and processing operations based on the requirements in the data analytics request. For example, ADAE may determine whether data should be collected from the application layer, the service enablement layer, the core network, or whether a data processing task should be performed using data from multiple layers/sources.

2.ADAE may collect existing data that can meet or partially meet the requirements of the data analytics request from sources with the "Data source role" IE set as "repository" in the data source profile (e.g., SEALDD storage server, Application-ADRF).

NOTE 1: ADAE Data Collection Requests/Responses may be realized via Subscriptions/Notifications.

3. ADAE collects data from other identified data sources. The request and response for data collection from a data source are defined in 6.3.1.3-4 and 6.3.1.3-5.

4. ADAE performs data processing operations as determined in step 1 and/or required by policies. For example, data samples that target the same performance metrics but originate from different sources may be normalized and validated. Such processing may remove samples that are inconsistent across different sources and keep samples that achieve consensus across all sources.

5. The collected (and optionally processed) data can be optionally stored in available repositories, such as a SEALDD storage server, Application-ADRF, etc.

The Data Source Profile includes Information about the Data Generation/Production Capability of the Data Source to support Data Collection for Data Analytics Service and the Availability/Accessibility of the Generated/Produced Data, as defined in Table 6.3.1.3-1.

Table : Data source profile

Information element	Status	Description
Source ID	M	ID of the source
Data source entity	M	Specifies the type of the entity, such as a vertical application server, a SEAL server/client, EES/EEC, EAS, etc.(NOTE 1)
Information type	M	Type of information can be provided by the data source, e.g., performance indicators, resource usage data, server load data, etc. The information types may also include those obtained from NWDAF or OAM events, or from service layer original sources such as application performance (solution #1), edge load (solution #3), (NOTE 2)
Data generation schedule	O	The schedule of data generation, e.g. when the data source is active to produce data.
Data source role	O	Role of the data source, e.g., original source, repository, logging server, etc.
Original source	O	If the data source role is not "original source, specifies the original data source of the data provided by this data source.
Data freshness	O	If the data source role is not "original source, length of time elapsed after the data is generated until is available at the data source. Alternatively, the data collection rate supported by the source is provided
Data storage capability	O	Indicates data storage capabilities, e.g. how long the data can be stored.
Anonymization capability	O	Indicates whether the data available at this data source can be anonymized before collection.
Pre-processing capabilities	O	Indicates capabilities of the data source to provide pre-processing functionality, such as aggregation, validation, etc.
Original source communication constraints	O	Constraints of the original source such as geographic constraints, access technology associated with the original data source, etc.
NOTE 1: The list of possible choices may be determined in the specification phase, based on ADAES capabilities to interact with other service layer entities NOTE 2: The values available for "information type" may be determined in the specification phase.		

1. 5G MSGin5G SBI Service based Interface representation for MSGin5G Service

The MSGin5G, as shown in the figure, is the Service based Architecture for MSGin5G Service.

The M5C Function is the MSGin5G Client.

The AC is the Application Client.

The L3G Function is a Service based function exhibited by Legacy 3GPP Message Gateway.
The N3G function is a Service based Function exhibited by Non-3GPP Message Gateway.

The M5S manages the Distribution of the Messages it has received from MSGin5G UE, from Application Server, or from N3G (on behalf of Non-3GPP UE) or from L3G (on behalf of Legacy 3GPP UE).

The M5S invokes Services provided by L3G/N3G to send MSGin5G Messages towards Legacy 3GPP UE or Non-3GPP UE.

The AS/L3G/N3G invokes Services provided by M5S to send MSGin5G Messages to M5S on behalf of Legacy 3GPP UE or Non-3GPP UE.

The M5S invokes Services provided by SEAL Group Management Function to do MSGin5G Group Management.

The M5S/L3G/N3G invokes Services provided by SEAL Configuration Management Function to do Service Configuration (including UE Service ID Provisioning).

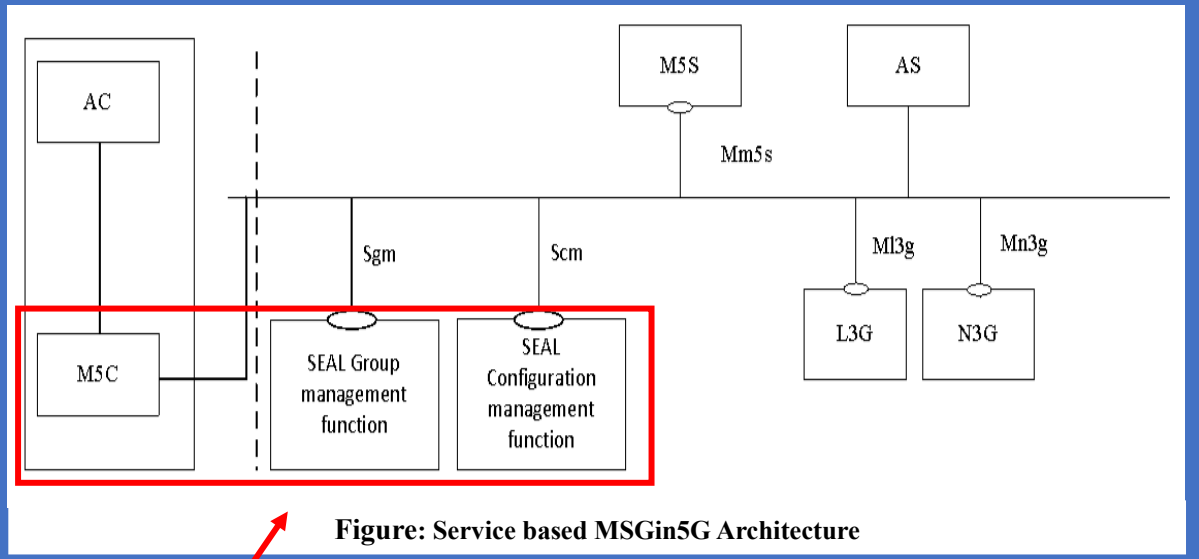


Figure: Service based MSGin5G Architecture

Table: Service based Interfaces supported by MSGin5G Service

Service based interface	Application function entity	Mapping server entity	APIs offered
Mm5s	MSGin5G Server function	MSGin5G Server	Specified in 9.1
MI3g	Legacy 3GPP Message Gateway function	Legacy 3GPP Message Gateway	Specified in 9.2.1
Mn3g	Non-3GPP Message Gateway function	Non-3GPP Message Gateway	Specified in 9.2.2

The MSGin5G Service is designed and optimized for massive IoT Device Communication including Thing-to-Thing (T2T) Communication and Person-to-Thing (P2T) communication.

The MSGin5G Service is a Message Enabler for applications.

An Application Client in a UE utilizes MSGin5G Service to send a message to another UE, to multiple UEs or to the Application Server, or the Application Server utilizes the MSGin5G Service to send a message to a UE or to multiple UEs. All messages will be routed via the MSGin5G Server in the 5G system. The MSGin5G Service flow is shown in figure 7.1-1.
If the UE supports a legacy 3GPP message service (e.g. SMS, NIDD, or CB) and does not support the MSGin5G Service (i.e. UE has no MSGin5G Client), the message will be translated to the appropriate message delivery mechanism by the Legacy 3GPP Message Gateway. A UE that does not support any 3GPP message service can connect to the MSGin5G Service via Non-3GPP Message Gateway that facilitates the translation between the MSGin5G Service and non-3GPP message delivery mechanism. The connection between such UE and the gateway can be via 3GPP access or non 3GPP access (e.g. WLAN) and is out of scope of the present specification.
An Application Server resides outside the 3GPP domain and connects to the MSGin5G Server via a CAPIF-aware reference point.
The message communication models include:

- Point-to-Point messaging: message that is originated at a UE (UE A) and terminated at another UE (UE B, a Legacy 3GPP UE or a Non-3GPP UE).

- Application-to-Point Messaging: message that is originated at an Application Sever and terminated at a UE.
- Point-to-Application messaging: message that is originated at a UE and terminated at an Application Sever
- Group Messaging: message that is originated at a UE or an Application Server and is terminated at a group of UEs (a group member can be of type UE A, Legacy 3GPP UE or Non-3GPP UE).

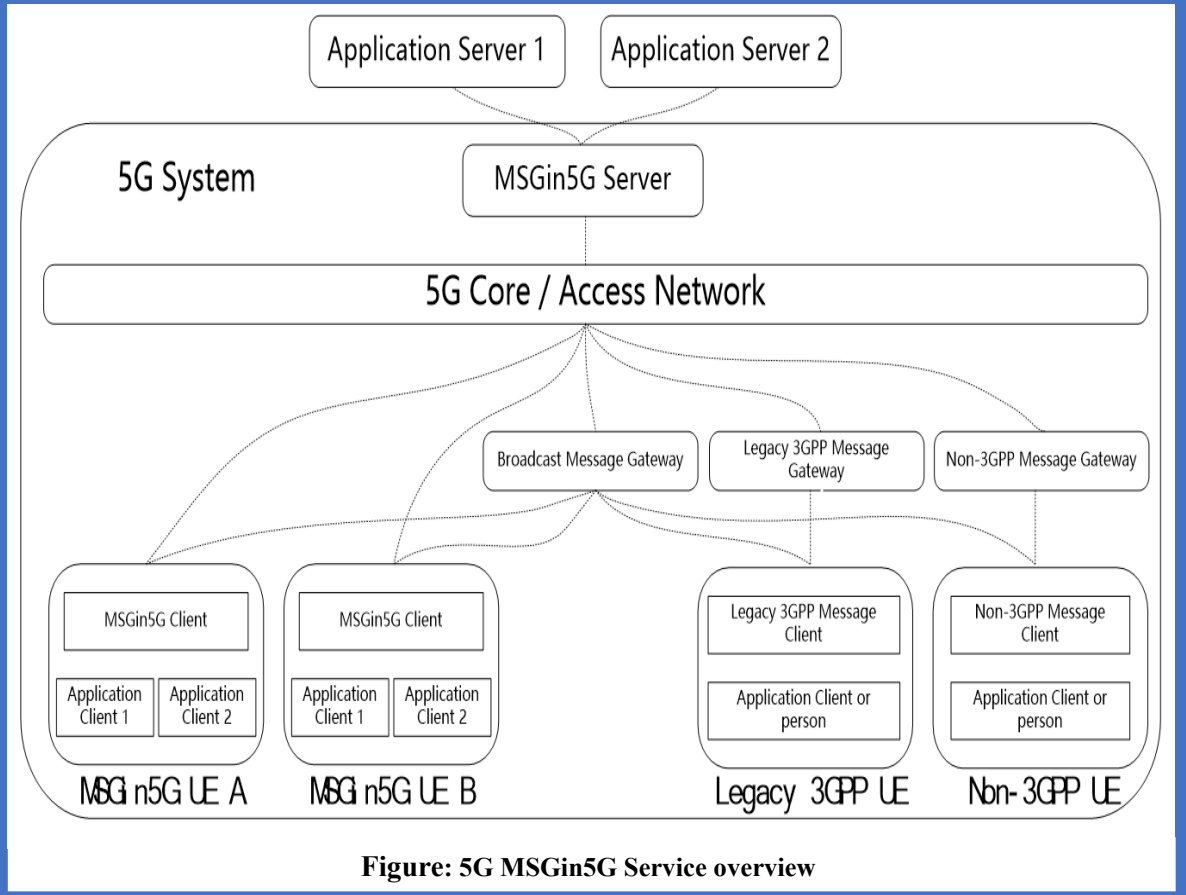


Figure: 5G MSGin5G Service overview

3GPP 5G MSGin5G Application Architecture, Rel. 18, June 2022

5G SEAL Data Delivery (SEALDD) Enabler for Vertical Applications

Solution #8: SEALDD Server Discovery and Selection in EDN (Edge Data Network)

The following solution corresponds to the key issue #6 on SEALDD coordination with EEL (Edge Enabling Layer).

There can be scenarios of how SEALDD service is used:

- Scenario (a): SEALDD Service is used for both Signaling & Data Traffic Transfer.

- Scenario (b): SEALDD Service is used only for Data Traffic Transfer.

NOTE: For the same VAL application, VAL servers for Scenario (a) and Scenario (b) and VAL servers without SEALDD service may coexist in the same EDN. The three types of servers may use different EAS IDs or other information (e.g. EAS service, additional associated SEALDD server information) to differentiate each other for EAS discovery.
After VAL server subscribes SEALDD service from the SEALDD server, the VAL server registers associated SEALDD server information to EES. In EAS discovery procedure, EEC can get the associated SEALDD server(s) information of the desired the VAL server(s). Then SEALDD client can use the SEALDD server information to establish the data delivery connection for the VAL client (AC) and VAL server (EAS).

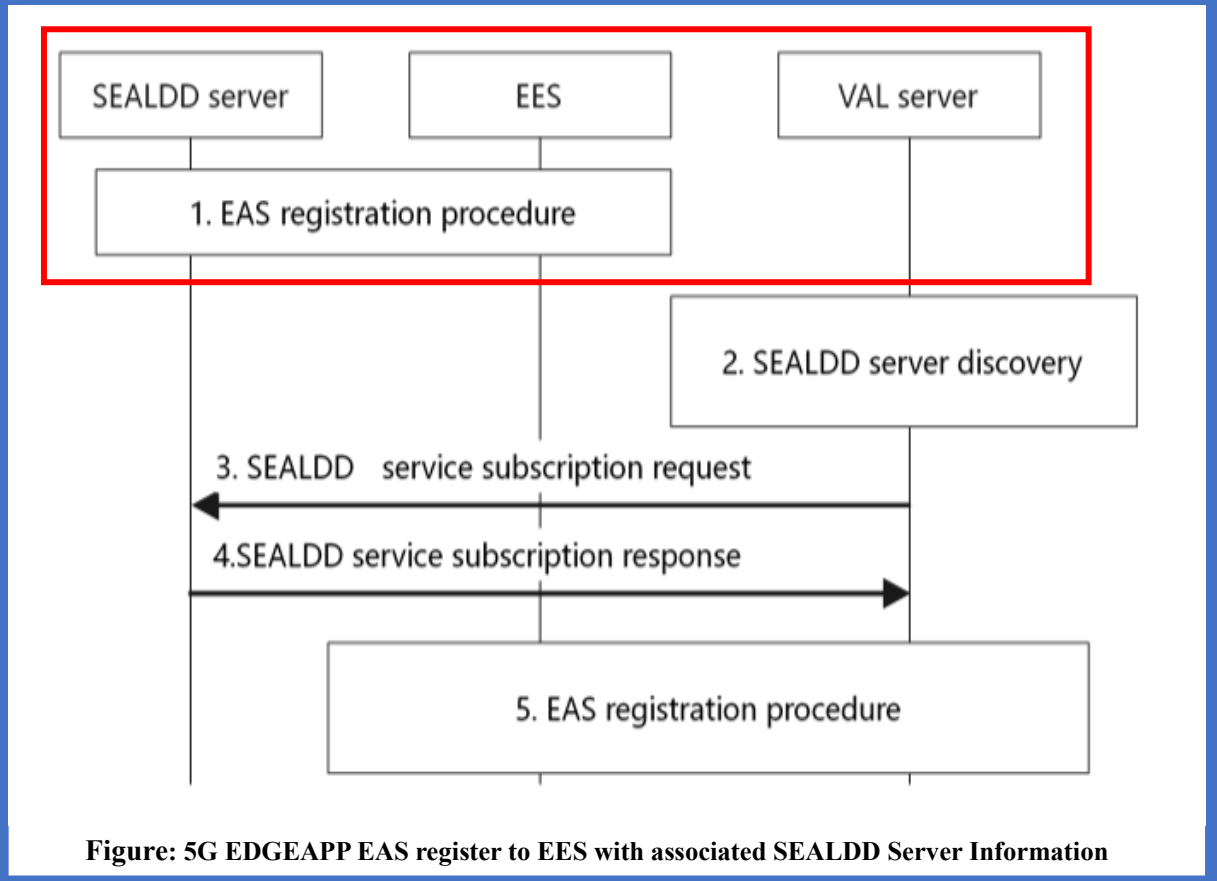


Figure: 5G EDGEAPP EAS register to EES with associated SEALDD Server Information

3GPP RAN & O-RAN

Stand-alone (SA) - NR-U (NR-Unlicensed)

connected to 5GC.

