5G Advanced

Towards Beyond 5G (B5G) and 6G Networks with 5G Advanced

Intent-based Management with enhanced Network Data Analytics

for

B5G and 6G Data-centric Services

with

Performance and User Experience Guarantees

Ike Alisson

2023 - 10 - 05 Rev PA06

Table of Contents

1. Introduction - focus in the 5G Advanced specified 5G System Capabilities paving B5G & 6G Capabilities presentation on the red circled topics below

NGMN

6G Position Statement

An Operator View

v1.0

Date: 26.09.2023

NGMN

CLOUD NATIVE MANIFESTO

An Operator View

v1.0

Date: 06.09.2023

INNOVATIONS AND NEW SERVICES

1. 6G provides an opportunity to support innovative new IMT-2030 features such as joint sensing and communications, AI, extended AR/VR, enhanced positioning etc.
2. 6G should facilitate seamless integration and interoperability with fixed and satellite networks.
3. 6G should inherently support network related APIs, fostering new service offerings which leverage network capabilities.

OPERATIONAL PRIORITIES

1. Network simplification leading to lower operational cost whilst retaining scalability and flexible deployment models.
2. Absolute energy reduction when assessed across mobile and fixed networks to support the transition towards low carbon economies.
3. Features (such as AI) that support automated network operations and orchestration to enable efficient, dynamic service provisioning.
4. Proactive network management capabilities across fixed and mobile networks to predict and address issues before they impact user experience.
5. Quantum safe infrastructure, resistant to attack by Quantum computers.

On our journey to highly flexible, sustainable, and resilient networks for the future, we believe in applying the following cloud native principles to all layers of network infrastructure, applications, and services*:

1. Decoupled infrastructure and application lifecycles over vertical monoliths;
2. 'API first' over manual provisioning of network resources;
3. Declarative and intent-based automation over imperative workflows;
4. GitOps** principles over traditional network operations practices;
5. Unified Kubernetes (or the like) resource consumption patterns over domain-specific resource controllers;
6. Unified Kubernetes (or the like) closed-loop reconciliation patterns over vendor-specific element management practices; and
7. Interoperability by well-defined certification processes over vendor-specific optimisation.

We also believe that openness and compatibility principles need to be key drivers of future Telecom and network services implementations to ensure we leverage Cloud Native principles to encourage software – orchestration – and hardware disaggregation.

1. Mobile Networks to evolve from:

a Design that offers "Best-effort Services

to

a Design that offers Performance and User Experience Guarantees

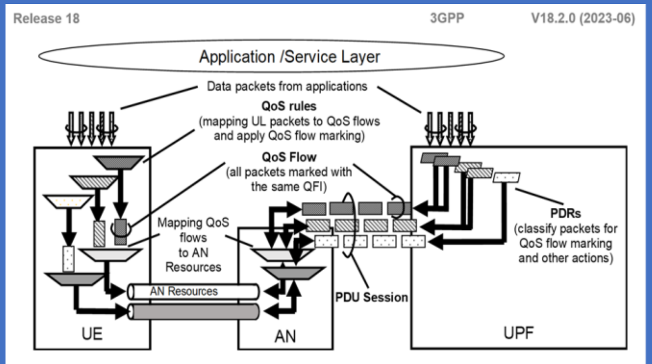


Figure: The 5G Principle for Classification and User Plane (UP) marking for QoS Flows and mapping to AN Resources

Capabilities related to e.g.:

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

2G 3G

4G LTE

=>

5G

5G ADVANCED

6G

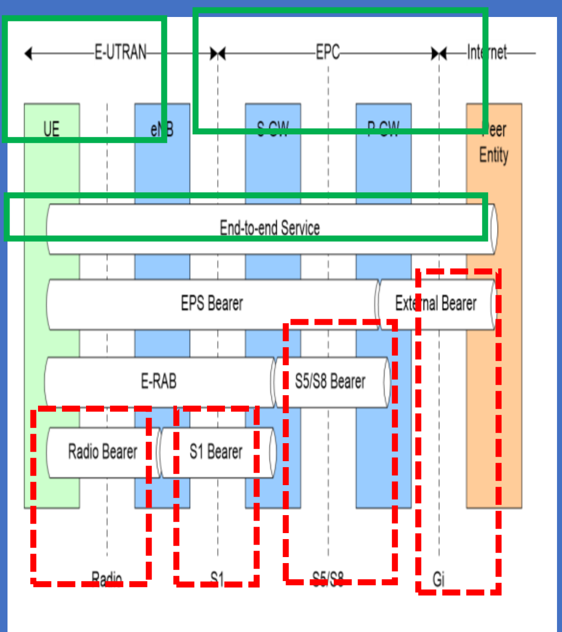


Figure : EPS Bearer Service Architecture

=>

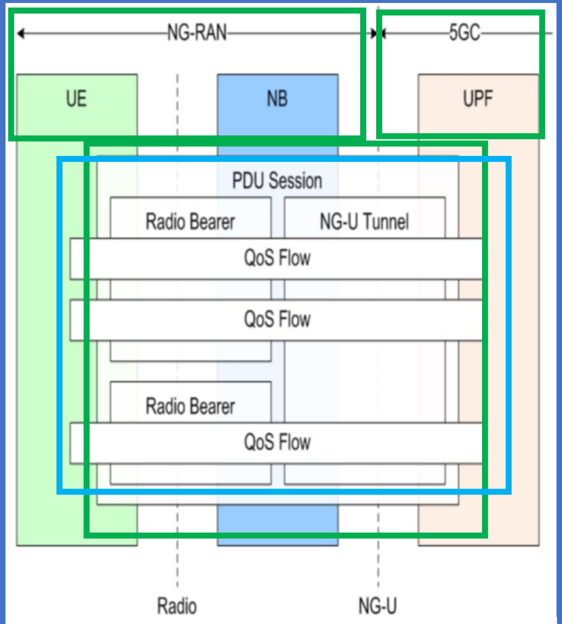


Figure: 5G CN NG-RAN Bearer Services QoS Architecture

Measurement Assistance Information shall include the addressing information of *a* ***Performance Measurement Function*** (**PMF**) **in the UPF, the UE can send PMF protocol messages** incl.:

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

The current *5G Networks* brings more *Operational Complexities*, and the *Telecom System* need to be able to adapt their Operation to the Business Objectives of the *Operator* (*MNO/CSP*) as well as expectations of Customer (*CSC/Resource Owner*), which is ***driving Customer to shift the focus from "How" to "What".***

An *"Intent driven System*" will be able to "learn" the behaviour of Networks and Services and allows a *Customer to provide the desired "State*"*, without detailed *"Knowledge"* of how to get to the desired *"state".*

Note: elaboration of "state" of 5G Services UE/Resource Owner, as part of the "Context" use & definition in 5G NDL (Network Data Layer with "Structured" & "Unstructured" Data storage in 5G CN) is not provided hereby due to limitation of scope & respectively volume of the this Presentation).

Thus, the "*Intent driven Management*" is introduced to reduce the Complexity of Management without getting into the intricate detail of the underlying Network Resources.

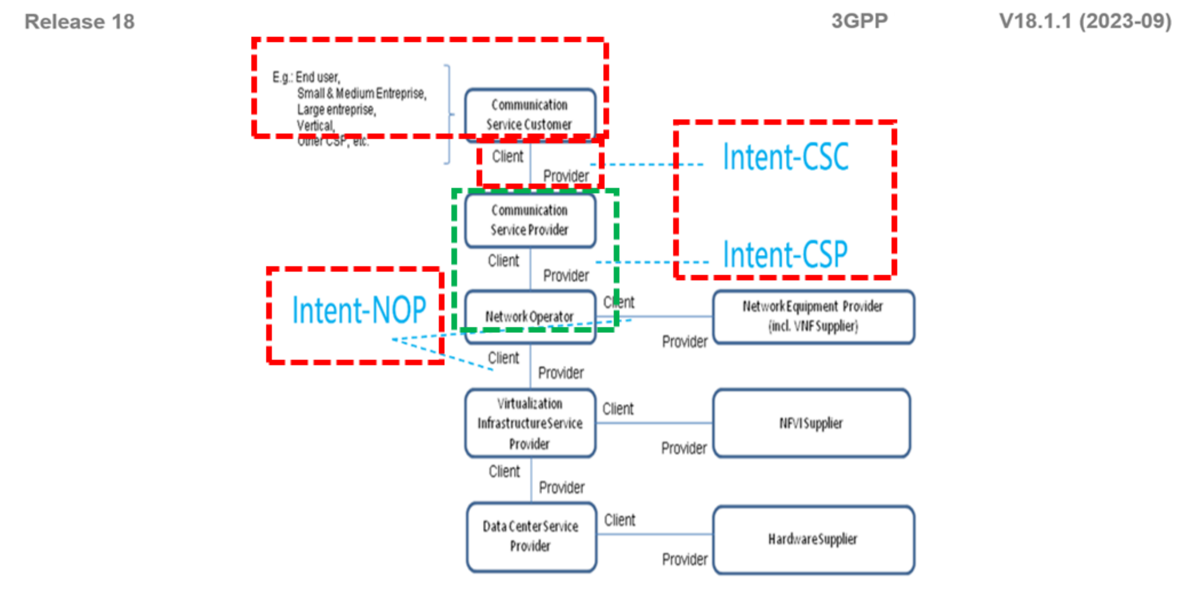


Figure: 5G High-level Model of different kind of Intents expressed by different Roles

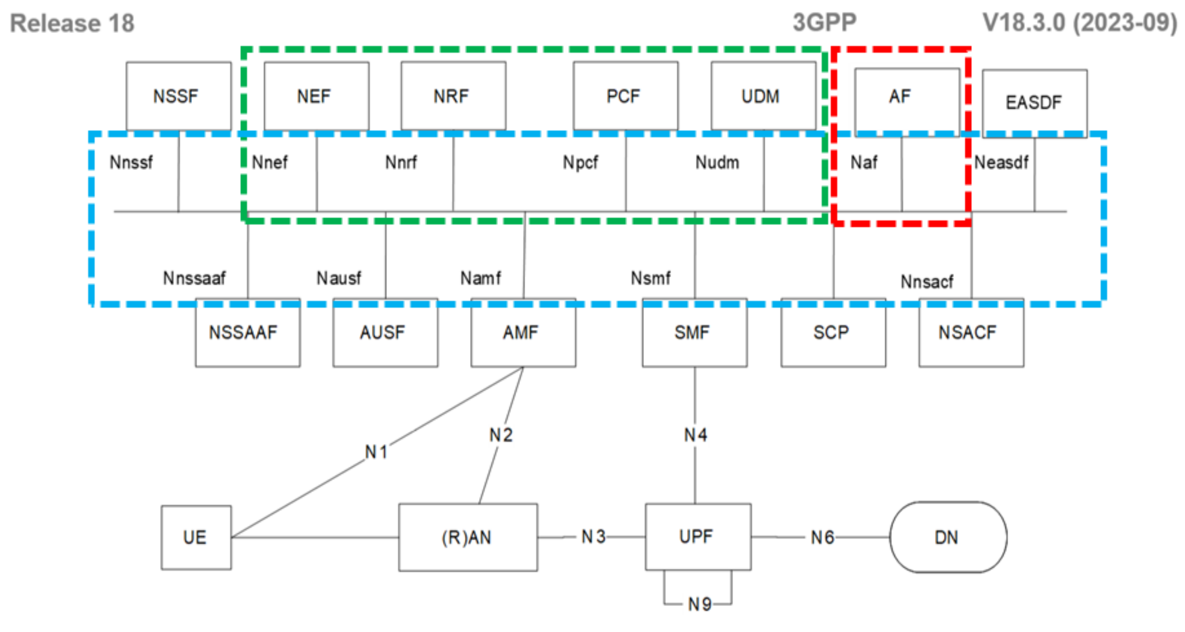


Figure: 5G System Non-Roaming Architecture

The state related to "Entity" as being defined within the updated definition of "Context" used in 3GPP 5G System Architecture and ETSI*

1.1.1 5GS Intent driven Management Framework - 2   Intent Categories based on User types

Based on "Roles" related to 5G Networks and Network Slicing Management defined in 5GS Management and Orchestration UCs, Concepts and Requirements, different kinds of "Intents" are applicable for different kinds of Standardized Reference Interfaces.

An *Intent* specifies the expectations including Requirements, Goals and Constraints for a specific Service or Network Management Workflow.

The *Intent* may provide information on particular Objective and possibly some related details.

Following are some general Concepts for intent:

- An *Intent* is typically understandable by *Humans,* and also needs to be interpreted by the Machine without any ambiguity.

- An *Intent* focuses more on describing the "*What needs to be achieved"*, but ***less on "How" that outcomes should be achieved".***

The *Intent* expresses *the metrics that need to be achieved* and **not how to achieve them.**

Intent describes the Properties that allows a Satisfactory Outcome.

- The *Expectations* expressed by an *Intent* is *agnostic* to the underlying system implementation, technology and infrastructure. Area can be used as managed object in the expectations expressed by an intent to achieve system implementation, technology and infrastructure agnostic.

- An *Intent* needs to be quantifiable from Network Data so that the fulfilment Result can be measured and evaluated.
Intent can be categorized based on different User Types or different Management Scenario Types.

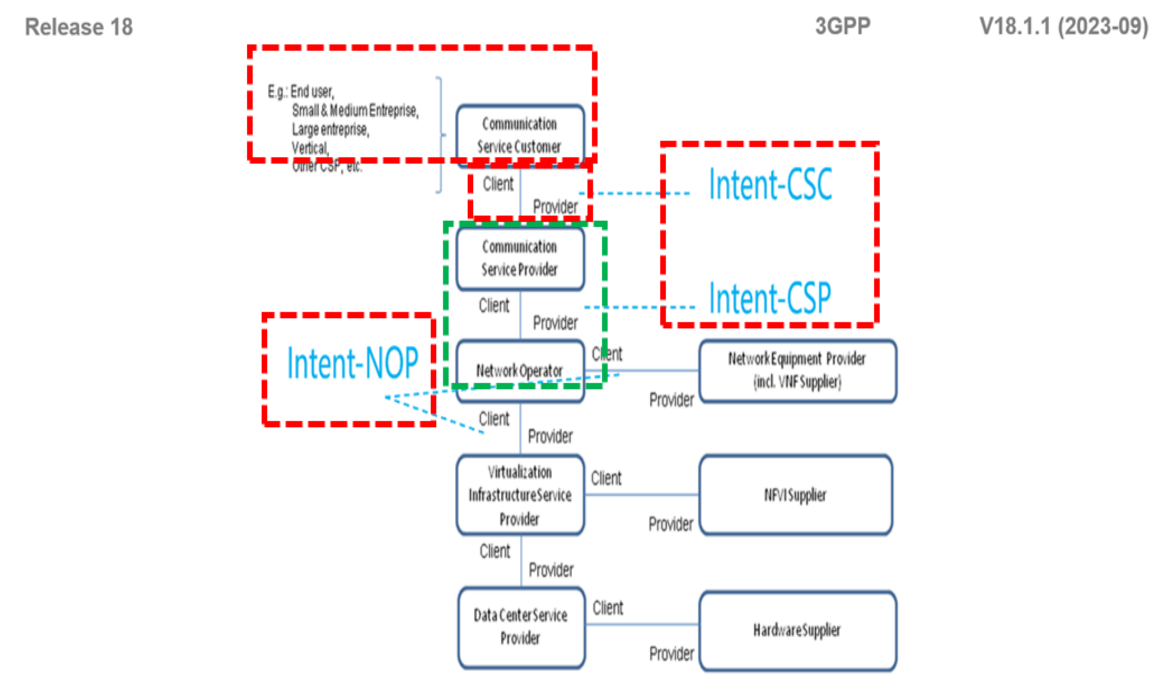


Figure: 5G High-level Model of different kind of Intents expressed by different Roles

Introduction of Service-based Architecture (SBA) for 5G, in combination with Functional Model of Business Roles, exceeds the Level of Complexity for Managing Network in different Scenarios (including Scenarios for Design/Planning, Deployment, Maintenance and Optimization), both in a Single and Multi-Vendor Network.

Actions of an Intent driven *MnS related to the Fulfilment of Intents* may be categorized as:

1. *Intent Deployment* and
2. *Intent Assurance*.

An *Intent driven MnS* allows its "*Consumer"* to express intents for managing the Network and Services and obtain the feedback of intent evaluation result.

The *Intent-driven MnS "Producer"* have the following *Intent* handling Capabilities:
- Translate the received intent to executable actions as follows:
- Performing Service or Network Management Tasks.
- Identifying, Formulating and Activating Policies for Service or Network Management.
- Evaluate the Result/Information about the Intent Fulfilment, including Intent Deployment (e.g. the Intent is initially satisfied or not) and Intent assurance (e.g. the Intent is continuously satisfied).

The Figure shows the 5G Model of Intent-driven MnS.

When the *intent* is created by "*MnS Producer*" based on "*MnS Consumer's*" request, the "*MnS Producer*" may consume other Management Service(s) (including Non-Intent driven MnS and Intent driven MnS) to fulfil or satisfy the Intent, e.g. creating new assurance Closed Control Loop Instance(s) or using Assurance Closed Control Loop Instance (s) to satisfy the intent.
The internal implementation of the intent fulfilment will however not be standardized.

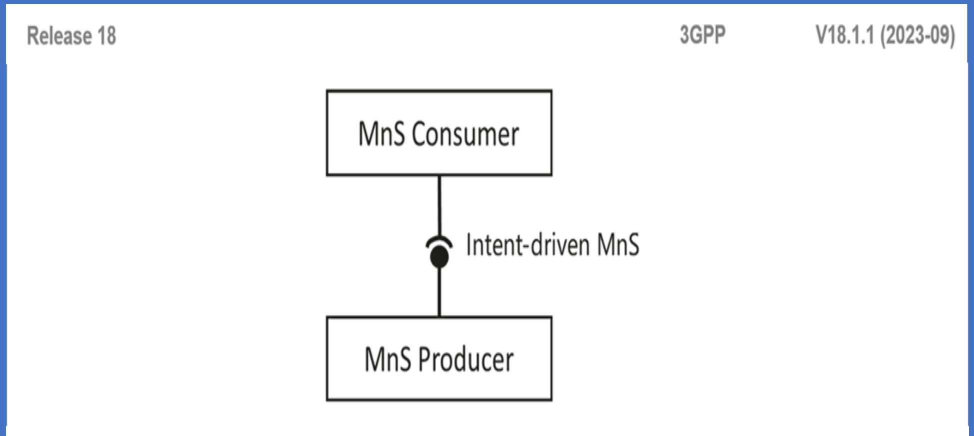


Figure: 5G System Intent-driven MnS

The intents may be fulfilled by *utilizing Multiple Mechanisms* including among others:

- Rule-based Mechanisms,
- Closed Loop Mechanisms and
- ***AI/ML based Mechanisms***.

These Mechanisms can be combined in Solutions of various Complexity, ranging from a "simple" approach Rule-based Mechanisms, to ***more elaborate Solutions combining AI/ML***, Closed Loop Automation to ensure the fulfilment of intents.

The Intent driven MnS "Producer" is the provider of Intent driven MnS and is responsible for deriving activities for Networks and Services or other intent(s).

The MnS "Consumer" may consume *Intent Driven MnS(s)* provided by the *Intent driven MnS "Producer(s)"* or may have the *"Consumer*" Role for Non-Intent MnS *"Producers*".

The conflict(s) including conflict between the intent and other intent(s) and/or Non-intent requirements needs to be detected and resolved during the intent translation.

The Figure illustrate the potential way to satisfy intent-CSC :

- *Intent-CSC MnS "Producer"* provides intent driven MnS for Communication Services. I

Intent-CSC MnS "Producers" receive the *expressed intent* and translate it to *Intent-CSP* or *Network Requirements*, then may consume Intent-CSP MnS(s) or Non-Intent MnS(s) for network to fulfil the intent-CSC.

- *Intent-CSP MnS "Producer"* provides *intent driven MnS for Network Services*.

Intent-CSP MnS "Producers" receive the intent and translate it to new Intents for *NOP* or *Network Requirements*, then may consume Intent-NOP MnS(s) or Non-Intent MnS(s) for NE to fulfil the Intent-CSP.

- *Intent-NOP MnS "Producer"* provides intent driven MnS for Network Equipment (NE). *Intent-NOP MnS "Producers"* receive the expressed intent, and translate it to detailed Network Requirements, then takes some internal actions to fulfil the intent-NOP.

Release 18 3GPP V18.1.1 (2023-09)

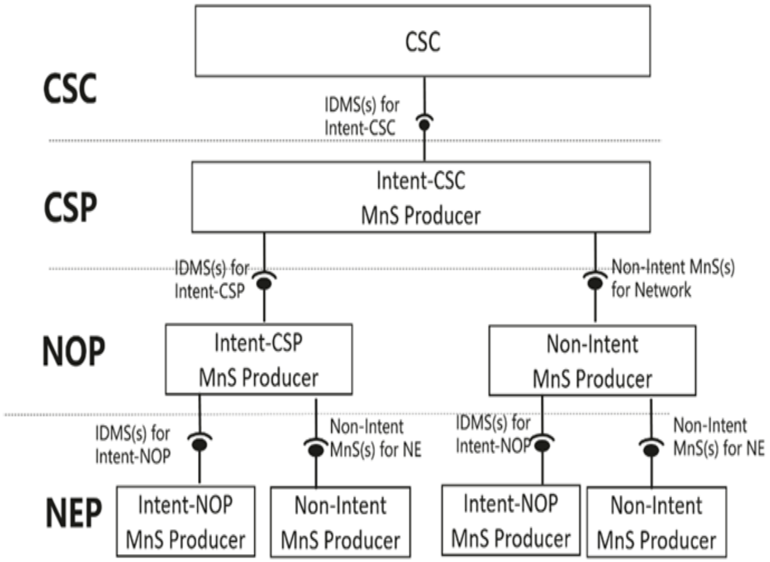


Figure: 5G System Intent-translation to satisfy Intent Communication Service Customer (CSC)

1.1.1 5GS Intent driven Management - 5

5GS Network Layer support for NF Service "Producer" - NF Service "Consumer" Interaction

In 5GS, a NF Service is one (1) *"Type of Capability"* exposed by an ***NF*** (*NF Service "Producer")* to other authorized **NF** (*NF Service "Consumer"*) through a *Service-based Interface (SBI*).

A Network Function (NF) may expose one (1) or more NF Services. The following Criteria specifyi NF Services:
- *NF Services* are derived from the *System Procedures* that describe *End-to-End (E2E) Functionality*, where applicable (see 5GS Architecture Procedure specification, Annex B drafting rules).

Services may also be defined based on *information flows from other 3GPP specifications.*

- 5G System Procedures can be described by a sequence of NF Service Invocations.

- NF Services may communicate "directly" between NF Service "Consumers" and NF Service "Producers", or "indirectly" via an SCP.

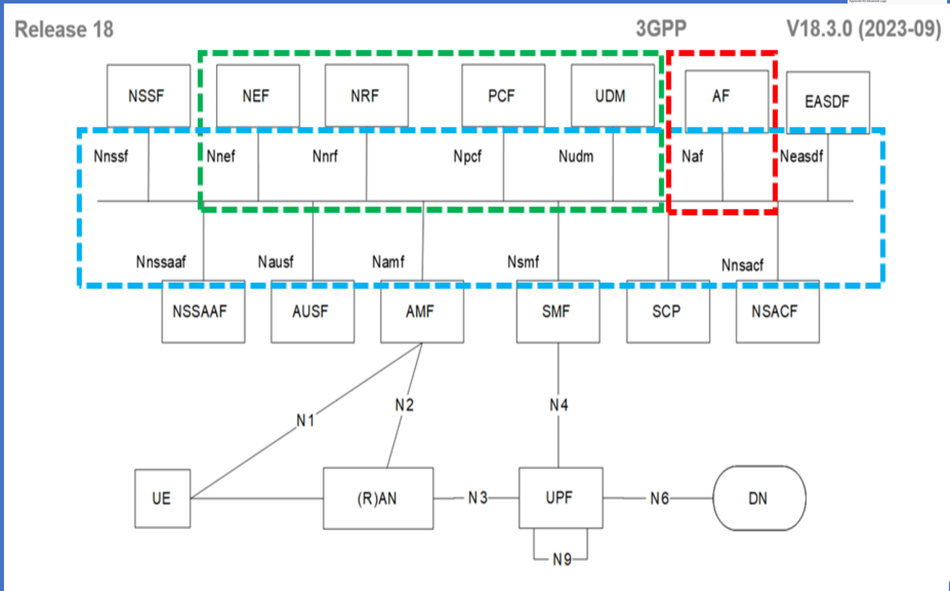


Figure: 5G System Non-Roaming Architecture

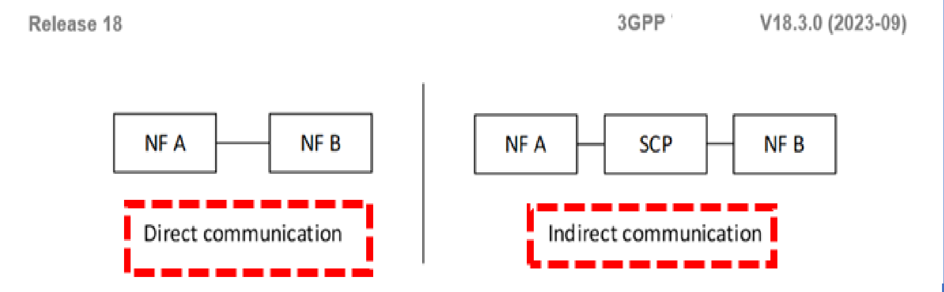


Figure: 5G System Architecture NF-to-NF Service Inter Communication

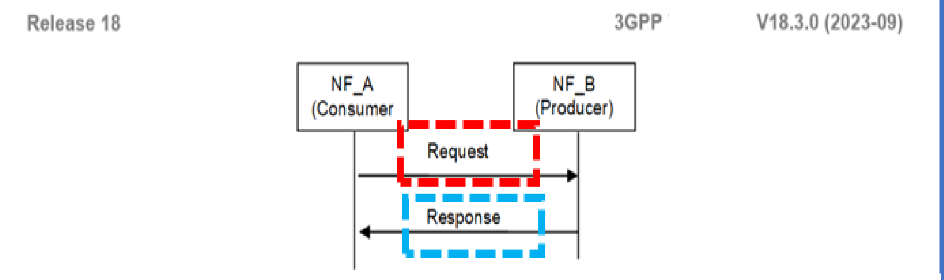


Figure: 5G System Architecture "Request-Response" NF Service Communication

5GS Network Layer support for: NF Service "Producer" - NF Service "Consumer" Interaction

The *E2E interaction* between (2) Network Functions, *"Consumer" and "Producer"*, within this *NF Service Framework* follows *two (2) Mechanisms*, irrespective of whether *"Direct Communication" or "Indirect Communication"* is used:

- *"Request-Response":* **A Control Plane (CP) NF_B** (*NF Service "Producer"*) is requested by another **Control Plane (CP) NF_A** (*NF Service "Consumer"*) to provide a certain *NF Service*, which either A) Performs an Action or B) Provides Information or C) Both.
NF_B provides an NF Service based on the request by NF_A.
In order to fulfil the request, NF_B may in turn "consume" NF Services from other NFs.

In "*Request-Response" Mechanism*, Communication is one to one between two NFs (Consumer and "Producer") and a one-time response from the producer to a request from the "Consumer" is expected within a certain timeframe.

The *NF Service "Producer"* may also *add a Binding Indication* in the Response, which may be used by the *NF Service "Consumer"* to select suitable *NF Service "Producer" instance(s)* for subsequent Requests.

For *indirect communication*, the *NF Service "Consumer"* copies the *Binding Indication* into the *Routing Binding indication*, that is included in subsequent requests, to be used by the *SCP* to discover a *suitable NF Service "Producer" instance(s).*

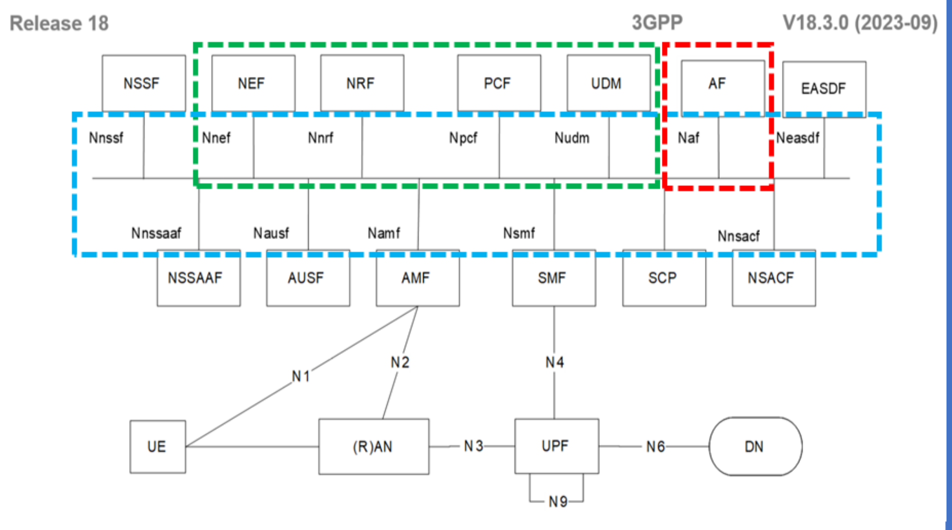


Figure: 5G System Non-Roaming Architecture

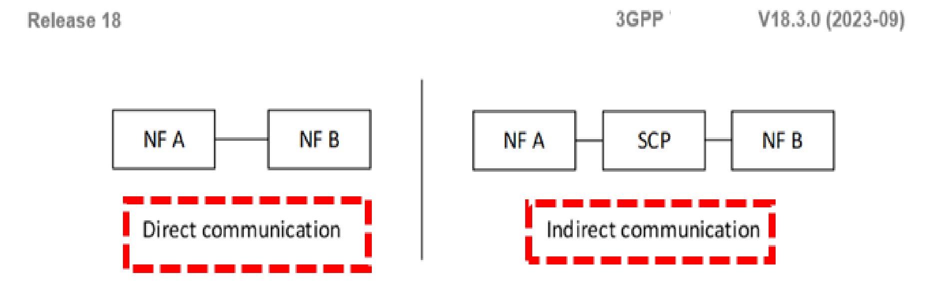


Figure: 5G System Architecture NF-to-NF Service Inter Communication

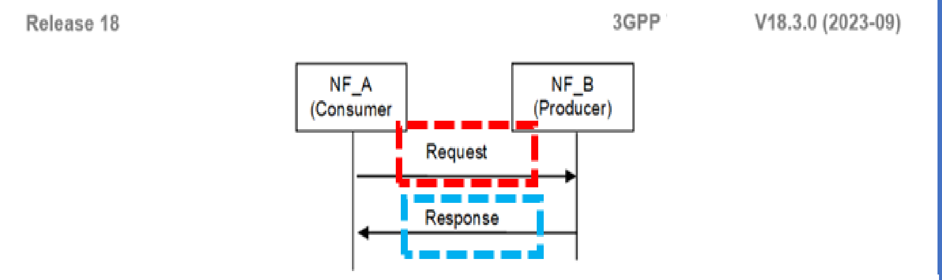


Figure: 5G System Architecture "Request-Response" NF Service Communication

5GS Network Layer support for: NF Service "Producer" - NF Service "Consumer" Interaction

Model A - *Direct Communication without NRF interaction*: Neither NRF nor SCP are used. "Consumers" are configured with "Producers' "NF Profiles" and directly communicate with a "Producer" of their choice.

Model B - *Direct Communication with NRF interaction*: "Consumers" do discovery by querying the NRF. Based on the discovery result, the *"Consumer"* does the selection. The *"Consumer"* sends the request to the selected *"Producer".*

Model C - *Indirect Communication* without delegated discovery: *"Consumers"* do discovery by querying the NRF. Based on discovery result, the *"Consumer"* does the selection of an *NF Set* or a specific *NF instance of NF set*. The *"Consumer"* sends the request to the SCP containing the address of the selected *Service "Producer"* pointing to a NF Service Instance or a set of NF service instances. In the latter case, the SCP selects an *NF Service instance*. If possible, the SCP interacts with NRF to get selection parameters such as Location, Capacity, etc. The SCP routes the request to the selected *NF Service "Producer" instance*.

Model D - *Indirect Communication* with delegated discovery: "*Consumers"* do not do any discovery or selection. The *"Consumer*" adds any necessary discovery and selection parameters required to find a suitable "Producer" to the Service Request. The SCP uses the request address and the discovery and selection parameters in the request message to route the request to a suitable *"Producer" Instance*. The SCP can perform discovery with an NRF and obtain a discovery result.

Release 18 3GPP V18.3.0 (2023-09)

Table: 5G System Architecture Communication Models for NF-to-NF Services Interaction

Communication between consumer and producer	Service discovery and request routing	Communication model
Direct communication	No NRF or SCP; direct routing	A
	Discovery using NRF services; no SCP; direct routing	B
Indirect communication	Discovery using NRF services; selection for specific instance from the Set can be delegated to SCP. Routing via SCP	C
	Discovery and associated selection delegated to an SCP using discovery and selection parameters in service request; routing via SCP	D

Release 18 3GPP V18.3.0 (2023-09)

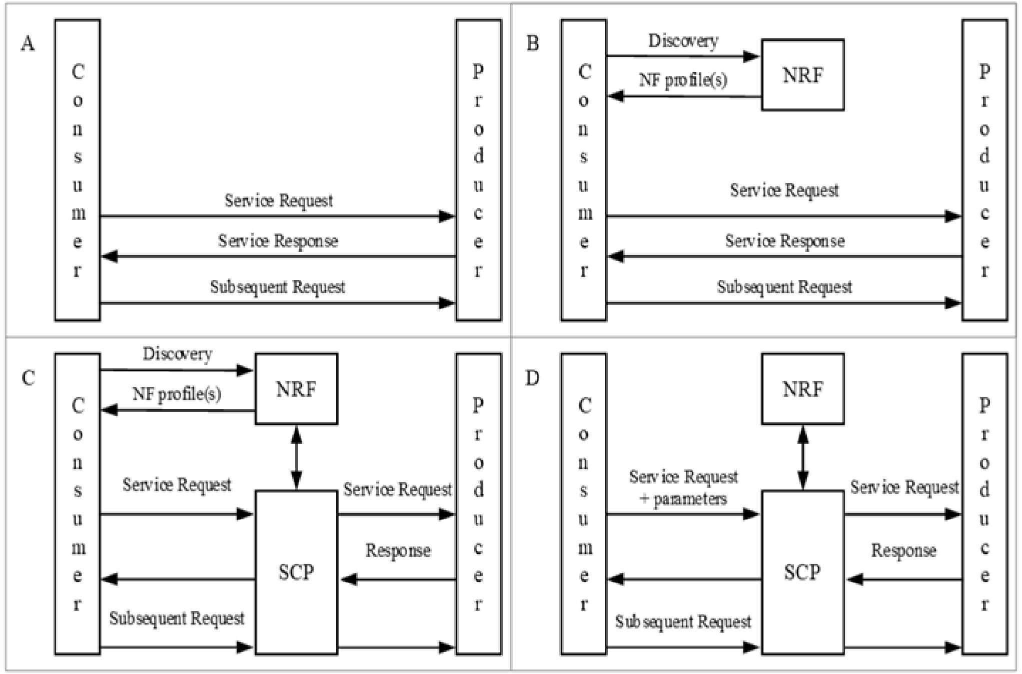


Figure: 5G System Architecture Communication Models for NF-to-NF Services Interaction

5GS Management Service (*MnS*) *"Producers", "Consumers" and "Exposure"*

The **Management Services** (*MnSs*) for a Mobile Network with or without Network Slicing may be produced by any Entity.

For example, it can be *Network Functions (NFs),* or Network Management Functions.

The ***Entity**** may provide ("*produce")* such Management Services as, for example, the
- Performance Management Services,
- Configuration Management Services and
- Fault Supervision Services

The **Management Services** (*MnSs*) can be "*consumed" by another Entity,* which may in turn "*produce" (expose) the Service to other Entities.*

The Figure shows an example of the *Management Service X*, which is initially "*produced" by the "Entity A*", which is an *NF*, then "*consumed" by another "Entity B"* which is a Network Management Function (*NMF*). Then "*Entity B"* in turn *exposes* it (the *same "Management Service X*" to the *"Entity C".*

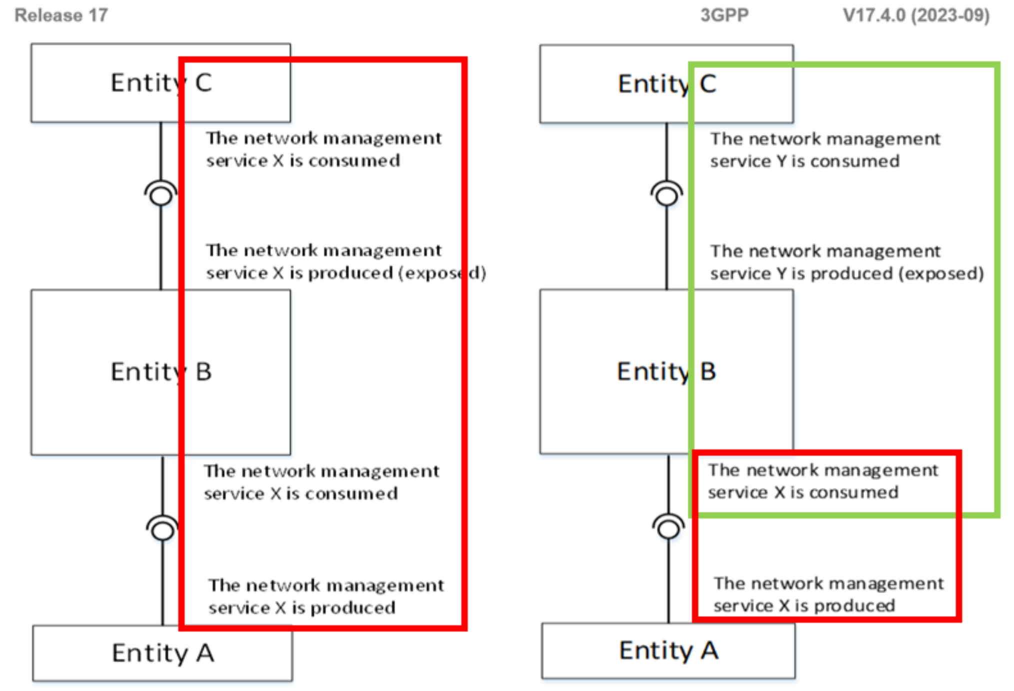


Figure: 5G System Management Architecture Framework Reference Model for Management Service (MnS) Producers, Consumers and Exposure

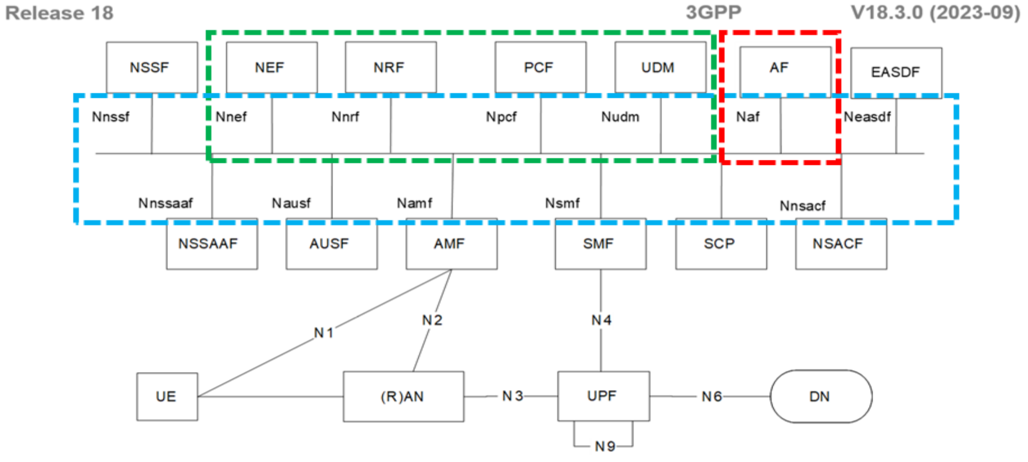


Figure: 5G System Non-Roaming Architecture

**Entity*"* *as being defined within the updated definition of "Context" used in 3GPP 5G System Architecture and ETSI*

1.1.1 5GS Intent driven Management Framework - 9

Intent containing an expectation for 5G Core Network (CN)

A *MnS "Consumer"* expresses Intent containing an expectation related to *5GC Network* to the intent driven *MnS "Producer."* In this scenario, *MnS "Consumer"* expresses its intent expectation which may include Location Information (e.g. Geographic Location, Data Center), Type of the Network (e.g. ToB (5G to Business)), included 5GC NF list (e.g. NF Types Information, Range of NF Instance ID), PLMN Information, Supported APN Information, Transport related Parameters (e.g. list of related End Point addresses information), and Target Network Capacity information (e.g. Number of PDU Session of Network, Number of Registered Subscribers, UL/DL Throughput).