This Scenario targets NPN

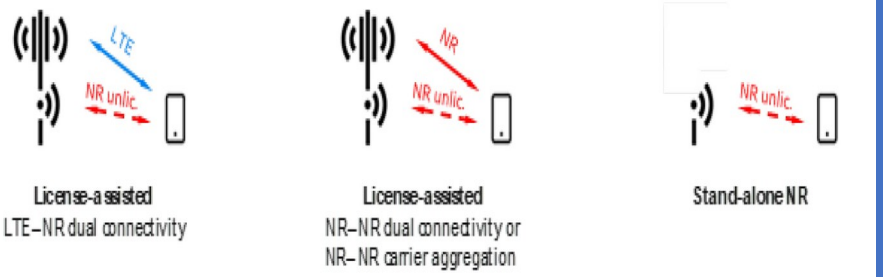


Fig. 3.10. License-assisted (left and middle) and stand-alone (right) operation of NR in unlicensed spectra.

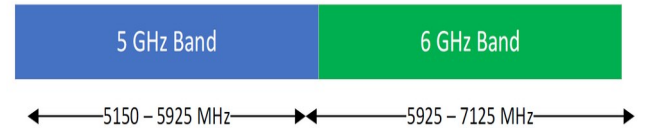


Fig. 3.9. Spectrum priorities for NR-U.

In 3GPP Rel. 16, NR was extended to support operation also in Un-licensed Spectra, with focus on the 5 GHz (5150-5925 GHz) & 6 GHz (5925 – 7150 GHz) bands (Figure 3.9).

- In contrast to LTE, which only supports License-Assisted-Access (LAA) operation in Un-licensed Spectrum,
- NR supports both LAA & Stand-alone (SA) Un-licensed Operation, see Figure 3.10.

In the case of LAA, a NR carrier in unlicensed spectrum is always operating jointly with a carrier in licensed spectrum, with the carrier in licensed spectrum used for initial access and mobility.

- The licensed carrier can be an NR carrier, but it can also be an LTE carrier. Dual connectivity is used in case of the licensed carrier using LTE. If the licensed carrier is using NR, either dual connectivity or carrier aggregation can be used between the licensed and unlicensed carrier.

In case of SA operation, an NR carrier in Un-licensed spectrum operates without support of a licensed carrier.

Thus, initial access and mobility are handled entirely using unlicensed spectra.

- The 5 GHz band is used by existing Technologies such as Wi-Fi & LTE-based LAA and it was a requirement, for the design of NR-U, or NR in Un-licensed spectrum,

Ref. 5G Americas, 3GPP Rel 16 & 17, & Beyond, Jan 2021: 34

The frequency ranges in which NR can operate according to this version of the specification are identified as described in Table 5.1-1.

Table 5.1-1: Definition of frequency ranges

Frequency range designation	Corresponding frequency range
FR1	410 MHz – 7125 MHz
FR2	24250 MHz – 52600 MHz

NR is designed to operate in the FR2 operating bands defined in Table 5.2-1.

Table 5.2-1: NR operating bands in FR2

Operating Band	Uplink (UL) operating band BS receive UE transmit	Downlink (DL) operating band BS transmit UE receive	Duplex Mode
	F_{UL_low} – F_{UL_high}	F_{DL_low} – F_{DL_high}	
n257	26500 MHz – 29500 MHz	26500 MHz – 29500 MHz	TDD
n258	24250 MHz – 27500 MHz	24250 MHz – 27500 MHz	TDD
n259	39500 MHz – 43500 MHz	39500 MHz – 43500 MHz	TDD
n260	37000 MHz – 40000 MHz	37000 MHz – 40000 MHz	TDD
n261	27500 MHz – 28350 MHz	27500 MHz – 28350 MHz	TDD
n262	47200 MHz – 48200 MHz	47200 MHz – 48200 MHz	TDD

Supplementary UL & DL (SUL & SDL)

To improve UL coverage for high frequency scenarios, SUL can be configured. With SUL, the UE is configured with 2 ULs for one (1) DL of the same cell as depicted on Figure B.1-1 below:

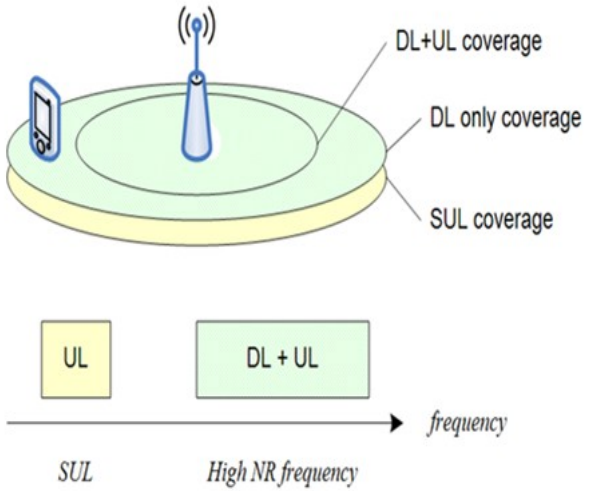


Figure B.1-1: Example of Supplementary Uplink

In case of FDD System, UL frequency is different from DL frequency. Thus, when Radio Resource restriction scenario is discussed, care should be taken by considering these variations e.g. Frequency used for both DL/ UL, UL only or DL only.

5G System introduces further flexibility in using Frequency Band, e.g. SUL (Supplementary UL) & SDL (Supplementary DL) can be used to replace the base frequency band, If the SUL &/or SDL band is restricted for a certain Network Slice (SST), some UEs may experience reduced coverage for the Network Slice.

Aspects related to carrier aggregation also needs to be considered similarly, because it is used to support QoS requirement by using different combination of DL bands & UL bands, e.g. using three DL bands together with one UL bands to boost downlink data rate.

3GPP RAN and O-RAN Alliance

O-RAN.WG1.Slicing-Architecture-v06.00

Technical Specification

O-RAN Working Group 1
Slicing Architecture

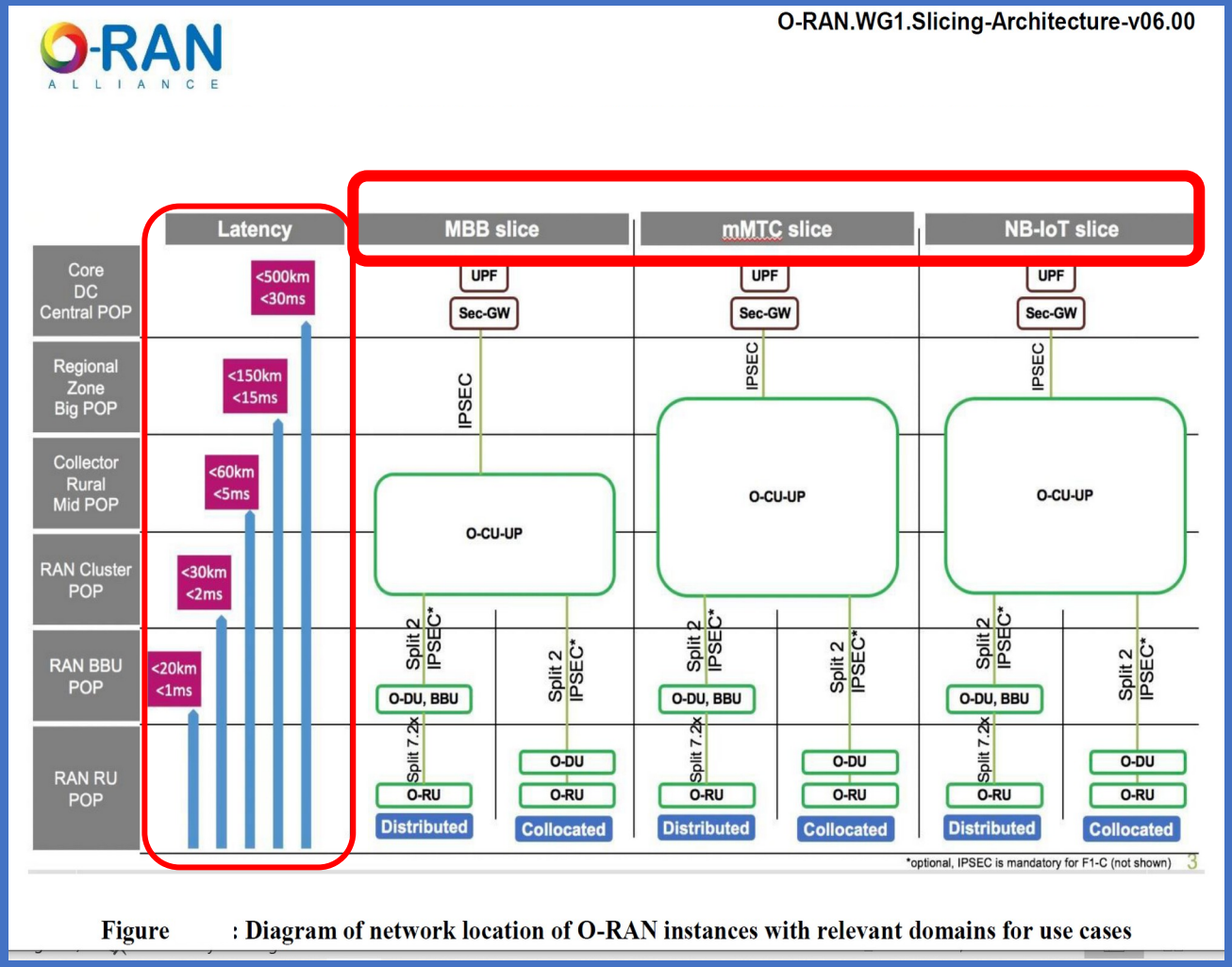


Figure : Diagram of network location of O-RAN instances with relevant domains for use cases

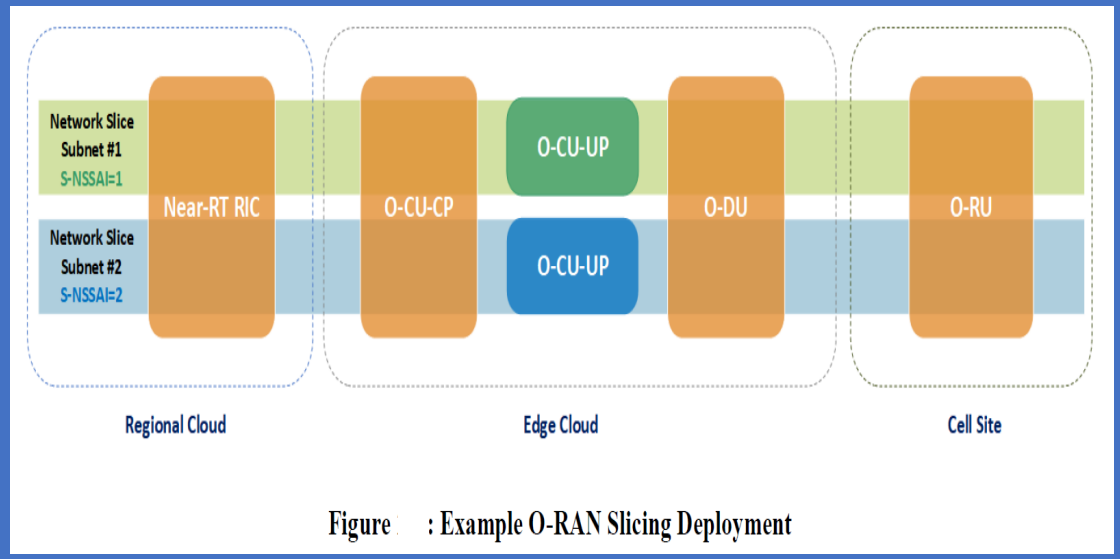


Figure : Example O-RAN Slicing Deployment

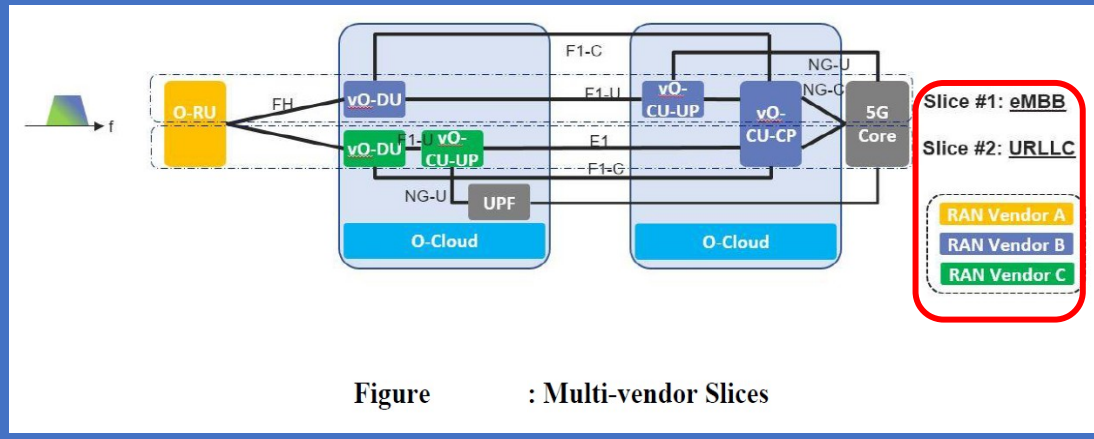


Figure : Multi-vendor Slices

3GPP RAN and O-RAN Alliance

O-RAN.WG1.Slicing-Architecture-v06.00

3) Flat mapping of standards based 5QI (Table 5.7.4-1 of 3GPP TS 23.501) <> DSCP <> QoS in TN domain

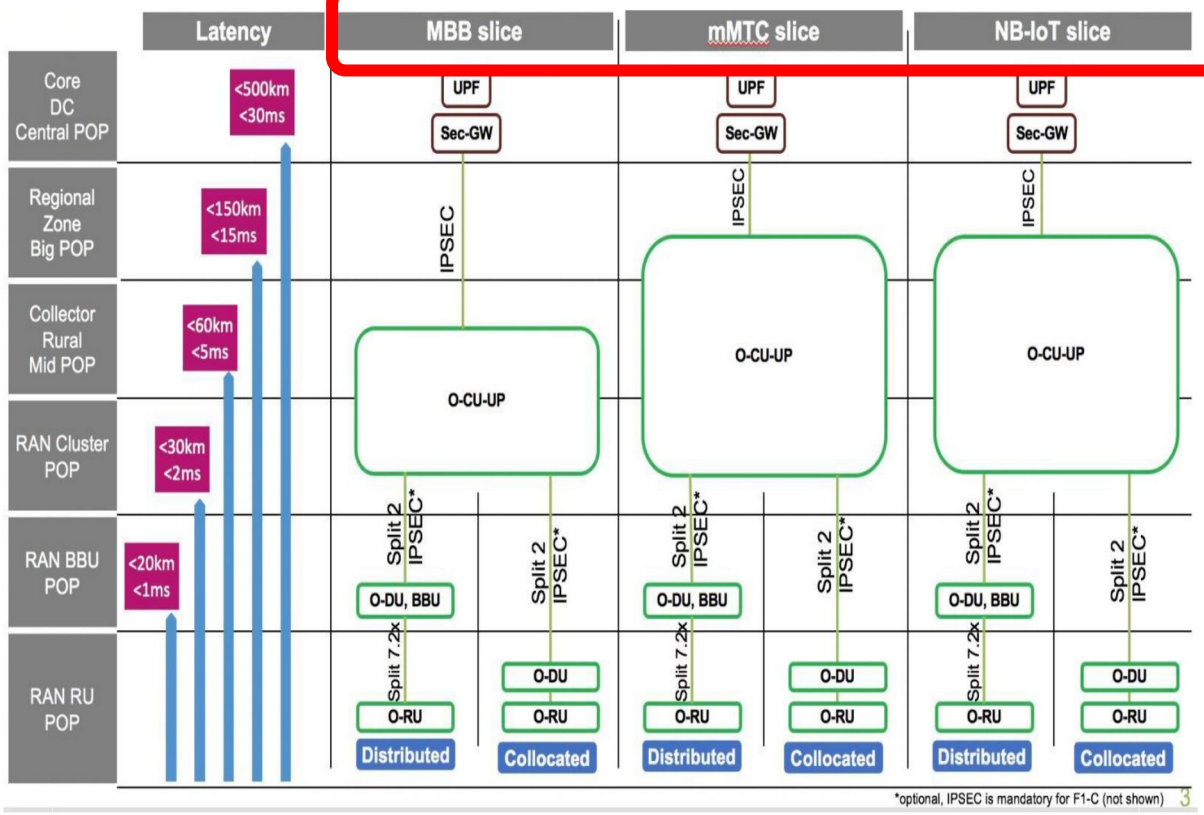


Figure B.1-5: Diagram of network location of O-RAN instances with relevant domains for use cases

O-RAN.WG1.Slicing-Architecture-v06.00

Chapter 2. Slicing Overview

Network Slicing is expected to play a critical role in 5G networks because of various use cases and services 5G will support. It allows a network operator to provide services tailored to customers' requirements. Network slice is defined as a logical network with a bundle of specified network services over a common network infrastructure. A single physical network is sliced into multiple virtual networks that can support different service types over a single RAN. 3GPP has standardized 4 different service types: eMBB, URLLC, MIoT and V2X [3].

3GPP defined 5G architecture and procedures containing network slicing and related concepts in Release 15. Furthermore, management and orchestration of 5G networks featuring slicing was defined in the 3GPP specifications. Other standard groups e.g. GSMA, ETSI NFV-MANO, ETSI ZSM and ONAP focus on the different aspects of network slicing. Further information regarding network slicing and other SDO's contributions was discussed in the Study on O-RAN Slicing Technical Report [24].

A sample RAN slicing deployment of O-RAN network functions based on the select initial deployment option, option B as described in [20], is shown in Figure 2-1, with some of the network functions shared between RAN slice subnets (such as O-CU-CP, O-DU, O-RU) and some network functions dedicated to a particular RAN slice subnet (such as O-CU-UP).

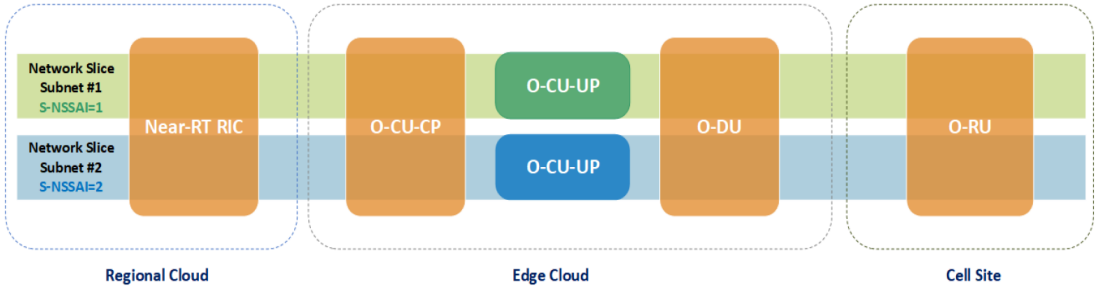


Figure 2-1: Example O-RAN Slicing Deployment

Table 5.15.2.2-1: 5G Standardized Slice/Service Type (SST) Values

Slice/Service type	SST value	Characteristics
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband.
URLLC	2	Slice suitable for the handling of ultra- reliable low latency communications.
MIoT	3	Slice suitable for the handling of massive IoT.
V2X	4	Slice suitable for the handling of V2X services.
HMTC	5	Slice suitable for the handling of High-Performance Machine-Type Communications.

Attribute		Value
Availability		99.999
Device Velocity		0
UE density (per km^2)		1000
Mission critical support		Mission critical
	Mission-critical capability support	Inter-user prioritization
	Mission-critical service support	MCData
Slice quality of service	3GPP 5QI	83

Table 72 List of attributes needed for NEST for HMTC SST

Attribute		Value
Availability		99,9
Slice quality of service	3GPP 5QI	9
Supported device velocity		2
UE density		100000

Table 71 List of attributes needed for NEST for MIoT SST

3GPP RAN and O-RAN Alliance

Table : O-RAN Slice Subnet Instance Creation Use Case

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	Creation of a new O-RAN network slice subnet instance (O-NSSI) or use an existing O-NSSI to satisfy the RAN slice subnet related requirements (see clause 5.1.2 in TS 28.531 [6]).	
Actors and Roles	NSSMS_C such as NSMF, who acts as an example network slice subnet management service consumer. NSSMS_P such as NSSMF, who acts as an example of network slice subnet management service provider. NFMS_P such as SMO OAM Functions or NFMF who acts as an example of network function management service provider. O-Cloud M&O, who acts as O-Cloud management and orchestration provider within SMO. Non-RT RIC O-RAN Network Functions: NFs such as Near-RT RIC, O-CU-CP, O-CU-UP, O-DU and O-RU.	
Assumptions	NSSMS_P is aware of O-Cloud M&O to manage the lifecycle of VNFs and interconnection between the VNFs and PNFs.	
Pre conditions	VNF packages for virtualized O-RAN network functions to be included in the O-RAN slice subnet instance have been already on-boarded.	
Begins when	NSSMS_P receives request for a network slice subnet instance. The request contains network slice subnet related requirements.	
Step 1 (M)	NSSMS_P checks the feasibility of the request, based on the received network slice subnet related requirements.	O-RAN Slice Subnet Feasibility Check
Step 2 (M)	NSSMS_P decides to create a new O-NSSI or use an existing O-NSSI.	
Step 3 (M)	If an existing O-NSSI is decided to be used, NSSMS_P may trigger modification of the existing O-NSSI to satisfy the network slice subnet related requirements. Go to "Step 11". Otherwise, NSSMS_P triggers creation of a new O-NSSI, continue with Step 4	O-RAN Slice Subnet Instance Modification Use Case
Step 4 (M)	NSSMS_P derives the requirements for the constituent NSSI(s).	
Step 5 (O)	If the required O-NSSI contains constituent NSSI(s) managed by other NSSMS_P(s), NSSMS_P may trigger creation of respective constituent NSSI(s) through other NSSMS_P(s) which manages the constituent NSSI(s). In that case, NSSMS_P receives the constituent NSSI information from the other NSSMS_P(s) and associates the constituent NSSI(s) with the required O-NSSI.	(O-RAN) Slice Subnet Instance Creation Use Case (to create constituent (O-)NSSI(s) managed by other NSSMS_P(s))
Step 6 (M)	NSSMS_P determines the service related requirements and triggers a service request to O-Cloud M&O for instantiation of virtual O-RAN network functions and virtual links within the determined O-Cloud(s). Based on the service request, O-Cloud M&O performs corresponding NF instantiation procedures and virtual link establishment.	FFS in WG6
Step 7 (M)	NSSMS_P associates the service response received from O-Cloud M&O with the corresponding O-NSSI.	FFS in WG6
Step 8 (M)	NSSMS_P uses (O-RAN) NF provisioning service exposed by NFMS_P to configure (O-)NSSI constituents.	FFS in WG1
Step 9 (M)	NSSMS_P configures the O-NSSI MOI with each constituent (O-)NSSI MOI identifier.	FFS in WG1
Step 10 (M)	NSSMS_P triggers O-RAN TN Manager coordination procedure to establish necessary links such as for A1, E2, and midhaul and fronthaul connectivity.	FFS in WG9
Step 11 (M)	NSSMS_P notifies Non-RT RIC with network slice subnet requirements and respective O-NSSI information.	FFS in WG2
Step 12 (M)	NSSMS_P notifies NSSMS_C with the resulting status of this process and relevant O-NSSI information.	
Ends when	O-RAN O-NSSI and relevant O-RAN NFs are created, and Non-RT RIC is configured with slice requirements and O-NSSI information.	
Exceptions	One of the steps identified above fails.	
Post Conditions	O-NSSI is ready to satisfy the network slice subnet related requirements.	
Traceability	REQ-SL-FUN14, REQ-SL-FUN20 - REQ-SL-FUN27	

O-RAN ALLIANCE

O-RAN.WG1.Slicing-Architecture-v06.00

Technical Specification

O-RAN Working Group 1
Slicing Architecture

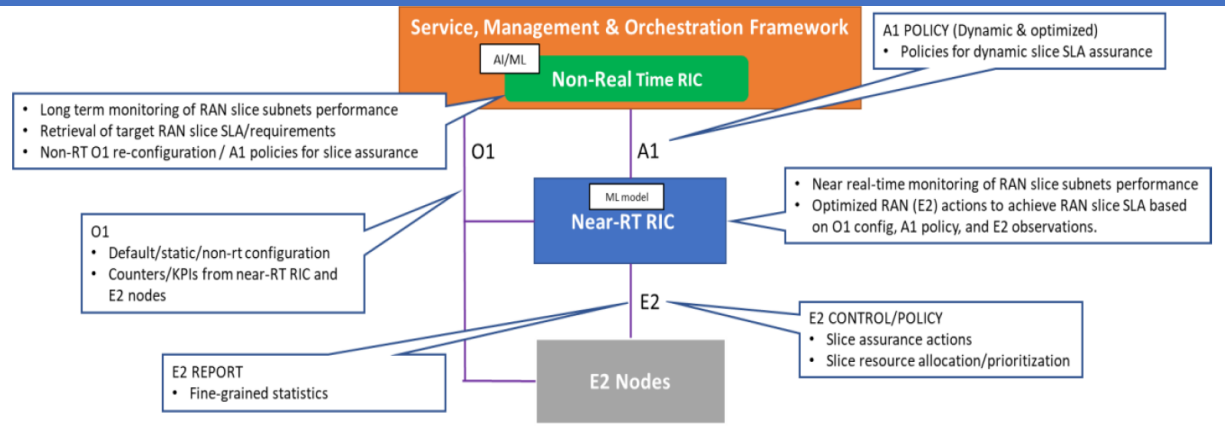


Figure : RAN Slice SLA Assurance use case overview

The more detailed functions provided by the entities for RAN slice SLA assurance are listed as below:

1) Non-RT RIC:
   a) Retrieve RAN slice SLA target from respective entities such as SMO, NSSMF
   b) Long term monitoring of RAN slice subnet performance measurements
   c) Training of potential ML models that will be deployed in Near-RT RIC for optimized slice assurance
   d) Support deployment and update of AI/ML models into Near-RT RIC
   e) Send A1 policies and enrichment information to Near-RT RIC to drive slice assurance

3GPP RAN and O-RAN Alliance

The Option 2 depicts the expectation of the target capabilities of the systems, including capabilities on the Option 1.