Based on the Intent containing an expectation related for 5GC Network as received, the intent driven *MnS "Producer"* decides whether to deploy a new 5GC Network in the *specified Location* or to *re-use and modify an existing 5GC Network*.

If a "new" 5GC Network is to be delivered, the Intent driven *MnS "Producer"* translates the intent expectations into *appropriate 5GC Network Provisioning Operations*, this may include generation of Network Configuration Parameters (including 5GC Network/NFs Configuration Parameters and Transport Network Configuration Parameters) and triggering NS/VNF Creation procedure by interworking with ETSI NFV MANO.

If an existing 5GC Network is to be re-used, the intent driven MnS Producer identifies the potential *5GC Performance Issues* (e.g. Low Performance because of High Load) for the existing 5GC Network, modifies the 5GC NF Configuration Parameters if needed to satisfy the Performance Expectation Targets (this may also trigger Scaling Procedure by interworking with ETSI NFV MANO). Multiple interactions between the Intent MnS consumer and the Intent driven MnS producer may be needed based on the intent management capabilities (e.g. intent translation and intent feasibility check) provided by intent driven MnS producer.
The Intent driven MnS producer continuously monitors the 5GC performance (e.g. mean number of registered UE, mean number of created PDU session), and decides whether 5GC related expectation is satisfied .If the 5GC related expectation is not satisfied, the intent MnS producer identifies the potential 5GC performance issues and modifies the 5GC NF configuration parameters if needed to satisfy the performance expectation targets.
On a regular basis, the Intent driven MnS producer notifies MnS consumer about the fulfilment information of the intent.

Release 18 3GPP V18.1.1 (2023-09)

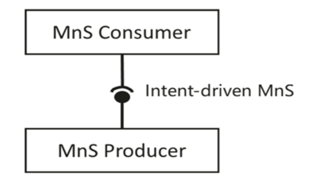


Figure: 5G System Intent-driven MnS

Release 18 3GPP V18.1.1 (2023-09)

YAML document example for Intent containing an expectation for delivering 5GC network


```
Intent:
  userLabel: '5GC_Network_Deliver'
  IntentExpectation:
    - expectationId: '1'
      expectationVerb: 'Deliver'
      expectationObjects:
        - objectType: '5GC_SubNetwork'
        - objectContexts:
            - contextAttribute: 'NfType'
              contextCondition: 'IS_ALL_OF'
              contextValueRange:
                - 'UPF'
            - contextAttribute: 'NfInstanceLocation'
              contextCondition: 'IS_ALL_OF'
              contextValueRange:
                 - 'Beijing, China'
            - contextAttribute: 'PLMN'
              contextCondition: 'IS_ALL_OF'
              contextValueRange:
                 - '46000'
            - contextAttribute: 'Tai'
              contextCondition: 'IS_ALL_OF'
              contextValueRange:
                 - '460000x65'
      expectationTargets:
        - targetName: 'MaxNumberofPDUsessions'
          targetCondition: 'IS_LESS_THAN'
          targetValueRange: '250000'
        - targetName: 'maxNumberofRegisteredsubscribers'
          targetCondition: 'IS_LESS_THAN'
          targetValueRange: '2500'
```


Release 18 3GPP V18.3.0 (2023-09)

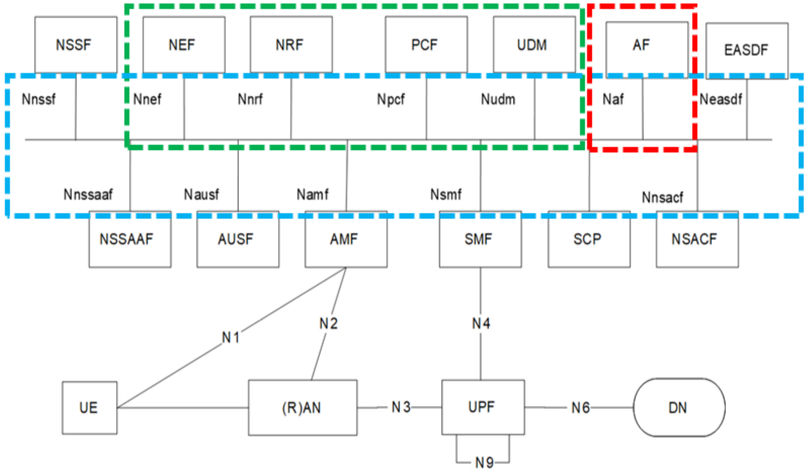


Figure: 5G System Non-Roaming Architecture

1.1.1 5GS Intent driven Management Framework - 10: Intent containing an expectation for delivering Radio Network and Service

Intent containing an expectation for delivering Radio Network

A MnS "Consumer" express intent containing an expectation for delivering a "Radio Network in the specified area to a MnS Producer.

In this scenario, MnS "Consumer" expresses its intent expectation for delivering a "Radio Network" to MnS "Producer", which may include "Coverage Area information" (e.g. Geographical Areas), Radio Setting Parameter Sets (e.g. Frequency information, Range of gNB Id, Range of PCI, Range of Cell Id, Range of nRTAC), Transport Setting Parameters (including OM Transport information (e.g. OMlocalIPaddress, OMremoteIPaddress, OMNextHopInfo) and NG Transport information (e.g. List of NGlocalIPaddress, List of NGremoteIPaddress)), and supported Network Capacity information (e.g. Maximum UE Number) and Network Performance information (e.g. UL/DL Throughput).

Based on the intent containing an expectation for Radio Network Provisioning received, MnS "Producer" identifies corresponding RAN NEs discovered in the specified Coverage Area, Analyses and generates the Configuration Parameters (including Radio Configuration Parameters and Transport Configuration Parameters) for each identified RAN NE and corresponding Cells, creates MOI(s) for each RAN NEs and Cells and configure the created MOI(s), and performs verification for configured RAN NEs to enable the Radio Network in the specified Area is successfully delivered and satisfy the received intent.

MnS "Producer" notifies MnS "Consumer" about the fulfilment information of the intent containing an expectation for delivering Radio Network after the verification is finished.

Intent containing an expectation for delivering a Radio Service

A *MnS Consumer* express intent containing an expectation for delivering *Radio Service (Radio Network as Service)* in the *specified Area* to a *MnS Producer. MnS Consumer* expresses its intent containing an expectation for delivering a *Radio Service to MnS Producer*, which may include Coverage Area Information (e.g. Geographical Areas), and *supported Service Capacity information* (e.g. *maxNumberofUEs, activityFactor*) & *Service Performance Information* (e.g. *ServiceType,* dLThptPerUEPerSubnet, uLThptPerUEPerSubnet).

NOTE: The Slice agnostic Parameters in RAN Slice Profile can be used for Service Capacity Information and Service Performance Information. MnS Producer decides to use Radio Network with Slicing or Radio Network without Slicing to support the intent:

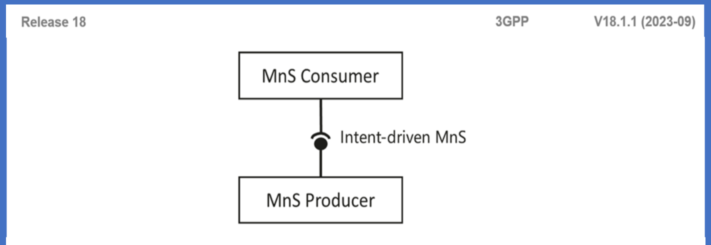
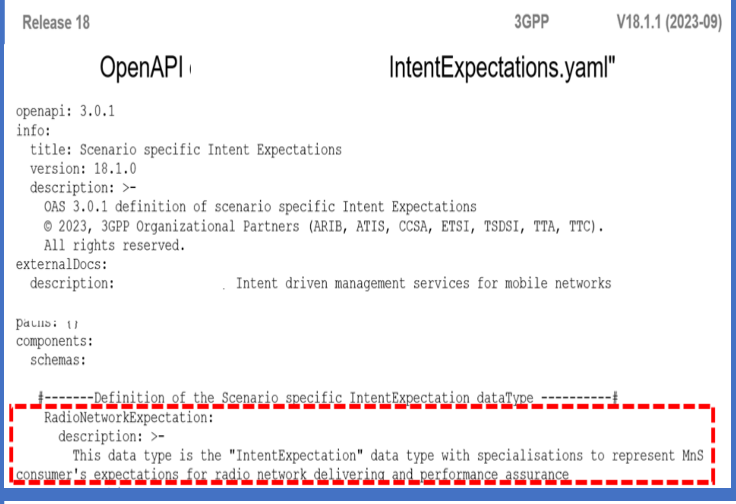


Figure: 5G System Intent-driven MnS


Release 18 3GPP V18.1.1 (2023-09)

OpenAPI IntentExpectations.yaml"

```
openapi: 3.0.1
info:
  title: Scenario specific Intent Expectations
  version: 18.1.0
  description: >-
    OAS 3.0.1 definition of scenario specific Intent Expectations
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
externalDocs:
  description: Intent driven management services for mobile networks
paths: {}
components:
  schemas:

   #-------Definition of the Scenario specific IntentExpectation dataType ----------#
    RadioNetworkExpectation:
      description: >-
        This data type is the "IntentExpectation" data type with specialisations to represent MnS
consumer's expectations for radio network delivering and performance assurance
```

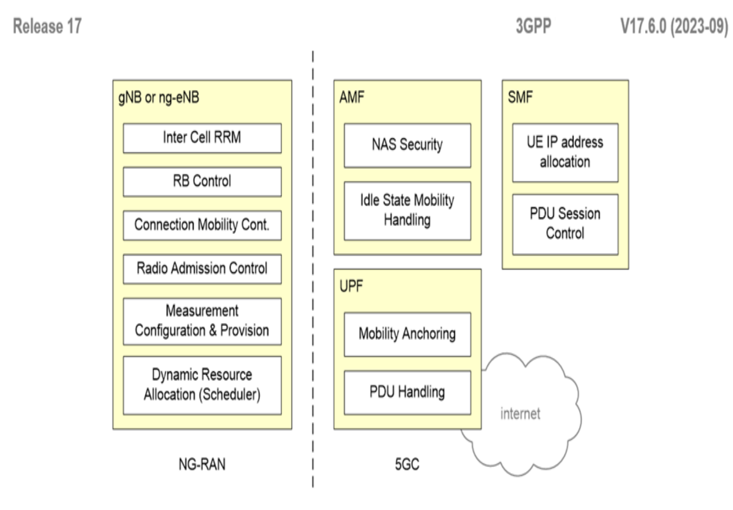


Figure: 5GS Architecture Functional Split between NG-RAN and 5G Core

1.1.1 5GS Intent driven Management Framework - 11

Intent containing an expectation for delivering a Service at the "Edge".

The MnS "Consumer", express the Intent containing an expectation for delivering a *Service at the "Edge"* of the Network.

The Intent Expectation for a Service includes Service Type (eMBB, URLLC, MIoT, V2X, HMTC, HDLLC), Service Requirements (Number of Concurrent Subscribers and Number of Concurrent Sessions), Service Availability and the Target Location.

REQ-Intent_Deploy_Net-CON-1 the intent driven MnS shall have Capability enabling *Authorized MnS "Consumer*" to express Intent containing an expectation for delivering a Service at the Edge of the Network to "*MnS Producer*".

Intent containing an Expectation on Coverage Performance to be assured

MnS consumer expresses its intent containing an expectation on Coverage Performances to be assured in the specified Areas to NEP, which may include Area Information (e.g. Geographical Area), RATs (e.g. NR only, EUTRAN only, or all RATs), Coverage Targets (e.g. Target Average RSRP, Target Weak Coverage Ratio).

Based on the intent containing an expectation on Coverage Performance to be assured received, *MnS Producer* collects and analyses Corresponding Coverage related Data (e.g. RSRPs of the Serving Cell and Neighbour Cells *reported by each UE with Anonymous id (e.g. C-RNTI)* and Location Information in the MDT Reports of corresponding RAN NEs in the Specified Areas, identifies the potential coverage issues which will impact the coverage targets satisfaction, analyses the identified coverage issue and corresponding solutions, evaluates, decides and adjusts the coverage configuration parameters. *The Artificial intelligence (AI) or Machine Learning* (*ML) technologies* may be used in above workflow to satisfy the intent, e. g. online iteration optimization Technologies may be used to selecting the best coverage configuration parameters rapidly.
MnS Producer continuously monitors the Coverage Performance (e.g. Weak Coverage Ratio, Average RSRP) for the Specified Area, and decides whether coverage targets described in the intent is satisfied. If not satisfied, NEP iteratively executes above workflows (including collect, identification, analysis, evaluation, decision and adjustment) to fulfil the coverage targets.
MnS Producer may notify *MnS Consumer* about the intent fulfilment information, including Coverage Performance for the specified area (e.g. weak coverage ratio, coverage hole ratio, average RSRP) which enables *MnS Consumer* to monitor the intent containing an expectation on coverage performance to be assured. *MnS Consumer* may also request to MnS producer to report the intent fulfilment information.

Release 18 3GPP V18.1.1 (2023-09)

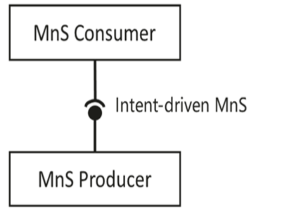


Figure: 5G System Intent-driven MnS

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

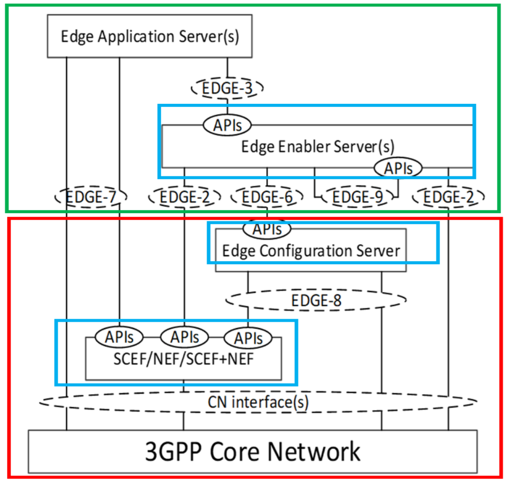


Figure: 5G Architecture Capability Exposure APIs for enabling Edge Applications

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

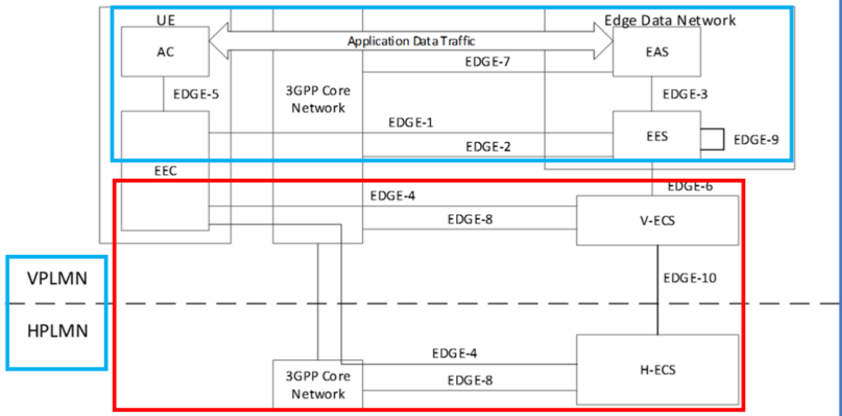


Figure: 5G Architecture for enabling Edge Applications (EDGEAPP) Services Roaming: Local breakout (LBO) for UE AC towards VPLMN EAS and EES over EDGE-1 and Home-Routed for UE EEC to H-ECS in HPLMN via V-ECS in VPLMN over EDGE-4

Annex 5 - 3GPP 5G Advanced Release specification for NPNs/SNPNs (Non-Public Network(s)/Stand-alone NPNs)

Support of Non-Public Network (NPN) as a Network Slice (SST) of a PLMN

The PLMN Operator can provide Access to an NPN by using Network Slicing Mechanism(s).

NOTE: *Access to PLMN Services can be supported in addition to PNI-NPN Services, e.g. based on different S-NSSAI/DNN for different services.*

The following are some considerations in such a PNI-NPN Case:
1. The UE has Subscription & Credentials for the PLMN;
2. The PLMN & NPN SP have an Agreement of where the NPN Network Slice (SST) is to be deployed (i.e. in which TAs of the PLMN &, optionally including Support for Roaming PLMNs);
3. The PLMN Subscription includes Support for Subscribed S-NSSAI to be used for the NPN;
4. The PLMN Operator can offer possibilities for the NPN SP to manage the NPN Network Slice;
5. When the UE registers the 1st time to the PLMN, the PLMN can configure the UE with URSP including NSSP associating Applications to the NPN S-NSSAI (if the UE also is able to access other PLMN Services);
6. The PLMN can configure the UE with "Configured NSSAI" for the Serving PLMN;
7. The PLMN & NPN can perform a Network Slice specific Authentication & Authorization using additional NPN Credentials;
8. The UE follows the logic as defined by 3GPP for Network Slicing in 5GS Architecture;
9. The Network selection Logic, Access Control etc. are following the principles for PLMN selection;
10. The PLMN may indicate to the UE that the NPN S-NSSAI is rejected for the RA when the UE moves out of the coverage of the NPN Network Slice. However, limiting the availability of the NPN S-NSSAI would imply that the NPN is not available outside of the Area agreed for the NPN S-NSSAI, e.g. resulting in the NPN PDU Sessions being terminated when the UE moves out of the coverage of the NPN Network Slice. Similarly access to NPN DNNs would not be available via non-NPN cells.
11. In order to prevent access to NPNs for authorized UE(s) in the case of Network Congestion/ Overload & if a dedicated S-NSSAI has been allocated for an NPN, the Unified Access Control (UAC) can be used using the Operator-defined Access Categories with Access Category Criteria type as defined in 5GS Architecture CP set to the S-NSSAI used for an NPN.
12. ***If NPN isolation is desired, it is assumed that a dedicated S-NSSAI is configured for the NPN & that the UE is configured to operate in Access Stratum Connection Establishment NSSAI Inclusion Mode "a", "b" or "c", see 5GS Architecture clause, such that NG-RAN receives Requested NSSAI from the UE and it can use the S-NSSAI for AMF selection.***

Release 18 3GPP V18.2.0 (2023-06)

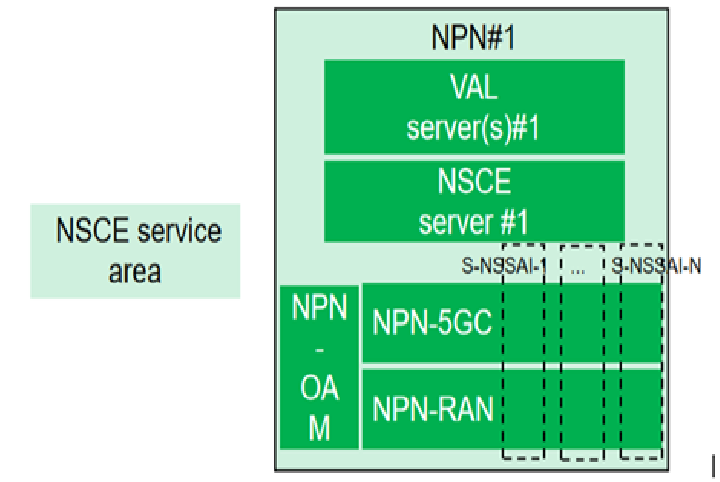


Figure: 5G System Illustration of Non-Public Network (NPN) Network Slice Capability Enablement (NSCE) deployment

Release 18 3GPP V18.2.0 (2023-06)

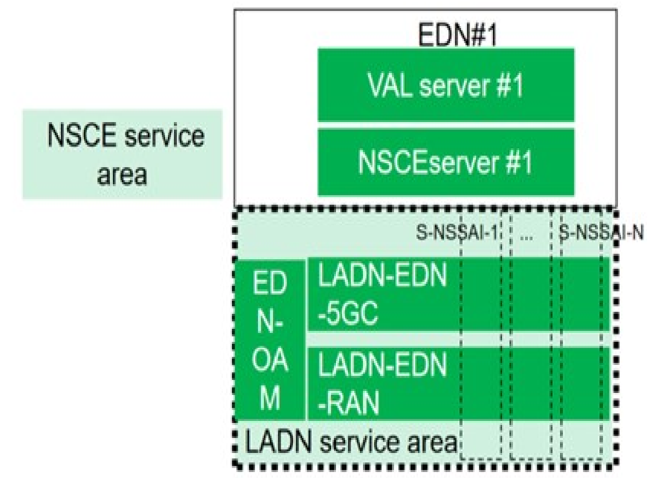


Figure: 5G System Illustration of Edge Network Slice Capability Enablement (NSCE) deployment

5G NPNs/SNPNs 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

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

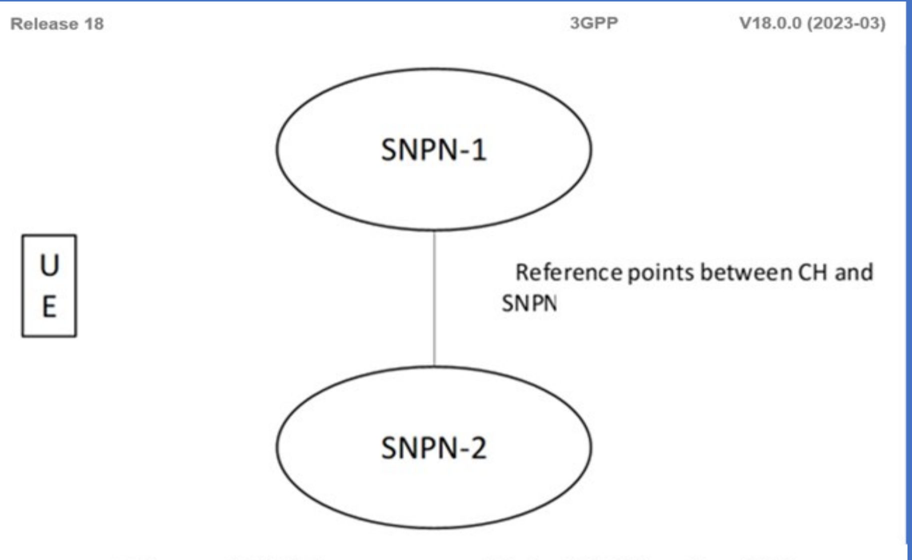


Figure: 5G UE accesses multiple SNPNs using CH

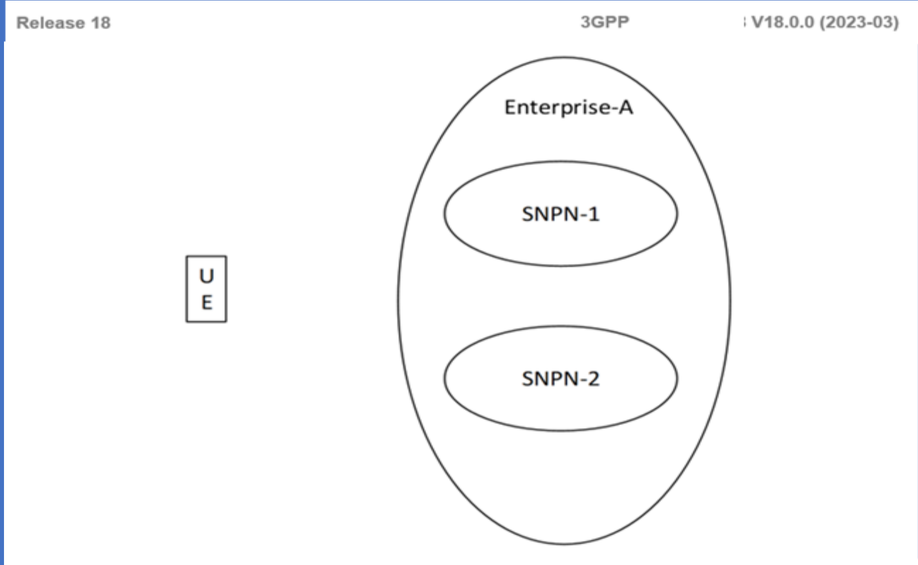


Figure: 5G UE accesses multiple SNPNs belonging to the same Administrative Entity

3GPP 5G Advanced Release specification for PINs (Personal IoT Network(s)) - 1

PIN Definitions of terms and abbreviations

Personal IoT Network: A configured and managed group of PIN Element that are able to communicate each other directly or via PIN Elements with Gateway Capability (PEGC), communicate with 5G network via at least one PEGC, and managed by at least one PIN Element with Management Capability (PEMC).

PIN Element (PINE): A UE or non-3GPP device that can communicate within a PIN (via PIN "direct" connection, via PEGC, or via PEGC and 5GC), or outside the PIN via a PEGC and 5GC.

PIN Element with Gateway Capability: A PIN Element with the ability to provide connectivity to and from the 5G network for other PIN Elements, or to provide relay for the communication between PIN Elements.

PIN Element with Management Capability: A PIN Element with capability to manage the PIN.

NOTE: A PIN Element can have both PIN Management Capability and Gateway Capability.

PINE-to-PINE communication: communication between two PINEs which may use PINE-to-PINE direct communication or PINE-to-PINE indirect connection.

PINE-to-PINE direct connection: the connection between two PIN Elements without PEGC, any 3GPP RAN or core network entity in the middle.

PINE-to-PINE indirect connection: the connection between two PIN Elements via PEGC or via UPF.

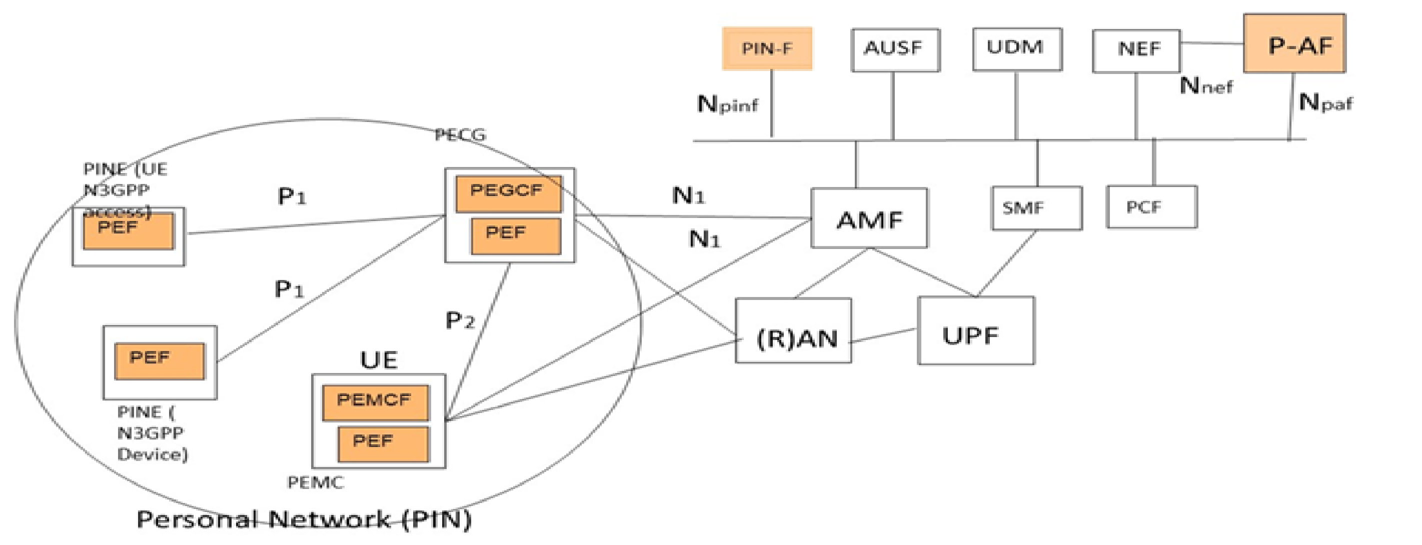
PINE-to-PINE routing: the traffic is routed by a PEGC between two PINEs, the two PINEs direct connect with the PEGC via non-3GPP access.

PINE-to-Network routing: the traffic is routed by a PEGC between PINE and 5GS, the PINE direct connects with the PEGC via non-3GPP access separately.

Network local switch for PIN: the traffic is routed by UPF(s) between two PINEs, the two PINEs direct connect with two PEGCs via non-3GPP access separately.

Abbreviations

PIN	Personal IoT Networks
PINE	PIN Element
PEGC	PIN Elements with Gateway Capability
PEMC	PIN Elements with Management Capability
P2P	PINE-to-PINE
P2N	PINE-to-Network
NLSP	Network Local Switch for PIN



5G System PIN Solution Reference Architecture

- Management of PIN,
- Access of PIN via PIN Element (PINE) with Gateway Capability (PEGC), and
- Communication of PIN (e.g. PINE (e.g. a UE) communicates with
  - other PINE (UE) "directly" or
  - via PEGC or
  - via PEGC and 5GS.

- Security related when identifying PIN and the PINE when:
  - How to identify PIN and the PINEs in the PIN at 5GC level to serve for Authentication& Authorization
  - Management as well as Policy and Routing Control enforcement:

- Management of a PIN.
- PIN & PINE Discovery

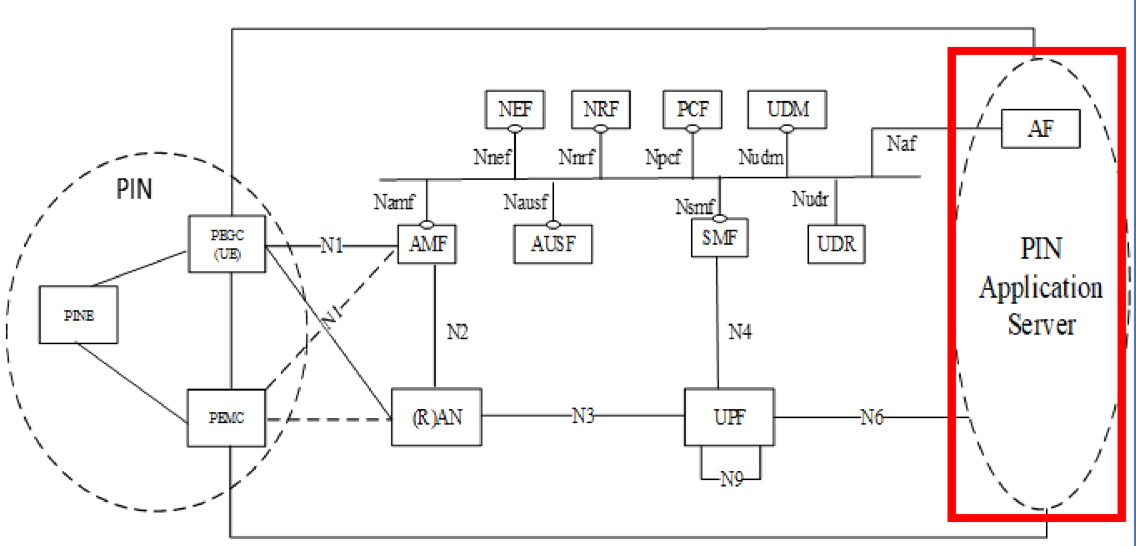


Figure: 5GS PIN Personal IoT Network Reference Architecture

A **Personal IoT Network (PIN)** in **5GC** consists of:

- 1 (one) or more Devices providing Gateway/Routing Functionality known as **the PIN Element with Gateway Capability (PEGC)**, and

- 1 (one) or more Devices providing PIN Management Functionality known as the **PIN Element with Management Capability (PEMC)** to manage the Personal IoT Network; and

- Device(s) called the PIN Elements (PINE). A PINE can be a non-3GPP Device.

The PIN can also have a PIN Application Server (AS) that includes an AF (Application Function) functionality.

The AF can be deployed by Mobile Operator or by an Authorized Third (3rd) Party.

When the AF is deployed by 3rd Party, the interworking with 5GS is performed via the NEF.

The PEMC and PEGC communicates with the PIN Application Server (AS) at the Application Layer over the User Plane. The PEGC and PEMC can communicate with each other via "Direct" Communication

Only a 3GPP UE can act as PEGC and/or PEMC.

PINs and CPNs (Customer Premises Networks)

Personal IoT Networks (PINs) and Customer Premises Networks (CPNs) provide local connectivity between UEs and/or Non-3GPP Devices.

The CPN via an eRG, or PIN Elements (PINEs) via a PIN Element with Gateway Capability (PEGC) can provide access to 5G Network Services for the UEs and/or Non-3GPP Devices on the CPN or PIN.

CPNs and PINs have in common that, in general, they are:
- owned, Installed and/or (at least partially) Configured by a Customer of a Public Network Operator.

A Customer Premises Network (CPN) is a Network located within
- a Premises (e.g. a Residence, Office or Shop).
- via an evolved Residential Gateway (eRG), the CPN provides connectivity to the 5G Network. The eRG can be connected to the 5G Core Network via wireline, wireless, or hybrid access.
- A *Premises Radio Access Station* (**PRAS**) is a Base Station installed in a CPN. Through the PRAS, UEs can get Access to the CPN and/or 5G Network Services.

The **PRAS** can be configured to use
- Licensed,
- Unlicensed, or
- Both Frequency bands.

Connectivity between the **eRG** and the **UE**, **non-3GPP Device**, or **PRAS** can use any suitable **Non-3GPP Technology** (e.g. **Ethernet, optical, WLAN).**

A Personal IoT Network (PIN) consists of **PIN Elements (PINEs)** that communicate using PIN
- "Direct Connection" or
- "Direct Network Connection

and is managed locally using a PIN Element (PINE) with Management Capability (PEMC).

Examples of PINs include Networks of Wearables and Smart Home / Smart Office Equipment.

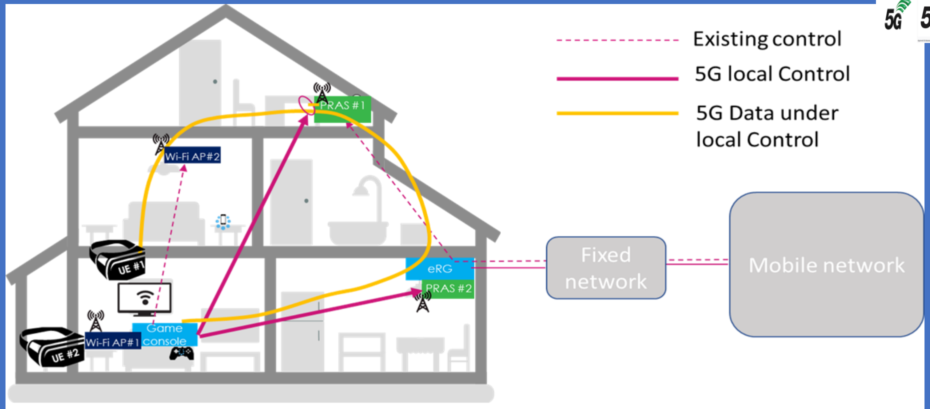


Figure: 5G Local Control of Premise Radio Access Stations (PRASs) for UE to access CPN Device

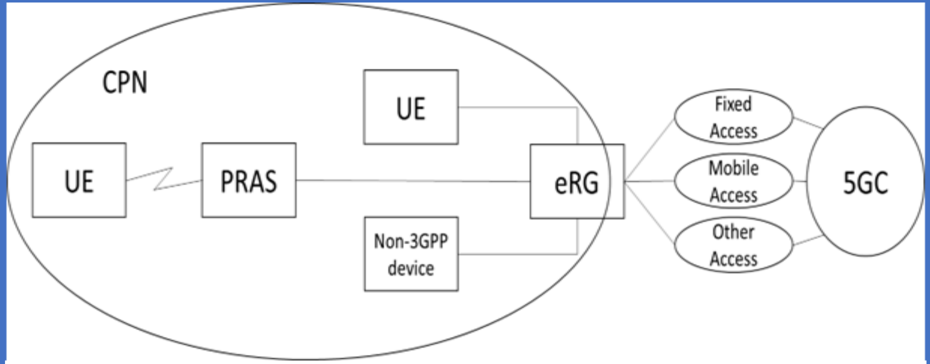


Figure: Customer Premises Network (CPN) connected to 5GC


Vodafone unveils Open RAN 5G network-in-a-box

Feb 17, 2023

Vodafone's Yago Tenorio shows off the operator's 5G network-in-a-box.

- Vodafone has unveiled a new mini 5G network the size of a Wi-Fi router
- It has a core and radio software, a mini computer and a software-defined radio chipset
- It is just a prototype currently
- But if offered as a product could revolutionise the 5G private network sector

A Current Smart Home IoT Deployment Example

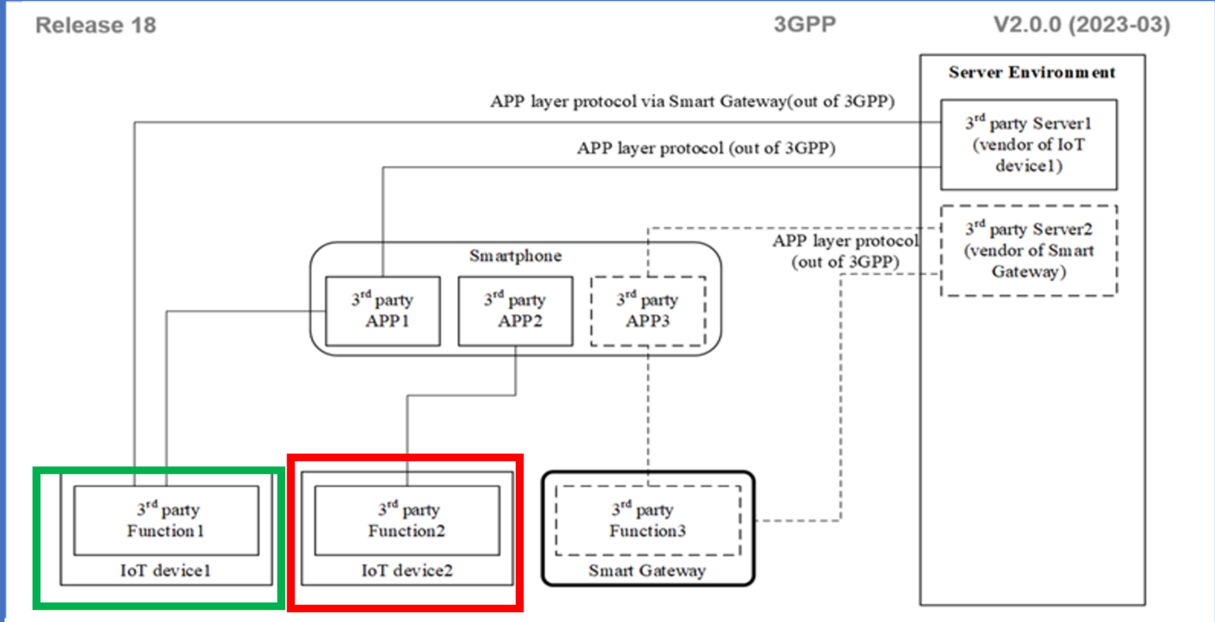


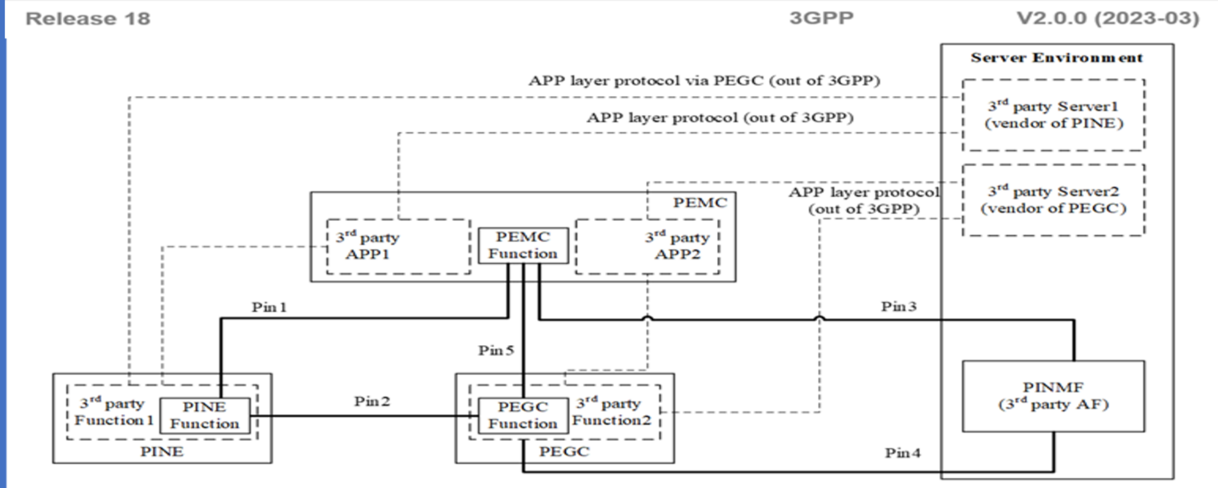
Figure: Example of Current IoT Smart Home Deployment

The IoT Device1 is initially discovered by a Smartphone using the 3rd Party APP1 installed in the Smartphone, and then the Smartphone is able to connect with the IoT Device1 assisted by the 3rd Party APP1.

The 3rd Party APP1 is developed by the Vendor of the IoT Device1. The IoT Device1 is able to visit the 3rd Party Server1 over Internet via the Smart Gateway, and the 3rd Party APP1 also can visit the 3rd Party Server1 over Internet, so that the Smartphone is able to control the IoT Device1 via internet assisted by the 3rd Party Server1.

The IoT Device2 is manufactured by a different Vendor from that of the IoT Device1, and is not able to be controlled by a Smartphone via Internet.

A Deployment Example of the PIN that the PINMF can be a NF, Trusted AF, or 3rd Party AF.



NOTE 1: The PEMC Function instance can be a function in a 3rd party APP, a standalone APP, or middleware,

Figure: 5G PIN Deployment Functions Example

For the case of NF/trust AF, one Operator only has one (1) PINMF, the PEMC can use pre-configured information for PIN Service Operations, e.g. FQDN of the Operator's PINMF.

For the Case of 3rd Party AF, there may be multiple PINMFs, which one is used determines by the User, and the Serving PINMF should register itself for the User to handle the PIN Service Operations.

If both PINMF as NF/trust AF and PINMF as 3rd party AF are deployed, which one is used is determined by PEMC implementation.
In the deployment example, the 3rd party APP and 3rd party Function can assist the initial discovery and initial direct connection setup between PINE/PEGC and PEMC without user input information.

An example of the use case with the deployment example is as following:

Intent containing an expectation for End-to-End (E2E) Network Optimization

MnS "Consumer" expresses its intent containing an Intent Expectation with *targets on the whole Network including RAN and Core*.

The intent may for example be for optimization of the *Network Resources*, i.e. the intent expectation captures the *Objectives for an Entity** that *undertakes Optimization for the Network.*

The expectation may be termed as *Network Resources Expectation*. The Network Resources Expectation Targets may express the desired Performance Optimization Outcomes.

Depending on the stated targets, the *MnS Producer* may as such configure one (1) or more Optimization Functions to achieve the desired targets.

The Network Optimization expectation targets may for example be *End-to-End (E2E) KPI Targets* that the optimization is required to achieve.

The Network Optimization expectation may include relative prioritizations of the different targets which indicate the relative interests of the *Intent MnS Consumer* on the different Network Attributes.

Release 18 3GPP V18.1.1 (2023-09)

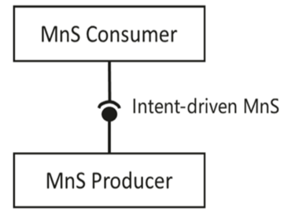


Figure: 5G System Intent-driven MnS

Release 18 3GPP V18.1.1 (2023-09)

OpenAPI specification

OpenAPI ProvMnS.yaml"

OpenAPI definition of the provisioning MnS which includes the provisioning MnS operations and the provisioning MnS notifications

OpenAPI IntentNrm.yaml"

```
openapi: 3.0.1
info:
  title: Intent NRM
  version: 18.1.0
  description: >-
    OAS 3.0.1 definition of the Intent NRM
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

  description:              Intent driven management services for mobile networks

paths: {}
components:
  schemas:

   #-------Definition of generic IOCs ----------#

    SubNetwork-Single:
      allOf:
      - $ref:         _GenericNrm.yaml#/components/schemas/Top'
```

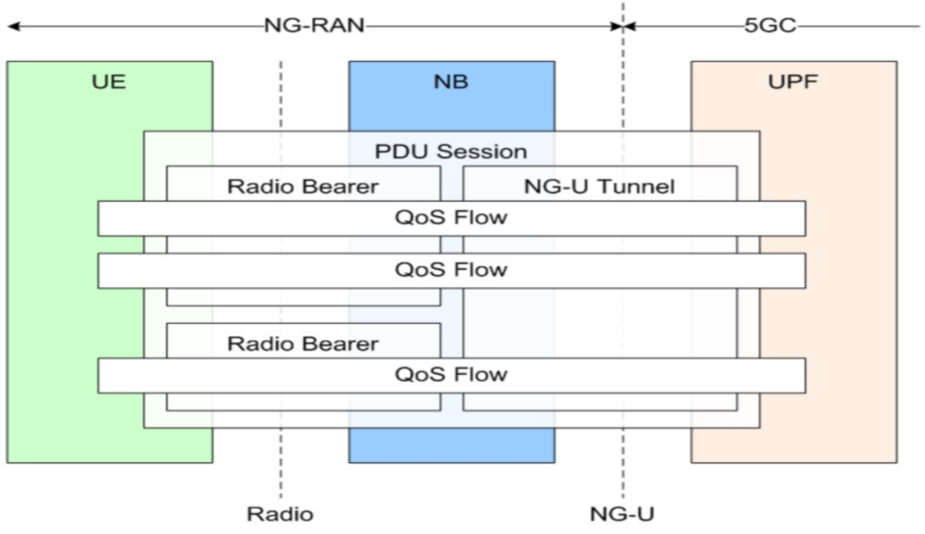


Figure: 5G CN NG-RAN Bearer Services QoS Architecture

**Entity"* as being defined within the updated definition of "Context" used in 3GPP 5G System Architecture and ETSI*

PlantUML source code

Procedures for intent management

Create an intent

```
@startuml
title "[Create an intent]"
actor "MnS Consumer" as MnS_Consumer
participant "MnS Producer" as MnS_Producer
Collections "ManagedEntity" as ManagedEntity
MnS_Consumer -> MnS_Producer: 1. Request to create an intent instance (list of attributes of intent
IOC)
MnS_Producer -> MnS_Producer: 2. Create and configure intent MOI
MnS_Producer -> MnS_Consumer: 3. Response for create an intent instance
MnS_Producer -> MnS_Producer: 4. Perform the feasibility check of the intent instance

alt feasibility check result is "Feasible"
  Ref over MnS_Producer, ManagedEntity: 5a. Perform service or network management tasks
  loop
   Ref over MnS_Producer, ManagedEntity: 6. Evaluate intent fulfilment
     opt
  Ref over MnS_Producer, ManagedEntity: 7. Adjust to fulfil the intent requirement
     end
  end
  MnS_Producer -> MnS_Consumer:8. Notify of intent report Information

else feasibility check result is "inFeasible"
  MnS_Producer -> MnS_Consumer: 5b. Notify of intent infeasibile information
end

hide footbox
@enduml
```

Summary: 5G System Intent Driven Management Services for 5G Mobile Networks

The current 5G Networks brings more Operational complexities, & the **Telecom System** need to be able to adapt their Operation to the **Business Objectives** of the Operator as well as expectations of Customer, which is driving Customer to shift the focus from "How" to "What". An "Intent-driven System" will be able to "learn the behaviour of Networks & Services" & allows a Customer to provide the "Desired State", without detailed Knowledge of "How" to get to the desired state. The "Intent-driven Management" is introduced to reduce the complexity of Management without getting into the intricate detail of the underlying Network Resources. An "Intent" is typically understandable by Humans, & also needs to be interpreted by the Machine without any ambiguity. The "expectations" expressed by an "Intent" is agnostic to the underlying System implementation, Technology & Infrastructure. "Area" can be used as "Managed Object" in the expectations expressed by an "Intent" to achieve System Implementation, Technology & Infrastructure Agnostic. Intent from Communication Service Customer (CSC) enables CSC to express which properties of a Communication Service (CS) the CSC may request from CSP without knowing "how" to do the detailed management for CS, e.g., Intent-CSC can be 'Enable a V2X CS for a Group of Vehicles in certain time'.

The fundamental building block of the *Service Based Management Architecture* (**SBMA**) is the *Management Service* (**MnS**). A **MnS** is "a Set of Offered Capabilities for Management & Orchestration of Network & Services. A **MnS** provided by an "**MnS Producer"** can be consumed by any Entity with appropriate Authorisation & Authentication. The **Management Services (MnSs)** *can be consumed by another **Entity,** which may in turn produce (**expose**) the Service to other **Entities***. Figure below shows an example of the MnS "X", which is initially *produced by* the ***Entity A,*** which is an **NF**, then *consumed* by another **Entity B** which is a Network Management Function (**NMF**). Then **Entity B,** in turn, exposes it to the "**Entity C".** An "MnS Producer" offers its Services via a Standardized Service Interface composed of individually specified MnS Components. If the "MnS Consumer" & the "MnS Producer" to be accessed are inside the same Domain, Authentication Service "Producer" may be deployed at Domain Level to support Authenticating the "MnS Consumer" explicitly or implicitly. If the "MnS Consumer & the "MnS Producer" to be accessed are in the different Domain, Authentication Service "Producer" is deployed in a Centralized manner to support Authenticating the "MnS Consumer" explicitly or implicitly.

The intents may be fulfilled by utilizing multiple Mechanisms including among others: Rule-based, Closed-loop & AI/ML based. These Mechanisms can be combined in Solutions of various Complexity, ranging from a simple approach Rule-based, to more elaborate solutions combining AI/ML, Closed-loop Automation to ensure the fulfilment of intents.

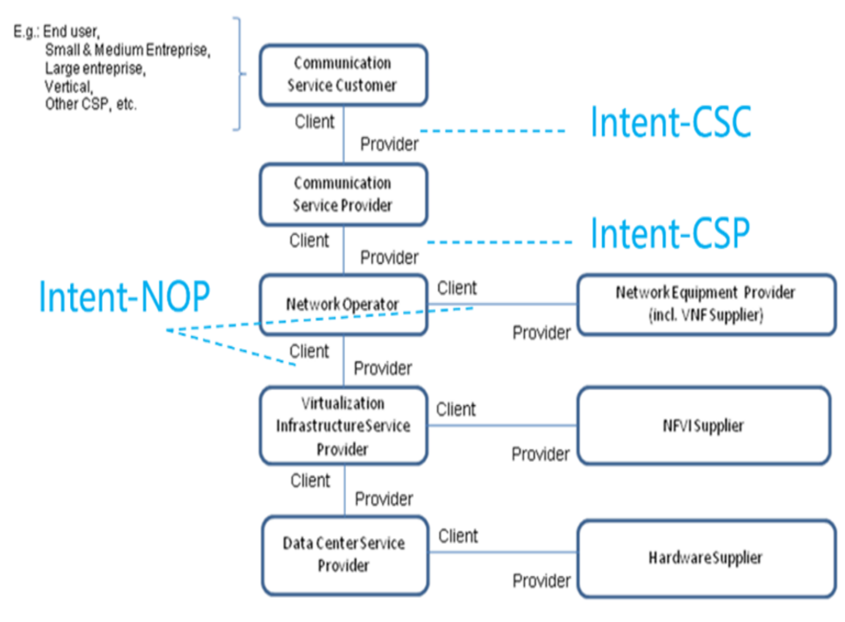


Figure: 5G High-level Model of different kind of Intents expressed by 5G different Roles

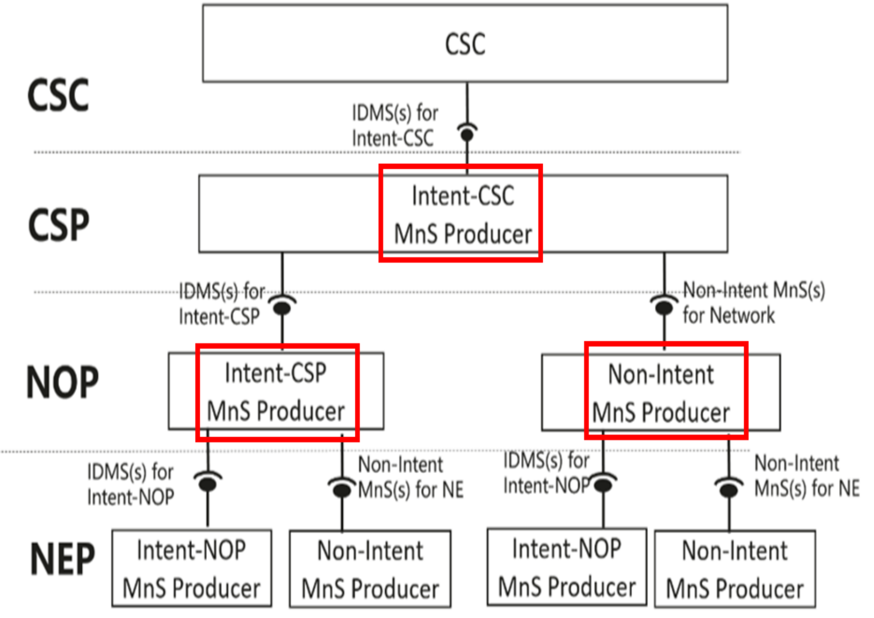


Figure: 5G Potential way to satisfy Intent-CSC originating from CSC

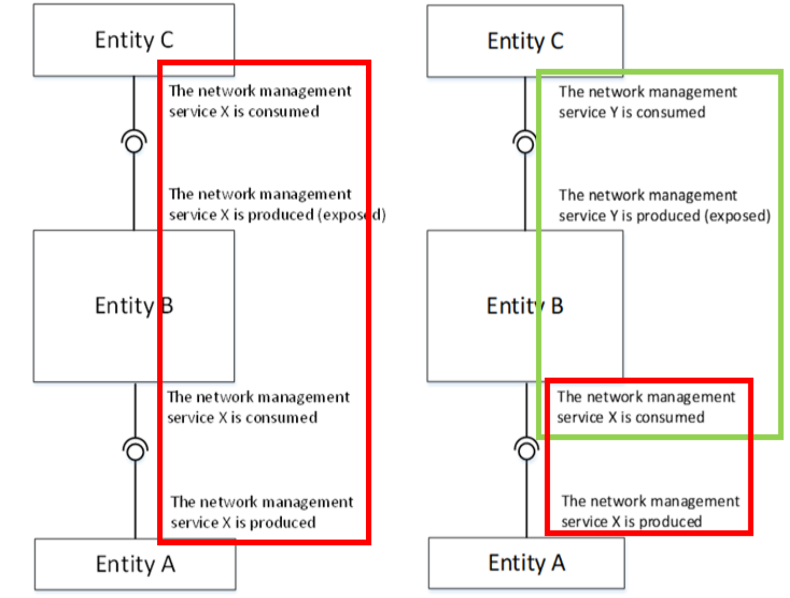


Figure: 5G Architecture Reference Model for Management Service (MnS) Producers, Consumers and Exposure

5G System Data Collection and Analytics Reference Architecture - 1

5GS Architecture specification 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 Data Collection AF (*DCAF*) may support 5G Architecture Common API Framework (CAPIF) to provide APIs to other Applications (i.e. API Invokers), as defined in 5GS Architecture.

NOTE 1: It is presumed that the User (Resource Owner) has granted "Consent" for its UE Data to be collected, reported and subsequently exposed through interactions with the MNO or the Application Service Provider (ASP), and via any applicable SLA between the MNO and Application Service Provider (ASP).

See on the next slide the Table showing the set User Consent for Data Collection client API Method as specified in 5GS Architecture.

NOTE 2: *The Collection, Reporting and Exposure of Location-based UE Data is expected to comply with Regional Regulatory Requirements and may be further limited by MNO Policy.*

This reference architecture is intended to be instantiated in Domain-specific ways to suit the needs of different features of the 5G System as e.g. the Reference Architecture may be instantiated separately in **different Slices (SST) of a Network.**

Each type of UE Data subject to Collection, Reporting and subsequent Event Exposure in the 5G System is associated with a Logical UE Data domain.

Each such UE Data Domain is associated with a Domain Owner – either the 5G System itself (embodied in a particular deployment by an MNO) or the Application Service Provider (ASP).

Precedence rules on the Exposure (and consequent Collection and Reporting) of UE Data vis-à-vis conflicts between ASP Provisioning Information and System pre-configuration by the MNO or

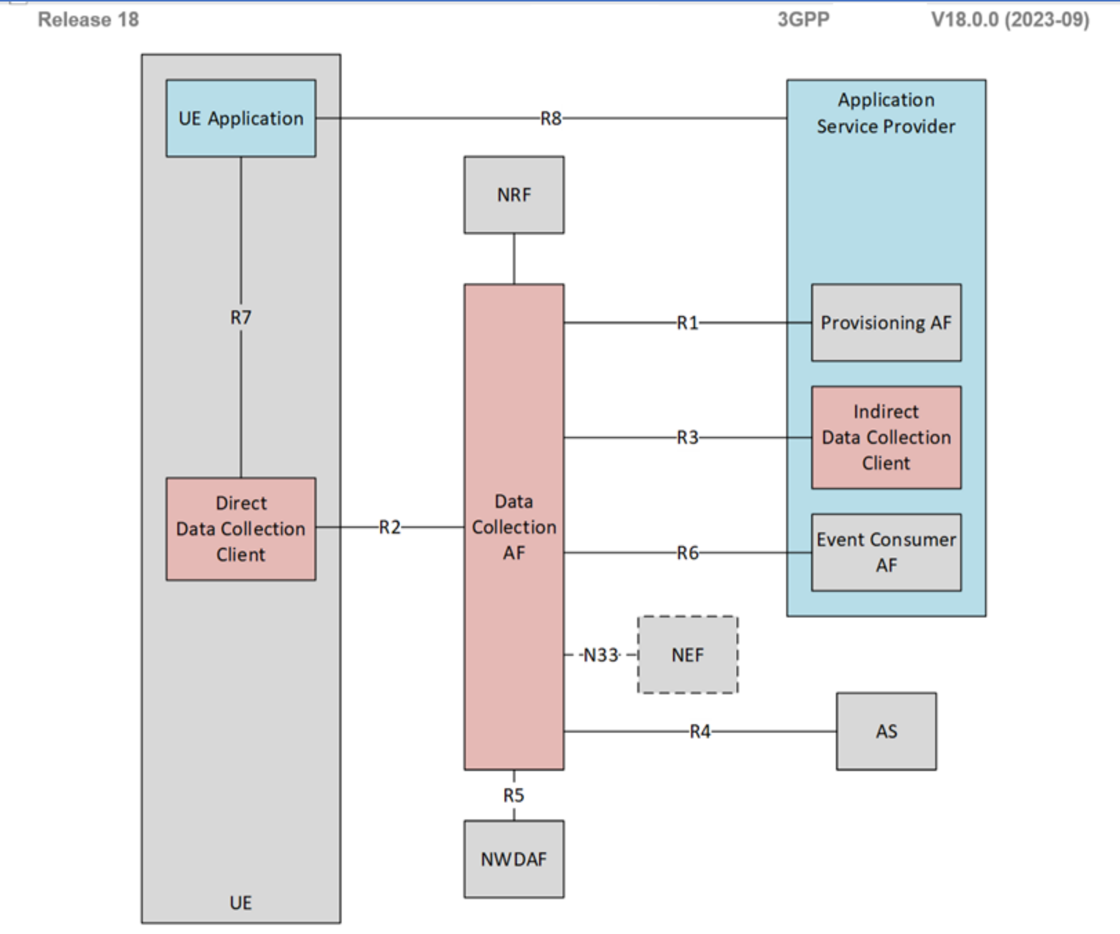


Figure: 5G System Reference Architecture for Data Collection and Reporting in 5G SBA Reference Point notation

Note: *The Data Collection AF (**DCAF**) may be deployed outside the trusted domain, in which case the Services it exposes to API Invokers are mediated by the 5G CN NEF node. The Logical Relationships denoted by the Reference Points are unaffected by such deployment choices.*

Application registration procedure

Upon activation, the UE Application requests its UE Data Collection and reporting Configuration from the Direct Data Collection Client by invoking the *registerUeApplication* Method at Reference Point *R7*.

The UE Application provides as input parameters its
- External Application Identifier,
- Application Service Provider identifier, and
- Information on its callback listener (for receiving notifications from the Direct Data Collection Client).

The UE Application also indicates its "*consent*" for the *UE Identity (i.e. GPSI*) to be included in *Data Reports sent to the Data Collection AF.*

The *Direct Data Collection Client* establishes a new Data Reporting Session with the *Data Collection AF* using the Procedure specified in the %GS Reference Architecture.

The *Ndcaf_DataReporting_CreateSession* invocation includes the GPSI of the UE (if consent is given by the UE Application) or otherwise the Direct Data Collection Client shall instead generate an opaque Client reporting Identifier that is Globally unique and stable (e.g. a UUID) and include this in the invocation of the Service operation.

Release 18 3GPP V18.0.0 (2023-09)

Table: 5G System Reference Architecture for Data Collection and Reporting Methods invoked by the UE Application on the Direct Data Collection Client

Method name	Type	Description
registerUeApplication	State change	UE Application registers with the Direct Data Collection Client, including a callback listener for receiving event notifications.
deregisterUeApplication	State change	UE Application deregisters with the Direct Data Collection Client.
setUserConsent		UE Application grants permission for the Direct Data Reporting Client to include the GPSI when creating Data Reporting Sessions.
getDataCollectionAndReportingConfiguration	Configuration request	UE Application obtains its UE data collection and reporting configuration from the Direct Data Collection Client.
reportUeData	Data report	UE Application reports collected UE data to the Direct Data Collection Client according to its configuration. The UE Application may indicate (by setting a Boolean method parameter to *true*) that the data report includes UE data requiring expedited processing by the Direct Data Collection Client and, consequently, by the Data Collection AF.
resetClientReportingIdentifier		UE Application requests that the Direct Data Collection Client generates a new opaque client reporting identifier for use in data reporting until further notice. This requires any existing Data Reporting Session to be destroyed and a new one (including the replacement client reporting identifier) to be created.
uEApplicationBusy	Notification	UE Application notifies the Direct Data Collection Client that it is temporarily unable to perform UE data collection and reporting due to a busy or stalled condition.
impendingUeApplicationFailure	Notification	UE Application notifies the Direct Data Collection Client of an impending fatal error condition that will cause abrupt shutdown of the UE Application.

Procedure for changing Consent to report the UE identifier

The UE Application can change its Consent to reveal the *GPSI of the UE in Data Reports* sent to *the Data Collection AF* during the course of a Data reporting session by invoking the *setUserConsent M*ethod on the *Direct Data Collection Client* at *Reference Point R7.*
The Direct Data Collection Client shall destroy the current Data Reporting Session and create a new one that includes **either** *the GPSI of the UE* ***or*** the *Opaque Client Reporting Identifier*, according to ***whether Consent is granted or withdrawn***.

UE Data Collection, Reporting and Notification API

The 5GS Data Collection and Reporting Reference Architecture specifies:
- UE Data Collection, Reporting and Notification API used by internal UE Entities, namely a *UE Application* and the *associated Direct Data Collection Client*, in support of *UE Data Collection* by the *Direct Data Collection Client* for subsequent *reporting to the Data Collection AF*, and related exchange of notifications.

As noted in the Reference Architecture specification, this API is not used when the *Direct Data Collection Client is embedded in the UE Application* (i.e., Collaboration between UE and the DCAF as specified) (see the Figure on "Collaboration" and the text below).

However, this can serve as "guidance" to the Design of the Internal APIs for a UE Application with an embedded Direct Data Collection Client.

5GS Data Collection & Reporting Architecture Collaboration between UE and DCAF

As specified in this scenario, the *Data Collection Client* is deployed as a sub-Function of the *UE Application*. Therein, *Reference Point R7* is subsumed into the *UE Application*.

The *Direct Data Collection Client* could, e.g., be realized as a SW Library that implements the appropriate Protocol at *Reference Point R2*. In such a realization, the Procedures defined in *Reference Point R7* would likely form *the API of the Data Collection Client Library.*

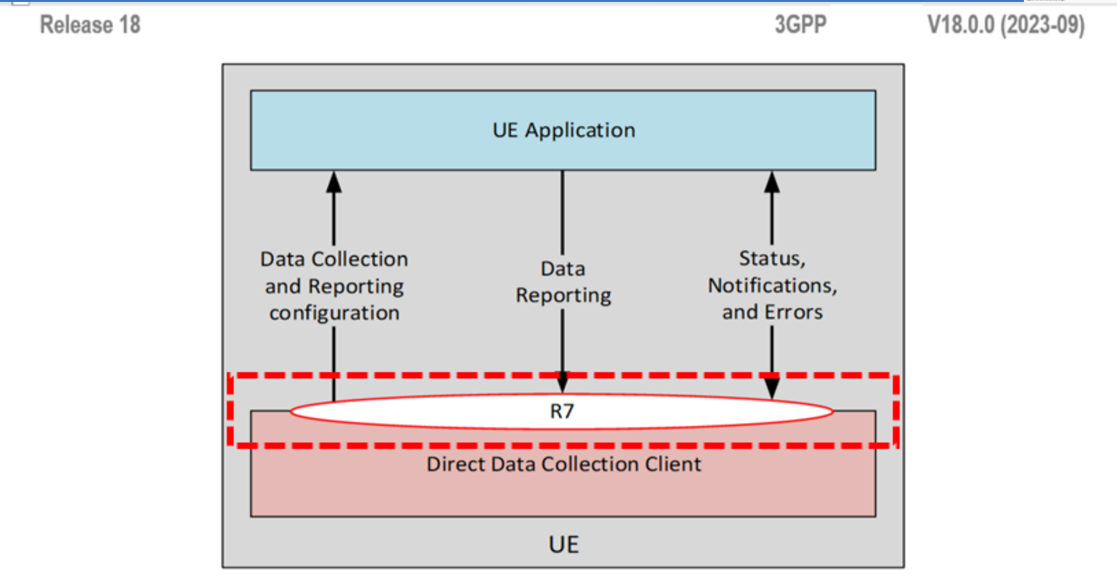


Figure: 5G System Reference Architecture for Data Collection and Reporting UE Architecture for Data Collection, Reporting and Notification via R7 API

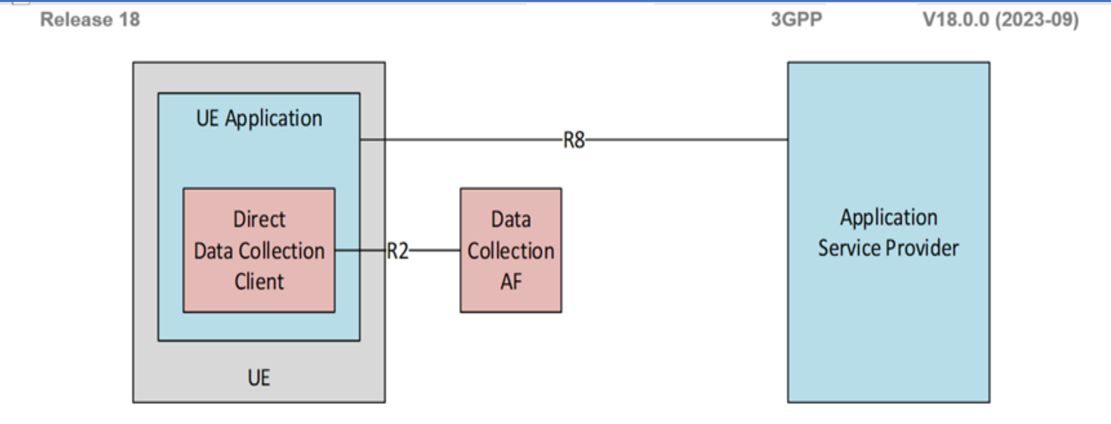


Figure: 5G System Reference Architecture for Data Collection and Reporting Collaboration with UE Data Collection Client deployed as part of the UE Application

The Figure depicts the case where the *Data Collection AF* (*DCAF)* is instead deployed outside the Trusted Domain, along with the Application Service Provider (ASP) and the (external) AS (Application Server).

In this case, *the sub-functions of the Application Service Provider (ASP*) and the (external) AS do not interact with the *Data Collection AF (DCAF*) via the *5G System Service bus*.

The *Ndcaf Service* is therefore not required in such deployments.

Release 18 3GPP V18.0.0 (2023-09)

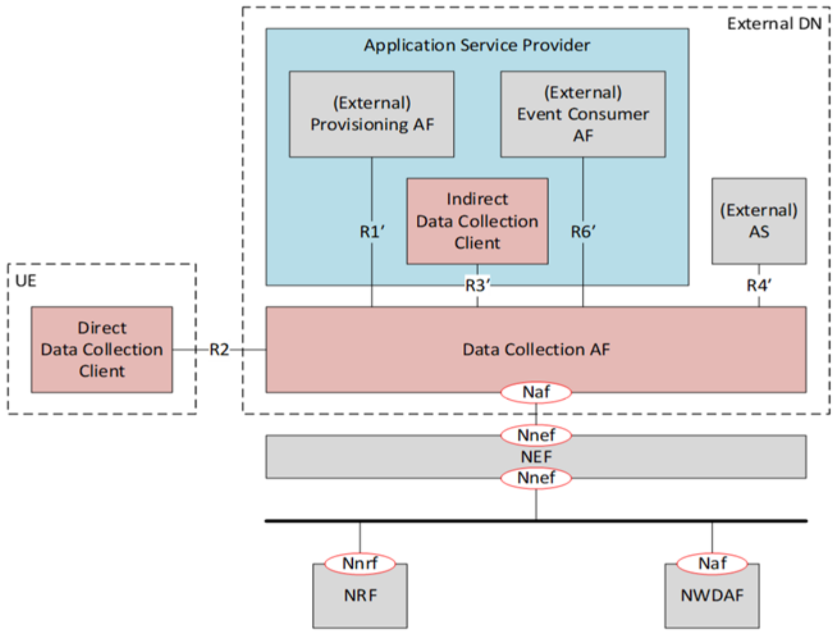


Figure: 5G System Reference Architecture for Data Collection and Reporting in 5G SBA notation when the Data Collection AF is deployed outside the Trusted Domain

5GS Reference **Architecture Data Collection Domain Model(s)**

The Figure depicts the Static Data Model for the Data Collection and Reporting Domain and is further described in the Figure:

5GS Architecture Service exposure via Common API Framework (CAPIF) for Northbound APIs

When CAPIF is supported in the specified 5G Network configuration, then:
- the Data Collection AF shall *support the CAPIF API Provider Domain* functions as part of a distributed CAPIF deployment, i.e. Ndcaf and Naf via CAPIF 2/2e; and CAPIF 3, CAPIF 4 and CAPIF 5, as specified in 5G Common API Framework Architecture specification;

- the *Data Collection AF* shall support the CAPIF Core Function (CCF) and API provider domain functions as part of a centralized CAPIF deployment, i.e. Ndcaf and Naf via CAPIF 2/2e, as specified in 5G Common API Framework Architecture specification.

The *CAPIF and associated API provider domain functions* are specified in 5G Common API Framework Architecture specification.

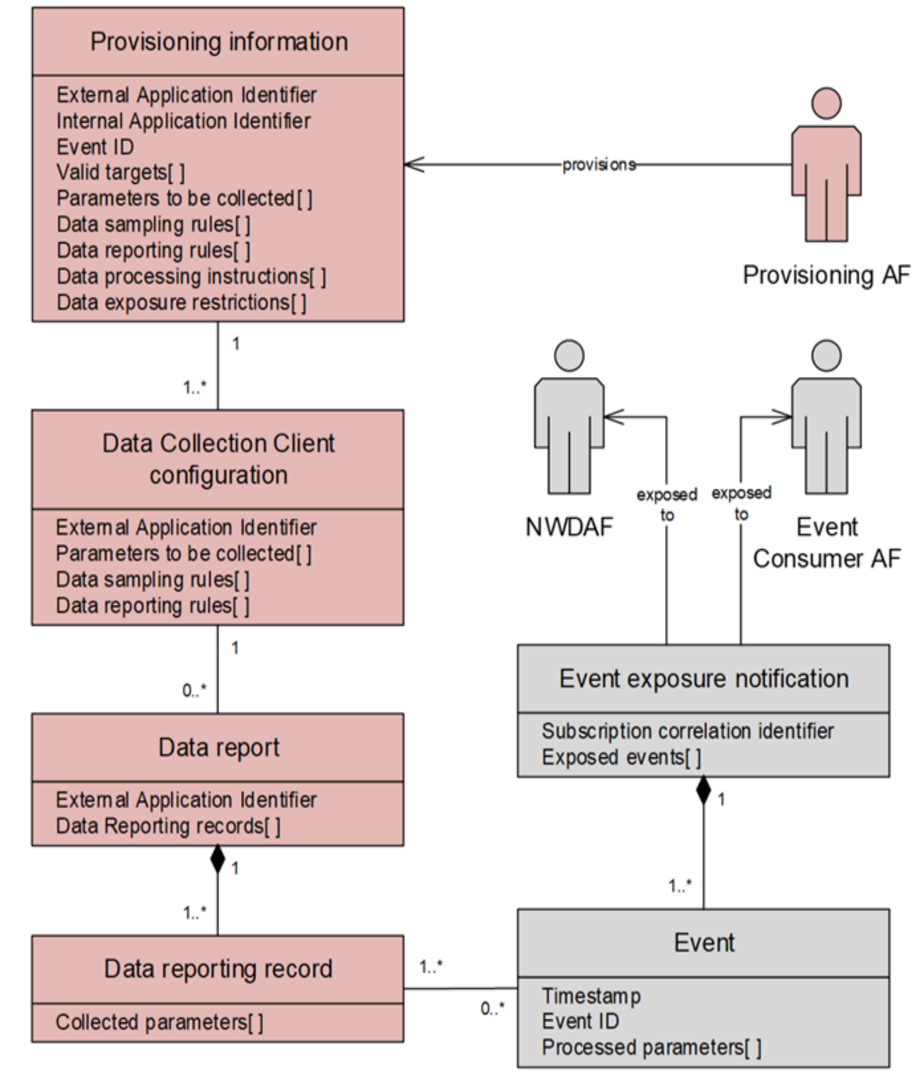


Figure: 5G Data Reporting and Analytics Reference Architecture Static Domain Model

5G System Data Collection and Analytics Reference Architecture: *Network Layer* - 4

The *5G System Architecture* allows any ***5GC NF*** to request *Network Analytics Information from **NWDAF** (Network Data Analytics Function*) containing *Analytics Logical Function* (**AnLF**). *The NWDAF* belongs to the same *PLMN as the 5GC NF* that consumes the Analytics information.

The *Nnwdaf interface* is defined for *5GC NFs*, to:
- Request *Subscription* to Network Analytics Delivery for a particular Context,

- Cancel Subscription to Network Analytics Delivery and to request a specific report of network analytics for a particular context.

NOTE 1: The 5G System Architecture also allows other "*Consumers*" such as *OAM and CEF (Charging Enablement Function*) to request Network Analytics information from NWDAF.

The 5G System Architecture allows any NF to obtain Analytics from an NWDAF using a *DCCF (Data Collection and Coordination Function)* with associated *Ndccf Services*, as specified.

The *5G System Architecture* allows *NWDAF and DCCF* to request *Historical Analytics from an NWDAF* with associated *Nnwdaf_DataManagement Services* as specified.

The *5G System Architecture* allows ***MFAF*** to fetch *Historical Analytics* from an ***NWDAF*** with associated *Nnwdaf_DataManagement Service* as specified.

As depicted in the Figure, the *Ndccf interface* is defined for *any NF to support Subscription Request(s) to Network Analytics,* to cancel subscription for Network Analytics and to request a Specific Report of Network Analytics.

If the Analytics is not already being collected, the *DCCF* requests the Analytics from the *NWDAF* using *Nnwdaf Services*. The *DCCF* may collect the Analytics and deliver it to the *NF*, or the *DCCF* may rely on a Messaging Framework to collect Analytics and deliver it to the NF.

Release 18 3GPP V18.3.0 (2023-09)

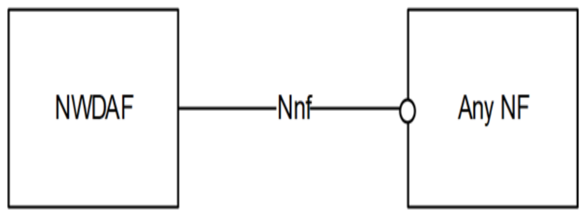


Figure: 5G System Data Analytics Collection and Reporting Architecture from any 5G Core Network Function (NF)

Release 18 3GPP V18.3.0 (2023-09)

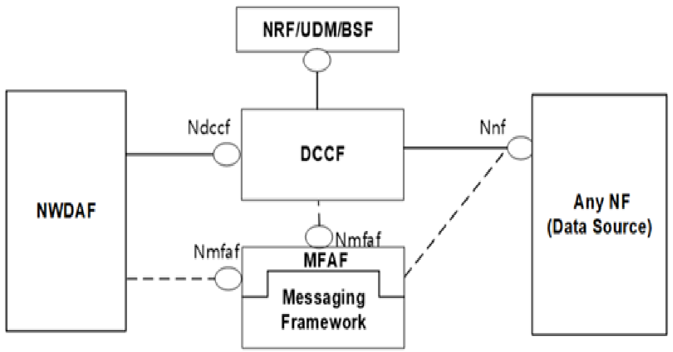


Figure: 5G System Data Analytics Collection and Reporting Architecture using Data Collection Co-ordination

The 5G System Architecture allows NWDAF containing Analytics Logical Function (AnLF) to use trained Machine Learning (ML) Model Provisioning Services from another NWDAF containing Model Training Logical Function (MTLF).

NOTE 2: Analytics Logical Function (AnLF) and Model Training Logical Function (MTLF) are described in clause 5.1.

The *NWDAF* provides *Analytics* to *5GC NFs* and *OAM* as defined.

An ***NWDAF*** may contain the following ***Logical Functions***:

- ***Analytics logical function (AnLF)***: A *Logical Function in NWDAF*, which performs *inference,* derives analytics information (i.e. *derives statistics and/or predictions* based on *Analytics "Consumer" Request*) and exposes Analytics Service i.e. *Nnwdaf_AnalyticsSubscription* or *Nnwdaf_AnalyticsInfo.*

- *Model Training Logical Function (**MTLF**)*: A *Logical Function in NWDAF,* which trains *Machine Learning (**ML**) Models* and exposes New Training Services (e.g. providing Trained ML Model) as defined in this Architecture specification.