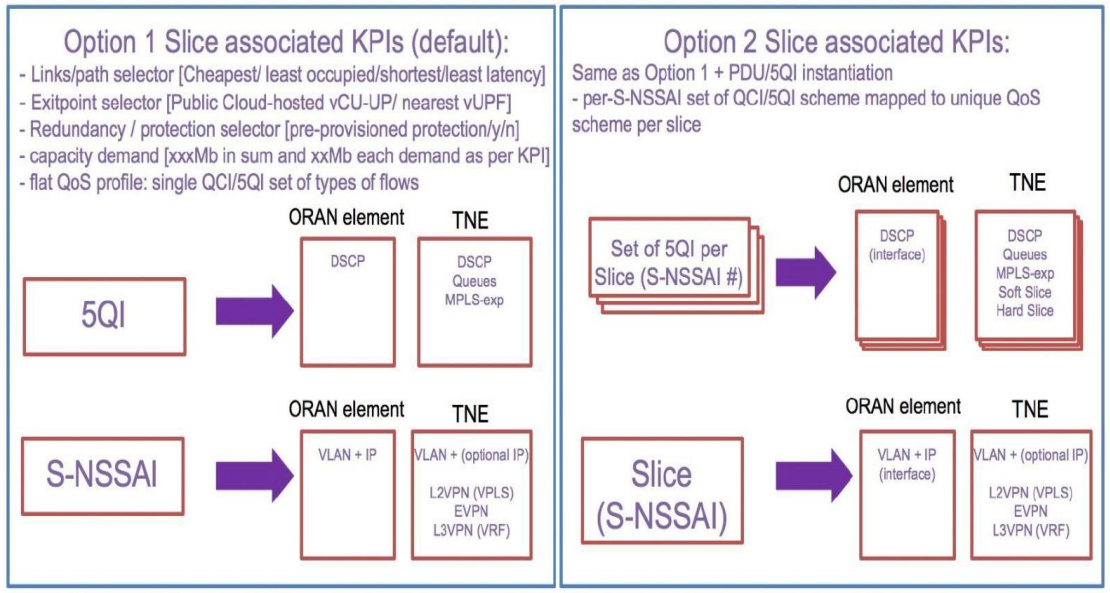


Figure : Options for slicing, demapping orthogonal plane of 5QI per slice in Option 1 and multiple planes of 5QI as attribute per planes of slices

For Phase 1 following constrains are assumed:

1) Single operator with one O-NSSI MBB, one O-NSSI mMTC, one O-NSSI NB-IoT slice
2) Fix mapping of slices inter to intra – DC

** 5QI QoS Identifiers, the Priority Level (if explicitly signaled), and other NG-RAN traffic parameters (e.g., ARP) in O-RAN and Core domains mapped to DSCP and ToS or CoS parameters, aligned with TN domain with accordance to 3GPP NRM in TS 28.541, with the flow depicted in the chart below:

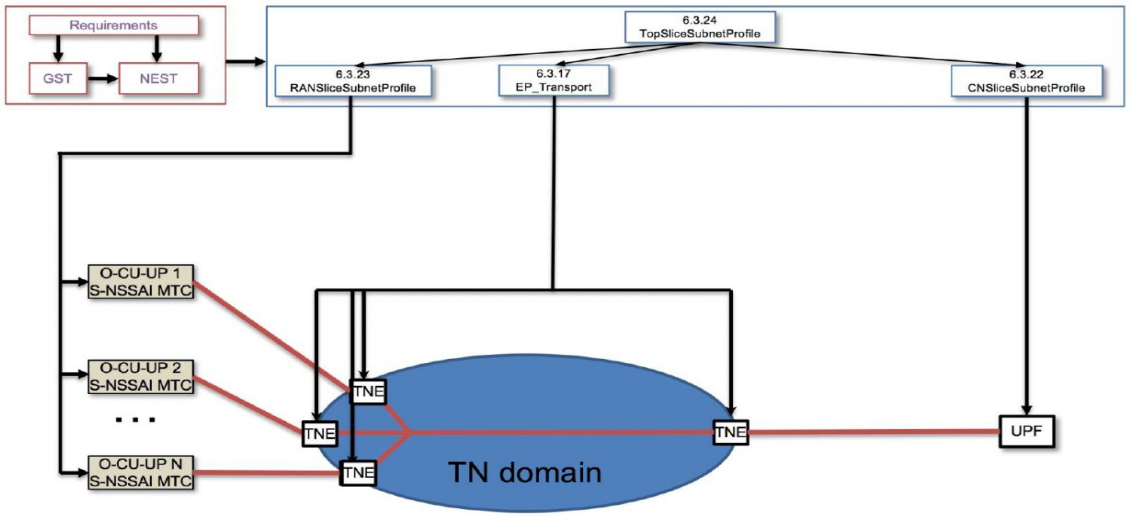


Figure : Diagram of profiles information model parameters mapped to the domains to form a slice

According to these parameters, the relation of RANSliceSubnetProfile and RANSliceSubnetProfile with VLAN and IP mapping could be established with corresponding EP_Transport VLAN and IP mapping, allowing TN domain to perform separation allocation of resources per slice.

Phase 2 assumes the following constrains:

1) Single operator with enterprise slices use case
2) Number of slices: many.
3) Multiple exit points and multiple UPFs
4) Per-slice (tenant) 5QI<>DSCP<>QoS model in TN domain

3GPP RAN and O-RAN Alliance

O-RAN.WG1.Slicing-Architecture-v06.00

Technical Specification

O-RAN Working Group 1
Slicing Architecture

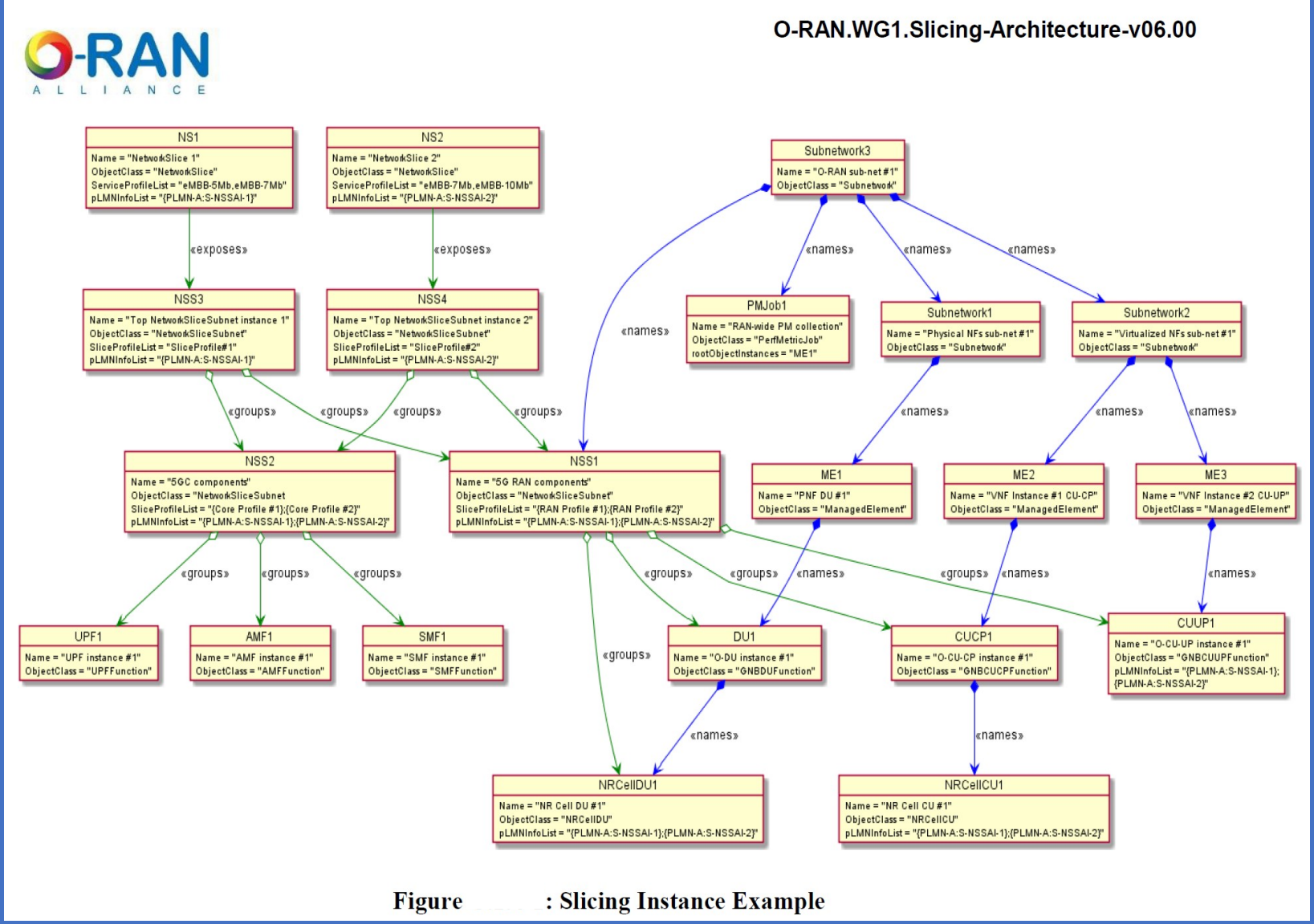


Figure : Slicing Instance Example

3GPP RAN and O-RAN Alliance

O-RAN.WG1.O-RAN-Architecture-Description-v06.00

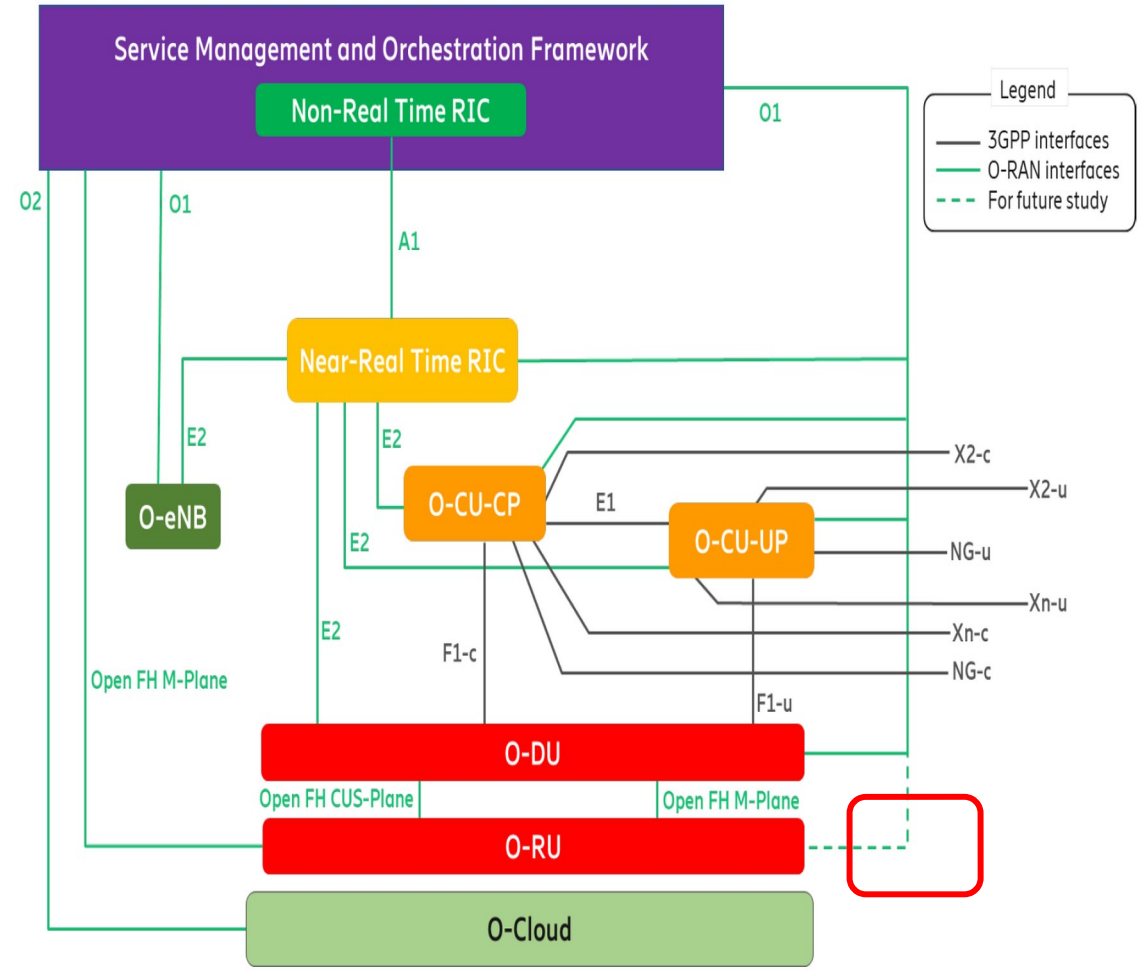


Figure : Logical Architecture of O-RAN

O-RAN.WG1.O-RAN-Architecture-Description-v06.00

4.2 O-RAN Control Loops

The O-RAN architecture supports at least the following control loops involving different O-RAN functions:

- Non-RT (Non-Real Time) control loops
- Near-RT (Near-Real Time) control loops
- RT (Real Time) control loops

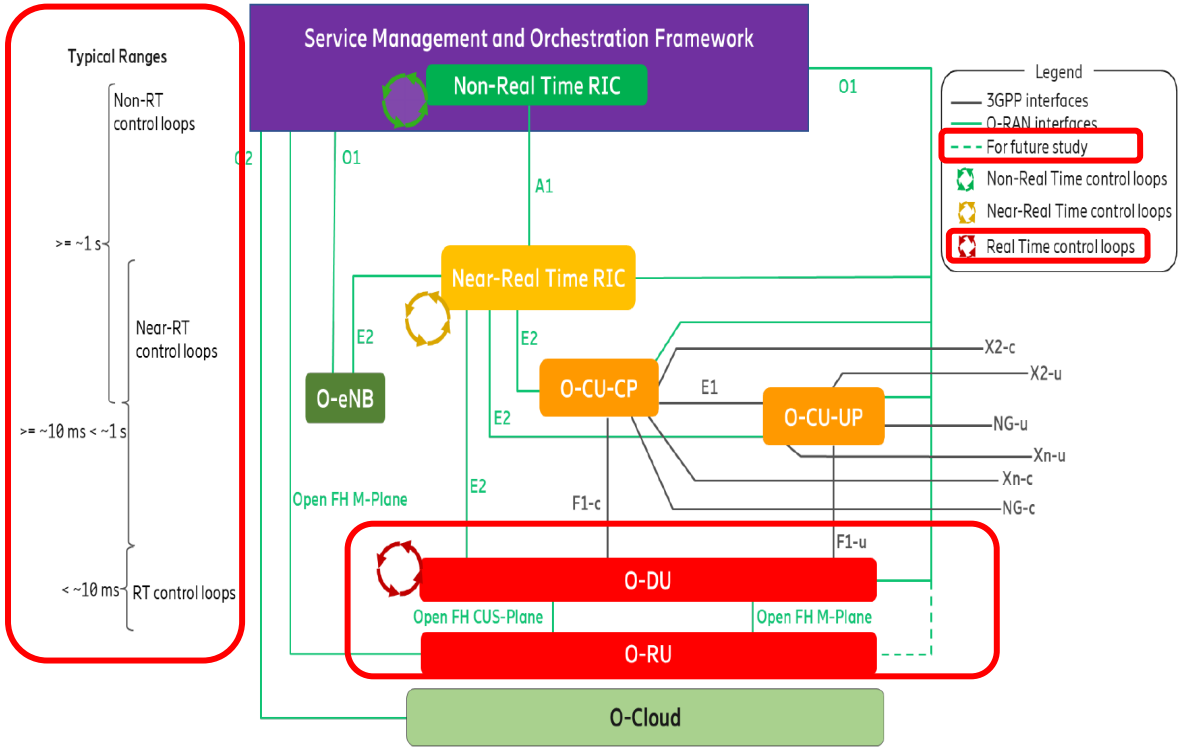


Figure : O-RAN Control Loops

that enable rApps" outside the Non-RT RIC (i.e., into the SMO Framework), as shown in this figure, denotes that the R1 services being exposed may either come from the Non-RT RIC or the SMO.

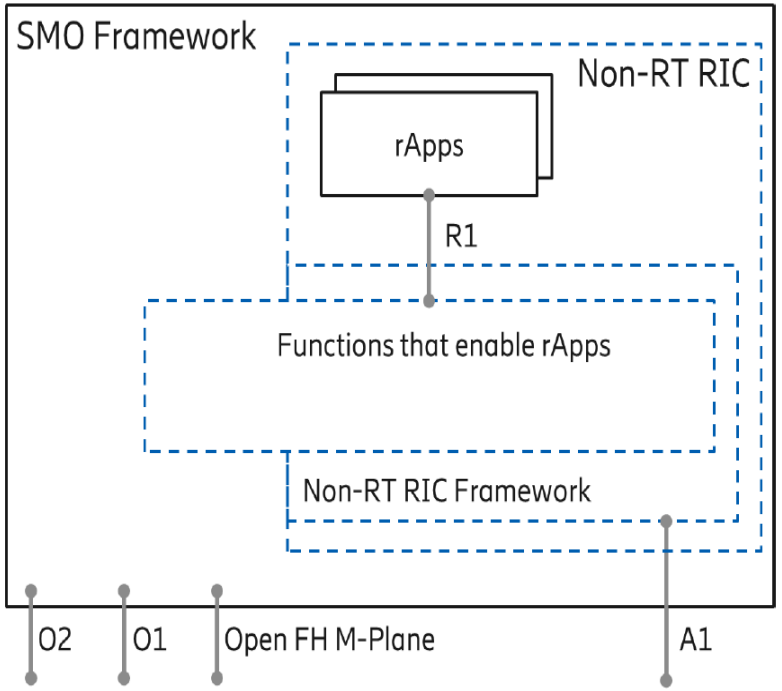


Figure : Exposure of SMO and Non-RT RIC Framework Services

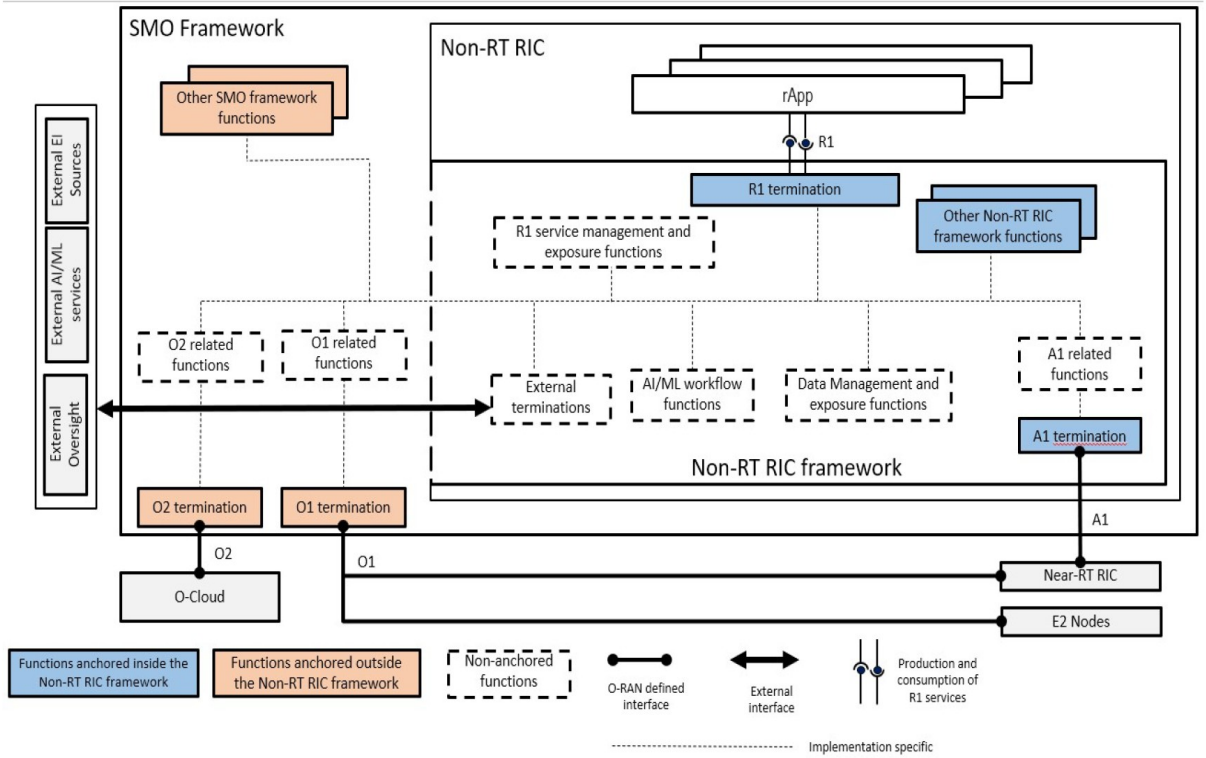


Figure 4-1: Non-RT RIC Reference Architecture

There are 3 Categories of Logical Functions in Non-RT RIC & SMO Framework:
1. Functions anchored inside the Non-RT RIC Framework, which are indicated in solid blue box in Figure 4-1.
2. Functions anchored outside the Non-RT RIC Framework, which are indicated in solid orange box in Figure 4-1.
3. Non-anchored functions, which are indicated in dashed line box in Figure 4-1.

3GPP RAN and O-RAN Alliance

O-RAN.WG1.O-RAN-Architecture-Description-v06.00

Technical Specification

O-RAN Architecture Description

O-RAN.WG1.O-RAN-Architecture-Description-v06.00

A.3 Near-RT RIC

The Near-RT RIC can control multiple E2 Nodes or can control a single E2 Node. The following figures show two implementation options of Near-RT RIC.

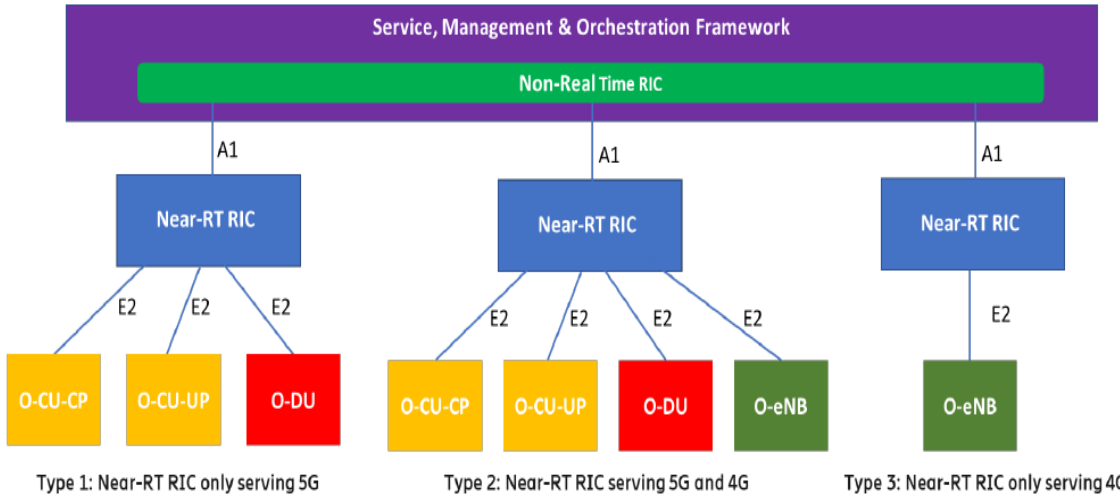


Figure Centralized Near-RT RIC Serving 4G and 5G Simultaneously

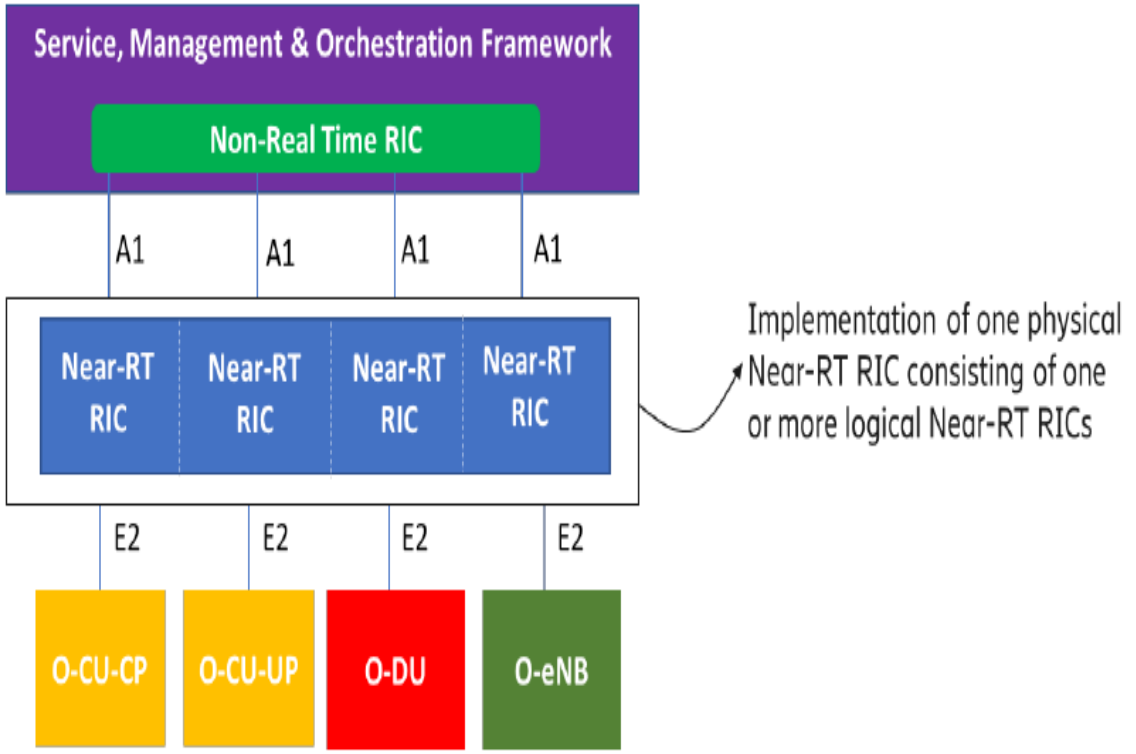


Figure : Distributed Near-RT RIC

3GPP RAN and O-RAN Alliance

UE Identifier	UE Id=1, S-NSSAI =1	UE Id=2, S-NSSAI =2	UE Id=3, S-NSSAI =3
User Traffic	5QI=1: Voice 5QI=8: FTP, Email	5QI=1: Voice 5QI=8: Email 5QI=83: Advanced Driving	5QI=1: Voice 5QI=8: Progressive Video 5QI=8: File sharing
Mobility Pattern	Stationary	High mobility	Low Mobility

The UEs are in an area covered by three frequency bands identified by Cell A, Cell B and Cell C respectively. Cell A is the macro licensed cell with the best coverage. Cell B is the unlicensed cell with limited coverage and Cell C is a licensed cell with narrow bandwidth but provides greater coverage area than cell B.

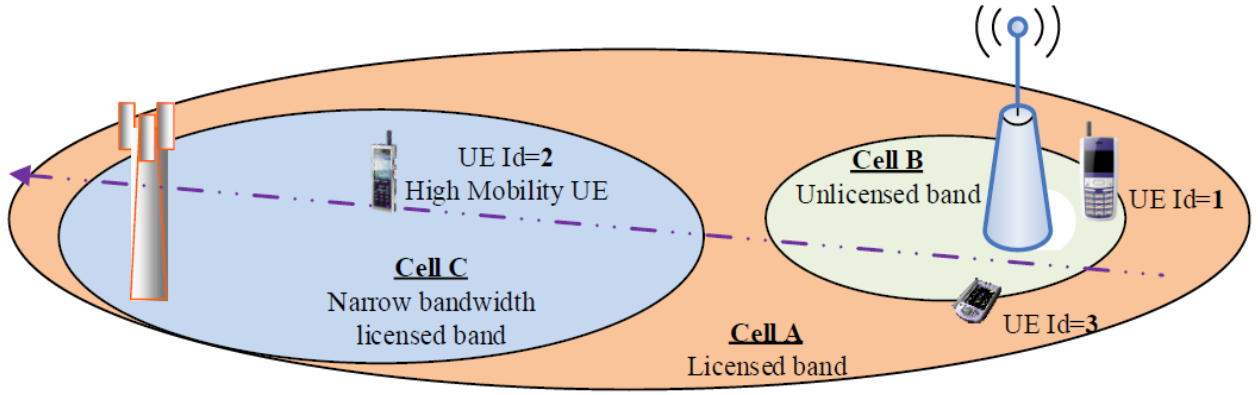


Figure : Cell layout for multi-access use case

O-RAN Alliance SMO foreseen potential evolvement

Multi-vendor RAN support

The role of SMO in Standardized Development and Execution Environments is to support Multi-Vendor RAN.

SMO is an Automation Platform for Cloud RAN/Open RAN and Purpose-built RAN.

SMO offers Platform Capabilities using which Automation Applications can be built to support most common management Use Cases (UCs) for Multi-Vendor RAN Networks.

The Application Development and Run-time Environment in SMO offers a Structured and Standardized way to address these Automation-led Network Operations:

- The Design Environment enables rapid Application Development and Automation artifacts.

- The Run time Environment enables Multi-Vendor Applications to run on the Platform by offering Capabilities such as Application Life-Cycle Management (LCM) , AI/ML Training and Execution, Security, Data Management, Policy, Analytics, Service and Resource Orchestration etc.

The Capabilities are exposed to the Multi-Vendor Applications (rApps) over the R1 Interface.