NOTE 1: *NWDAF* can contain an *MTLF or an AnLF or both Logical Functions (LFs).*

Release 18 3GPP V18.3.0 (2023-09)

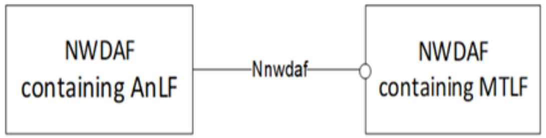


Figure: 5G System Data Analytics Collection and Reporting Architecture using Trained Machine Learning (ML) Analytics Logical Function (LF) and Model Training Logical Function (MTLF)

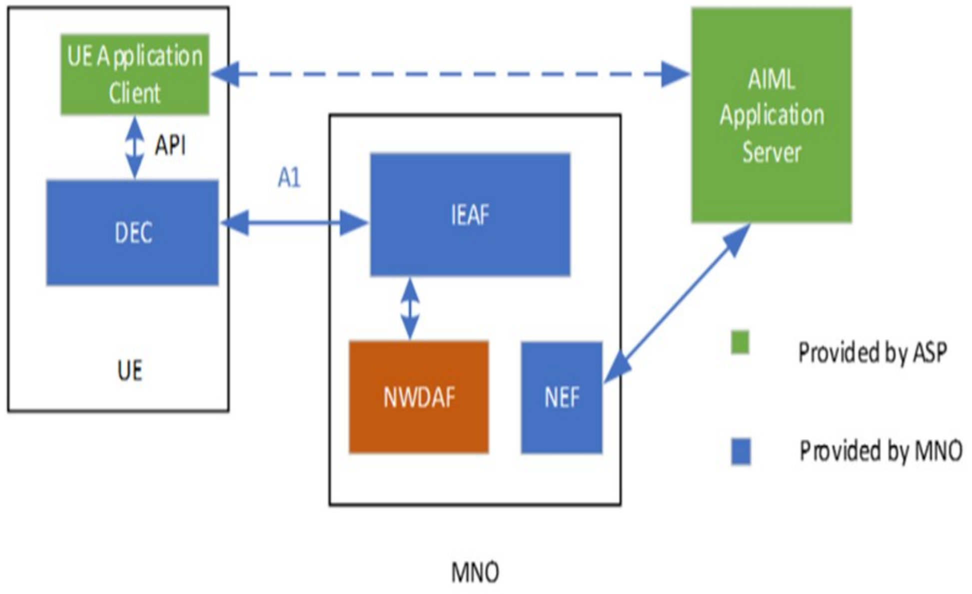


Figure: 5G Data Analytics, Collection and Reporting Architecture evolved IEAF Data Information Collection Function

UE ID retrieval - IEAF based solution

Based on the justification in clause 6.2.1, the following information may be requested by UE application Client from 5GC to assist the Application layer AIML operation:

- QoS Sustainability Analytics.
- User Data Congestion Analytics.

Note: Whether and how the UE can use 5GC information (e.g. as above) for AI/ML operations is FFS and needs to be described with valid justification before solution can be adopted, considering also that the same information will be used by the AI/ML application server as well.

NOTE x:Support for analytics IDs that only support any UE as the target of analytics reporting is subject to SA WG3 evaluation on how to address security and privacy concerns when sharing analytics generated from other UEs to an individual UE.
The UE Data Exposure Client (DEC) is responsible for sending data request to the Data Information AF (IEAF) to collect data from NWDAF as an input for application layer AIML operation. The IEAF is always in the MNO domain and the DEC is based on 3GPP defined procedures and security and therefore is also under the control of MNO. The data collection request from UE Application may trigger the IEAF to collect Data from NWDAF.

NOTE 1: Both IEAF and DEC are controlled and managed by the MNO e.g. with 3GPP defined procedures.

The IEAF is configured based on the SLA above for each AI/ML Application. NWDAF follows existing Service User Consent checks as specified in 5G and Network Consent checks for the IEAF (as a NWDAF Service Consumer).
The IEAF may be also configured by the operator to do some data processing before sending the exposure data to DEC.
The following information are pre-configured in the UE by MNO or provisioned (via PCF) to the UE as part of AIML policy by using the procedure as defined in clause 4.2.4.3 in TS 23.502 [4] and used in the communication with IEAF:

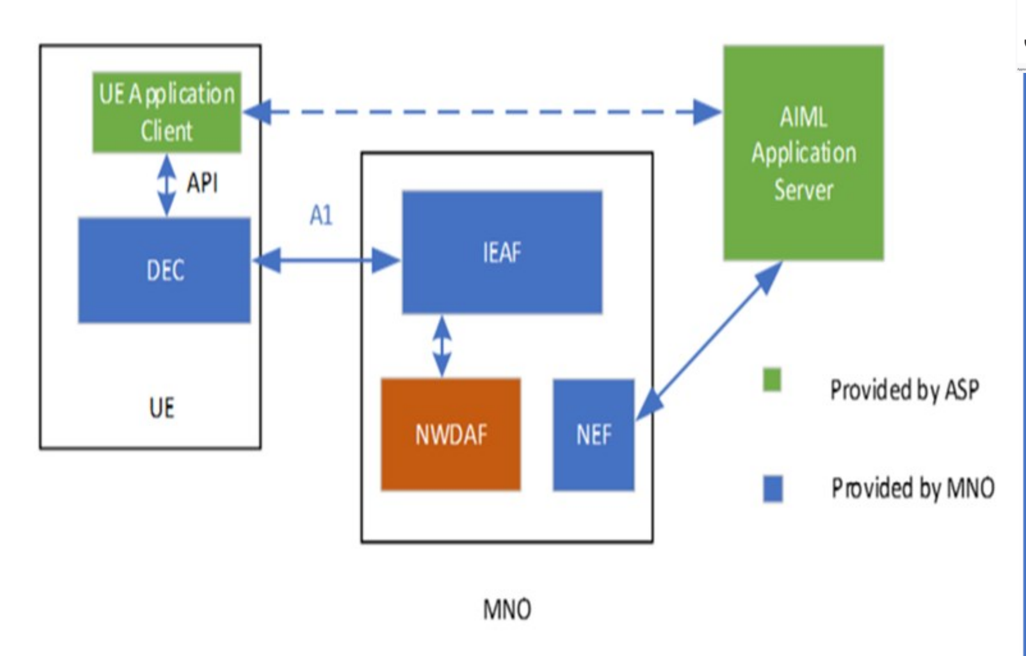


Figure: 5G Data Analytics, Collection and Reporting Architecture evolved IEAF Data Information Collection Function

The **DEC** communicates to the IEAF over User Plane (UP) via a PDU session established by the UE.

*NOTE 2: The **DEC** is deployed per Application in this Release.*

The SLA between the Operator and the AIML Application Service Provider (SP) determines per Application ID in use by the ASP:

- **The Analytics ID(s) that the 5GC is allowed to expose, subject to User Consent and Network Consent.**

- The S-NSSAI for the AIML Application Service Provider (SP).
- The Authentication information that enable the IEAF to verify the authenticity of the DEC that collects data.

5G System Data Collection and Analytics Reference Architecture - 7

5GS Analytics and Data Reporting Reference Architecture 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 NWDAF.

The Training Data that are used to train an *ML Model are usually Historical Data (Data stored in the Analytics Data Repository Function (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*, or the *Number of Users Accessing Services* via the *Core Network (**CN**)* may considerably increase *(e.g. Tourist Season in the Summer).*

Such 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.*

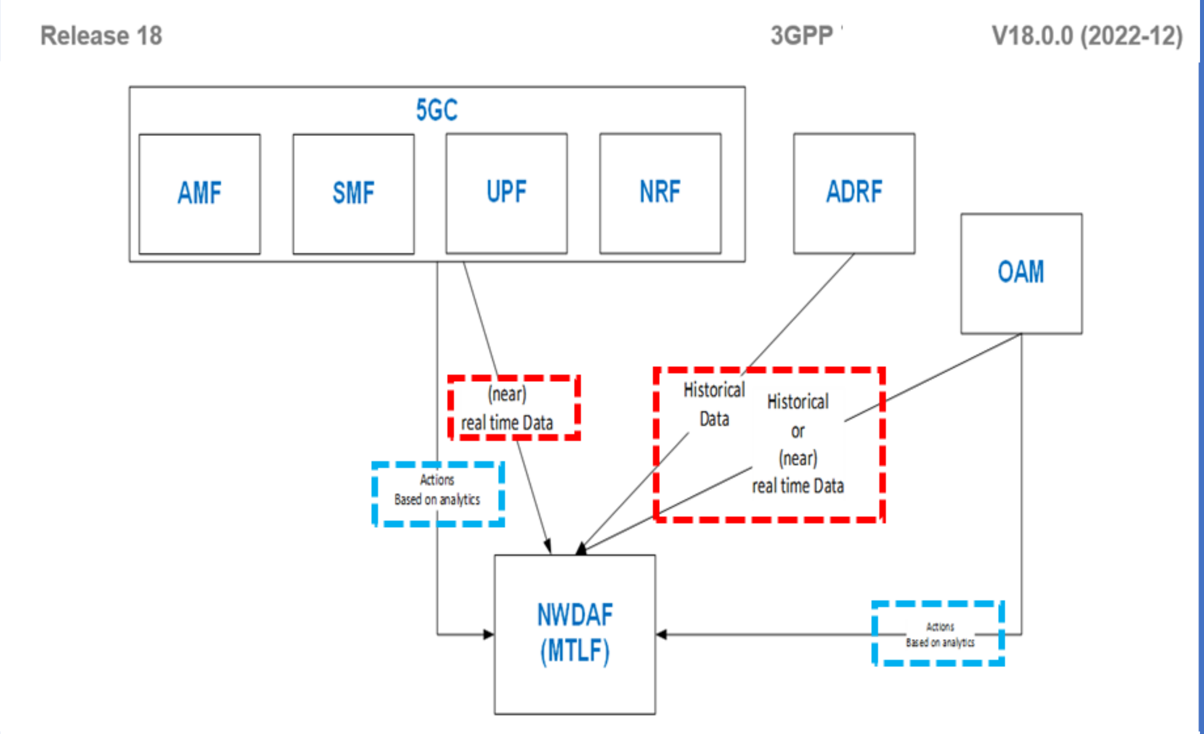


Figure: 5G System Data Analytics Collection and Reporting Architecture Model drift detected at Network Data Analytics Function (NWDAF) Model Training Logical Function (MTLF)

A "simple" Solution to this problem is to *Re-Train an ML Model Periodically*. Such approach will ensure that the *NWDAF always uses an "Up-to-Date Training Data" for an ML Model.* However, such approach requires *"considerable" Resources and is not energy efficient*.

Hence a Solution is required to allow the *Network (i.e. NWDAF*) to determine when an *ML Model requires Re-Training.*

The Solution proposed hereby focuses on the *NWDAF* to evaluate if an action taken by a "*Consumer"* would result in a Model drift and then evaluate if the *Training Data* are *"Up-to-Date".*

Roaming Capability Architecture

Based on Operator's *Policy* and Local Regulations (e.g. *Privacy*), *Data* or *Analytics* may be *exchanged between PLMNs* (i.e. *HPLMN* and *VPLMN*).

In a *PLMN*, an *NWDAF* is used as exchange point to exchange Analytics and to collect *Input Data for Analytics* with other *PLMNs*.

The NWDAF with Roaming exchange Capability is called *Roaming Exchange NWDAF (RE-NWDAF).*

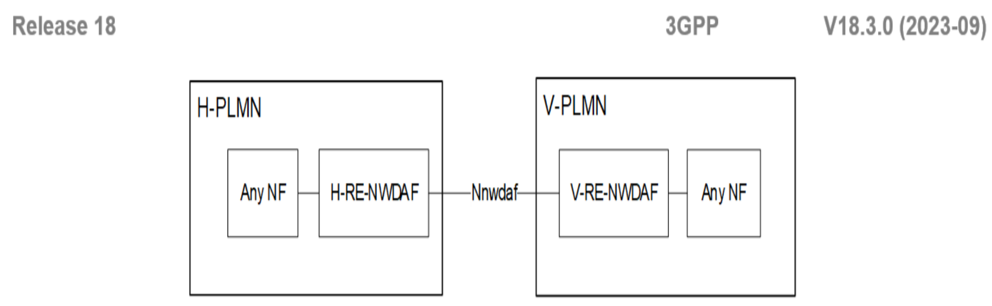


Figure: 5G System Data Analytics Collection and Reporting Roaming Architecture to exchange Input Data or Data Analytics between V-PLMN and H-PLMN

Using the Architecture shown in the Figure:

- For *Outbound Roaming Users*, the *NF "Consumer*" in the *HPLMN* can retrieve *Analytics* from the *VPLMN* via the *H-RE-NWDAF in HPLMN* and *V-RE-NWDAF in VPLMN.*

NOTE 1: *The Analytics from the VPLMN may be generated by the V-RE-NWDAF in the VPLMN or by other NWDAFs in the VPLMN.*

- For Outbound Roaming Users, the *H-RE-NWDAF in HPLMN* can collect *Data* from the *VPLMN via V-RE-NWDAF in VPLMN*.

- For *Inbound Roaming Users*, *the NF "Consumer*" in the *VPLMN* can retrieve *Analytics* from the *HPLMN* via *V-RE-NWDAF in VPLMN and H-RE-NWDAF in HPLMN.*

NOTE 2: The Analytics from the HPLMN may be generated by H-RE-NWDAF in the HPLMN or other NWDAFs in the HPLMN. For Inbound Roaming Users, the V-RE-NWDAF can collect data from the HPLMN via the H-RE-NWDAF.

NOTE 3: *Both Local Breakout (LBO) and Home Routed (HR) Roaming Architectures support the Data or Analytics exchanging between PLMNs.*

NOTE 4: Interactions between RE-NWDAFs of different PLMNs may be via ***SEPPs,*** which are not depicted in the Architecture for the sake of clarity.

*5G System Architecture Application Data Analytics Enablement (**ADAE) internal Architecture***

In ADAE Framework, **A-DCCF** and **A-ADRF** can be defined as Functionalities within the *internal ADAE Architecture* and can offer the following Functionalities:

- ***Application Layer*** - *Data Collection and Coordination Function (**A-DCCF**)*

A-DCCF coordinates the Collection and Distribution of Data requested by the "*Consumer" (ADAE Server*).

Data Collection Coordination (**DCC**) is supported by a ***A-DCCF.***
ADAE Server can send requests for Data to the ***A-DCCF*** rather than directly to the *Data Sources*.
A-DCCF may also perform Data Processing/Abstraction and Data Preparation based on the VAL Server Requirements.

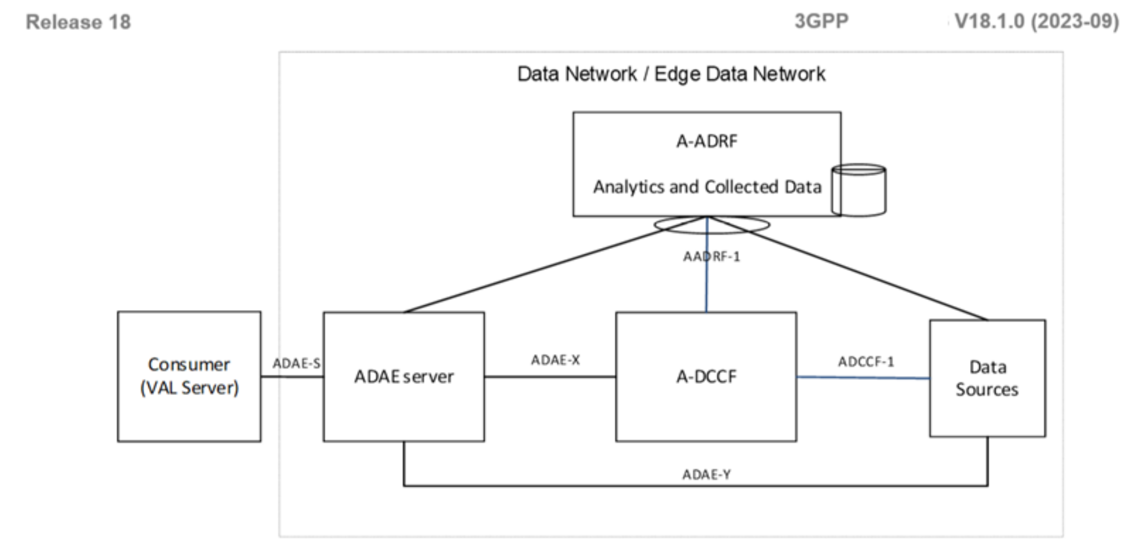


Figure: 5G System Data Analytics Collection and Reporting Architecture Application Data Analytics Enablement Internal Functional Architecture

- *Application Layer - Analytics and Data Repository Function (**A-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* (*e.g. ADAE Server).*

After the "*Consumer"* obtains Data and/or Analytics*, "Consumer*" may store *Historical Data* and/or *Analytics in an A-ADRF*.

Whether *the "Consumer"* directly contacts *the A-ADRF* or goes via the *A-DCCF* is based on configuration.

The Figure illustrates *the Generic Functional Model for ADAE* when re-using the ***3GPP Network Data Analytics (NWDAF) Model.***

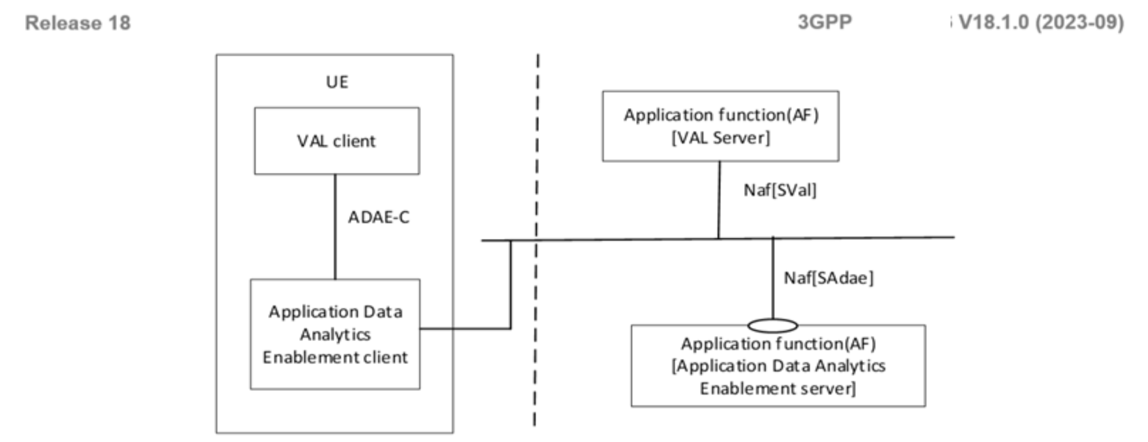


Figure: 5G System Architecture for Application Data Analytics Enablement in 5G Service-based Interface (SBI) Representation

*5G System Architecture Application Data Analytics Enablement (**ADAE) Deployment Scenarios***

There could be three (3) ADAE Deployment Options:

1. *ADAES can be deployed at a Centralized Cloud Platform*, and collects Data from multiple EDNs

2. *ADAES can be deployed at the Edge Platform* (3GPP EDGEAPP)

3. *Coordinated ADAES deployment*, where multiple ADAE Services are deployed in Edge or Central Clouds.

Such deployment allows *for Local-Global Analytics for System wide optimization*

ADAE Layer APIs
The following ADAE Capabilities are offered as APIs:
- ADAE Server APIs;
- A-ADRF APIs;

The Service Enablement Architecture Layer and Network Slice capability Enablement Service APIs are specified and support:

- Group Management Server APIs;
- Location Management Server APIs;
- Configuration Management Server APIs;
- Identity Management Server APIs;
- Key Management Server APIs; and
- Network Slice Capability Enablement APIs.

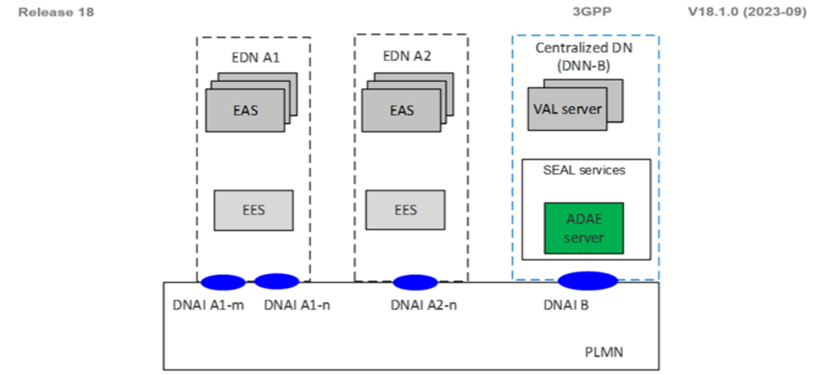


Figure: 5G System Architecture for Application Data Analytics Enablement Cloud deployment ADAE option

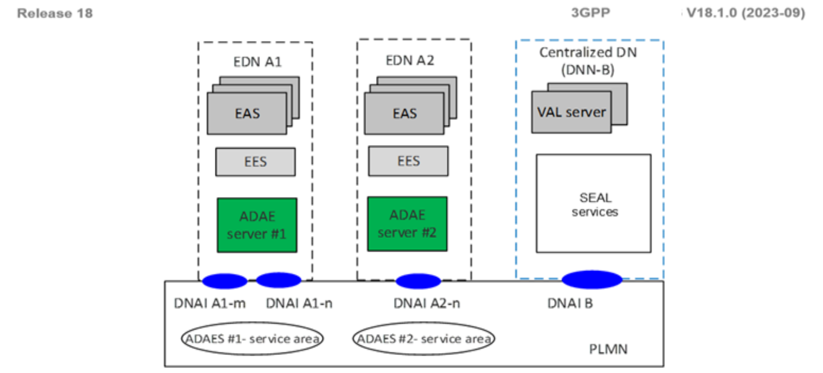


Figure: 5G System Architecture for Application Data Analytics Enablement 5G EDGEAPP Architecture deployed ADAE option

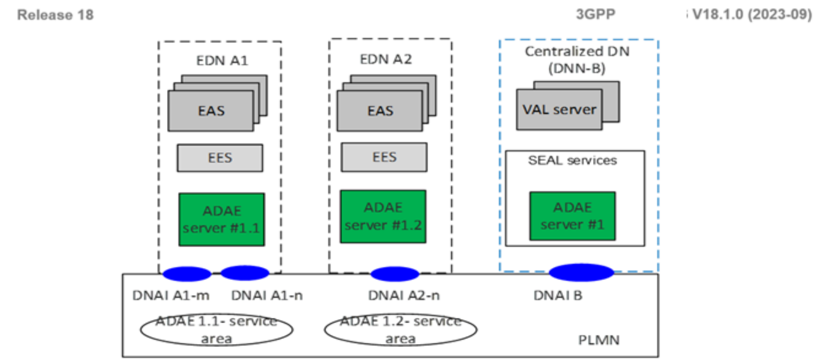


Figure: 5G System Architecture for Application Data Analytics Enablement Co-ordinated deployed ADAE option

Summary-1 of 5G Advanced implementation of AI/ML Applications and ML Model Transfer Capabilities

In 5G, AI/ML is specified to be used in a range of Application Domains across Industry sectors. In 5G Mobile Communications Systems, Mobile Devices (e.g. Smartphones, Automotive, Robots) are increasingly replacing conventional algorithms (e.g. Speech Recognition, Image Recognition, Video Processing) with AI/ML Models to enable Applications. **The 5G System (5GS) can at least support three (3) types of AI/ML operations**: ***1. The UE Data Exposure Client (DEC)*** is responsible for sending *Data request to the Data Information AF* (***IEAF,*** evolved Rel. 17 ***DCAF/AF)*** to collect Data from **NWDAF** as an input for **Application Layer AIML operation.** The **IEAF** is always in the MNO Domain & the **DEC** is based on **3GPP defined Procedures & Security &** *therefore is also under the control of MNO.* The Data Collection Request from UE Application may trigger the **IEAF** to collect Data from **NWDAF (IEAF deployment shown below). *2. AI/ML Model/Data Distribution & Sharing over 5GS*** (the Model Performance at the UE needs to be monitored constantly). ***3. Distributed/Federated Learning (FL) over 5GS*** (The Cloud Server trains a Global Model by aggregating Local Models partially-trained by each End Device via 5G UL). The Server aggregates the Interim Training results from the UEs & updates the Global Model. The Updated Global Model is then distributed back to the UEs & the UEs can perform the Training for the Next Iteration. Based on Operator Policy, 5GS shall be able to provide means to predict & expose predicted Network Condition changes (i.e. Bitrate, Latency, Reliability) per UE, to an Authorized 3rd Party. **Subject to User Consent, Operator Policy & Regulatory Constraints**, the 5GS shall be able to support **a Mechanism** to expose Monitoring & Status Information of an AI-ML Session to a 3rd Party AI/ML Application & be able to expose information (e.g. candidate UEs) to an Authorized 3rd Party to assist the 3rd Party to determine Member(s) of a Group of UEs (e.g. UEs of a FL Group). ***Depending on Local Policy or Regulations, to protect the Privacy of User Data, the Data Collection, ML Model Training & Analytics generation for a Subscriber/User id, Internal or External_Group_Id or "any UE" may be subject to User Consent*** **bound to a Purpose, such as Analytics or ML Model Training. The User Consent is "Subscription Information**" stored in the 5G CN, which includes: **A)** whether the User authorizes the Collection & Usage of its Data for a Particular Purpose; **B)** the **Purpose** for Data Collection, e.g. **Analytic or Model Training.**

5GS (System) proposes a Common **Solution Framework** to assist various Application AI/ML Operations with Assistance Info & Procedures from 5GC. In this Framework, the similar **Service Requirements & Operational behaviours** are organized into various *Application AI/ML Assistance* **(AaaML)** *Service Profiles* where *Each Profile defines specific AaaML Service*. The **AaaML Services** are a Set of Collective Extensions to the existing 5GC Services & the new 5GC Services which are defined specifically to assist the Application Layer AI/ML Service Operation. An **AaaML Service Profile** is composed of 3 main parts of information: A) **Objective** of Target AaaML Operation; **B) Input of Provisioned Service Parameter(s)** (e.g. Minimum One Way Delay, Predicted QoS Performance within the next 5 min.; **C) Output** (*e.g. List of Candidate UEs, Event Report for the Group of UE's Bandwidth Consumption.*

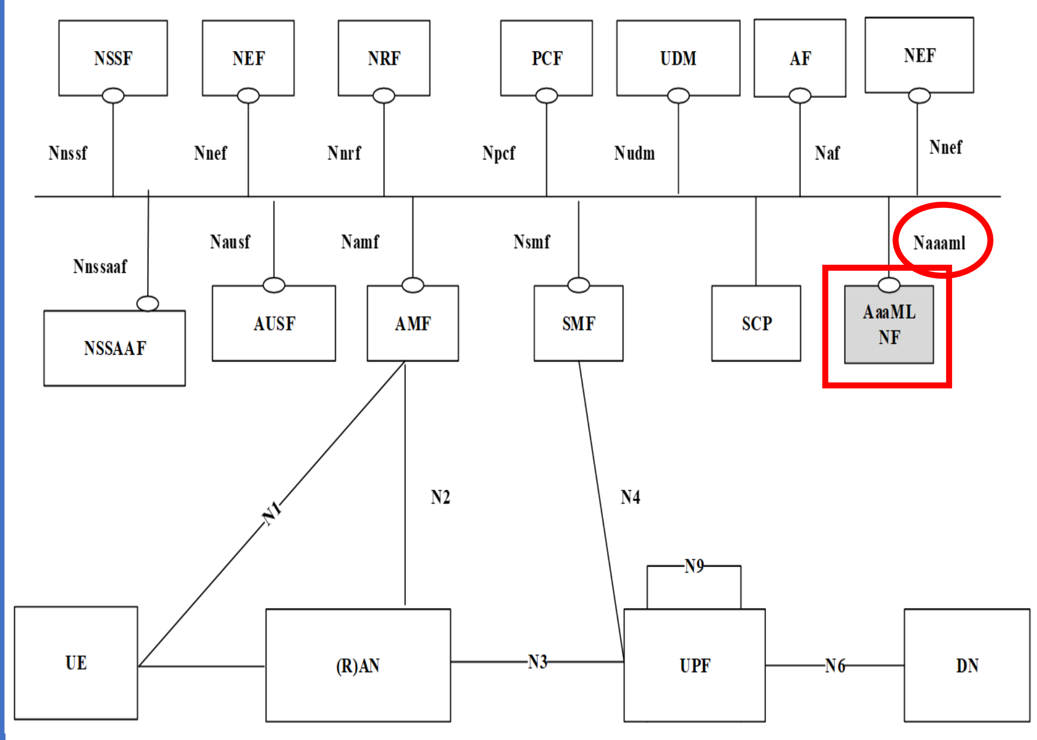


Figure: 5G System Service Architecture with AaaML NF

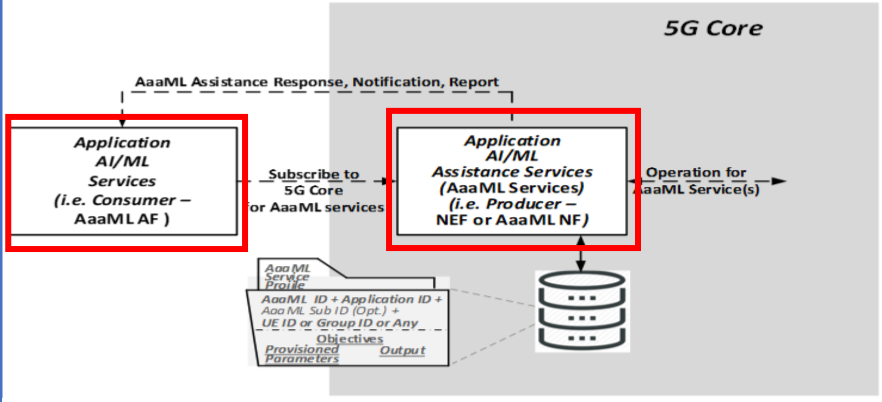


Figure: 5G Application AI/ML Service Assistance Framework

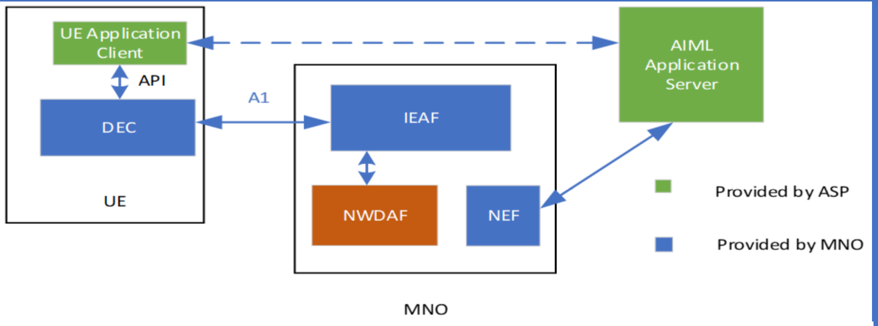


Figure: 5G IEAF (Data Information AF)

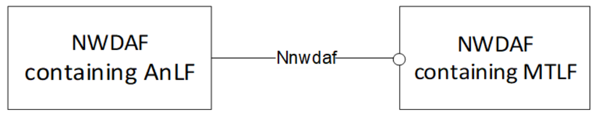


Figure: 5G NWDAF containing AnLF (Analytics Logical Function) for request and subscribe to ML Model Provisioning Architecture

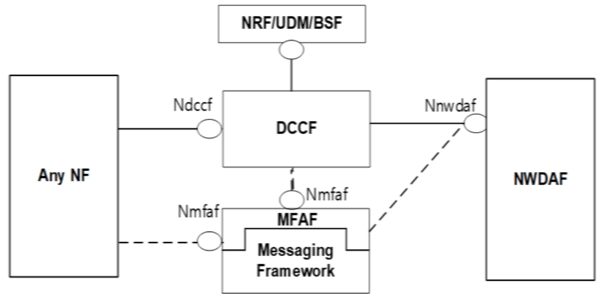


Figure: 5G Network Data Analytics Exposure Architecture using DCCF

Table: 5G NFs Consumed by DCCF or NWDAF to determine which NF instances are serving UE

Type of NF instance (serving the UE) to determine	NF to be contacted by DCCF	Service
UDM	NRF	Nnrf_NFDiscovery
AMF	UDM	Nudm_UECM
SMF	UDM	Nudm_UECM
BSF	NRF	Nnrf_NFDiscovery
PCF	BSF	Nbsf_Management
NEF	NRF	Nnrf_NFDiscovery
NWDAF	UDM	Nudm_UECM

Summary-2: 5G Advanced UE ID retrieval IEAF Data Information Collection based Solution with UE DEC (Data Exposure Client)

In 5G, ***UE DEC (Data Exposure Client) Application Client*** may request from 5GC to assist the *Application Layer AI/ML Operation* with information about ***QoS Sustainability Analytics & User Data*** Congestion Analytics. The UE Data Exposure Client (**DEC**) is responsible for sending Data request to *the Data Information AF* (***IEAF***) to collect Data from NWDAF as an input for Application Layer AIML Operation. The IEAF is always in the MNO Domain & the **DEC** is based on 3GPP defined Procedures & Security & therefore is also under the control of MNO. The Data collection request from UE Application may trigger the IEAF to collect Data from NWDAF. Both IEAF & DEC are controlled and managed by the MNO e.g. with 3GPP defined procedures. The DEC communicates to the IEAF over User Plane (UP) via a PDU session established by the UE. The DEC is deployed per Application. The ***SLA** between the Operator & the AIML Application Service Provider* (***ASP***) determines per Application ID in use by the ASP such as 1) the Analytics ID(s) that the 5GC is allowed to expose, subject to User Consent & Network Consent, 2) the S-NSSAI for the AIML Application Service Provider (ASP), 3***) the Authentication*** information that *enable the IEAF to verify the Authenticity of the DEC that collects Data.* The 5G System Architecture allows ***ADRF (Analytics Data Repository Function***) to store and retrieve the Collected Data & Analytics.

Based on the NF Request or Configuration on the ***DCCF***, the ***DCCF*** may determine the ***ADRF*** & interact directly or indirectly with the ADRF to request or store Data. A ***Consumer NF*** may specify in requests to a ***DCCF*** that ***Data*** *provided by a Data Source needs to be stored in the ADRF*. The ***ADRF*** checks if the ***Data Consumer*** is authorized to access ADRF Services & provides the requested Data using the Procedures 5G System specified Procedures.

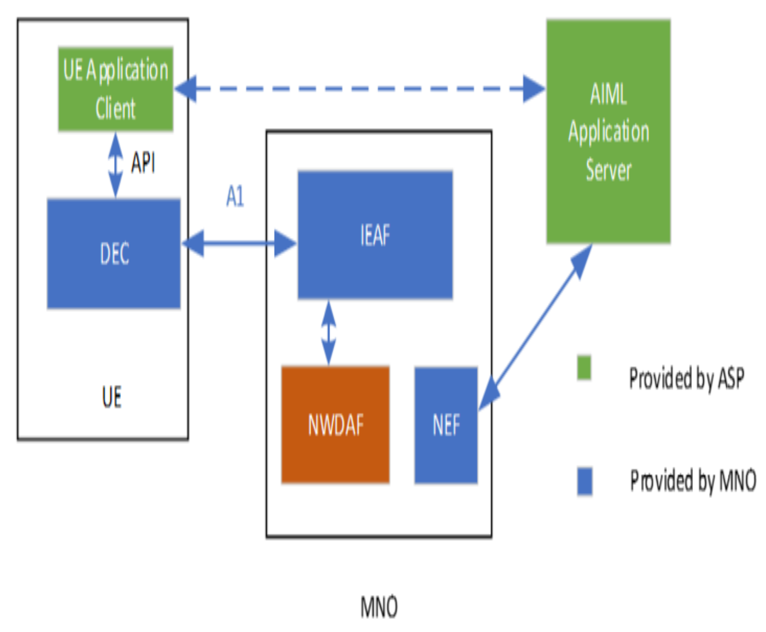


Figure: 5G IEAF Data Information Collection

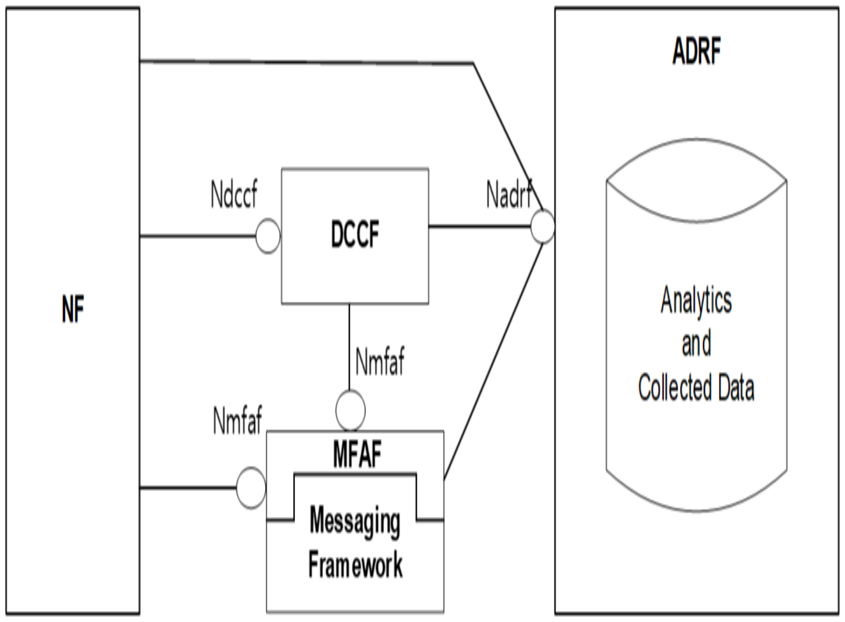


Figure: 5G Data Storage for Analytics and Collected Data

Table: 5G KPI Table of AI/ML Inference Split between UE and Network Server/AF

Uplink KPI					Downlink KPI				
Max allowed UL end-to-end latency	Experienced data rate	Payload size	Communication service availability	Reliability	Max allowed DL end-to-end latency	Experienced data rate	Payload size	Reliability	Remarks
2 ms	1.08 Gbit/s	0.27 MByte	99.999 %	99.9 %				99.999 %	Split AI/ML image recognition
100 ms	1.5 Mbit/s				100 ms	150 Mbit/s	1.5 MByte/ frame		Enhanced media recognition
	4.7 Mbit/s				12 ms	320 Mbit/s	40 kByte		Split control for robotics
NOTE 1: Communication service availability relates to the service interfaces, and reliability relates to a given system entity. One or more retransmissions of network layer packets can take place in order to satisfy the reliability requirement.									

Table: 5G KPI Table of Federated Learning (FL) between UE and Network Server/AF

Max allowed DL or UL end-to-end latency	DL experienced data rate	UL experienced data rate	DL packet size	UL packet size	Communication service availability	Remarks
1s	1.0Gbit/s	1.0Gbit/s	132MByte	132MByte		Uncompressed Federated Learning for image recognition
1s	80.88Mbit/s	80.88Mbit/s	10Mbyte	10Mbyte	TBD	Compressed Federated Learning for image/video processing
1s	TBD	TBD	10MByte	10MByte		Data Transfer Disturbance in Multi-agent multi-device ML Operations

3GPP 5G System Architecture interworking (integrated) with IETF Deterministic Networking (DetNet) Architecture specification
An enhanced Architecture supporting the reporting of Mobile Network information to DetNet Control Layer is designed. 5G System report corresponding information to the DetNet Control Plane (CP) to assist the DetNet CP. ***The Architecture enhances the Network Functions (NFs) of NEF, SMF, & UPF respectively, so as to support the Information Collection, Subscription & Reporting of DetNet Capability.***

Provisioning DetNet (Deterministic Networking) Configuration from the DetNet Controller to 5GS (System) - mapping the End to End (E2E) Requirement to per Node Requirement.