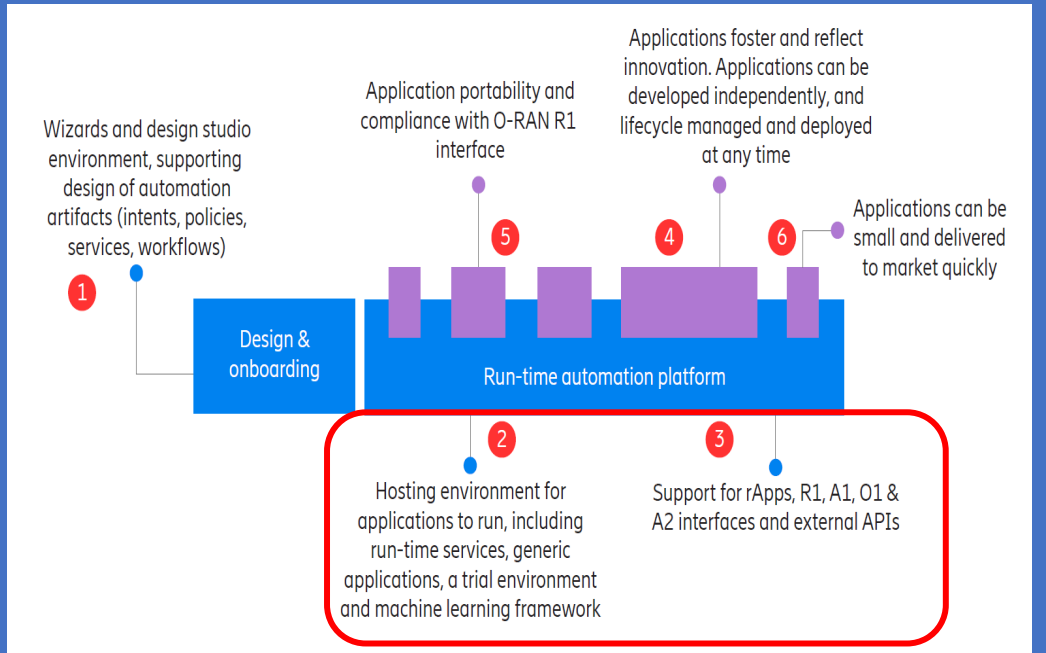


Figure 6. SMO application development and run time environments

Ref. Ericsson, Use of O-RAN SMO for Innovation, Nov., 2021

rApp Categorization and Classification Ericsson defines four (4) main rApp Categories which run on the underlying SMO/non-RT-RIC, forming the AI and Automation Foundation for all rApps:

1. Network Evolution
2. Network Deployment
3. Network Optimization
4. Network Healing

The Network Optimization & Healing rApps could be classified as SON rApps.

Network Evolution would include Capacity Planning Application rApps designed to visualize the future shape of the Network & impact of new Technologies on Performance & Experience.

Network Deployment rApps address areas of Planning and Deployment such as Automated Neighbor Relations (ANR).

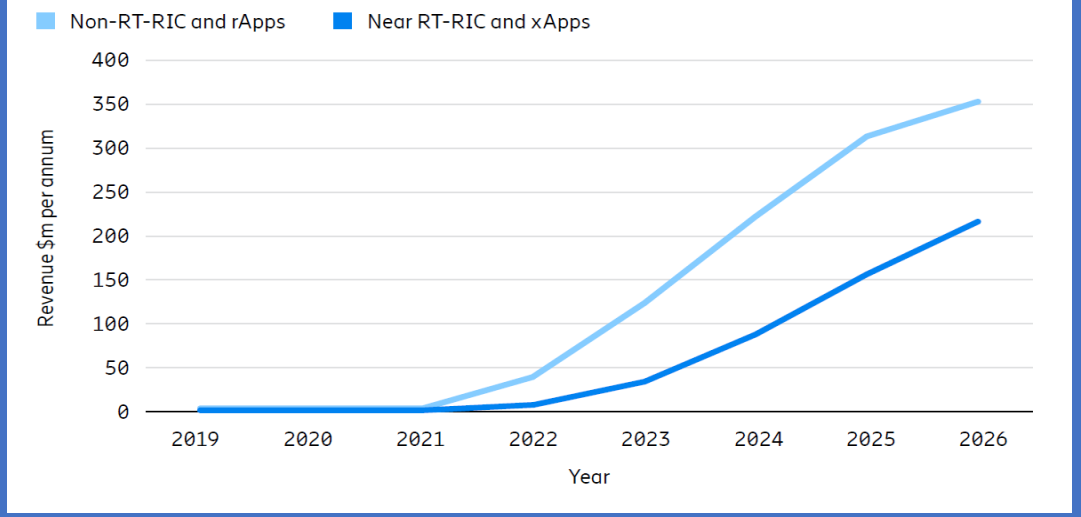
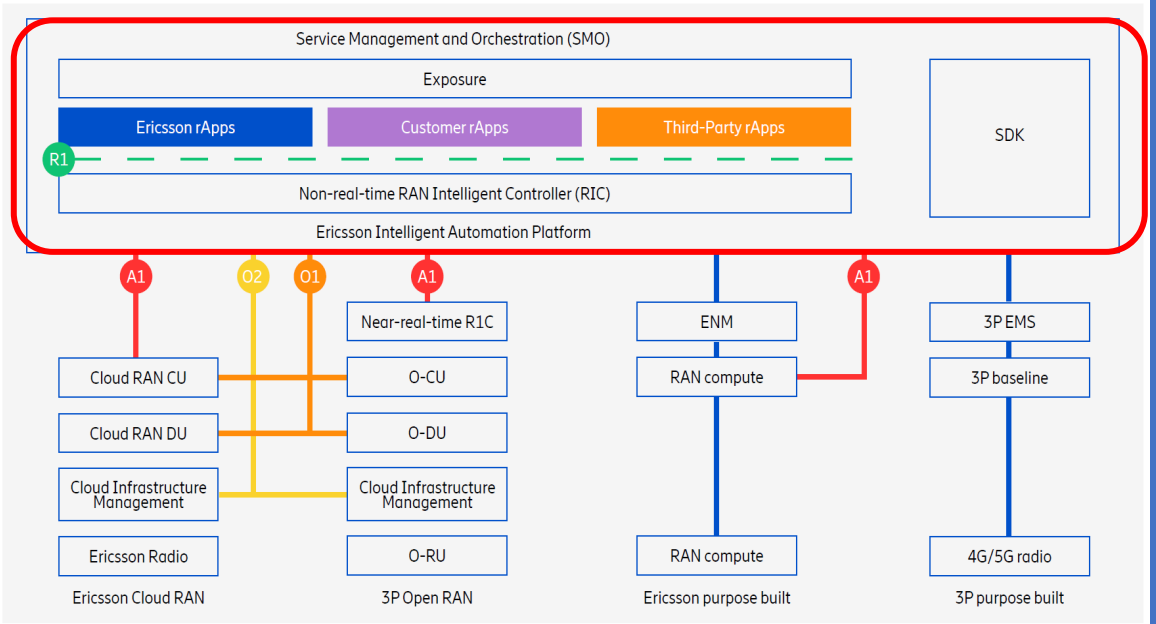


Figure 3: Key components of the Ericsson Intelligent Automation Platform
SMO architecture for multi-technology, multi-vendor RAN



[1] LightCounting RAN automation webinar – Nov 2021
[2] Omdia – Self-organizing networks and RAN intelligent control analysis – Dec 2021

rApps Development Toolkits and Ecosystems

Ericsson believes that there are three (3) Stages in Developing an rApps Ecosystem:

Stage 1: **Developer Resources** enable rapid creation, testing and deployment of rApps including the management of bugs, updates and developments. The best platform vendors will provide a comprehensive SDK.

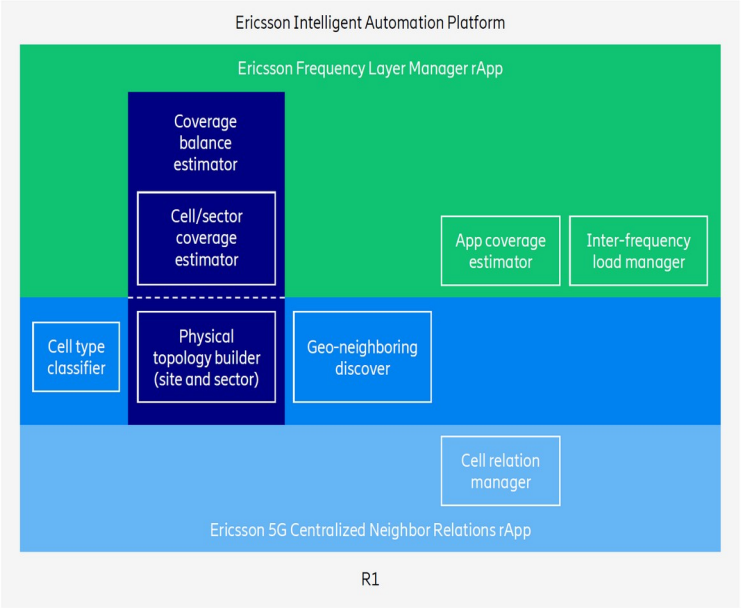
Stage 2: The Developer Community connects rApp and Platform Developers, enabling information to be shared. Ericsson expects leading vendors to provide technical support, testing and certification, as well as collaboration environments for development.

Stage 3: Mass-Market adoption is where we will see highly Developed and Mature ecosystems of Application Developers.

Delivery and Life Cycle Management (LCM) will be fully integrated with the Service Provider's Continuous Integration/Continuous Delivery (CI/CD) pipeline to standardize SW Asset Management.

Some organizations believe there will be a Common Marketplace that provides a Catalogue of rApps enabling simpler monetization. However, as rApps and xApps are focused on Network Automation in a Specific Telco Domain, any potential Marketplaces for Applications are unlikely to match the Scale of Consumer Marketplaces such as the Apple App Store or Google Play Store for the smartphone industry.

Figure 5: rApp hierarchies showing multiple small rApps creating a larger, more complex rApp



Example: Frequency Layer Manager (FLM)
The FLM rApp is composed of several smaller functions that provide the load balance recommendations. Some of these functions are also shared with other C-SON algorithms, such as automated neighbor relations (ANR), cell type classifier and physical topology builder.

Ref. Ericsson, Intelligent Automation Platform, How rApps drive Network Optimization & Monetization, March, 2022

The expected approach to rApp Development based on Complexity and Specificity

The ability to develop your own rApps is a way for **Service Providers (SPs)** to further differentiate their offering in the home market.

SPs may even commercialize these developments by making them available to other service providers outside their home market, effectively creating a new revenue stream by monetizing their rApp development investment.

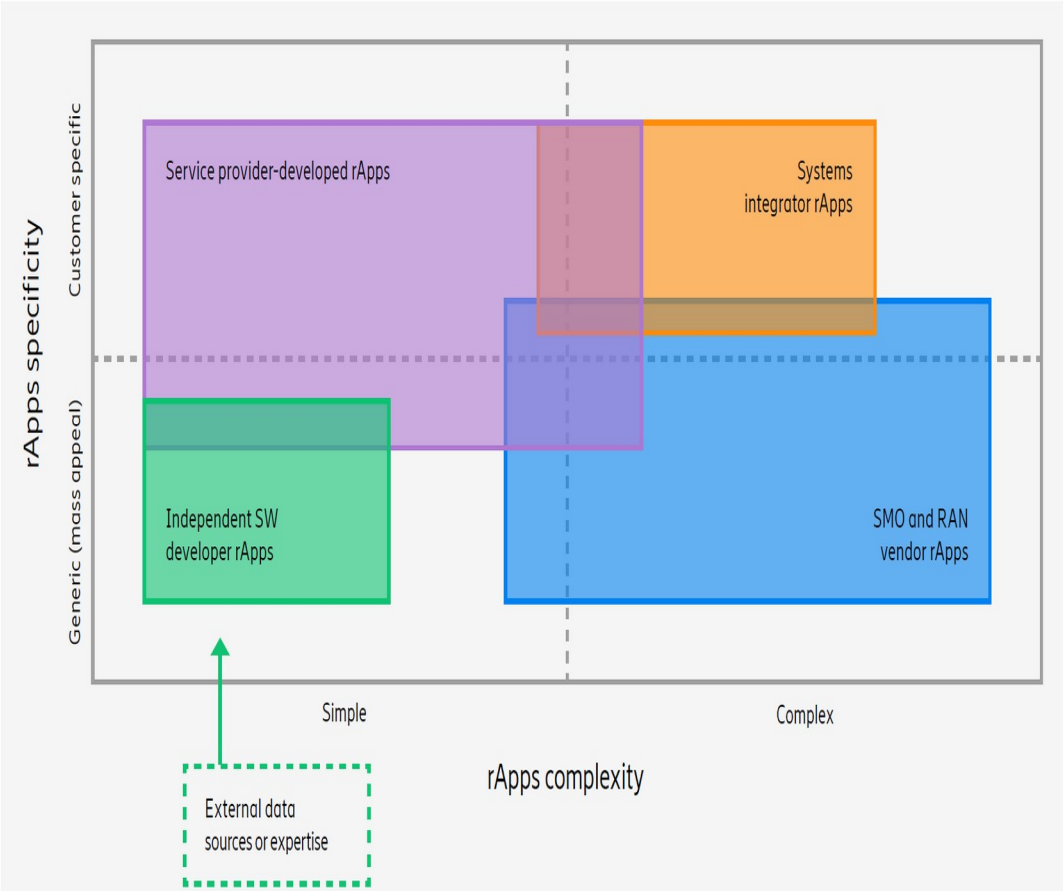
The expectation is that SPs will typically focus on the simpler Customization UCs , but there are also a number of highly innovative SPs who have the Resources, Knowledge & Experience to create highly Complex rApps and are expected to do so.

The final group of rApp Developers are arguably the most Diverse & Interesting.

These are Independent SW Developers, some of whom will be new to the Telecoms Industry.

The expectation is that these Companies will bring Specific, Detailed Knowledge and Data Sources which, when combined with existing SPs Data, will enable some very powerful and innovative rApp UCs.

Figure 7: The rApp developer ecosystem – expected approach to rApp development based on complexity and specificity



Service Orchestration Functionalities are at the Foundation of the Architecture to enable Service and Intent-based Automation.

Machine Learning (ML) Capabilities are present to enable Intent-based Automation Capabilities.