- Max-Latency to Required Delay.
- Min-Bandwidth to GFBR (Guaranteed Flow Bit Rate).
- Max-loss to Required PER (Packet Error Rate) (new in Rel-18).
- Max-Consecutive-Loss-Tolerance to Survival Time - when such mapping is possible, such as when there is only a Single Packet per Interval. Interval to Periodicity in TSC (Time-Sensitive Communication) info.
- Max-pkts-per-Interval * (Max-payload-Size + Protocol Header Size) to Max Burst Size.
- Max-pkts-per-Interval * (Max-payload-Size + Protocol Header Size)/ Interval to MFBR (Maximum Flow Bit Rate).
- DetNet Flow specification to 3GPP Flow description (also incl. the DSCP value & optionally IPv6 Flow label & IPsec SPI.

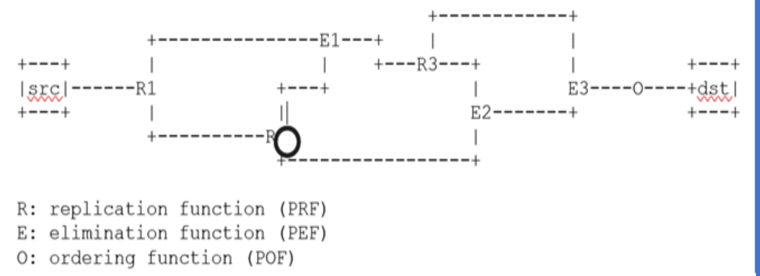


Figure: DetNet PREOF (Packet Replication, Elimination & Ordering Function) in a DetNet Network

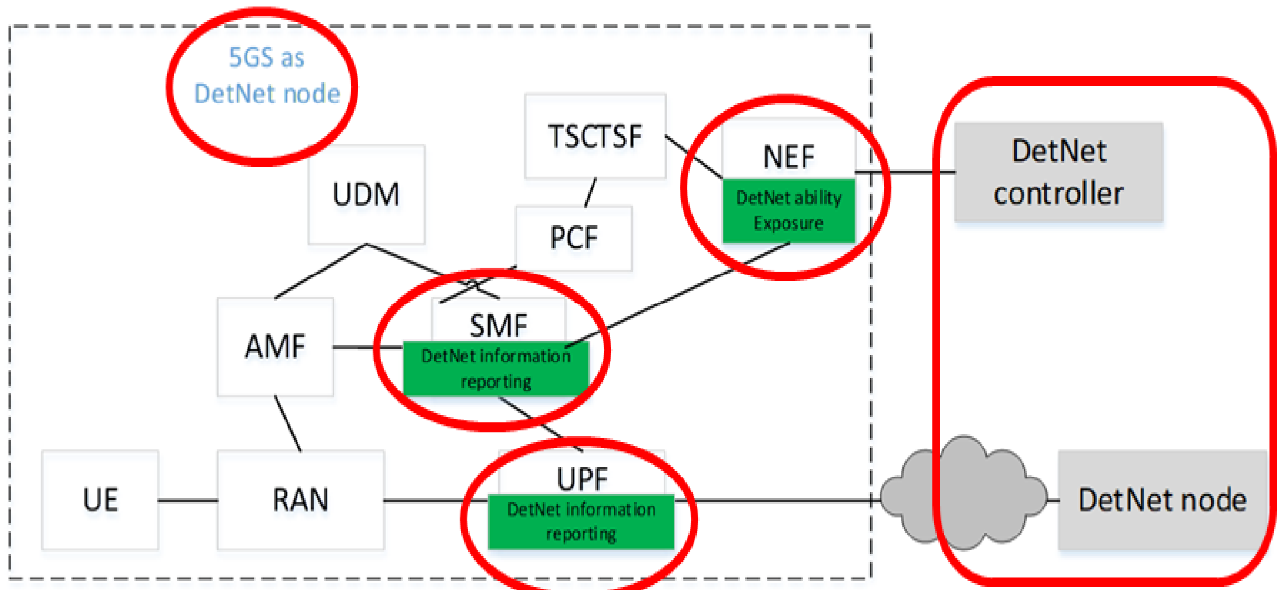


Figure: 5G System (as DetNet Node) Enhanced Architecture and Network Function (NF) to support 5GS DetNet Node reporting

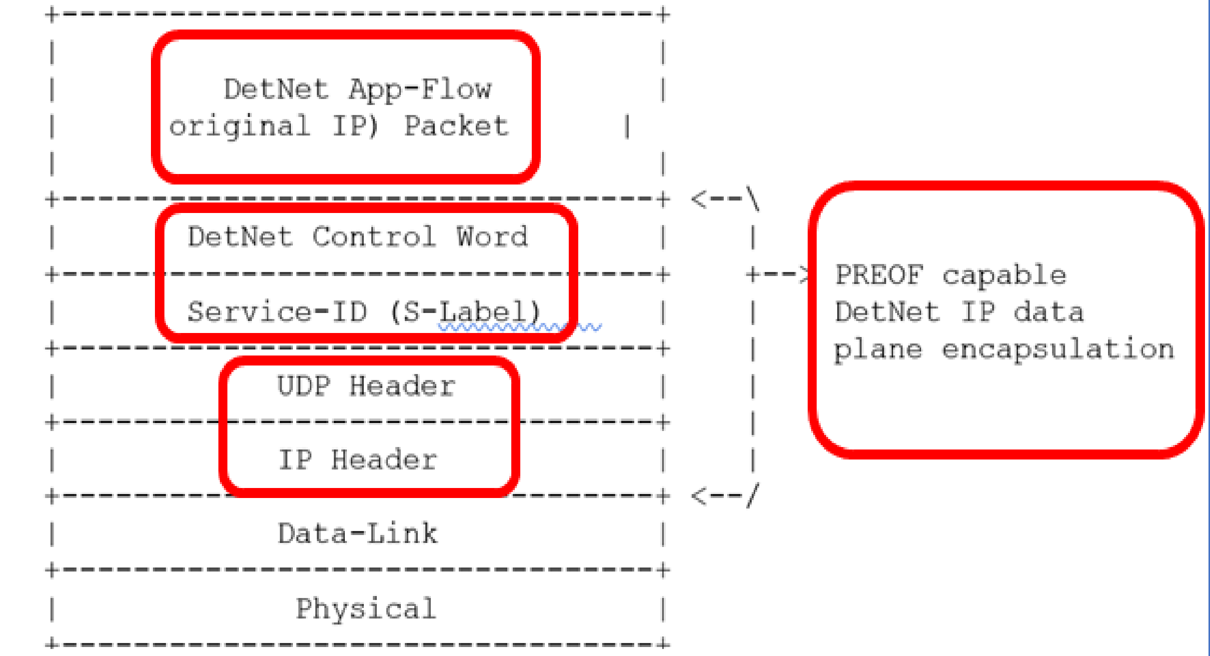


Figure: DetNet PREOF capable DetNet IP encapsulation

Workgroup: RAW
Published: 14 August 2023
Intended Status: Informational
Expires: 15 February 2024

Reliable and Available Wireless Architecture

Abstract

Reliable and Available Wireless (RAW) provides for high reliability and availability for IP connectivity across any combination of wired and wireless network segments. The RAW Architecture extends the DetNet Architecture and other standard IETF concepts and mechanisms to adapt to the specific challenges of the wireless medium, in particular intermittently lossy connectivity. This document defines a network control loop that optimizes the use of constrained spectrum and energy while maintaining the expected connectivity properties, typically reliability and latency. The loop involves DetNet Operational Plane functions, with a new recovery Function and a new Point of Local Repair operation, that dynamically selects the DetNet path(s) for the future packets to route around local degradations and failures.

Status of This Memo

Copyright Notice

"In-Progress" IETF RAW - Reliable and Available Wireless Architecture - 2

1. Introduction

Deterministic Networking is an attempt to emulate the properties of a serial link over a switched fabric, by providing a bounded latency and eliminating congestion loss, even when co-existing with best-effort traffic. It is getting traction in various industries including professional A/V, manufacturing, online gaming, and smartgrid automation, with both cost savings and complexity benefits (e.g., vs. loads of P2P cables).

Bringing determinism in a packet network means eliminating the statistical effects of multiplexing that result in probabilistic jitter and loss. This can be approached with a tight control of the physical resources to maintain the amount of traffic within a budgeted volume of data per unit of time that fits the physical capabilities of the underlying network, and the use of time-shared resources (bandwidth and buffers) per circuit, and/or by shaping and/or scheduling the packets at every hop.

This innovation was initially introduced on wired networks, with IEEE 802.1 Time Sensitive networking (TSN) - for Ethernet LANs - and IETF DetNet. But the wired and the wireless media are fundamentally different at the physical level and in the possible abstractions that can be built for IPv6 [IPv6], more in [IPoWIRELESS]. Nevertheless, deterministic capabilities are required in a number of wireless use cases as well [RAW-USE-CASES]. With new scheduled radios such as TSCH and OFDMA [RAW-TECHNOS] being developed to provide determinism over wireless links at the lower layers, providing DetNet capabilities is now becoming possible.

resources (bandwidth and buffers) per circuit, and/or by shaping and/or scheduling the packets at every hop.

This innovation was initially introduced on wired networks, with IEEE 802.1 Time Sensitive networking (TSN) - for Ethernet LANs - and IETF DetNet. But the wired and the wireless media are fundamentally different at the physical level and in the possible abstractions that can be built for IPv6 [IPv6], more in [IPoWIRELESS]. Nevertheless, deterministic capabilities are required in a number of wireless use cases as well [RAW-USE-CASES]. With new scheduled radios such as TSCH and OFDMA [RAW-TECHNOS] being developed to provide determinism over wireless links at the lower layers, providing DetNet capabilities is now becoming possible.

Wireless networks operate on a shared medium where uncontrolled interference, including the self-induced multipath fading cause random transmission losses. Fixed and mobile obstacles and reflectors may block or alter the signal, causing transient and unpredictable variations of the throughput and packet delivery ratio (PDR) of a wireless link. This adds new dimensions to the statistical effects that affect the quality and reliability of the link.

Reliable and Available Wireless (RAW) takes up the challenge of providing highly available and reliable end-to-end performances in a network with scheduled wireless segments. To achieve this, RAW leverages multiple links and parallel transmissions, providing enough diversity and redundancy to ensure the timely packet delivery while preserving energy and optimizing the use of the shared spectrum.

"In-Progress" IETF RAW - Reliable and Available Wireless Architecture - 3

As opposed to routing trees, Distance-Vector protocols can enable more than one feasible successors along non-equal-cost multipath forwarding graphs. This provide redundancy and allow to dynamically adapt the forwarding operation to the state of the links. But this protection is limited since only a subset of the nodes along the path will have an alternate feasible successor.

RAW solves that problem by defining Protection Paths that can be fully non-congruent and can be activated dynamically upon failures. This requires additional control to take the routing decision early enough along the possible paths to route around the failure. RAW defines a end-to-end control loop that dynamically controls the activation and deactivation of the feasible Protection Paths.

This document presents the RAW problem and associated terminology in Section 3.2, presents a conceptual model for RAW in Section 4, and, based on that model, elaborates on an in-network optimization control loop in Section 5.2.

RAW uses the following terminology and acronyms:

ARQ

Automatic Repeat Request, enabling an acknowledged transmission and retries. ARQ is a typical model at Layer-2 on a wireless medium. ARQ is typically implemented hop-by-hop and not end-to-end in wireless networks. Else, it introduces excessive indetermination in latency, but a limited number of retries within a bounded time may be used within end-to-end constraints.

FEC

Forward Error Correction, adding redundant data to protect against a partial loss without retries.

HARQ

Hybrid Automatic Repeat Request, combining FEC and ARQ.

MCS

Modulation and Coding Scheme. Controls the throughput of the Link to maintain reliable transmissions.

PAREO

Packet (hybrid) ARQ, Replication, Elimination and Ordering. PAREO is a superset Of DetNet's PREOF that includes leveraging lower-layer (typically wireless) techniques such as short range broadcast, MUMIMO, PHY rate and other Modulation Coding Scheme (MCS) adaptation, constructive interference and overhearing, separately or in combination, to increase the end-to-end reliability. PAREO functions that are actuated at the lower layers may be controlled through abstract interfaces by the RAW extensions within the DetNet Service sub-layer.

```
                +---------+
                | IoT G/W |
                +---------+
                    EGR  <=== Elimination at Egress
                    | |
           /------/   \-------\    Wired backbone
           |                  |
        +--|--+            +--|--+
        |  |  | Backbone   |  |  | Backbone
        |  |  | Router     |  |  | Router
        +--|--+            +--|--+
           |                  |
        o   \     o          /  lane
      o      o      o---o---o   o      o   o  o
              \  o /     o          o         o
       o   o   \  /       o         low power lossy network
                \/ o          o        o
             o  IN <=== Replication at recovery graph Ingress
                 |
                 o <- source device
```

Figure 1: Example IoT Recovery Graph to an IoT Gateway with 1+1 Redundancy

```
------------------- forward direction --------------------->

      a ==> b ==> C -=- F ==> G ==> H     T1       I: Ingress
    /              \   /      |        \ /         E: Egress
   I                 o        n         E -=- T2   T1, T2, T3:
    \              /   \      |        / \           External
      p ==> q ==> R -=- T ==> U ==> v     T3         Targets

     Uppercase: DetNet Relay nodes
     Lowercase: DetNet Transit nodes

     I ==> a ==> b ==> C : an forward Segment to targets F and o
     C ==> o ==> T: an forward Segment to target T (and/or U)
     G | n | U : a crossing Segment to targets G or U
     I --> F --> E : an forward Lane to targets T1, T2, and T3

     I, a, b, C, F, G, H, E : a path to T1, T2, and/or T3
     I, p, q, R, o, F, G, H, E : lane-crossing alternate path
```

Figure 2: A Recovery Graph and its Components

With respect to Communication Interfaces that are relevant for Vertical Applications in VAL in 5G, it is important to distinguish between:

- The Vertical Applications' point of view, and

- The 3GPP Network's point of view.

The relation between those two (2) (in the Figure a simplified version of the Communication stack presented) where:
- PHY Layer,
- MAC layer and
- IP Layer (some parts) are part of the 3GPP Network.

The Layers that are part of the 3GPP Network are referred to as *Lower Communication Layers* (**LCLs**).

The Communication Stack also includes an Application.

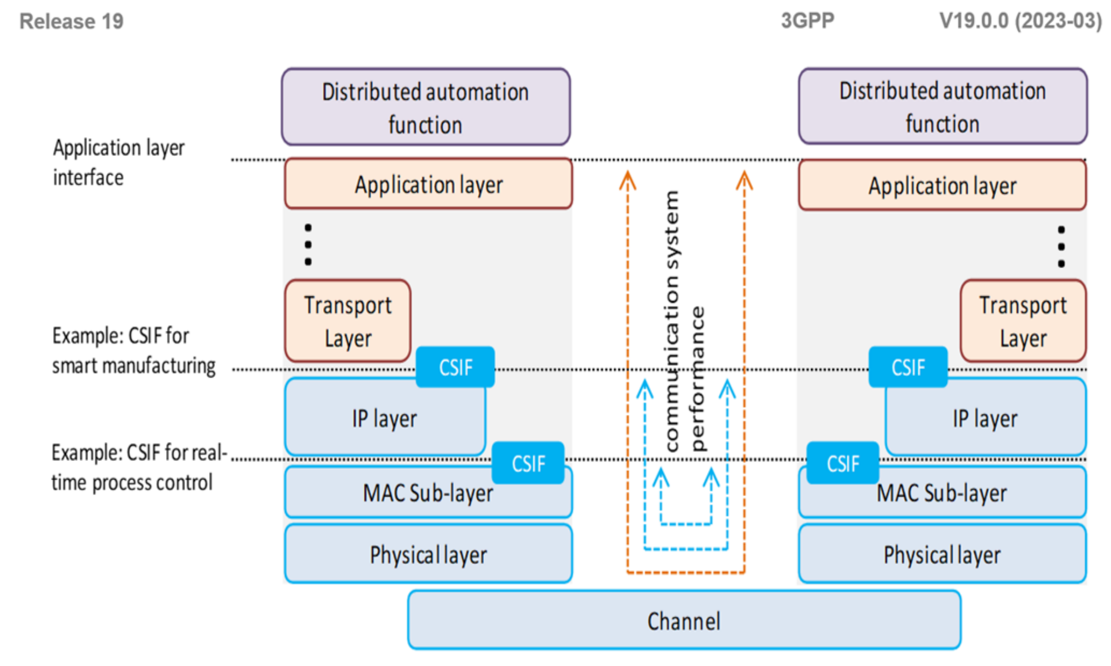


Figure: 5G System Network Performance Measurement at different Communication System Interfaces (CSIFs)

The *OSI Layers related to providing Data to the Application* are referred to as the "*Higher Communication Layers* (**HCL**).

The Interface between **LCL** and **HCL** is referred to as *Communication Service Interface* (**CSIF**).

For the assessment of the **overall System Performance**, it is important to differentiate between the 3GPP Network's Performance (i.e., including only the **LCL** and measured at the **CSIF**) and the overall System Performance including the Application Layer (i.e., including both, the **LCL** and the **HCL**).

In the Figure, the Orange arrow depicts the Vertical Application's point of view. The Blue Arrows indicate two (2) options to measure the 3GPP Network's Performance, i.e., including and excluding **the IP Layer**.

The Figure illustrates *How Messages are transmitted from a Source Application Device (e.g., a Programmable Logic Controller) to a Target Application Device (e.g. an Industrial Robot).*

The *Source Application Function* (**AF**) is executed in the Source Operating System (**OS**) and hands over a message to the Application Layer Interface of the Source Communication Device.

In the Higher Communication Layers (**HCL**), which are not part of the **3GPP System**, the Data is processed.

From the **HCL** the Data is transferred to *the Lower Communication Layers* (**LCL**), which are part of the **3GPP System**. After transmission through the Physical Communication Channel and the **LCL** of the Target Communication Device, the Data is passed to the HCL and lastly to the Target Application Device. Characteristic Parameters with respect to Time are defined in the Figure

From 3GPP System point of view:

- **Transfer interval of 5G System**: Time between the arrival of two (2) pieces of Data at the **Source CSIF.**

- **End-to-end (E2E) Latency**: Time measured from the point when a piece of Data received at the CSIF in the Source Communication Device until the same Piece of Data is passed to the *CSIF in the Target Communication Device*.

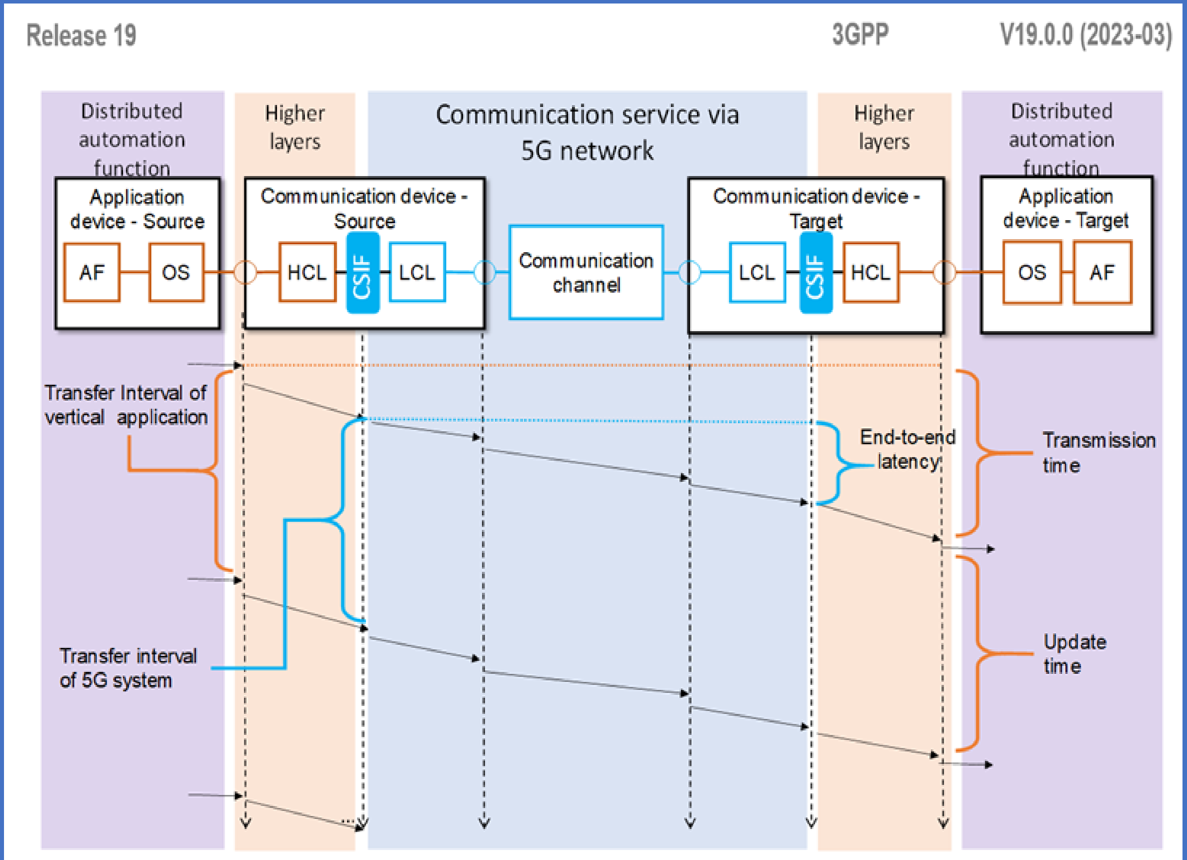


Figure: 5G System Network Communication System Interfaces (CSIFs) Relation between Application Device and Communication Device (DL example)

***The Figure** illustrates How Messages are transmitted from a Source Application Device (e.g., a Programmable Logic Controller) to a Target Application Device (e.g. an Industrial Robot).*

From Vertical Application Point of View:

- **Transfer Interval of Vertical Application**: Time between the transmission of two (2) successive pieces of Data from the Source Application.

- **Transmission Time**: Time measured from the point when a piece of Data is handed from the Application Layer Interface of the Source Application Device, until the same piece of Data is received at the Application Layer Interface of the Target Application Device.

- **Update Time**: Time between the reception of two (2) consecutive pieces of Data at the Application Layer Interface to the Target Application Device.

If not stated otherwise, the terms "End-to-End (E2E) Latency" and "Transfer Interval" refer to the 3GPP System / 5G Network Parameters.

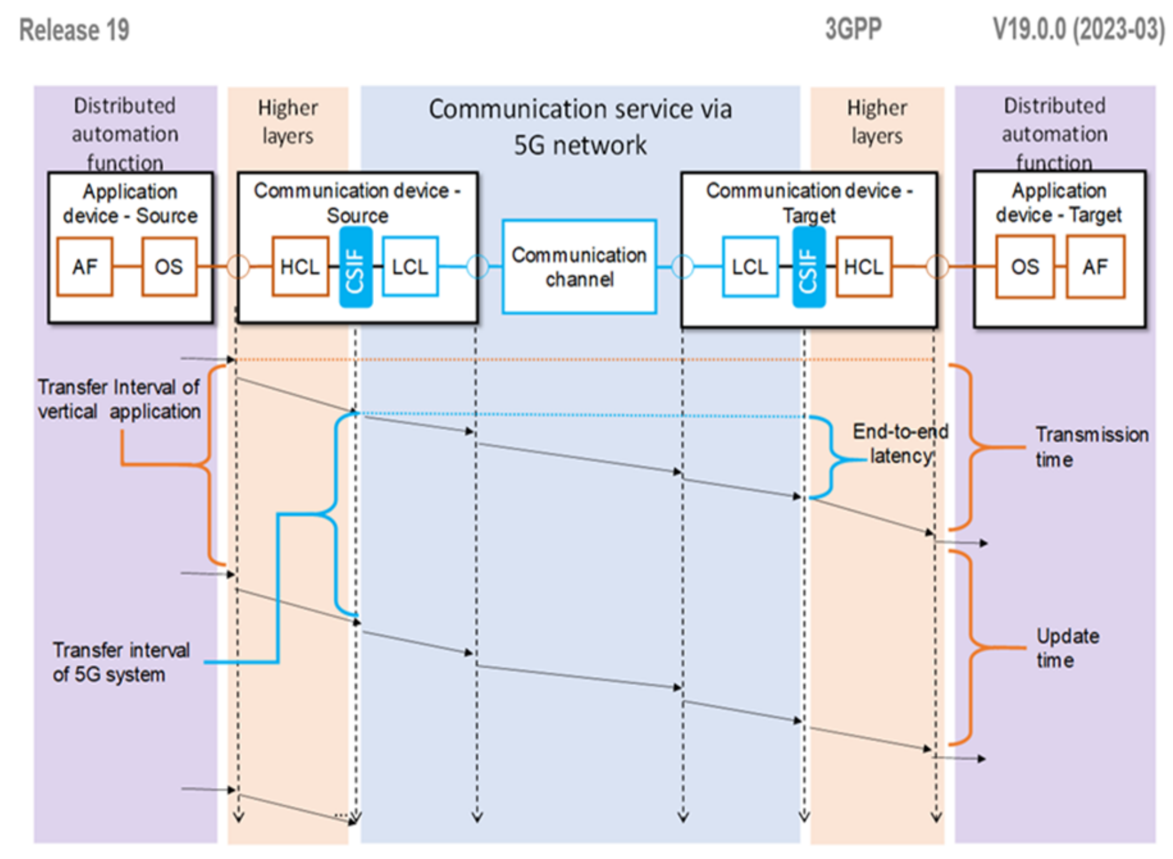


Figure: 5G System Network Communication System Interfaces (CSIFs) Relation between Application Device and Communication Device (DL example)

5G System Communication Services Fundamental Network perspectives

5GS brings two **(2) fundamental perspectives** concerning ***"Dependable Communication" in 5G Systems***, namely:

A) The **End-to-End (E2E) Communication Services** perspective &

B) The **Network** perspective (see Figure).

Communication Service Availability is considered an important Service Performance requirement for Cyber-physical Applications, especially for ***Applications with Deterministic Traffic.***

The ***Communication Service Availability*** depends on the "**Latency**" and "**Reliability**" (in the context of *Network Layer Packet Transmissions*, as defined in 5GS Service Requirements of the Logical Communication Link, as well as the Survival Time of the Cyber-Physical Application.

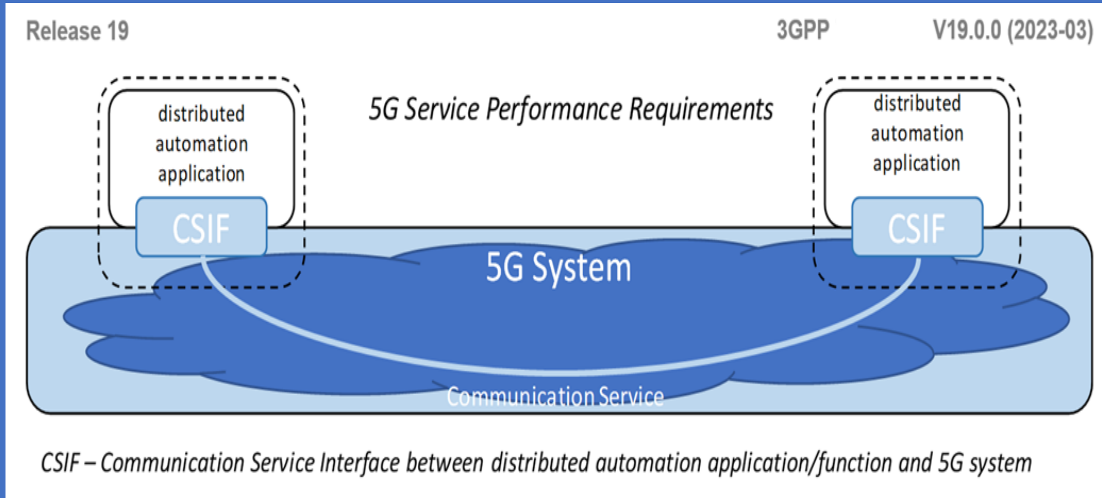


Figure: 5G System Network perspective

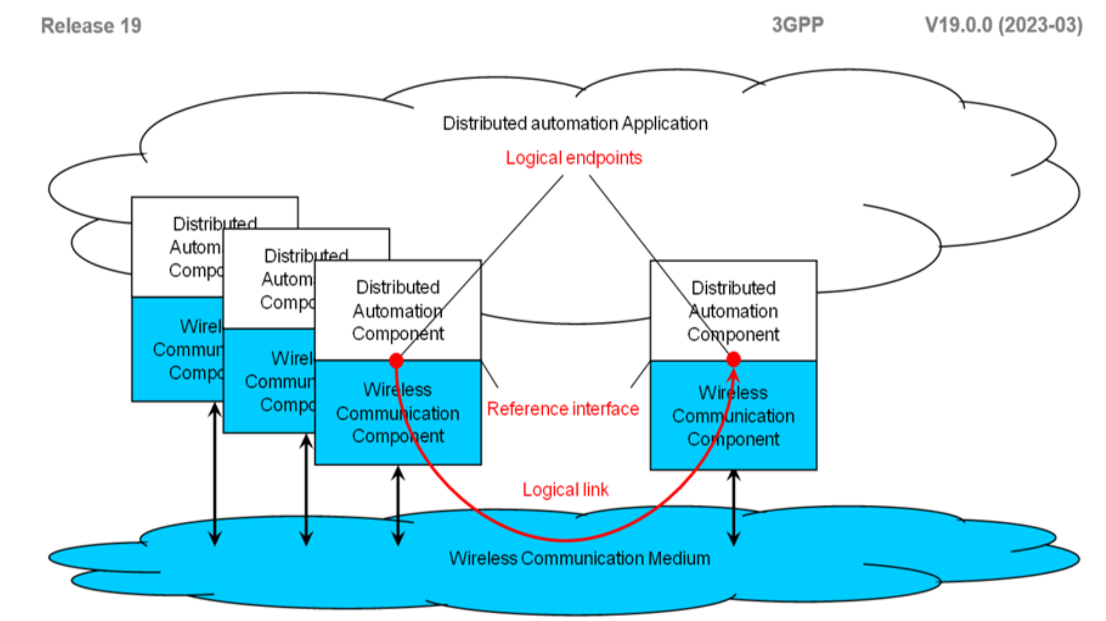


Figure: 5G System Communication Logical Link in Automation abstract diagram for Industrial Radio Communication

The "**Communication Service Reliability**" requirements also depend on the *Operation Characteristics* of the corresponding *Cyber-Physical Applications.*

Typically, the Communication Services critical for the Automation Application also come with stringent **Communication "Service Reliability"** requirements.

Note that the **Communication Service Reliability** requirement has no direct relationship with the **"Communication Service Availability"** requirement.

The "# of UEs" in the tables in the following slides is intended to give an indication of the "UE density" that would need to be served within a given Service Area.

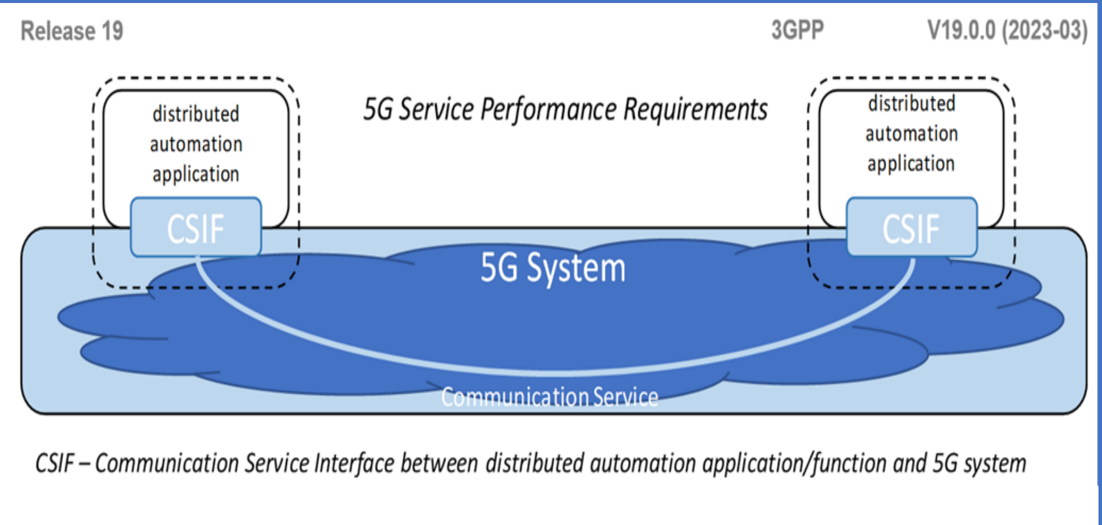


Figure: 5G System Network perspective

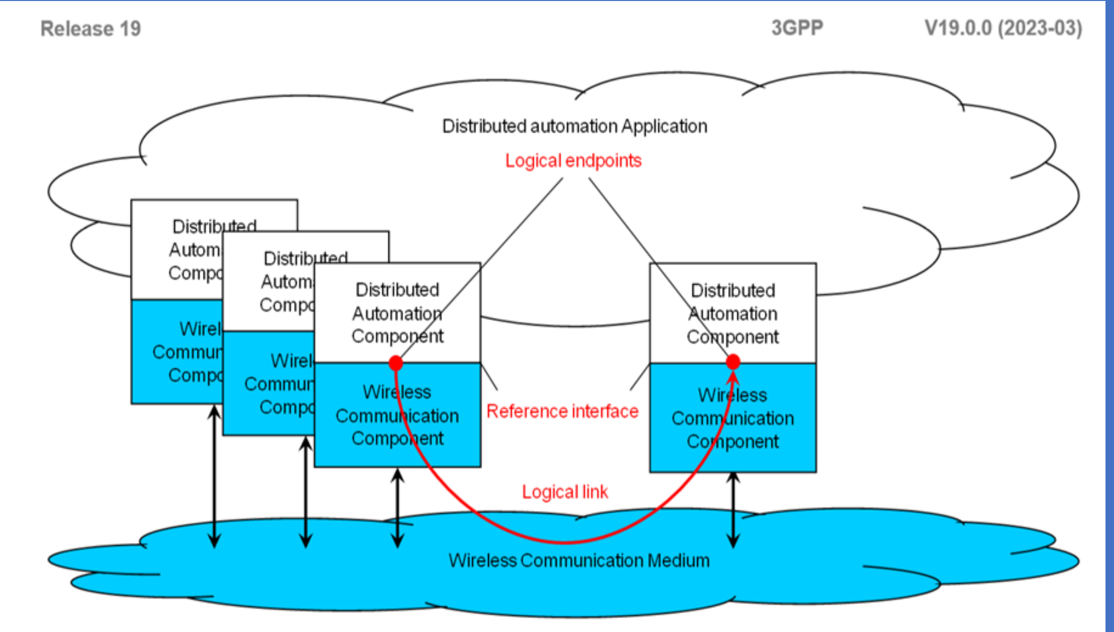


Figure: 5G System Communication Logical Link in Automation abstract diagram for Industrial Radio Communication

5G defined Service Availability and Reliability

Relation of reliability and communication service availability

Availability and reliability are used both in 3GPP and vertical industries, but with different meanings. Communication service availability addresses the availability of a communication service. This definition follows the vertical standard IEC 61907 [7]. On the other hand, reliability is a 3GPP term and addresses the availability of a communication network. The relation of both terms is depicted for a mobile network.

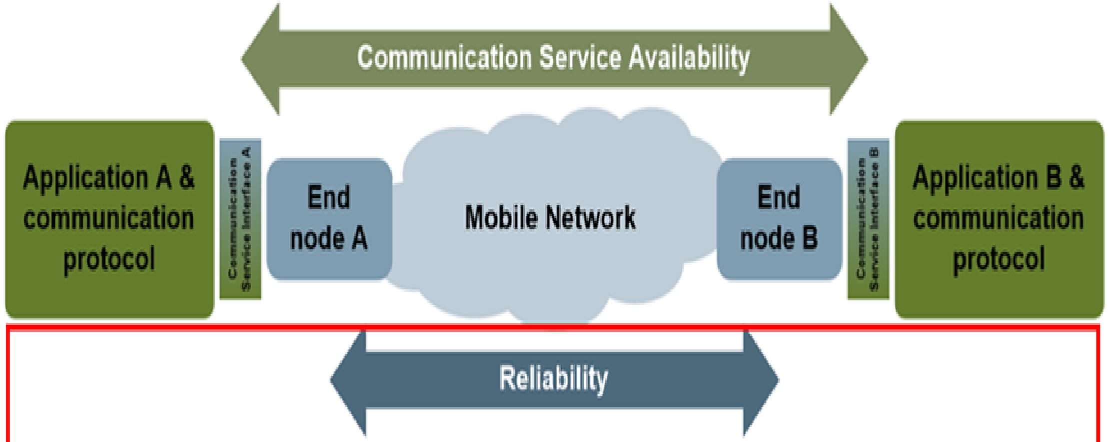


Figure : Illustration of the concepts reliability and communication service availability.

As depicted, reliability covers the communication-related aspects between two nodes (here: end nodes), while communication service availability addresses the communication-related aspects between two communication service interfaces. This might seem to be a small difference, but this difference can lead to situations, where reliability and communication service availability have different values.

Release 19 3GPP V19.0.0 (2023-03)

Example: packets dropped at the communication service interface

The related scenario is depicted .

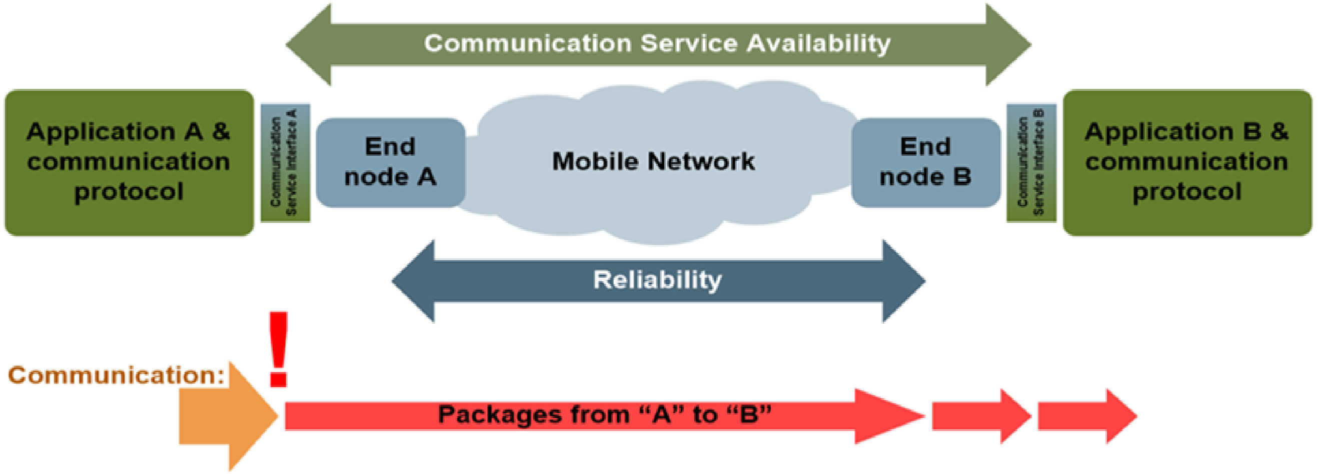


Figure : Example in which reliability and communication service availability have different values. Only half of the packets handed over to the end node A are actually transmitted to end node B and then handed over to application B at the communication service interface B.