The Open R1 interface drives innovation

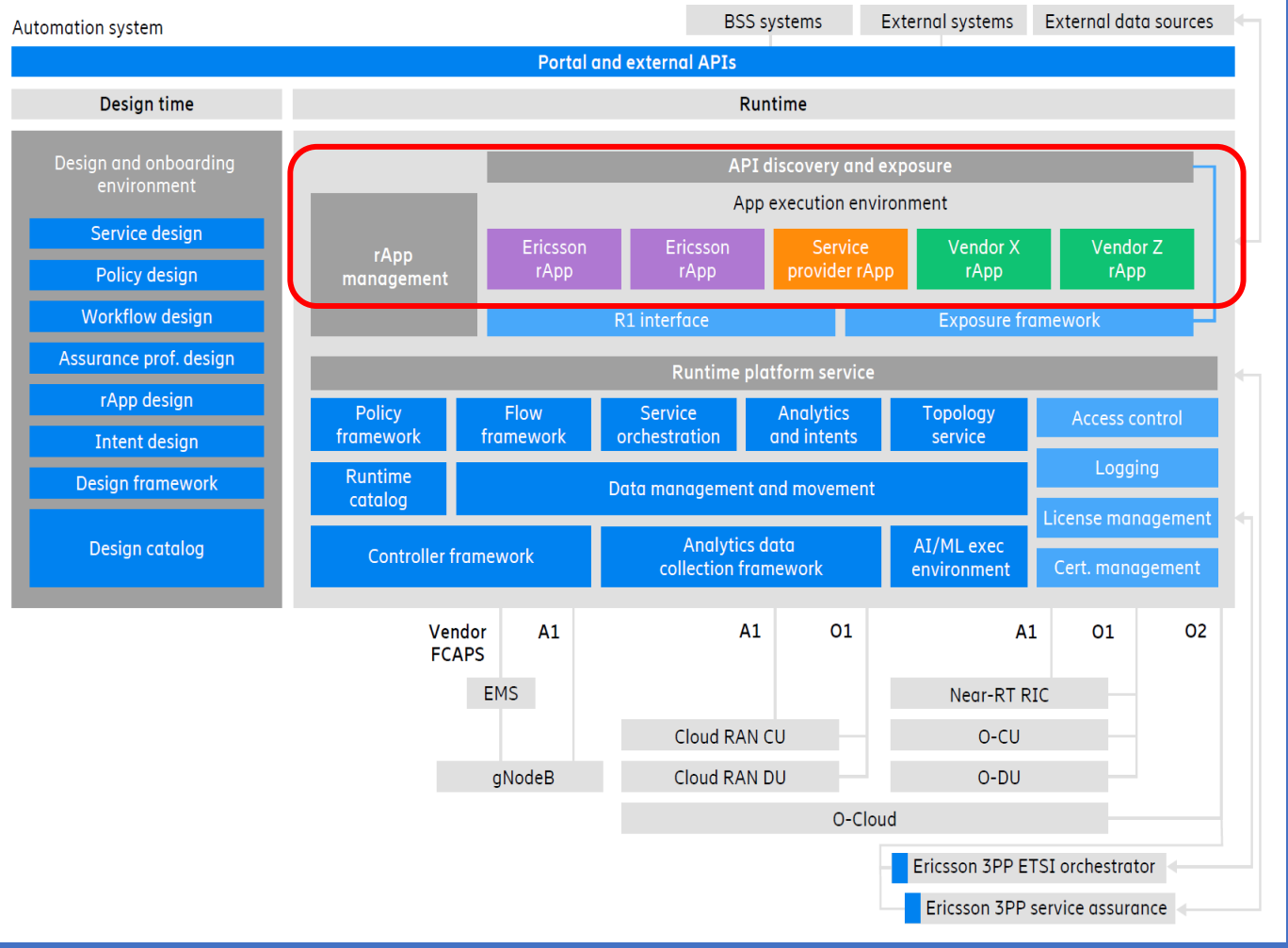
An Open R1 Interface enables rApp Portability.

Once the O-RAN Alliance completes specification, the interface should be published and standardized to reduce the need for rApp interoperability testing across different vendors' SMOs.

For an rApp Developer, a Standardized R1 Interface increases opportunities to monetize specific rApps which are not locked to a specific vendor.

Ideally, the R1 interface would allow out-of-the-box Interoperability, but in reality, a level of simple Interoperability Testing and Certification is expected.

Figure 3: The Ericsson Intelligent Automation Platform



Ref. Ericsson, Intelligent Innovation, Intelligent Automation Guidelines, May 2022,

Business

Enterprise open source for innovation

Consider the following findings from our survey:

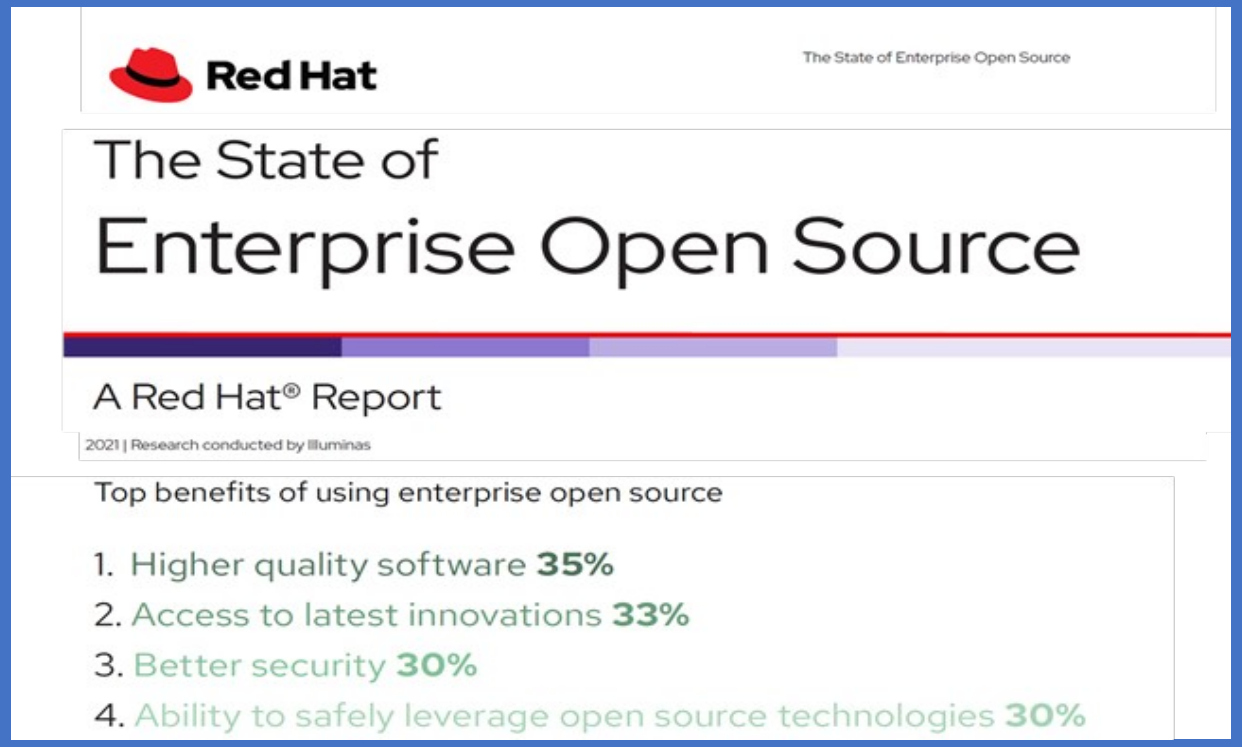
Two years ago, lower cost of ownership was cited as the top benefit of enterprise open source. This year it's fallen to the sixth spot, well below "access to the latest innovations" in second. This year, 82% of IT leaders also agreed with the statement that "enterprise open source is used by the most innovative companies." About the same number, 81%, said that it "provides flexibility to customize solutions to meet company needs."

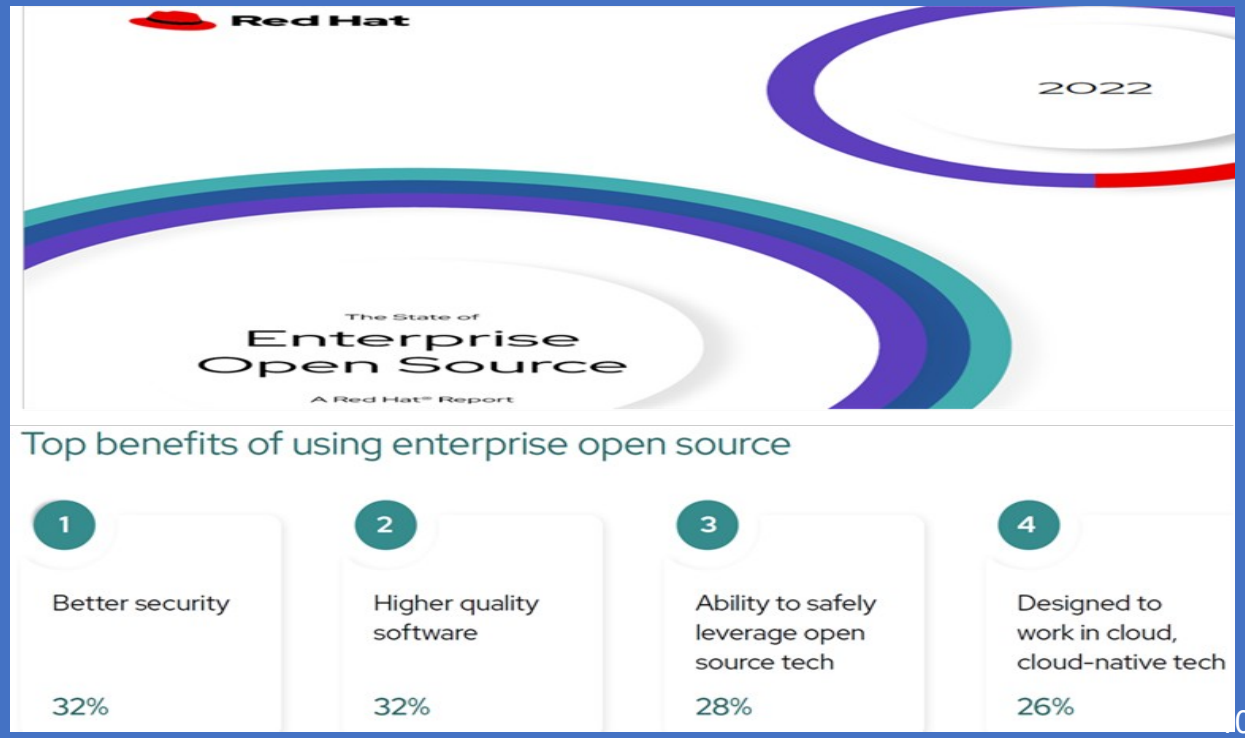
We see specific examples of enterprise open source adoption in emerging technology areas. 79% of respondents expect that over the next two years, their organization will increase use of enterprise open source software for emerging technologies. In the two most prevalent emerging tech areas, edge computing/IoT and artificial intelligence/machine learning (AI/ML), use of enterprise open source is expected to significantly outpace proprietary software over the same period. In edge computing/IoT, enterprise open source is expected to increase from 55% of cases to 72% two years from now. And, for AI/ML, our survey found that proprietary software use is actually expected to decrease, while enterprise open source use shoots up from 48% to 65%.

The benefits are broad and strategic

When we began running this survey four years ago, the top benefit of enterprise open source was clear: lower total cost of ownership (TCO). This result was likely a surprise to no one. Linux, along with enterprise open source more generally, was adopted by companies in no small part because it was a less expensive alternative to proprietary UNIX and proprietary networking-related applications. Even if this view of enterprise open source began to increasingly diverge from reality, it remained a stereotype. However, we have seen a steady shift away from enterprise open source being defined as cheaper software rather than better software. Of course, this is not to say that enterprise open source can't be less expensive to acquire and operate than proprietary software. But price is not how IT leaders generally frame their thinking about enterprise open source today.

This year's top two benefits? Better security and higher quality software. By contrast, lower TCO has declined dramatically in importance. It is now near the bottom of the benefits list in ninth place.





5G Architecture for Hybrid and Multi-Cloud Environments

A Unified Approach to Developing, Deploying & Operating 5G Services - including 5G RAN, Core, OSS & BSS Applications – in Public & Private Cloud Environments is a Key Enabler for Communication Service Providers (CSPs) to successfully adopt a Hybrid & Multi-Cloud Strategy. The "main benefits" are "Faster Time to Market" (TTM) & "Lower Total Cost of Ownership" (TCO). As *Figure 2* illustrates, this approach could *lead to a lot of Diversity & Heterogeneity in the Deployment Targets for Network SW* Vendors. Designing & Operating an Application that is capable of utilizing such a Diverse Set of HCP Managed Services also creates *Several Challenges for Network SW* Vendors & CSPs alike. **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** such 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**. As shown in *Figure 1*, **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 Telco, as each CSP creates &/or selects its own Cloud infrastructure.