This scenario describes unicast communication of evenly interspersed packets from application A to B. The packets are handed over at the communication service interface A from the application to the communication network, and the packets are then transmitted to the end node B. However, only every second packet is actually successfully handed over to end node A and then transmitted to end node B. Thus, only half of the packets arrive at application B. Note though that the reliability of the mobile network is 100%, since all packets transmitted by end node A are delivered to end node B within the time constraint required by the targeted service. However, depending on the agreed QoS, the communication service availability can be of the same value as the reliability or much lower. For instance, if the agreed survival time is equal to or larger than the end-to-end latency, reliability and communication service availability are equal. However, if the survival time is smaller, the reliability is two times the communication service availability.

Note that the shortest time interval over which the communication service availability should be calculated is the sum of maximum allowed end-to-end latency and survival time.

The *Communication Service* in the Figure may be implemented as a Logical Communication Link:

A) between a UE, on one side and a Network Server on the other side or

B) between a UE on one side and a UE on the other side.

In some cases, a Local Approach (e.g. Network Edge) is preferred for the Communication Service on the Network side in order to reduce the Latency, to increase Communication Service Availability, or to keep "Sensitive Data" in a *Non-Public Network* (**NPN/SNPN**) on the Factory site.

The tables in the following slides provide Sets of Requirements where "***Periodicity"*** and ***"Determinism***" are critical to meeting Cyber-Physical Control Application needs in various Vertical Scenarios.

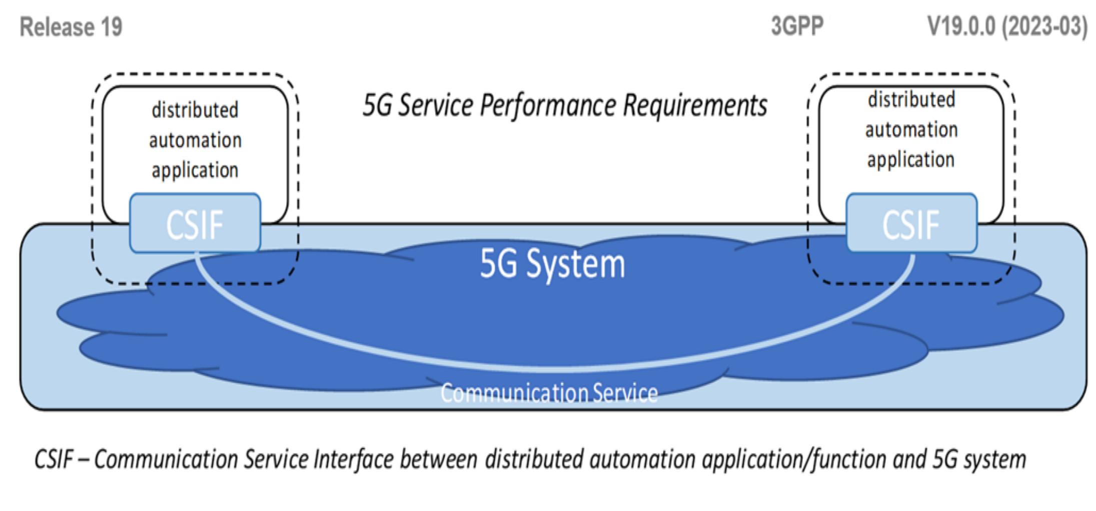


Figure: 5G System Network perspective

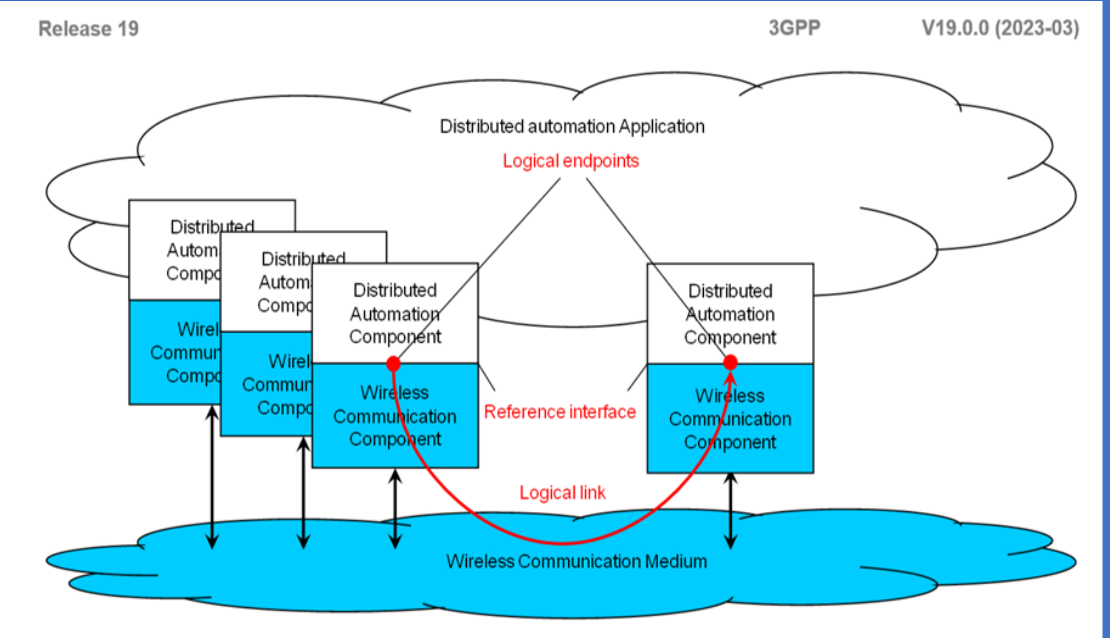


Figure: 5G System Communication Logical Link in Automation abstract diagram for Industrial Radio Communication

While many UCs have similar KPI values, the important distinction is that in order to meet the needs of different Verticals and different Use Cases (UCs), **the 5GS will need to be sufficiently flexible to allow Deployment Configurations that can meet the different Sets of KPIs specific to each UC.**

Communication Service Availability is considered an important Service Performance requirement for Cyber-Physical Applications, especially for ***Applications with Deterministic Traffic***.

The **Communication Service Availability** depends on the **Latency** and **Reliability** (in the **context of Network Layer Packet Transmissions**, as defined in 5GS Service Requirements of the Logical Communication Link, as well as the Survival Time of the Cyber-Physical Application.

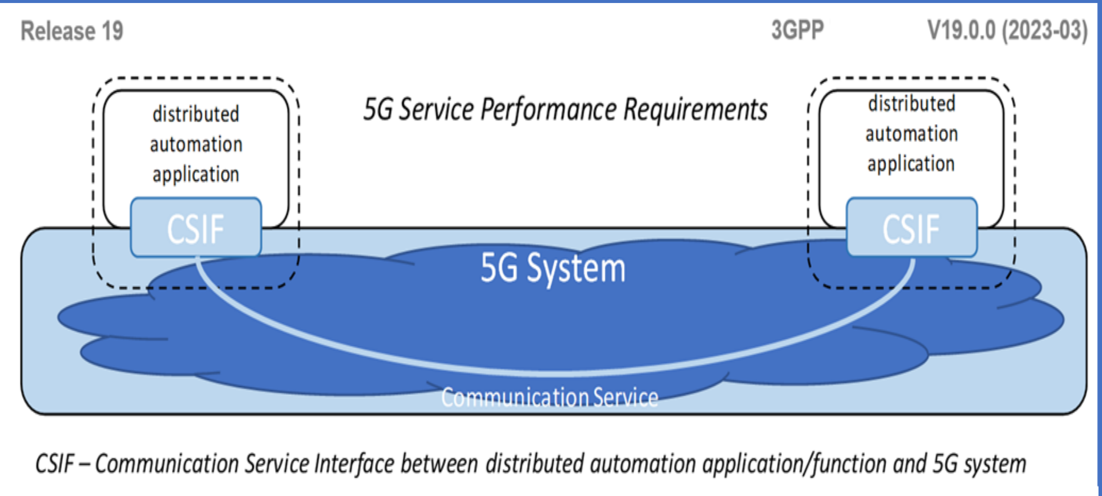


Figure: 5G System Network perspective

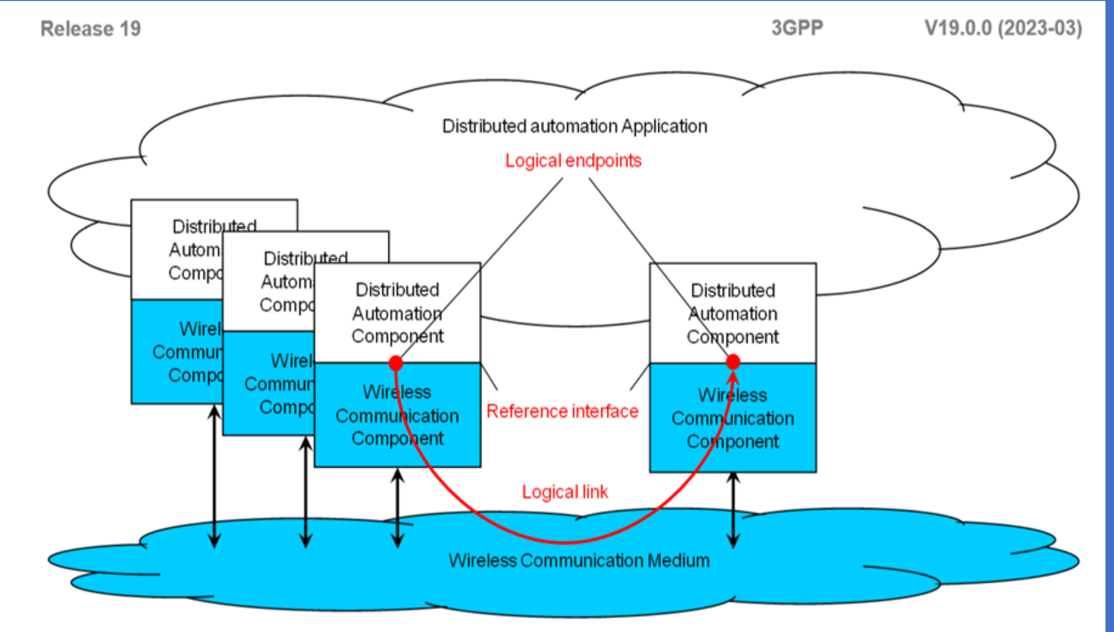


Figure: 5G System Communication Logical Link in Automation abstract diagram for Industrial Radio Communication

An example of the relationship between **Reliability** (in the context of ***Network Layer Packet Transmissions***, as defined in the 5GS Service Requirements), ***Survival Time and Communication Service Availability*** of a Logical Communication Link is illustrated in the Table.

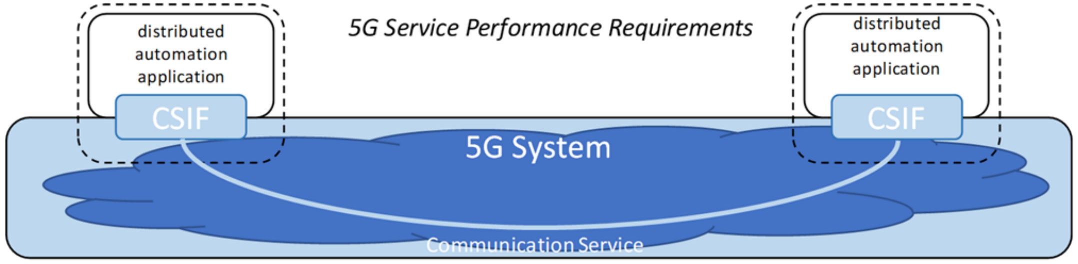
This is done for a special Case where Packet Errors are uncorrelated, which in many Cases is an unrealistic assumption.

Release 19 3GPP V19.0.0 (2023-03)

Table: 5G System example of relationship between Reliability (as defined in 5GS Service Requirements) and Communication Service Availability when the Survival Time is equal to the Transfer Interval

Communication service availability	Reliability 1 - p
99.999 9 %	99.9 %
99.999 999 %	99.99 %
99.999 999 99 %	99.999 %
99.999 999 999 9 %	99.999 9 %
99.999 999 999 999 %	99.999 99 %

Release 19 3GPP V19.0.0 (2023-03)



CSIF – Communication Service Interface between distributed automation application/function and 5G system

Figure: 5G System Network perspective

Release 19 3GPP V19.0.0 (2023-03)

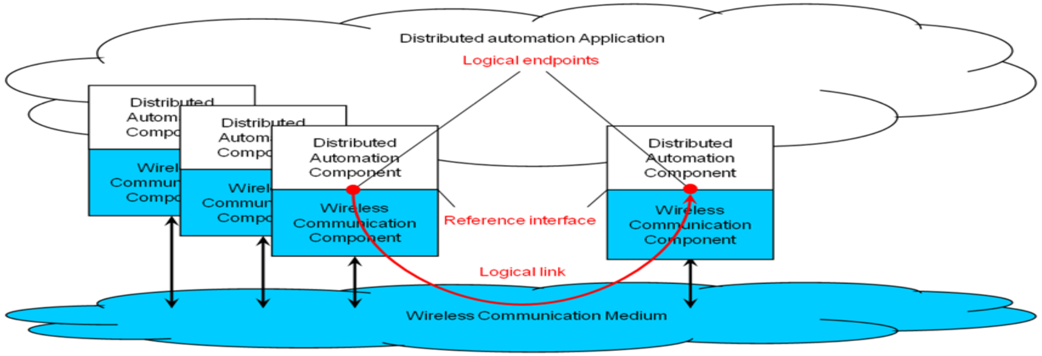


Figure: 5G System Communication Logical Link in Automation abstract diagram for Industrial Radio Communication

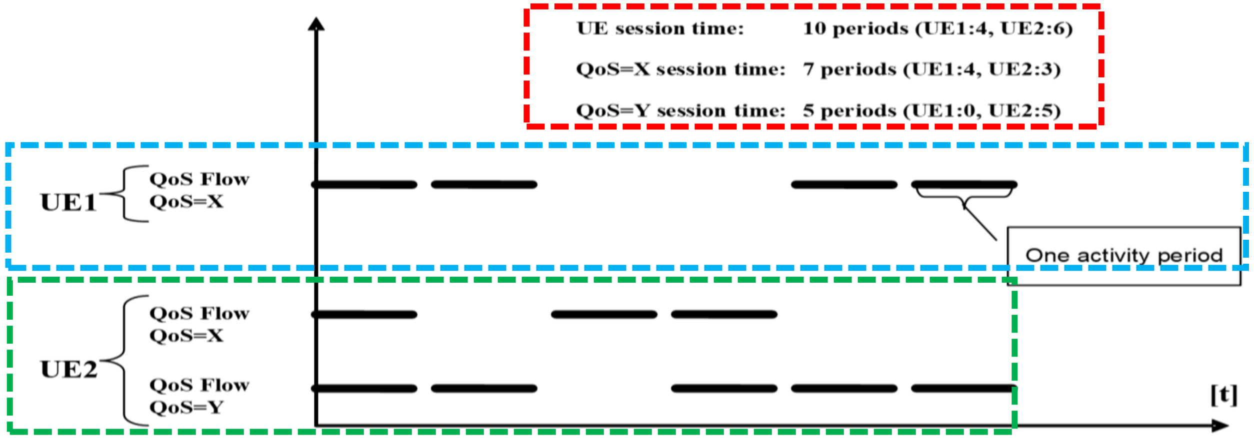
5GS QoS flow Retainability

To define (from a 5GS QoS flow Retainability point of view) if a QoS flow is considered active or not, the QoS flows can be divided into two (2) groups:

1. For QoS flows with "***Bursty Flow***", a QoS flow is said to be active if there is User Data in the PDCP queue in any of the directions or if any Data (UL or DL) has been transferred during the last 100 ms.

2. For QoS flows with "***Continuous Flow***", the QoS flow (& the UE) is seen as being "active" in the context of this measurement as long as the UE is in "RRC Connected" state, & the Session Time is increased from the first (1st) Data Transmission on the QoS Flow until 100 ms after the last Data Transmission on the QoS flow.

A ***particular QoS Flow*** is defined to be of type "*Continuous Flow"* if the mapped 5QI is any of {1, 2, 65, 66}.



Hence a measurement QoS flow Retainability on UE level is defined (R2) to provide a measurement for the overall QoS flow Retainability.

$$R2 = \frac{\Sigma_{QoS} QF.RelActNbr.QoS}{QF.SessionTimeUE}$$

d) SubNetwork, NRCellCU

e) The definition of the service provided by 5GS is QoS flows.

The retainability rate is defined as:

$$\frac{\text{Number of abnormally released QoS flow with data in any of the buffers}}{\text{Active QoS flow Time}} \quad [\text{Releases/Session time}]$$

$$\frac{\text{Number of abnormally released QoS flow with data in any of the buffers}}{} \quad [\text{Releases/Session time}]$$

5G UE RAN Throughput definition

To achieve a Throughput Measurement (below examples are given for DL) that is independent of file size and gives a relevant result, it is important to remove the volume and time when the Resource on the Radio Interface is not fully utilized. (Successful transmission, buffer empty in the Figure).

To achieve a Throughput Measurement that is independent of "Bursty Traffic" pattern, it is important to make sure that "idle gaps" between Incoming Data is not included in the measurements.

That shall be done as considering each Burst of Data as one (1) sample.

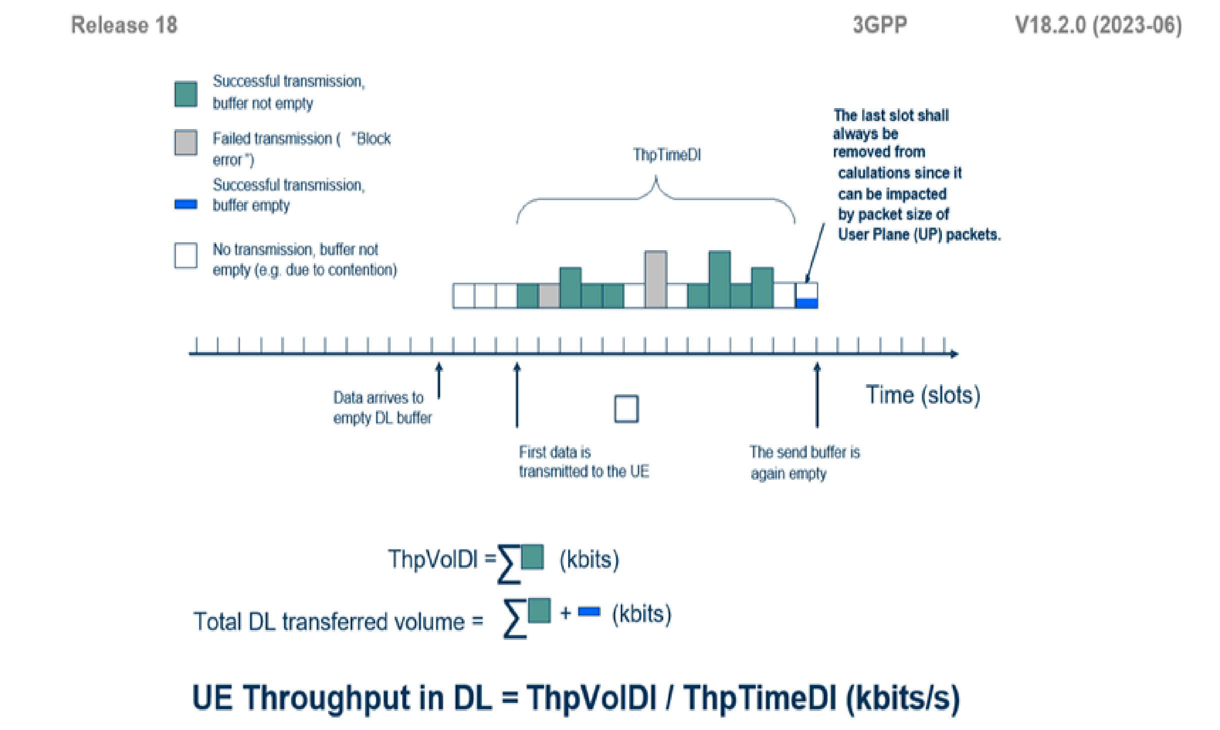


Figure: 5G UE RAN Throughput definition

5G System defined Periodic Deterministic Communication - 1

5G System Periodic Deterministic Communication is periodic with **stringent requirements on Timeliness and Availability** of the Communication Service. A transmission occurs every transfer interval.

Information on the underlying UCs of the sets of requirements in the following slides Table provides information on characteristic parameters and influence quantities.

The 5GS shall be able to provide Periodic Deterministic Communication with the Service Performance Requirements for Individual Logical Communication Links that realize the Communication Services reported in the Table.

Process and Asset Monitoring using Industrial Wireless Sensors is a special Case of Periodic Deterministic Communication with more relaxed Requirements on Timeliness and Availability.

These UCs put a slightly different Set of Requirements on the 5G System due to the specific constraints of Industrial Wireless Sensors.

These Requirements for Individual Logical Communication Links are listed in the Table.

Figure: 5G System Periodic Deterministic Communication Service Performance Requirements

Characteristic parameter				Influence quantity						
Communication service availability: target value (note 1)	Communication service reliability: mean time between failures	End-to-end latency: maximum (note 2) (note 12a)	Service bit rate: user experienced data rate (note 12a)	Message size [byte] (note 12a)	Transfer interval: target value (note 12a)	Survival time (note 12a)	UE speed (note 13)	# of UEs	Service area (note 3)	Remarks
99.999 % to 99.999 99 %	~ 10 years	< transfer interval value	–	50	500 µs	500 µs	≤ 75 km/h	≤ 20	50 m x 10 m x 10 m	Motion control (A.2.2.1)
99.999 9 % to 99.999 999 %	~ 10 years	< transfer interval value	–	40	1 ms	1 ms	≤ 75 km/h	≤ 50	50 m x 10 m x 10 m	Motion control (A.2.2.1)
99.999 9 % to 99.999 999 %	~ 10 years	< transfer interval value	–	20	2 ms	2 ms	≤ 75 km/h	≤ 100	50 m x 10 m x 10 m	Motion control (A.2.2.1)
99.999 9 %	–	< 5 ms	1 kbit/s (steady state) 1.5 Mbit/s (fault case)	< 1,500	< 60 s (steady state) ≥ 1 ms (fault case)	transfer interval	stationary	20	30 km x 20 km	Electrical Distribution – Distributed automated switching for isolation and service restoration (A.4.4); (note 5)
99.999 9 % to 99.999 999 %	~ 10 years	< transfer interval value		1 k	≤ 10 ms	10 ms	-	5 to 10	100 m x 30 m x 10 m	Control-to-control in motion control (A.2.2.2); (note 9)
99.999 9 % to 99.999 999 %	~ 10 years	< transfer interval value (note 5)	50 Mbit/s		≤ 1 ms	3 x transfer interval	stationary	2 to 5	100 m x 30 m x 10 m	Wired-2-wireless 100 Mbit/s link replacement (A.2.2.4)
99.999 9 % to 99.999 999 %	~ 10 years	< transfer interval value (note 5)	250 Mbit/s		≤ 1 ms	3 x transfer interval	stationary	2 to 5	100 m x 30 m x 10 m	Wired-2-wireless 1 Gbit/s link replacement (A.2.2.4)
99.999 9 % to 99.999 999 %	~ 10 years	< transfer interval value		1 k	≤ 50 ms	50 ms	-	5 to 10	1,000 m x 30 m x 10 m	Control-to-control in motion control (A.2.2.2); (note 9)
> 99.999 9 %	~ 10 years	< transfer interval value	–	40 to 250	1 ms to 50 ms (note 6) (note 7)	transfer interval value	≤ 50 km/h	≤ 2,000	≤ 1 km²	Mobile robots (A.2.2.3)
99.999 9 % to 99.999 999 %	~ 1 month	< transfer interval value	–	40 to 250	4 ms to 8 ms (note 7)	transfer interval value	< 8 km/h (linear movement)	TBD	50 m x 10 m x 4 m	Mobile control panels – remote control of e.g. assembly robots, milling machines (A.2.4.1); (note 9)

Figure: 5G System Periodic Deterministic Communication Service Performance Requirements

Characteristic parameter				Influence quantity						
Communication service availability: target value (note 1)	**Communication service reliability: mean time between failures**	**End-to-end latency: maximum (note 2)** (note 12a)	**Service bit rate: user experienced data rate** (note 12a)	**Message size [byte]** (note 12a)	**Transfer interval: target value** (note 12a)	**Survival time** (note 12a)	**UE speed** (note 13)	**# of UEs**	**Service area (note 3)**	**Remarks**
99.999 999 %	1 day	< 8 ms (note 14)	250 kbit/s	40 to 250	8 ms	16 ms	quasi-static; up to 10 km/h	2 or more	30 m x 30 m	Mobile Operation Panel: Emergency stop (connectivity availability) (A.2.4.1A)
99.999 99 %	1 day	< 10 ms (note 14)	< 1 Mbit/s	< 1024	10 ms	~10 ms	quasi-static; up to 10 km/h	2 or more	30 m x 30 m	Mobile Operation Panel: Safety data stream (A.2.4.1A)
99.999 999 %	1 day	10 ms to 100 ms (note 14)	10 kbit/s	10 to 100	10 ms to 100 ms	transfer interval	stationary	2 or more	100 m² to 2,000 m²	Mobile Operation Panel: Control to visualization (A.2.4.1A)
99.999 999 %	1 day	< 1 ms (note 14)	12 Mbit/s to 16 Mbit/s	10 to 100	1 ms	~ 1 ms	stationary	2 or more	100 m²	Mobile Operation Panel: Motion control (A.2.4.1A)
99.999 999 %	1 day	< 2 ms (note 14)	16 kbit/s (UL) 2 Mbit/s (DL)	50	2 ms	~ 2 ms	stationary	2 or more	100 m²	Mobile Operation Panel: Haptic feedback data stream (A.2.4.1A)
99.999 9 % to 99.999 999 %	~ 1 year	< transfer interval	–	40 to 250	< 12 ms (note 7)	12 ms	< 8 km/h (linear movement)	TBD	typically 40 m x 60 m; maximum 200 m x 300 m	Mobile control panels - remote control of e.g. mobile cranes, mobile pumps, fixed portal cranes (A.2.4.1); (note 9)
99.999 9 % to 99.999 999 %	≥ 1 year	< transfer interval value	–	20	≥ 10 ms (note 8)	0	typically stationary	typically 10 to 20	typically ≤ 100 m x 100 m x 50 m	Process automation – closed loop control (A.2.3.1)
99.999 %	TBD	~ 50 ms	–	~ 100	~ 50 ms	TBD	stationary	≤ 100,000	several km² up to 100,000 km²	Primary frequency control (A.4.2); (note 9)
99.999 %	TBD	~ 100 ms	–	~ 100	~ 200 ms	TBD	stationary	≤ 100,000	several km² up to 100,000 km²	Distributed Voltage Control (A.4.3) (note 9)

Figure: 5G System Periodic Deterministic Communication Service Performance Requirements

Characteristic parameter				Influence quantity						
Communication service availability: target value (note 1)	**Communication service reliability: mean time between failures**	**End-to-end latency: maximum (note 2)** (note 12a)	**Service bit rate: user experienced data rate** (note 12a)	**Message size [byte]** (note 12a)	**Transfer interval: target value** (note 12a)	**Survival time** (note 12a)	**UE speed** (note 13)	**# of UEs**	**Service area (note 3)**	**Remarks**
> 99.999 9 %	~ 1 year	< transfer interval value	–	15 k to 250 k	10 ms to 100 ms (note 7)	transfer interval value	≤ 50 km/h	≤ 2,000	≤ 1 km²	Mobile robots – video-operated remote control (A.2.2.3)
> 99.999 9 %	~ 1 year	< transfer interval value	–	40 to 250	40 ms to 500 ms (note 7)	transfer interval value	≤ 50 km/h	≤ 2,000	≤ 1 km²	Mobile robots (A.2.2.3)
99.99 %	≥ 1 week	< transfer interval value	–	20 to 255	100 ms to 60 s (note 7)	≥ 3 x transfer interval value	typically stationary	≤ 10,000 to 100,000	≤ 10 km x 10 km x 50 m	Plant asset management (A.2.3.3)
>99.999 999 %	> 10 years	< 2 ms	2 Mbit/s to 16 Mbit/s	250 to 2,000	1 ms	transfer interval value	stationary	1	< 100 m²	Robotic Aided Surgery (A.6.2)
>99.999 9 %	> 1 year	< 20 ms	2 Mbit/s to 16 Mbit/s	250 to 2,000	1 ms	transfer interval value	stationary	2 per 1,000 km²	< 400 km (note 12)	Robotic Aided Surgery (A.6.2)
>99.999 %	>> 1 month (< 1 year)	< 20 ms	2 Mbit/s to 16 Mbit/s	80	1 ms	transfer interval value	stationary	20 per 100 km²	< 50 km (note 12)	Robotic Aided Diagnosis (A.6.3)
99.999 9 % to 99.999 999 %	~ 10 years	< 0.5 x transfer interval	2.5 Mbit/s	250 500 with localisation information	> 5 ms > 2.5 ms > 1.7 ms (note 10)	0 transfer interval 2 x transfer interval (note 10)	≤ 6 km/h (linear movement)	2 to 8	10 m x 10 m x 5 m; 50 m x 5 m x 5 m (note 11)	Cooperative carrying – fragile work pieces; (ProSe communication) (A.2.2.5)
99.999 9 % to 99.999 999 %	~ 10 years	< 0.5 x transfer interval	2.5 Mbit/s	250 500 with localisation information	> 5 ms > 2.5 ms > 1.7 ms (note 10)	0 transfer interval 2 x transfer interval (note 10)	≤ 12 km/h (linear movement)	2 to 8	10 m x 10 m x 5 m; 50 m x 5 m x 5 m (note 11)	Cooperative carrying – elastic work pieces; (ProSe communication) (A.2.2.5)

Figure: 5G System Periodic Deterministic Communication Service Performance Requirements

Characteristic parameter				Influence quantity						
Communication service availability: target value (note 1)	**Communication service reliability: mean time between failures**	**End-to-end latency: maximum (note 2)** (note 12a)	**Service bit rate: user experienced data rate** (note 12a)	**Message size [byte]** (note 12a)	**Transfer interval: target value** (note 12a)	**Survival time** (note 12a)	**UE speed** (note 13)	**# of UEs**	**Service area (note 3)**	**Remarks**
> 99.9 %		DL: < 10 ms UL: < 10 ms	UL: > 16 Mbit/s (urban), 640 Mbit/s (rural) DL: > 100 kbit/s (note 15)	UL: 800 kbyte	UL: 10 ms			> $10/km^2$ (urban), > $100/km^2$ (rural) (note 16)		Distributed energy storage – monitoring (A.4.6)
> 99.9 %		DL: < 10 ms UL: < 1 s	UL: > 128 kbit/s (urban), 10.4 Mbit/s (rural); DL: > 100 kbit/s (note 15)	UL: 1.3 Mbyte DL: > 100 kbyte	UL: 1000 ms			> $10/km^2$ (urban), > $100/km^2$ (rural) (note 16)		Distributed energy storage – data collection (A.4.6)
> 99.99 %		General information data collection: < 3 s (note 17)	UL: < 2 Mbit/s DL: < 1 Mbit/s					< $10,000/km^2$ (note 18)		Advanced metering (A.4.7)
99.999 %		< 10 ms	2 Mbit/s to 10 Mbit/s		normal: 1 s; fault: 2 ms (note 24)			$54/km^2$ (note 19), $78/km^2$ (note 20)		Intelligent distributed feeder automation (A.4.4.3)
> 99.99 %		10 ms, 100 ms, 3 s (note 22)	> 2 Mbit/s (note 21)					500 in the service area (note 23)	Communication distance is from 100 m to 500 m, outdoor, indoor / deep indoor	Smart distribution –transformer terminal (A.4.8)
99.999 %		5 ms, 10 ms, 15 ms (note 25)	1.2 Mbit/s to 2.5 Mbit/s	< 245 byte	≤ 1 ms ≤ 2 ms (note 26)			≤ $100/km^2$	several km^2	High speed current differential protection (note 12a) (A.4.4.4)
99.999 9 %		3 ms	5.4 Mbit/s	140 byte	≤ 1 ms		stationary			Distributed Energy Resources (DER) and micro-grids (A.4.9)

Release 19 3GPP V19.0.0 (2023-03)

Figure: 5G System Periodic Deterministic Communication Service Performance Requirements

Characteristic parameter				Influence quantity						
Communication service availability: target value (note 1)	**Communication service reliability: mean time between failures**	**End-to-end latency: maximum (note 2)** (note 12a)	**Service bit rate: user experienced data rate** (note 12a)	**Message size [byte]** (note 12a)	**Transfer interval: target value** (note 12a)	**Survival time** (note 12a)	**UE speed** (note 13)	**# of UEs**	**Service area (note 3)**	**Remarks**
99.999 9 %		100 ms (note 12a and note 5)	< 1 kbit/s per DER				stationary			Ensuring uninterrupted communication service availability during emergencies (A.4.10)

NOTE 1: One or more retransmissions of network layer packets may take place in order to satisfy the communication service availability requirement.
NOTE 2: Unless otherwise specified, all communication includes 1 wireless link (UE to network node or network node to UE) rather than two wireless links (UE to UE).
NOTE 3: Length x width (x height).
NOTE 4: (void)
NOTE 5: Communication includes two wireless links (UE to UE).
NOTE 6: This covers different transfer intervals for different similar use cases with target values of 1 ms, 1 ms to 10 ms, and 10 ms to 50 ms.
NOTE 7: The transfer interval deviates around its target value by < ±25 %.
NOTE 8: The transfer interval deviates around its target value by < ±5 %.
NOTE 9: Communication may include two wireless links (UE to UE).
NOTE 10: The first value is the application requirement, the other values are the requirement with multiple transmission of the same information (two or three times, respectively).
NOTE 11: Service Area for direct communication between UEs. The group of UEs with direct communication might move throughout the whole factory site (up to several km²).
NOTE 12: Maximum straight-line distance between UEs.
NOTE 12a: It applies to both UL and DL unless stated otherwise.
NOTE 13: It applies to both linear movement and rotation unless stated otherwise.
NOTE 14: The mobile operation panel is connected wirelessly to the 5G system. If the mobile robot/production line is also connected wirelessly to the 5G system, the communication includes two wireless links.
NOTE 15: Service bit rate for one energy storage station.
NOTE 16: Activity storage nodes/km^2. This value is used for deducing the data volume in an area that features multiple energy storage stations. The data volume can be calculated with the following formula (current service bit rate per storage station) x (activity storage nodes/km^2) + (video service bit rate per storage station) x (activity storage nodes/km^2).
NOTE 17: One-way delay from 5G IoT device to backend system. The distance between the two is below 40 km (city range).
NOTE 18: Typical connection density in today's city environment. With the evolution from centralised meters to socket meters in the home, the connection density is expected to increase 5 to 10 times.
NOTE 19: When the distributed terminals are deployed along an overhead line, there are about 54 terminals per square kilometre.
NOTE 20: When the distributed terminals are deployed in power distribution cabinets, there are about 78 terminals per square kilometre.
NOTE 21: Service bit rate of the smart metering application between the smart distribution transformer terminal and the energy end equipment. Once there are multiple smart grid applications, the required service bit rate will be higher.
NOTE 22: The end-to-end latency depends on the applications supported by the smart distribution transformer terminal. The lower the end-to-end latency, the more applications can be supported.
NOTE 23: The service area is circular with a radius between 100 m and 500 m (0.031 km^2 to 0.79 km^2).
NOTE 24: During the normal working phase of the feeder system, the heartbeat packet is transmitted periodically with a 1 s transfer interval. When a fault occurs, the heartbeat is sent with a 2 ms transfer interval.
NOTE 25: The maximum allowed delay between two protection relays would be between 5 ms and 10 ms, depending on the voltage (see IEC 61850-90-1 for more details [aa]). For some legacy systems, the end-to-end latency is usually set to 15 ms.
NOTE 26: For a sampling rate of 600 Hz, the transfer interval is 1.7 ms. For 1200 Hz, the transfer interval is 0.83 ms.

Figure: 5G System Periodic Deterministic Communication Service Performance Requirements

Characteristic parameter				Influence quantity						
Communication service availability: target value (note 1)	**Communication service reliability: mean time between failures**	**End-to-end latency: maximum (note 2)** (note 12a)	**Service bit rate: user experienced data rate** (note 12a)	**Message size [byte]** (note 12a)	**Transfer interval: target value** (note 12a)	**Survival time** (note 12a)	**UE speed** (note 13)	**# of UEs**	**Service area (note 3)**	**Remarks**
99.999 9 %		100 ms (note 12a and note 5)	< 1 kbit/s per DER				stationary			Ensuring uninterrupted communication service availability during emergencies (A.4.10)

NOTE 1: One or more retransmissions of network layer packets may take place in order to satisfy the communication service availability requirement.
NOTE 2: Unless otherwise specified, all communication includes 1 wireless link (UE to network node or network node to UE) rather than two wireless links (UE to UE).
NOTE 3: Length x width (x height).
NOTE 4: (void)
NOTE 5: Communication includes two wireless links (UE to UE).
NOTE 6: This covers different transfer intervals for different similar use cases with target values of 1 ms, 1 ms to 10 ms, and 10 ms to 50 ms.
NOTE 7: The transfer interval deviates around its target value by < ±25 %.
NOTE 8: The transfer interval deviates around its target value by < ±5 %.
NOTE 9: Communication may include two wireless links (UE to UE).
NOTE 10: The first value is the application requirement, the other values are the requirement with multiple transmission of the same information (two or three times, respectively).
NOTE 11: Service Area for direct communication between UEs. The group of UEs with direct communication might move throughout the whole factory site (up to several km²).
NOTE 12: Maximum straight-line distance between UEs.
NOTE 12a: It applies to both UL and DL unless stated otherwise.
NOTE 13: It applies to both linear movement and rotation unless stated otherwise.
NOTE 14: The mobile operation panel is connected wirelessly to the 5G system. If the mobile robot/production line is also connected wirelessly to the 5G system, the communication includes two wireless links.
NOTE 15: Service bit rate for one energy storage station.
NOTE 16: Activity storage nodes/km². This value is used for deducing the data volume in an area that features multiple energy storage stations. The data volume can be calculated with the following formula (current service bit rate per storage station) x (activity storage nodes/km²) + (video service bit rate per storage station) x (activity storage nodes/km²).
NOTE 17: One-way delay from 5G IoT device to backend system. The distance between the two is below 40 km (city range).
NOTE 18: Typical connection density in today's city environment. With the evolution from centralised meters to socket meters in the home, the connection density is expected to increase 5 to 10 times.
NOTE 19: When the distributed terminals are deployed along an overhead line, there are about 54 terminals per square kilometre.
NOTE 20: When the distributed terminals are deployed in power distribution cabinets, there are about 78 terminals per square kilometre.
NOTE 21: Service bit rate of the smart metering application between the smart distribution transformer terminal and the energy end equipment. Once there are multiple smart grid applications, the required service bit rate will be higher.
NOTE 22: The end-to-end latency depends on the applications supported by the smart distribution transformer terminal. The lower the end-to-end latency, the more applications can be supported.
NOTE 23: The service area is circular with a radius between 100 m and 500 m (0.031 km² to 0.79 km²).
NOTE 24: During the normal working phase of the feeder system, the heartbeat packet is transmitted periodically with a 1 s transfer interval. When a fault occurs, the heartbeat is sent with a 2 ms transfer interval.
NOTE 25: The maximum allowed delay between two protection relays would be between 5 ms and 10 ms, depending on the voltage (see IEC 61850-90-1 for more details [aa]). For some legacy systems, the end-to-end latency is usually set to 15 ms.
NOTE 26: For a sampling rate of 600 Hz, the transfer interval is 1.7 ms. For 1200 Hz, the transfer interval is 0.83 ms.