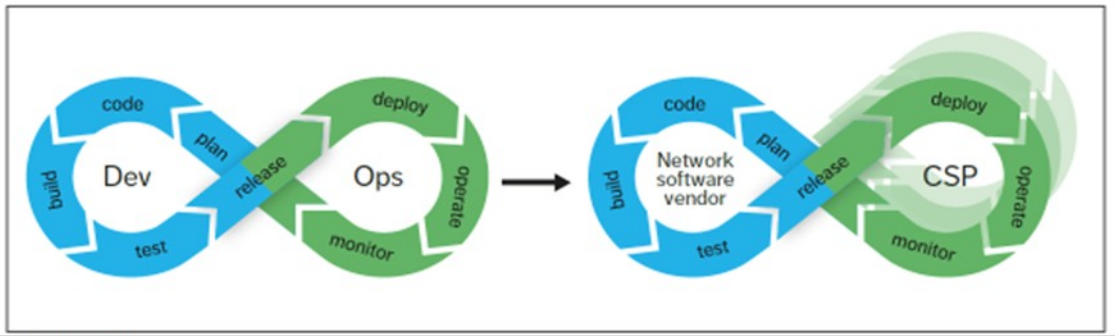


Figure 1: The DevOps and (Telecom) aaP Business Models

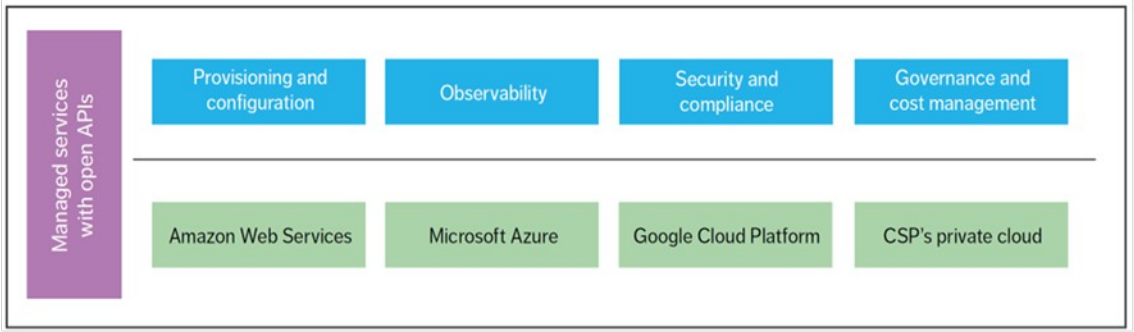


Figure 3: Key Enablers for a Multi-Cloud Native Application

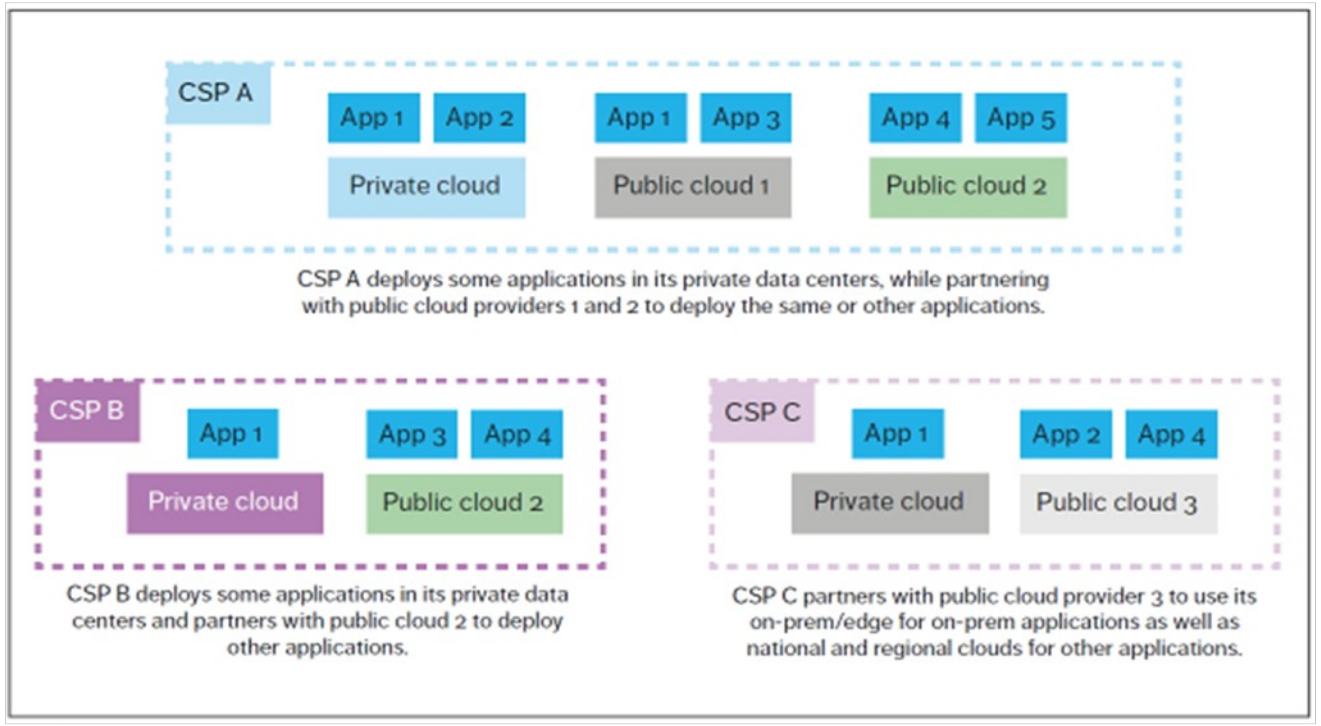


Figure 2: Examples of Hybrid and Multi-Cloud Deployment Scenarios that Applications must be able to support

In addition to hypervisor-based execution environments that offer hardware abstraction and thread emulation services, the OS container execution environment provides kernel services as well. Kernel services include:

- Process control.

EXAMPLE 1: OS process creation; scheduling; wait and signal events; termination.

- Memory management.

EXAMPLE 2: Allocation and release of regular and large pages; handling memory-mapped objects and shared memory objects.

- File system management.

- File management.

EXAMPLE 3: Creation, removal, open, close, read and write file objects.

- Device management.

EXAMPLE 4: Request, release, configuration and access.

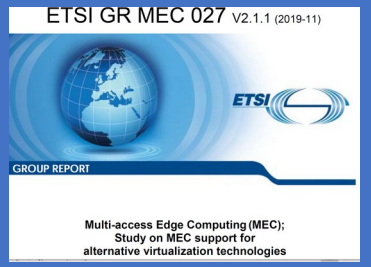
- Communication services.

EXAMPLE 5: Protocol stack services, channel establishment and release, PDU transmission and reception.

- System information maintenance.

EXAMPLE 6: Time and date, system and OS resource data, performance and fault indicators.

The OS container-to-VNFC logical interface is typically realized via:



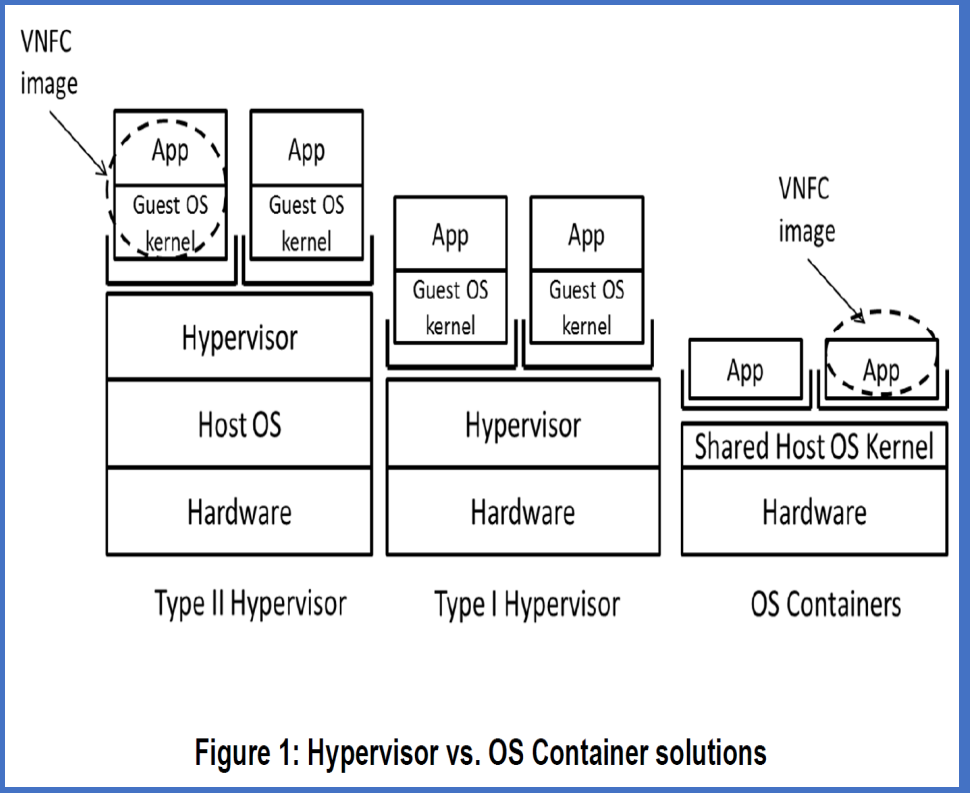
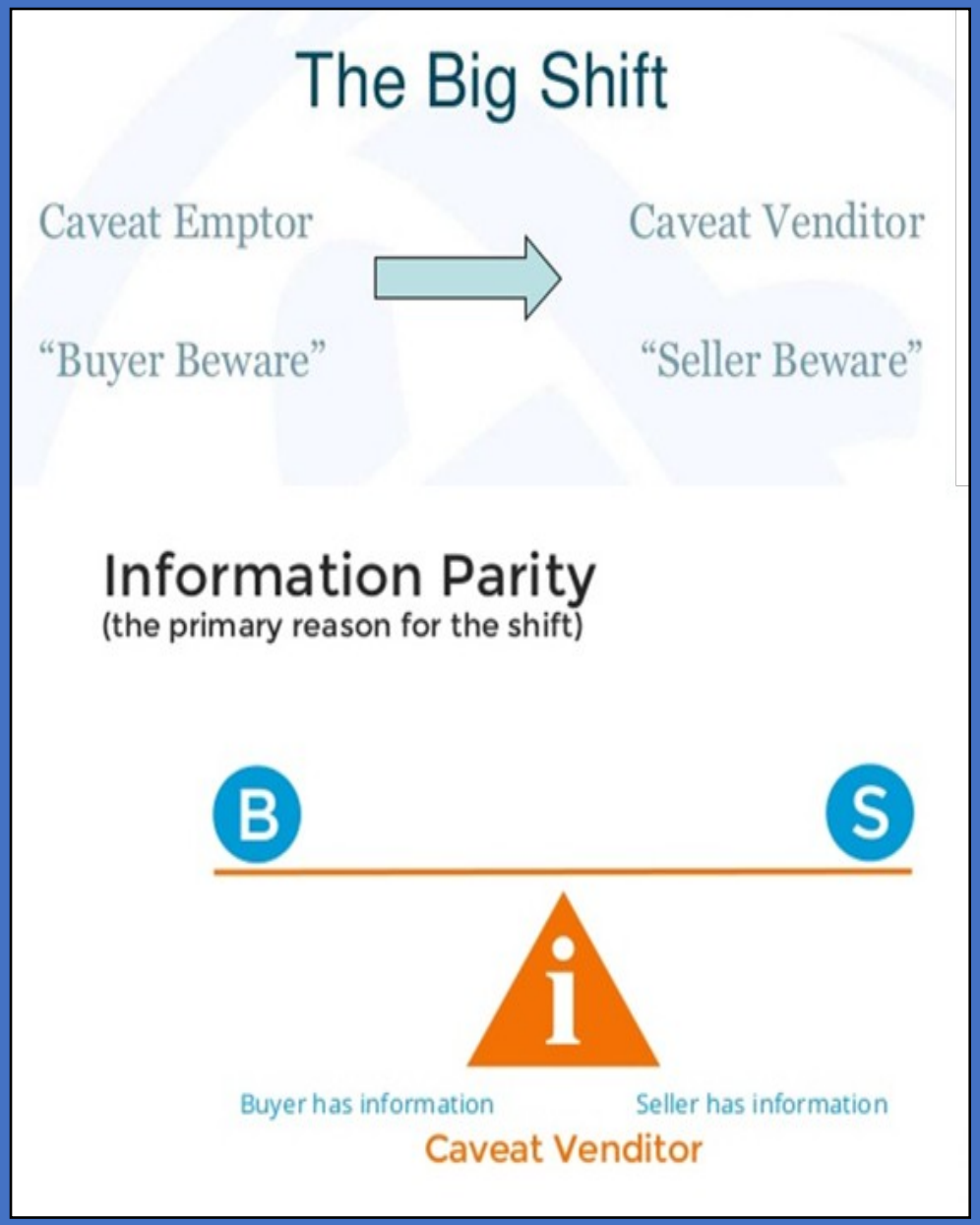


Figure 1: Hypervisor vs. OS Container solutions

1.1 The Big Shift - from "Caveat Emptor" to "Caveat Venditor" - 1



THE MARKET FOR "LEMONS":
QUALITY UNCERTAINTY AND THE
MARKET MECHANISM *

GEORGE A. AKERLOF

I. Introduction, 488. — II. The model with automobiles as an example, 489. — III. Examples and applications, 492. — IV. Counteracting institutions, 499. — V. Conclusion, 500.

When Information is Ubiquitous:

shift from **Information Inequality** to **Information Paritiy**

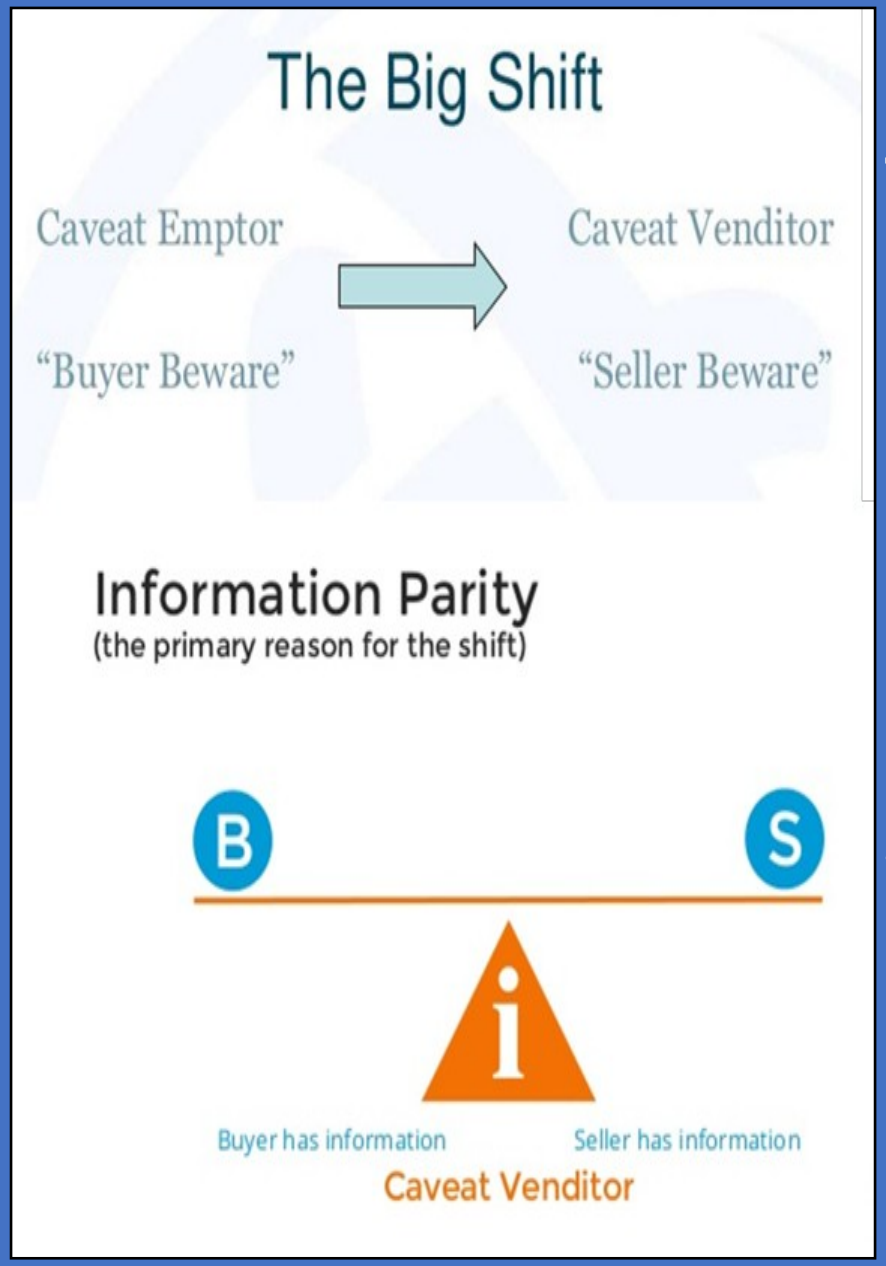
No longer enough

just to be able to Answer to Questions on Product/Solution/ Services

and/or present Platforms, Solutions, Services, Standards ...

Ref.: D.Pink, D-ve, 2012

1.1 The Big Shift - from "Caveat Emptor" to "Caveat Venditor" - 2



When Information is Ubiquitous

The Value of undertaking the role of "Unbiased Business Partner"

Shift in assigned importance **from**

"Problem - Solving"
to
"Problem-Identification/ Finding"

Ask the "Right Questions"
- to Identify Current Issues/Problems, curate the Vast Amount of Information &

- **Ability to Hypothesize/Clarify on Future** Problems, Inter-Dependencies

- **Outline Future Multi-Vendor Inter- Operability & Scalability**

- **Ground for Personalized, Business Model & Agile Service Deployment**

Ref.: D.Pink, D-ve, 2012

Remarks & Questions?