Table: 5G System Communication Service Performance Requirements for Industrial Wireless Sensors

Characteristic parameter						Influence quantity						
Communication service availability: target value	Communication service reliability: mean time between failure	End-to-end latency (note 6)	Transfer interval (note 1) (note 7)	Service bit rate: user experienced data rate (note 2) (note 7)	Battery lifetime [year] (note 3)	Message Size [byte] (note 7)	Survival time (note 7)	UE speed	UE density [UE / m²]	Range [m] (note 4)	Remarks
99.99 %	≥ 1 week	< 100 ms	100 ms to 60 s	≤ 1 Mbit/s	≥ 5	20 (note 5)	3 x transfer interval	stationary	Up to 1	< 500	Process monitoring, e.g. temperature sensor (A.2.3.2)
99.99 %	≥ 1 week	< 100 ms	≤ 1 s	≤ 200 kbit/s	≥ 5	25 k	3 x transfer interval	stationary	Up to 0.05	< 500	Asset monitoring, e.g. vibration sensor (A.2.3.2)
99.99 %	≥ 1 week	< 100 ms	≤ 1 s	≤ 2 Mbit/s	≥ 5	250 k	3 x transfer interval	stationary	Up to 0.05	< 500	Asset monitoring, e.g. thermal camera (A.2.3.2)

NOTE 1: The transfer interval deviates around its target value by < ± 25 %.
NOTE 2: The traffic is predominantly mobile originated.
NOTE 3: Industrial sensors can use a wide variety of batteries depending on the use case, but in general they are highly constrained in terms of battery size.
NOTE 4: Distance between the gNB and the UE.
NOTE 5: The application-level messages in this use case are typically transferred over Ethernet. For small messages, the minimum Ethernet frame size of 64 bytes applies and dictates the minimum size of the PDU sent over the air interface.
NOTE 6: It applies to both UL and DL unless stated otherwise.
NOTE 7: It applies to UL.

5G System defined Aperiodic Deterministic Communication

5G System Aperiodic deterministic communication is without a Pre-set Sending Time, but still with Stringent Requirements on Timeliness and Availability of the Communication Service.

Further information on Characteristic Parameters and influence Quantities are shown in the Table.

The 5G System shall be able to provide Aperiodic Deterministic Communication with the Service Performance Requirements for Individual Logical Communication Links that realize the Communication Services reported in the Table.

Figure: 5G System Aperiodic Deterministic Communication Service Performance Requirements

Characteristic parameter (KPI)				**Influence quantity**					
Communication service availability	**Communication service reliability: mean time between failures**	**Max Allowed End-to-end latency (note 1)** (note 5)	**Service bit rate: user-experienced data rate** (note 5)	**Message size [byte]** (note 5)	**Survival time**	**UE speed** (note 6)	**# of UEs**	**Service Area (note 3)**	**Remarks**
> 99.999 9 %	~ 1 week	10 ms	UL: > 10 Mbit/s	–	–	≤ 50 km/h	≤ 2,000	≤ 1 km^2	Mobile robots – video streaming (A.2.2.3)
99.999 9 % to 99.999 999 %	~ 1 month	< 30 ms	> 5 Mbit/s	–	–	< 8 km/h (linear movement)	TBD	TBD	Mobile control panels - parallel data transmission (A.2.4.1)
99.999 999 %	1 day	<8 ms (note 8)	250 kbit/s	40 to 250	16 ms	quasi-static; up to 10 km/h	2 or more	30 m x 30 m	Mobile Operation Panel: Emergency stop (emergency stop events) (A.2.4.1A)
99.999 9 %	–	< 50 ms	0.59 kbit/s 28 kbit/s	< 100	–	stationary	10 km^{-2} to 100 km^{-2}	TBD	Smart grid millisecond level precise load control (A.4.5)
> 99.9 %	~ 1 month	< 10 ms	–	–	–	< 8 km/h (linear movement)	≥ 3	20 m x 20 m x 4 m	Augmented reality; bi-directional transmission to image processing server (A.2.4.2)
99.999 9 % to 99.999 999 %	~ 10 years	< 1 ms (note 4)	25 Mbit/s	–	–	stationary	2 to 5	100 m x 30 m x 10 m	Wired-2-wireless 100 Mbit/s link replacement (A.2.2.4)
99.999 9 % to 99.999 999 %	~ 10 years	< 1 ms (note 4)	500 Mbit/s	–	–	stationary	2 to 5	100 m x 30 m x 10 m	Wired-2-wireless 1 Gbit/s link replacement (A.2.2.4)
> 99.9 %	–	DL: < 10 ms UL:<1 s (rural)	DL: > 100 kbit/s UL: > 5 Gbit/s (note 9)	–	–	stationary	> 100		Distributed energy storage; energy storage station video (A.4.6)
> 99.99 %	–	< 100 ms (note 10);	DL:<1 Mbit/s	–	–	–	–	–	Advanced metering (A.4.7)
> 99.999 %	–	20 ms	–	< 100 byte	–	–	–	several km^2	Distributed automated switching for isolation and service restoration (A.4.4.1) (note 7)
> 99.999 9 %		< 3 ms	–	160 byte	–	–	–	–	Distributed Energy Resources (DERs) and micro-grids (A.4.9) (note 7)

NOTE 1: Unless otherwise specified, all communication includes 1 wireless link (UE to network node or network node to UE) rather than two wireless links (UE to UE).
NOTE 2: (void)
NOTE 3: Length x width x height.
NOTE 4: Scheduled aperiodic traffic with transfer interval (max end-to-end allowed latency < transfer interval).
NOTE 5: It applies to both UL and DL unless stated otherwise.
NOTE 6: It applies to both linear movement and rotation unless stated otherwise.
NOTE 7: Communication includes two wireless links (UE to UE).
NOTE 8: The mobile operation panel is connected wirelessly to the 5G system. If the mobile robot/production line is also connected wirelessly to the 5G system, the communication includes two wireless links.
NOTE 9: The service bit rate in one energy storage station can be calculated as follows:12.5 Mbytes/s x 50 containers x 8 = 5 Gbit/s.
NOTE 10: The maximum allowed end-to-end latency is for accuracy fee control. It is the delay for one-way communication between the backend system and the 5G IoT device. The distance between the two is 40 km or lower (city range).

Non-deterministic Communication subsumes all other Traffic types than Periodic/Aperiodic Deterministic Communication.

This includes Periodic/Aperiodic Non-Real-Time Traffic.

Additional information on the underlying Use Cases (UCs) of the sets of Requirements are seen in the Table.

The 5G System shall be able to provide Non-deterministic Communication with the Service Performance Requirements for Individual Logical Communication Links that realize the Communication Services reported in the Table.

Release 19 3GPP V19.0.0 (2023-03)

Table: 5G System Non-deterministic Communication Service Performance Requirements

Characteristic parameter (KPI)		Influence quantity			
Communication service reliability: mean time between failures	Service bit rate: user-experienced data rate	UE speed (note 2)	# of UEs	Service area (note 1)	Remarks
~ 1 month	DL: ≥ 1 Mbit/s	~ 0 km/h ≤ 75 km/h	≤ 100	50 m x 10 m x 10 m	Motion control - software updates (A.2.2.1)
	UL: > 10 Mbit/s	≤ 50 km/h (linear movement)	≤ 2,000	≤ 1 km^2	Mobile robots; real-time video stream (A.2.2.3)
NOTE 1: Length x width x height NOTE 2: It applies to both linear movement and rotation unless stated otherwise.					

Mixed traffic

Mixed traffic cannot be assigned to one of the other communication patterns exclusively. Additional information on the underlying Use Cases of the sets of Requirements are shown in the Table.

The 5G System shall be able to provide Mixed Traffic Communication with the Service Performance Requirements for Individual Logical Communication Links that realize the Communication Services reported in the Table.

Release 19 3GPP TS V19.0.0 (2023-03)

Table: 5G System Mixed Traffic Communication Service Performance Requirements

Characteristic parameter (KPI)				Influence quantity					Remarks
Communication service availability	Communication service reliability: mean time between failures	Max Allowed End-to-end latency (note 1) (note 3)	Service bit rate: aggregate user-experienced data rate	Message Size [byte]	Survival time	UE speed	# of UEs	Service Area	
99.999 999 9 %	~ 10 years	16 ms				stationary	< 1,000	several km²	Wind power plant – control traffic (A.5.2)
99.999 9 % to 99.999 99 %	1 day	(note 4)	12 Mbit/s	250 to 1,500		quasi-static; up to 10 km/h	2 or more	30 m x 30 m	Mobile Operation Panel: Manufacturing data stream (A.2.4.1A)

NOTE 1: Unless otherwise specified, all communication includes 1 wireless link (UE to network node or network node to UE) rather than two wireless links (UE to UE).
NOTE 2: (void)
NOTE 3: It applies to both UL and DL unless stated otherwise.
NOTE 4: The mobile operation panel is connected wirelessly to the 5G system. If the mobile robot/production line is also connected wirelessly to the 5G system, the communication includes two wireless links.

1. 5G System Network Capability External Exposure

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

External exposure can be categorized as:

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

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

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

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

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

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

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

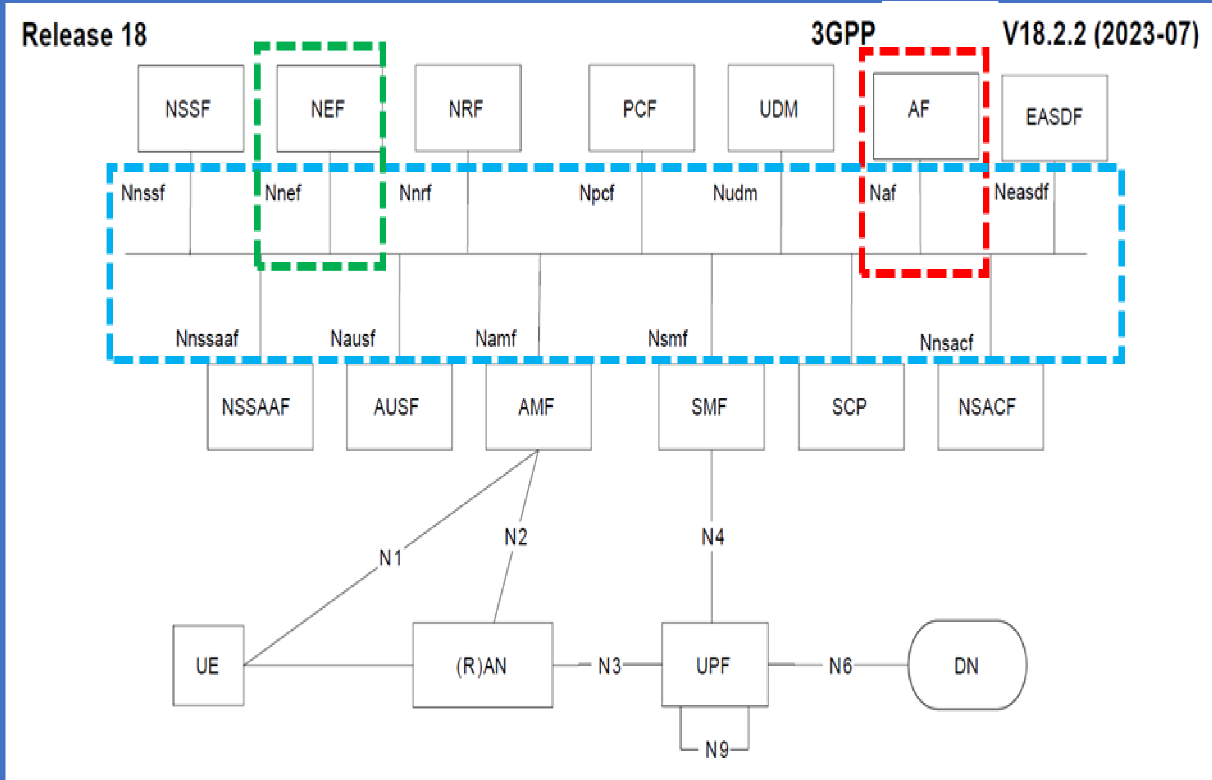


Figure: 5G System Non-Roaming Architecture

1. 5G System Network Capability External Exposure

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

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

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

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

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

- The Address of the UE as provided by the AF; this may be an IP Address or a MAC Address;

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

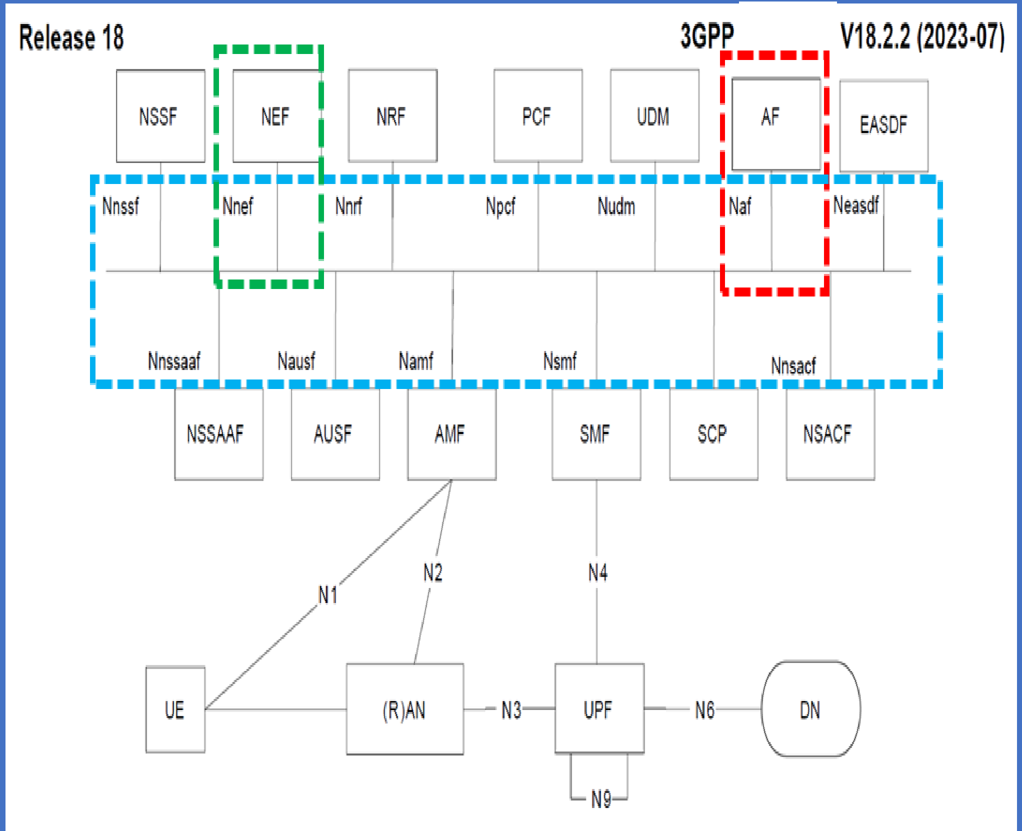


Figure: 5G System Non-Roaming Architecture

1. 5G System Network Capability External Exposure

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

The 5GC exposure may provide an AF specific UE Identifier to the AF:
- that has explicitly requested a translation from the address of the UE to a unique UE identifier (via Nnef_UEId service); or

- that has implicitly requested a translation from the Address of the UE to a AF specific UE Identifier by requesting external exposure about an individual UE identified by its address.

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

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

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

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

NOTE 1: This is to protect User Privacy.

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

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

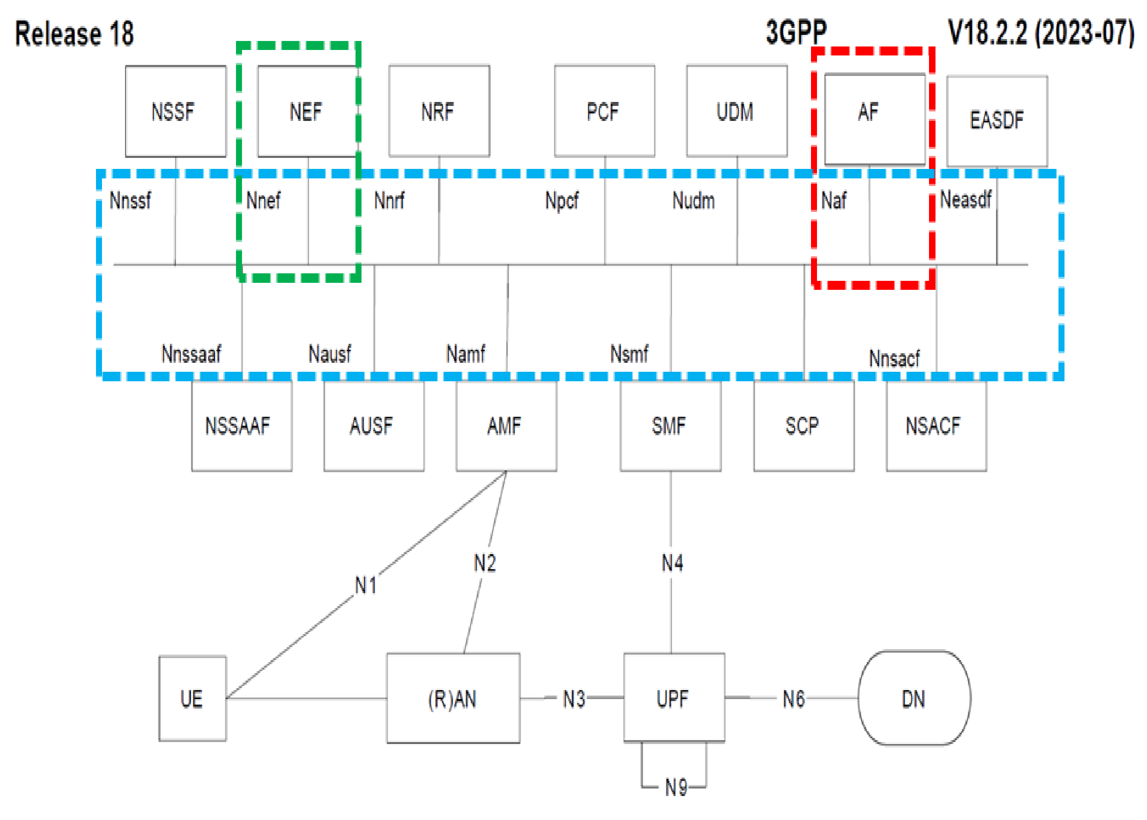


Figure: 5G System Non-Roaming Architecture

5G System Data Collection from an AF

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

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

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

Group Attribute Provisioning

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

An AF may provision attributes for a Group:

- **LADN Service Area**, the LADN Service Area is consisted of Tracking Area (TA) Identities or Geographical Information, it is applicable to each UE member within the Group and for a specific DNN and S-NSSAI.
  - The AF request additionally contains the LADN Service Area as part of DNN & S-NSSAI specific Group Parameters, & the LADN Service Area is stored in UDR as Subscription Data & delivered t to AMF. If the AMF receives the LADN Service Area for a Group, the AMF configures the DNN of the group as LADN DNN.
  - If the AF provides the LADN Service Area in the form of Geographical Information, the NEF maps the Geographical Information to a List of TAs before sending the Service Area to the UDM. LADN per DNN and S-NSSAI as defined in clause 5.6.5a is applicable for enforcement of LADN service area.

- **QoS**, the QoS refers to 5QI, ARP & 5QI Priority Level as defined in 5G System Architecture and it is applicable to each UE Member within the Group & for a specific DNN and S-NSSAI.
  - The AF request additionally contains the QoS for the Group, and the UDM stores such QoS in the UDR & uses such QoS to set 5GS Subscribed QoS Profile in Session Management Subscription data for each UE within the Group.
  - When a UE belongs to Multiple Groups simultaneously, the strictest QoS Profile among Groups the Group Member belongs to is selected.

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

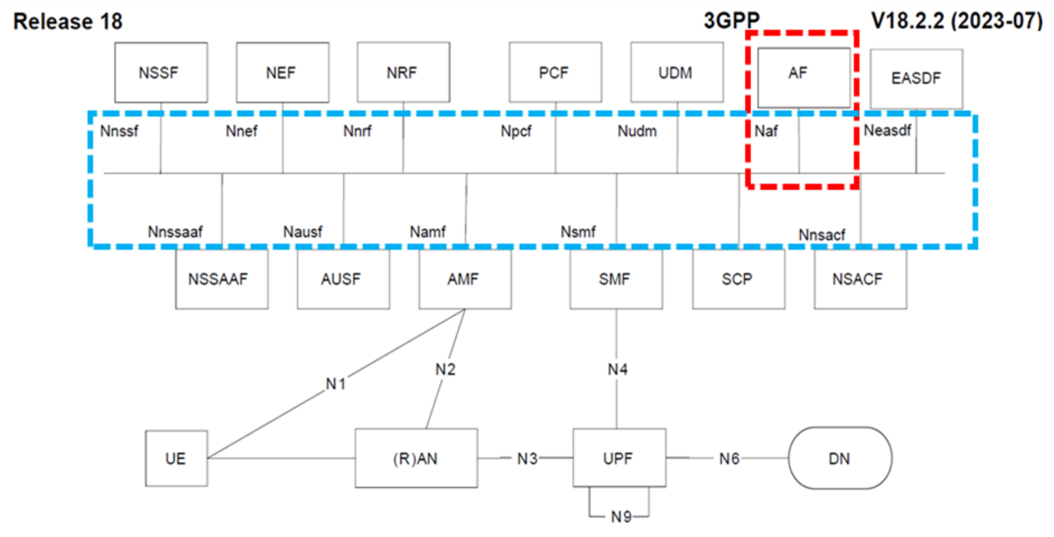


Figure: 5G System Non-Roaming Architecture

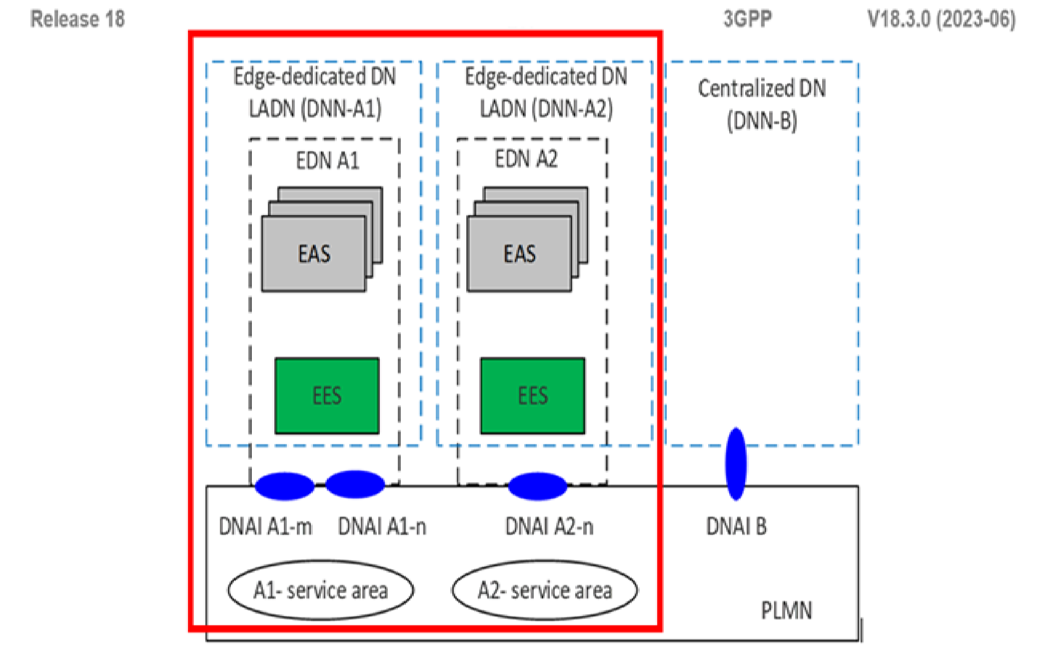


Figure: 5G Architecture for enabling Edge Applications Data Network (DN) Deployment Model for use of Local Area Data Network (LADN)

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

Group Attribute Provisioning

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

An AF may provision attributes for a Group:

Support Change of PDU Session Type for a group of UEs

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

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

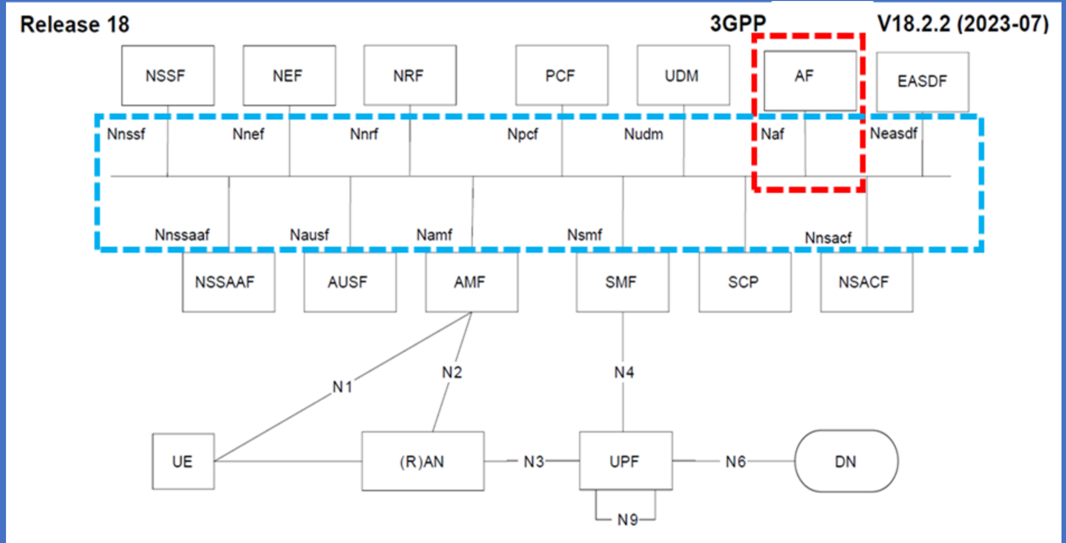
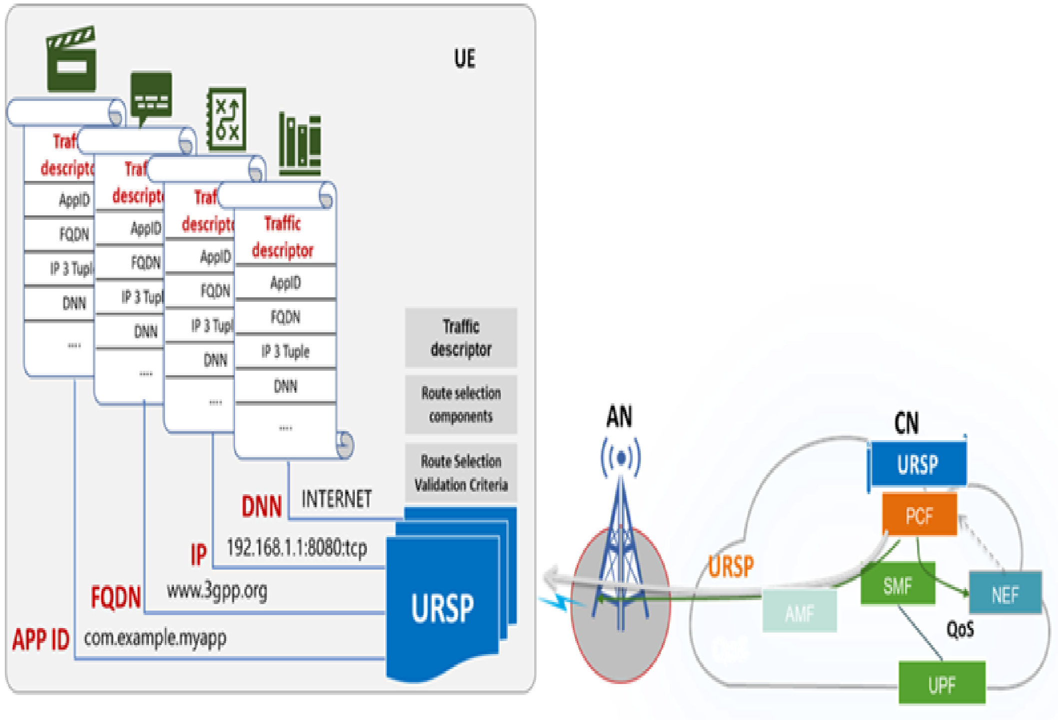


Figure: 5G System Non-Roaming Architecture



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

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

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

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

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

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

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

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

- QoS Monitoring information
- TSC Management Information

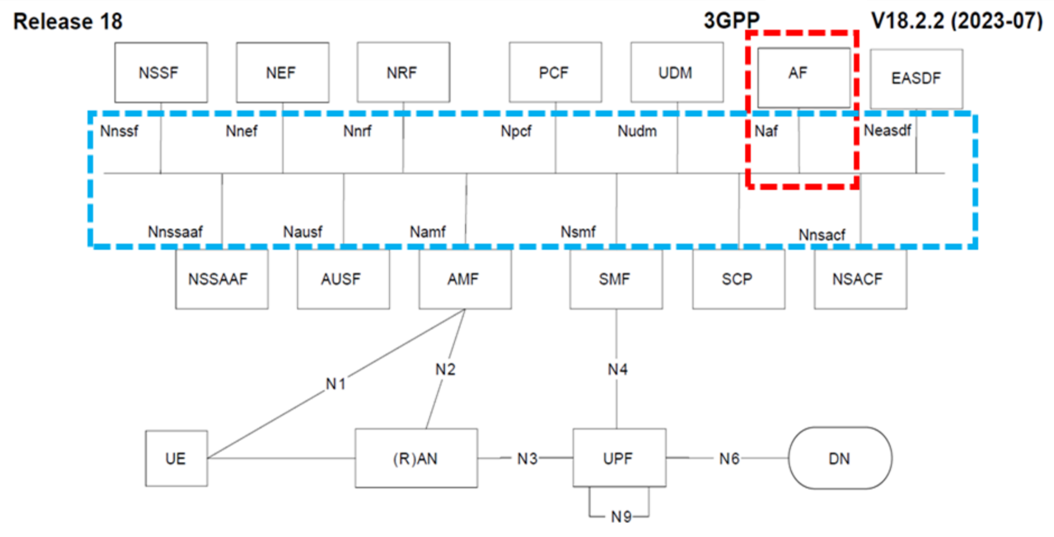


Figure: 5G System Non-Roaming Architecture

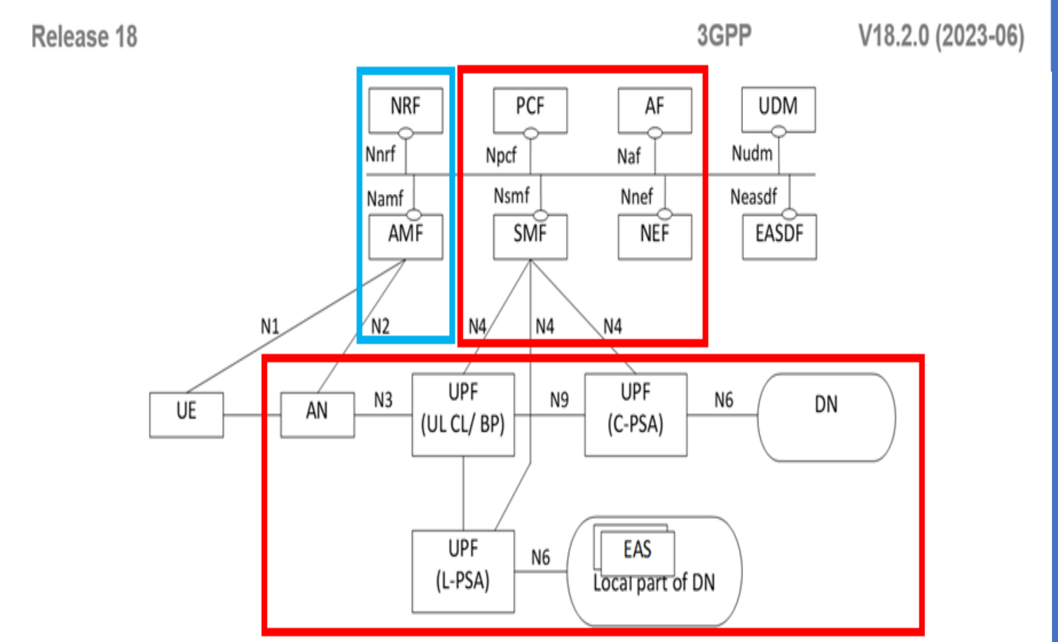


Figure: 5G System Architecture with UL CL/BP access to Edge Application Server (EAS) for Non-Roaming Scenario

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

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

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

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

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

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

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

-

-

-

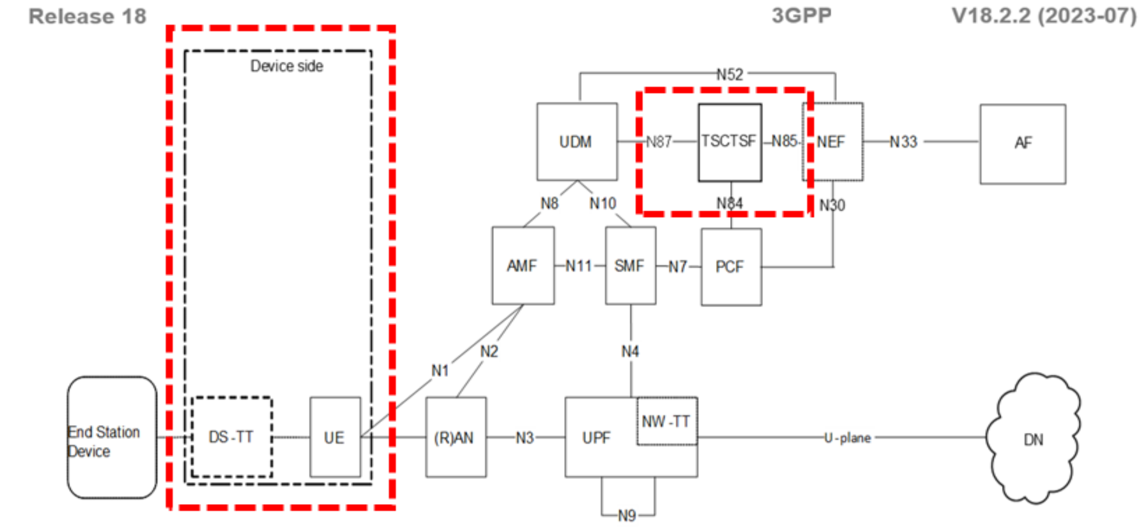


Figure: 5G System Architecture enabling Time Sensitive Communication and Time Synchronization Function (TSCTSF) Services

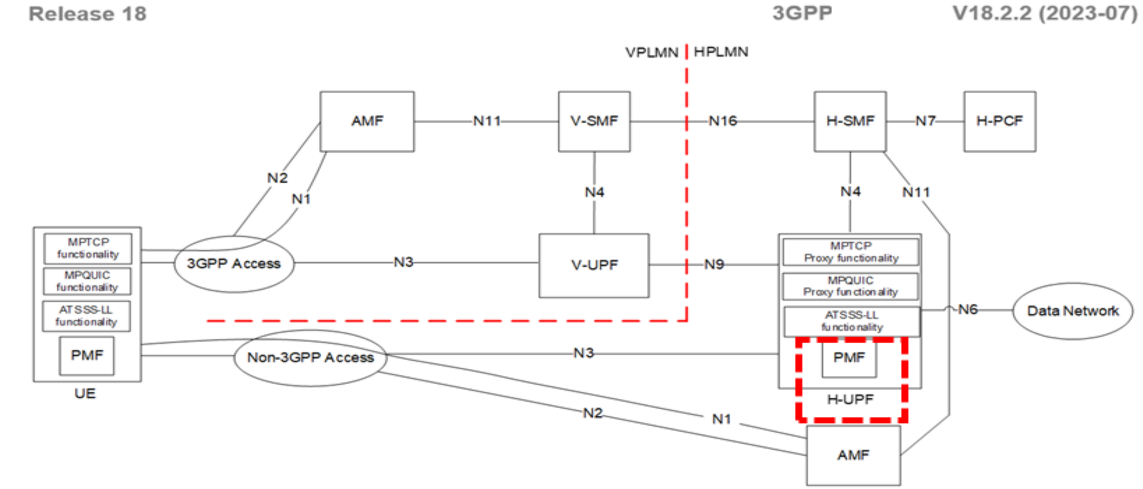


Figure: 5G System with Home-routed Architecture for ATSSS (Access Traffic Steering, Switching, Splitting) support with UE registered to different PLMNs

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

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

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

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

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

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

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

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

Table : Information element contained in AF request

Information Name	Applicable for PCF or NEF (NOTE 1)	Applicable for NEF only	Category
Traffic Description	Defines the target traffic to be influenced, represented by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information.	The target traffic can be represented by AF-Service-Identifier, instead of combination of DNN and optionally S-NSSAI.	Mandatory
Potential Locations of Applications	Indicates potential locations of applications, represented by a list of DNAI(s).	The potential locations of applications can be represented by AF-Service-Identifier.	Conditional (NOTE 2)
Target UE Identifier(s)	Indicates the UE(s) that the request is targeting, i.e. one or a list of individual UE(s), a group of UE represented by Internal Group Identifier(s) (NOTE 3), or any UE accessing the combination of DNN, S-NSSAI and DNAI(s).	GPSI can be applied to identify the individual UE, or External Group Identifier(s) can be applied to identify a group of UE (NOTE 3). External Subscriber Category(s) (NOTE 5).	Mandatory
Spatial Validity Condition	Indicates that the request applies only to the traffic of UE(s) located in the specified location, represented by areas of validity.	The specified location can be represented by geographical area.	Optional
AF transaction identifier	The AF transaction identifier refers to the AF request.	N/A	Mandatory
N6 Traffic Routing requirements	Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation (NOTE 4).	N/A	Optional (NOTE 2)
Application Relocation Possibility	Indicates whether an application can be relocated once a location of the application is selected by the 5GC.	N/A	Optional
UE IP address preservation indication	Indicates UE IP address should be preserved.	N/A	Optional
Temporal Validity Condition	Time interval(s) or duration(s).	N/A	Optional
Information on AF subscription to corresponding SMF events	Indicates whether the AF subscribes to change of UP path of the PDU Session and the parameters of this subscription.	N/A	Optional
Information for EAS IP Replacement in 5GC	Indicates the Source EAS identifier and Target EAS identifier, (i.e. IP addresses and port numbers of the source and target EAS).	N/A	Optional
User Plane Latency Requirement	Indicates the user plane latency requirements	N/A	Optional
Information on AF change	N/A	Indicates the AF instance relocation and relocation information.	Optional
Indication for EAS Relocation	Indicates the EAS relocation of the application(s)	N/A	Optional
Indication for Simultaneous Connectivity over the source and target PSA at Edge Relocation	Indicates that simultaneous connectivity over the source and target PSA should be maintained at edge relocation and provides guidance to determine when the connectivity over the source	N/A	Optional
EAS Correlation indication	Indicates selecting a common EAS for the application identified by the Traffic Description for the set of UEs.		Optional
Common EAS IP address	the common EAS for the application identified by the Traffic Description for a set of UEs the AF request aims at.		Optional
Traffic Correlation ID	Identification of a set of UEs targeted at by the AF request, and accessing the application identified by the Traffic Description.		Optional
FQDN(s)	FQDN(s) used for influencing EASDF-based DNS query procedure as defined in TS 23.548 [138] (NOTE 6).		Optional

NOTE 1: When the AF request targets existing or future PDU Sessions of multiple UE(s) or of any UE and is sent via the NEF, as described in clause 6.3.7.2, the information is stored in the UDR by the NEF and notified to the PCF by the UDR.
NOTE 2: The potential locations of applications and N6 traffic routing requirements may be absent only if the request is for subscription to notifications about UP path management events only or request is for indication of seleting Common EAS for a set of UEs.
NOTE 3: Internal Group ID can only be used by an AF controlled by the operator and only towards PCF. If a list of Internal/External Group IDs is provided by the AF, the AF request applies to the UEs that belong to every one of these groups, i.e. a single UE needs to be a member of every group in the list of Internal/External Group IDs.
NOTE 4: The indication of traffic correlation can be used for 5G VN groups as described in clause 5.29.
NOTE 5: External Subscriber category(s) can be combined with External Group ID(s) or any UE. If a list of External Subscriber categories are provided by the AF, the AF request applies to the UEs that belong to every one of these Subscriber categories.
NOTE 6: FQDN(s) is used for influencing EASDF-based DNS query procedure as defined in clause 6.2.3.2.2 of [illegible]].

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

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

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

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

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

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

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

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

Release 18 3GPP V18.2.2 (2023-07)

Table : Information element contained in AF request

Information Name	Applicable for PCF or NEF (NOTE 1)	Applicable for NEF only	Category
Traffic Description	Defines the target traffic to be influenced, represented by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information.	The target traffic can be represented by AF-Service-Identifier, instead of combination of DNN and optionally S-NSSAI.	Mandatory
Potential Locations of Applications	Indicates potential locations of applications, represented by a list of DNAI(s).	The potential locations of applications can be represented by AF-Service-Identifier.	Conditional (NOTE 2)
Target UE Identifier(s)	Indicates the UE(s) that the request is targeting, i.e. one or a list of individual UE(s), a group of UE represented by Internal Group Identifier(s) (NOTE 3), or any UE accessing the combination of DNN, S-NSSAI and DNAI(s).	GPSI can be applied to identify the individual UE, or External Group Identifier(s) can be applied to identify a group of UE (NOTE 3). External Subscriber Category(s) (NOTE 5).	Mandatory
Spatial Validity Condition	Indicates that the request applies only to the traffic of UE(s) located in the specified location, represented by areas of validity.	The specified location can be represented by geographical area.	Optional
AF transaction identifier	The AF transaction identifier refers to the AF request.	N/A	Mandatory
N6 Traffic Routing requirements	Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation (NOTE 4).	N/A	Optional (NOTE 2)
Application Relocation Possibility	Indicates whether an application can be relocated once a location of the application is selected by the 5GC.	N/A	Optional
UE IP address preservation indication	Indicates UE IP address should be preserved.	N/A	Optional
Temporal Validity Condition	Time interval(s) or duration(s).	N/A	Optional
Information on AF subscription to corresponding SMF events	Indicates whether the AF subscribes to change of UP path of the PDU Session and the parameters of this subscription.	N/A	Optional
Information for EAS IP Replacement in 5GC	Indicates the Source EAS identifier and Target EAS identifier, (i.e. IP addresses and port numbers of the source and target EAS).	N/A	Optional
User Plane Latency Requirement	Indicates the user plane latency requirements	N/A	Optional
Information on AF change	N/A	Indicates the AF instance relocation and relocation information.	Optional
Indication for EAS Relocation	Indicates the EAS relocation of the application(s)	N/A	Optional
Indication for Simultaneous Connectivity over the source and target PSA at Edge Relocation	Indicates that simultaneous connectivity over the source and target PSA should be maintained at edge relocation and provides guidance to determine when the connectivity over the source	N/A	Optional
EAS Correlation indication	Indicates selecting a common EAS for the application identified by the Traffic Description for the set of UEs.		Optional
Common EAS IP address	the common EAS for the application identified by the Traffic Description for a set of UEs the AF request aims at.		Optional
Traffic Correlation ID	Identification of a set of UEs targeted at by the AF request, and accessing the application identified by the Traffic Description.		Optional
FQDN(s)	FQDN(s) used for influencing EASDF-based DNS query procedure as defined in [illegible] (NOTE 6)		Optional

NOTE 1: When the AF request targets existing or future PDU Sessions of multiple UE(s) or of any UE and is sent via the NEF, as described in clause 6.3.7.2, the information is stored in the UDR by the NEF and notified to the PCF by the UDR.
NOTE 2: The potential locations of applications and N6 traffic routing requirements may be absent only if the request is for subscription to notifications about UP path management events only or request is for indication of seleting Common EAS for a set of UEs.
NOTE 3: Internal Group ID can only be used by an AF controlled by the operator and only towards PCF. If a list of Internal/External Group IDs is provided by the AF, the AF request applies to the UEs that belong to every one of these groups, i.e. a single UE needs to be a member of every group in the list of Internal/External Group IDs.
NOTE 4: The indication of traffic correlation can be used for 5G VN groups as described in clause 5.29.
NOTE 5: External Subscriber category(s) can be combined with External Group ID(s) or any UE. If a list of External Subscriber categories are provided by the AF, the AF request applies to the UEs that belong to every one of these Subscriber categories.
NOTE 6: FQDN(s) is used for influencing EASDF-based DNS query procedure as defined in clause 6.2.3.2.2 of [illegible]].

*5G System LoCation Services (**LCSs**) Privacy selection rule in Serving NF*

LCS Privacy selection Flow Rule

A *5GS-MT-LR* may be applied to more than one (1) *LCS Privacy Data* in the *LCS Privacy Profile (LPP),* e.g. one (1) or more Privacy Classes as defined hereby and *LCS Privacy Indicator (**LPI**)* as defined hereby.

The ***5GS-MT-LR*** may also require ***Privacy Override Indicator (POI***) as defined hereby.

The Privacy selection flow is shown in the Figure

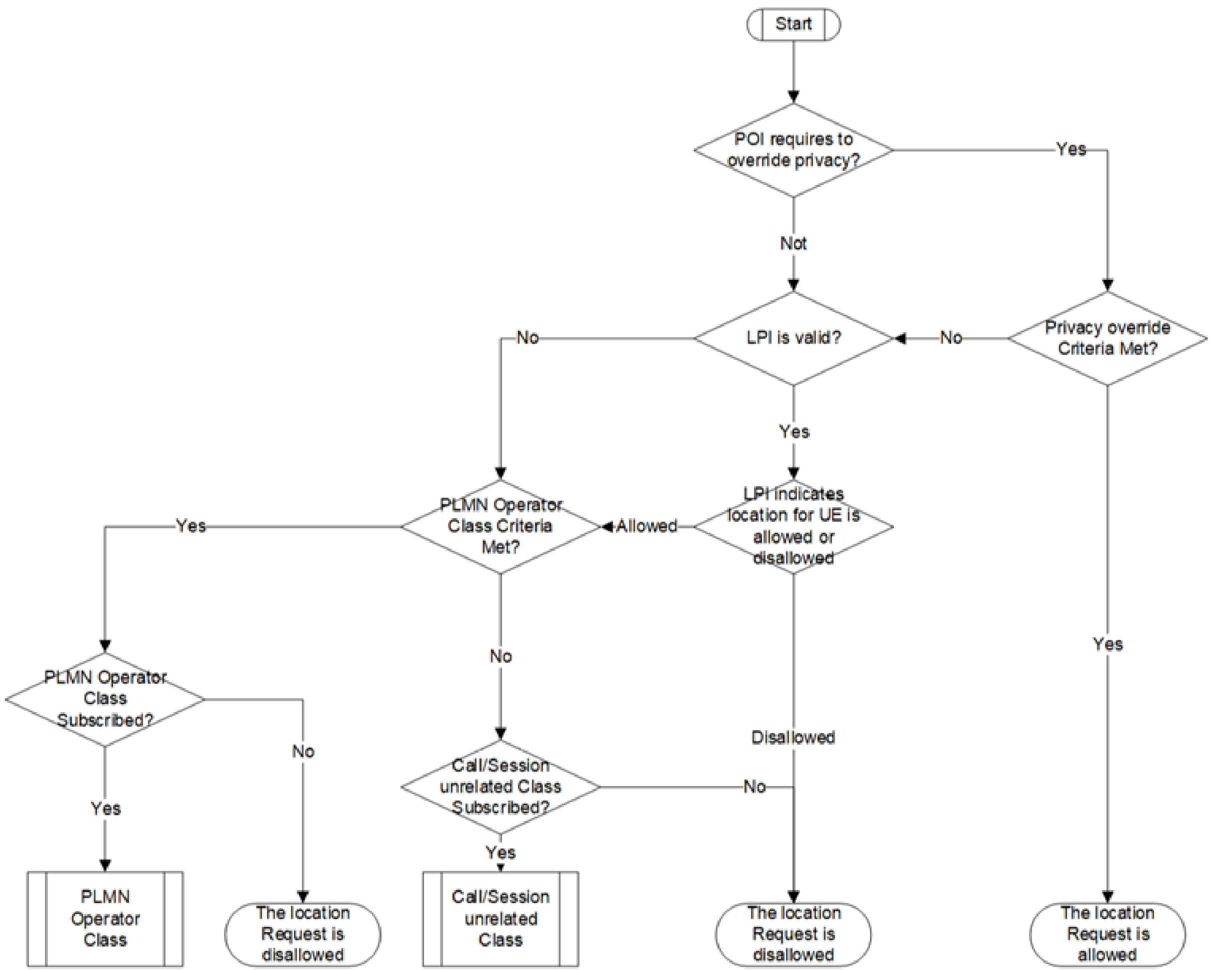


Figure: 5G System Location Services (LCS) Architecture Privacy selection Flow Diagram

*Public Network Integrated (**PNI**) - Non-Public Network (**NPN**)* Architecture to support *LoCation Service* (*LCS*) with Signalling Optimisation

The Figure shows the *PNI-NPN Architecture to support Location Services* with *Optimization of Signalling Latency and Privacy,* with the corresponding Functional descriptions are defined.

When UE accesses the NG-RAN in the Local Network, during the Registration Procedure or Service Request Procedure, NG-RAN selects the Serving AMF in the Public Network.

With appropriate configuration, Local AMF cannot be selected as the serving AMF for the UE.

Assuming NG-RAN 1 is the serving RAN of UE. NG-RAN 2 and NG-RAN 3 illustrated in the Figure is for Positioning Signal Measurement.

During the Positioning procedure, if LMF determines Network assisted Positioning Method, the Positioning Procedure defined is used and the AMF is the serving AMF.

If the LMF determines to obtain Non-UE Associated Network Assistance Data, the Positioning Procedure defined is used and the AMF is the local AMF.

For ***MO-LR***, immediate ***MT-LR*** and deferred ***MT-LR*****,** the *AMF* provides the *GMLC* contact address and a reference number to *LMF*.

When *LMF* determines *UE Location*, ***LMF*** provides the *UE Location* to ***GMLC*** directly, as defined.

NOTE 3: LMF should not determine to use ***E-CID*** *Positioning Method* for Location Service in ***PNI-NPN.***

Release 18 3GPP V18.3.0 (2023-09)

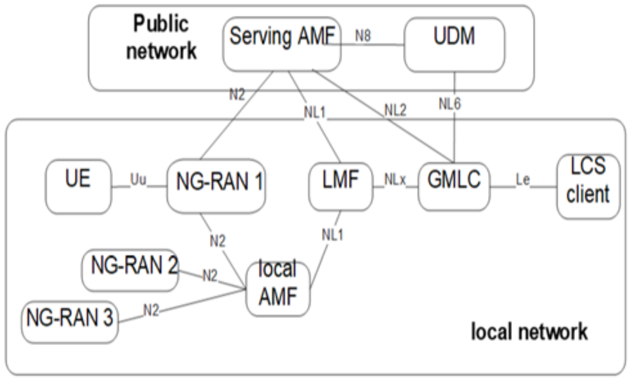


Figure: 5G System Location Services (LCS) Architecture Public Network Integrated (PNI) - Non-Public Network (NPN) Architecture to support Location Service with Signalling Optimization

Release 18 3GPP V18.3.0 (2023-09)

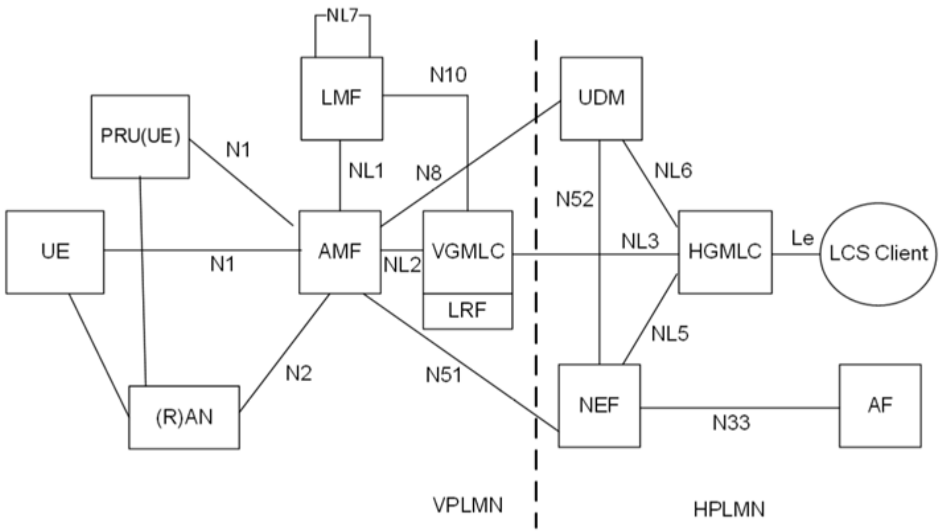


Figure: 5G System Location Services (LCS) Roaming reference Architecture in Reference Point representation

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

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

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

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

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

Inappropriate term is used and it may confuse the Readers.

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

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

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

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

3GPP TSG-SA WG6 Meeting #52-bis-e **S6-230407**
Online, 11th – 20th January 2022 **(revision of S6-230156)**

CR-Form-v12.2

CHANGE REQUEST

CR	**0101**	**rev**	**1**	**Current version:** 18.0.0

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

Proposed change affects: UICC apps [ ] ME [ ] Radio Access Network [ ] Core Network [X]

Title:	Modify a terminology for SNA
Source to WG:	NTT DOCOMO
Source to TSG:	SA6
Work item code:	SNAAPP — ***Date:*** 2023-01-10
Category:	**D** — ***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:	In SNA-related studies so far, SA6 and has used the term "subscriber-aware northbound API access," or SNA for its abbreviation. However, the CAPIF system should be aware of the resource owner, rather than the subscriber. Thus, the term "subscriber-aware northbound API access" is not appropriate for this use case.
Summary of change:	*Subscriber-aware northbound API access* is replaced with *resource owner-aware northbound API access*; SNA is replaced with *RNAA*.
Consequences if not approved:	Inappropriate term is used and it may confuse the readers.

Clauses affected:	3.1, 3.2, 4.17, 4.17.1, 5.2, 6.2.3			
	Y	**N**		
Other specs affected: (show related CRs)		X	Other core specifications	TS/TR ... CR ...
		X	Test specifications	TS/TR ... CR ...
		X	O&M Specifications	TS/TR ... CR ...
Other comments:				
This CR's revision history:				

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

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

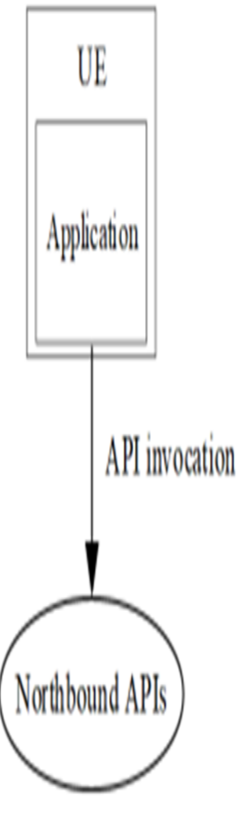


Fig.: UE-originated API Invocation

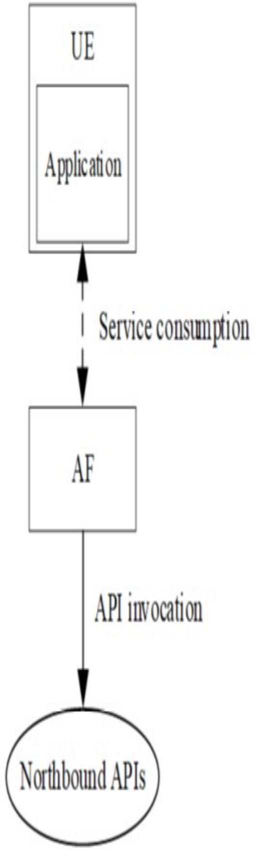


Fig.: AF-originated API Invocation

+

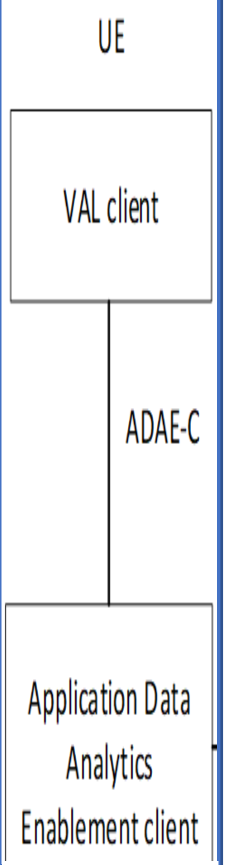


Fig.: ADAE-C

+

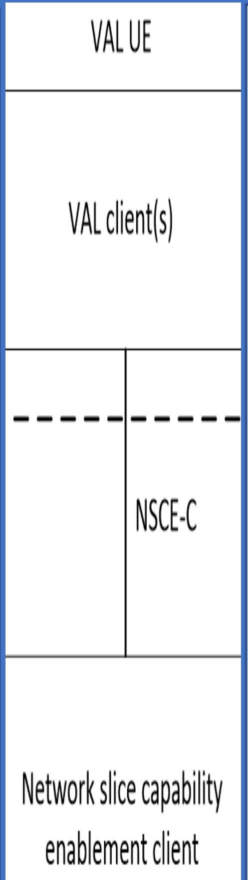


Fig.: NSCE-C

+

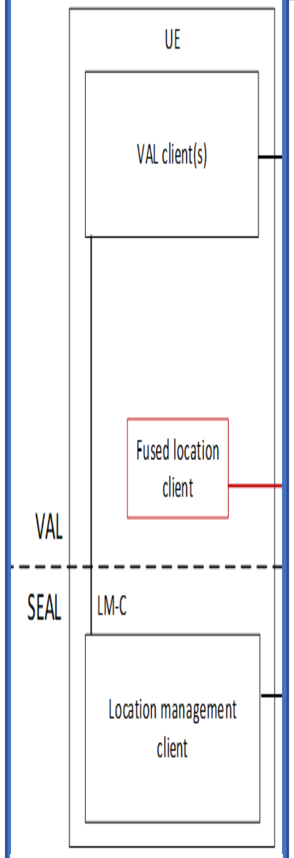
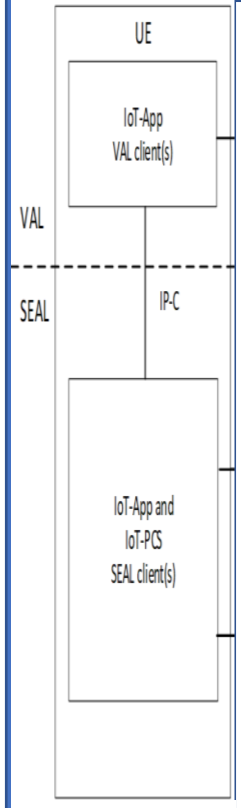


Fig. FLC leveraging SEAL LM

+



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

+

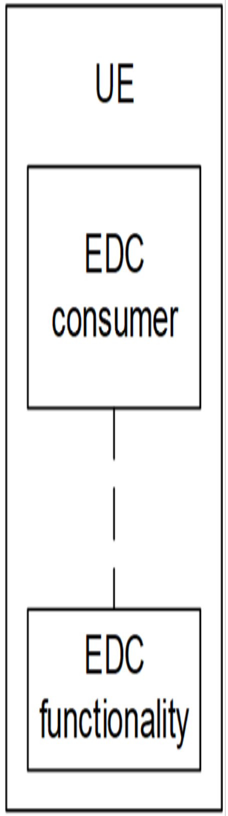


Fig.: Edge DNS Client Functionality

+

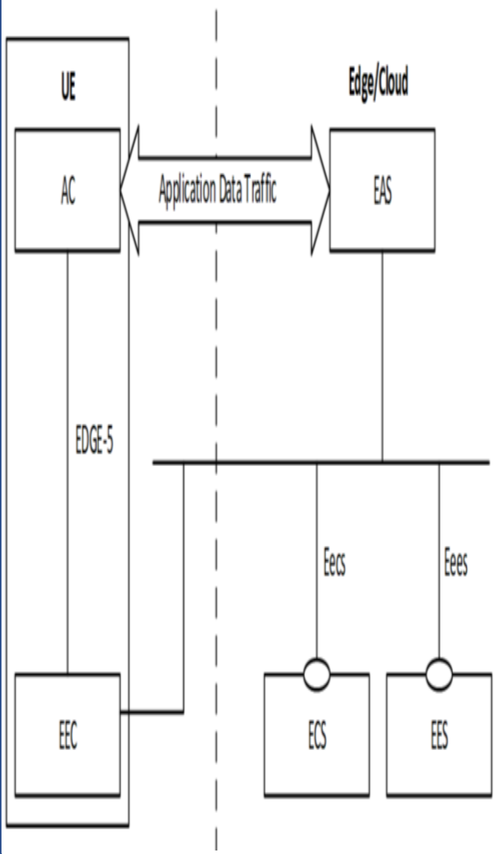


Fig.: Architecture for enabling Edge Applications - SBI representation

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

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

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

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

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

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

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

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

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

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

Release 19 3GPP V19.4.0 (2023-09)

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

Access Identity number	UE configuration
0	UE is not configured with any parameters from this table
1 (NOTE 1)	UE is configured for Multimedia Priority Service (MPS).
2 (NOTE 2)	UE is configured for Mission Critical Service (MCS).
3	UE for which Disaster Condition applies (note 4)
4-10	Reserved for future use
11 (NOTE 3)	Access Class 11 is configured in the UE.
12 (NOTE 3)	Access Class 12 is configured in the UE.
13 (NOTE 3)	Access Class 13 is configured in the UE.
14 (NOTE 3)	Access Class 14 is configured in the UE.
15 (NOTE 3)	Access Class 15 is configured in the UE.

NOTE 1: Access Identity 1 is used by UEs configured for MPS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN, PLMNs equivalent to HPLMN, and visited PLMNs of the home country.
Access Identity 1 is also valid when the UE is explicitly authorized by the network based on specific configured PLMNs inside and outside the home country.
NOTE 2: Access Identity 2 is used by UEs configured for MCS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN or PLMNs equivalent to HPLMN and visited PLMNs of the home country. Access Identity 2 is also valid when the UE is explicitly authorized by the network based on specific configured PLMNs inside and outside the home country.
NOTE 3: Access Identities 11 and 15 are valid in Home PLMN only if the EHPLMN list is not present or in any EHPLMN. Access Identities 12, 13 and 14 are valid in Home PLMN and visited PLMNs of home country only. For this purpose, the home country is defined as the country of the MCC part of the IMSI.
NOTE 4: The configuration is valid for PLMNs that indicate to potential Disaster Inbound Roamers that the UEs can access the PLMN. See clause 6.31.

Release 19 3GPP V19.4.0 (2023-09)

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

Access Category number	Conditions related to UE	Type of access attempt
0	All	MO signalling resulting from paging
1 (NOTE 1)	UE is configured for delay tolerant service and subject to access control for Access Category 1, which is judged based on relation of UE's HPLMN and the selected PLMN.	All except for Emergency, or MO exception data
2	All	Emergency
3	All except for the conditions in Access Category 1.	MO signalling on NAS level resulting from other than paging
4	All except for the conditions in Access Category 1.	MMTEL voice (NOTE 3)
5	All except for the conditions in Access Category 1.	MMTEL video
6	All except for the conditions in Access Category 1.	SMS
7	All except for the conditions in Access Category 1.	MO data that do not belong to any other Access Categories (NOTE 4)
8	All except for the conditions in Access Category 1	MO signalling on RRC level resulting from other than paging
9	All except for the conditions in Access Category 1	MO IMS registration related signalling (NOTE 5)
10 (NOTE 6)	All	MO exception data
11-31		Reserved standardized Access Categories
32-63 (NOTE 2)	All	Based on operator classification

NOTE 1: The barring parameter for Access Category 1 is accompanied with information that define whether Access Category applies to UEs within one of the following categories:
a) UEs that are configured for delay tolerant service;
b) UEs that are configured for delay tolerant service and are neither in their HPLMN nor in a PLMN that is equivalent to it;
c) UEs that are configured for delay tolerant service and are neither in the PLMN listed as most preferred PLMN of the country where the UE is roaming in the operator-defined PLMN selector list on the SIM/USIM, nor in their HPLMN nor in a PLMN that is equivalent to their HPLMN.
When a UE is configured for EAB, the UE is also configured for delay tolerant service. In case a UE is configured both for EAB and for EAB override, when upper layer indicates to override Access Category 1, then Access Category 1 is not applicable.
NOTE 2: When there are an Access Category based on operator classification and a standardized Access Category to both of which an access attempt can be categorized, and the standardized Access Category is neither 0 nor 2, the UE applies the Access Category based on operator classification. When there are an Access Category based on operator classification and a standardized Access Category to both of which an access attempt can be categorized, and the standardized Access Category is 0 or 2, the UE applies the standardized Access Category.
NOTE 3: Includes Real-Time Text (RTT).
NOTE 4: Includes IMS Messaging.
NOTE 5: Includes IMS registration related signalling, e.g. IMS initial registration, re-registration, and subscription refresh.
NOTE 6: Applies to access of a NB-IoT-capable UEto a NB-IOT cell connected to 5GC when the UE is authorized to send exception data.

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

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

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

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

- to allow the **3rd-Party** to manage a Trusted **3rd-Party Application** in a Service Hosting Environment (SHE)

- to improve User Experience, and

- to efficiently utilize Backhaul and Application Resources).

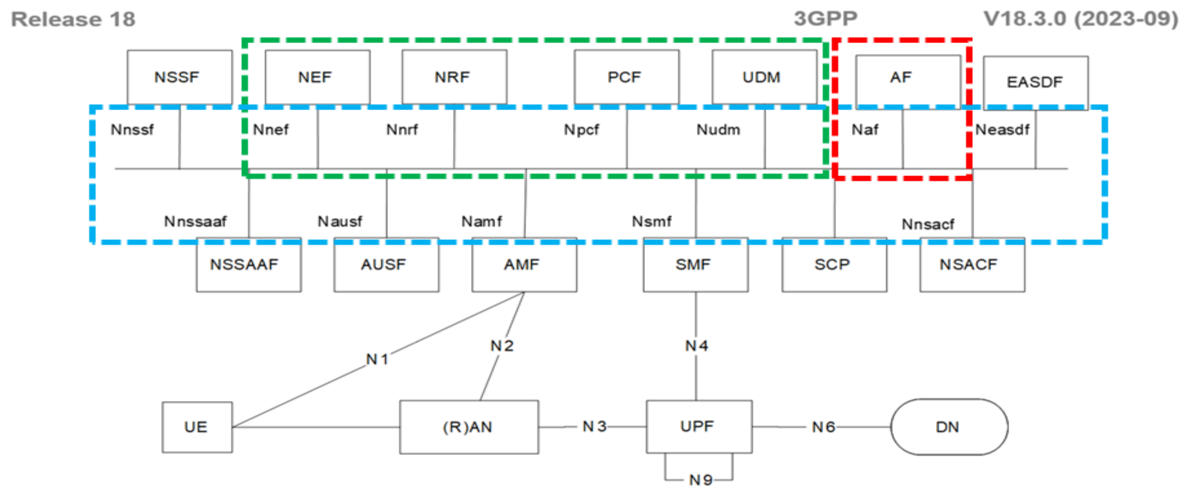


Figure: 5G System Non-Roaming Architecture

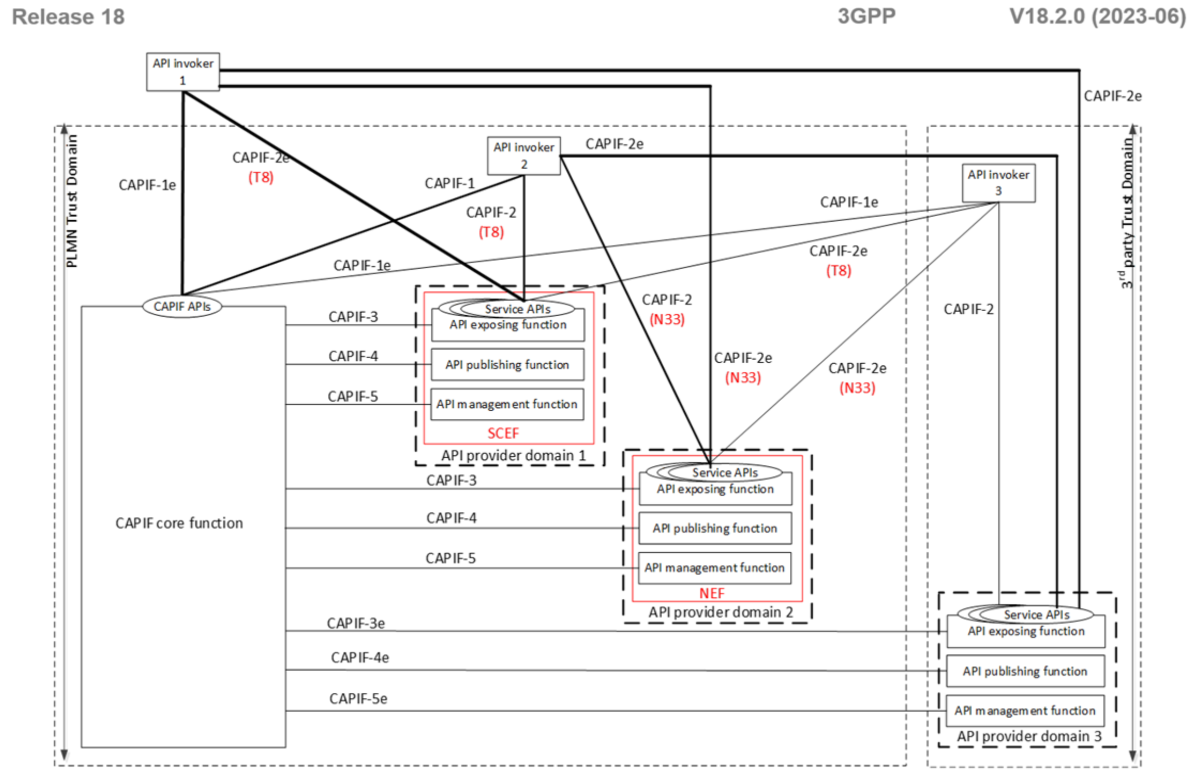


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

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

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

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

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

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

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

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

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

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

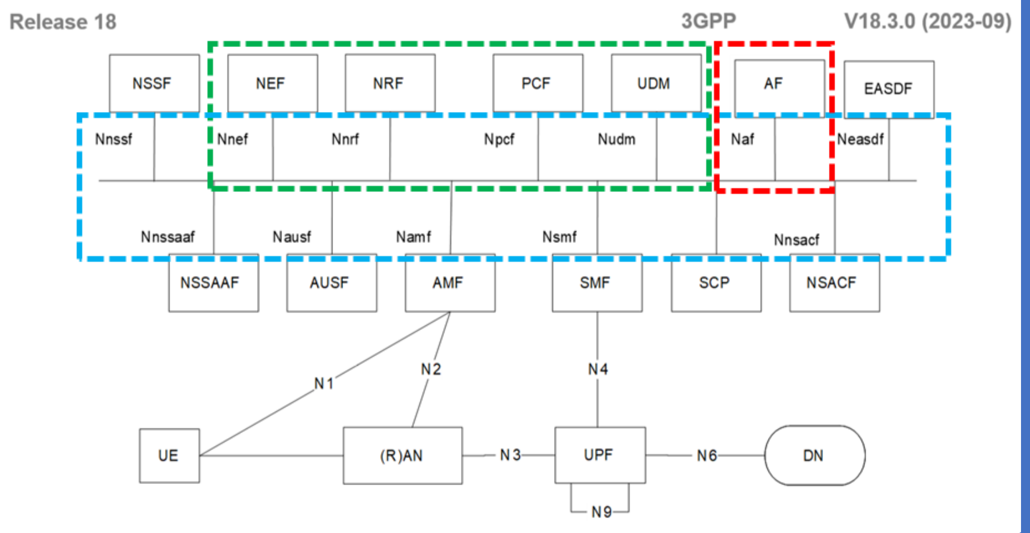


Figure: 5G System Non-Roaming Architecture

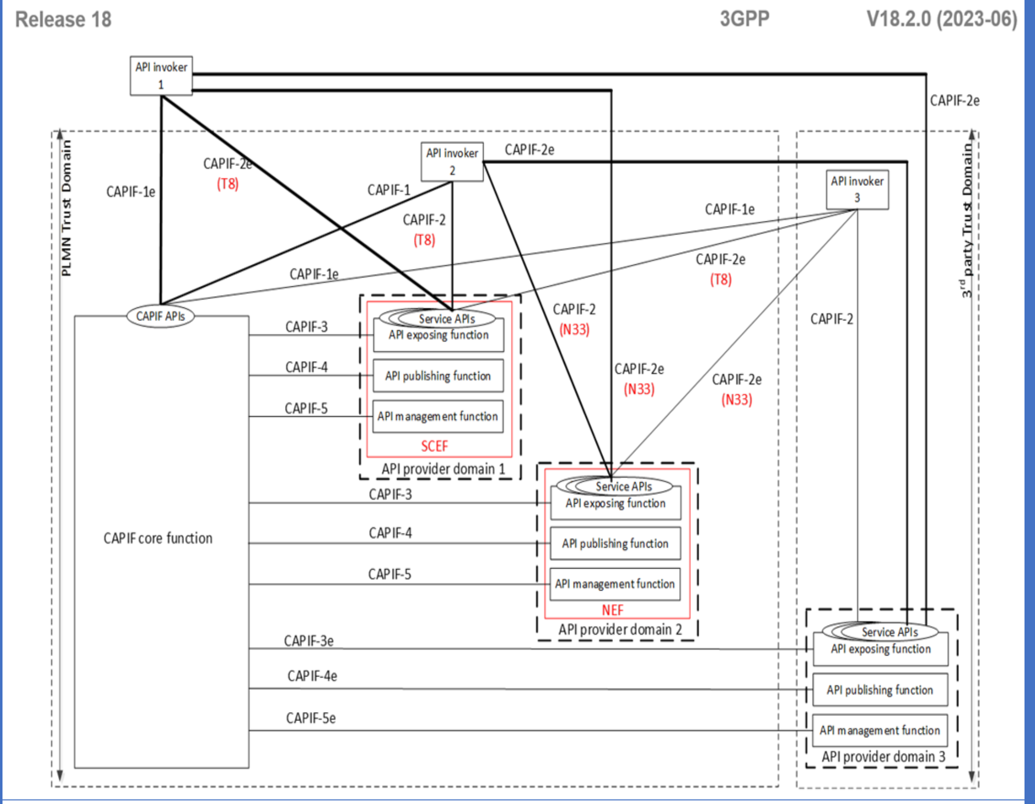


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

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

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

- Subscription,

- UE Capabilities, and

- Services provided by the Network Slice (SST).

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

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

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

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

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

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

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

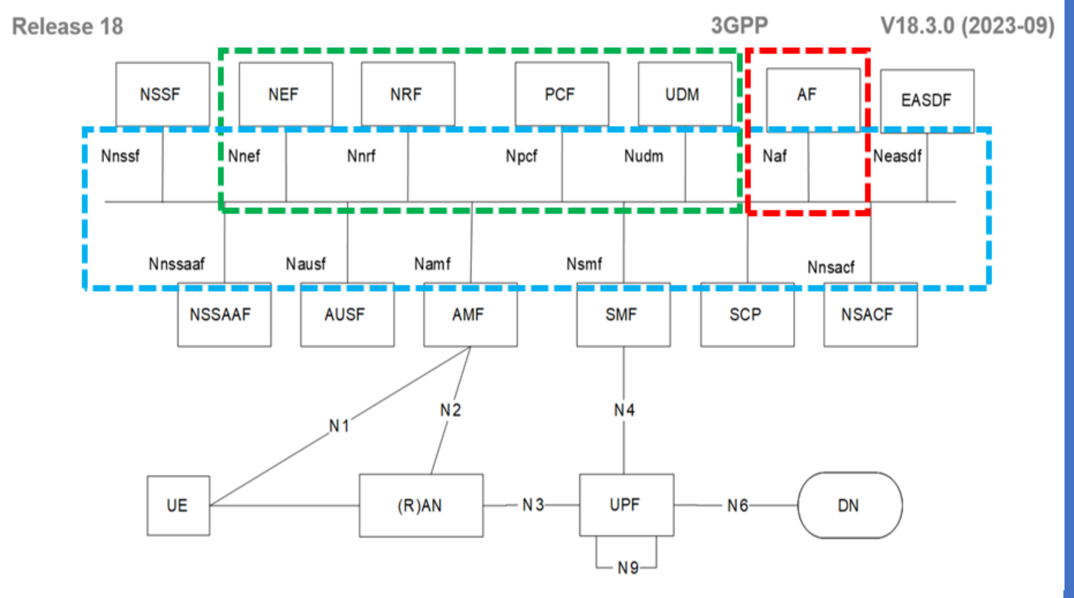


Figure: 5G System Non-Roaming Architecture

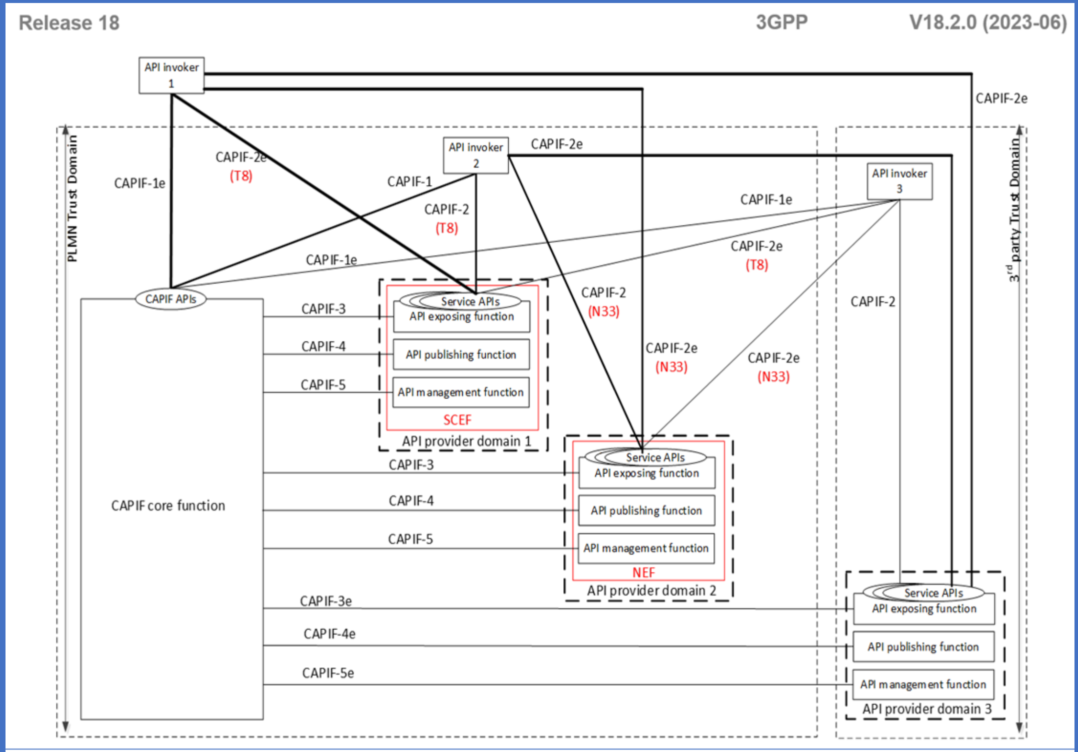


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

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

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

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

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

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

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

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

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

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

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

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

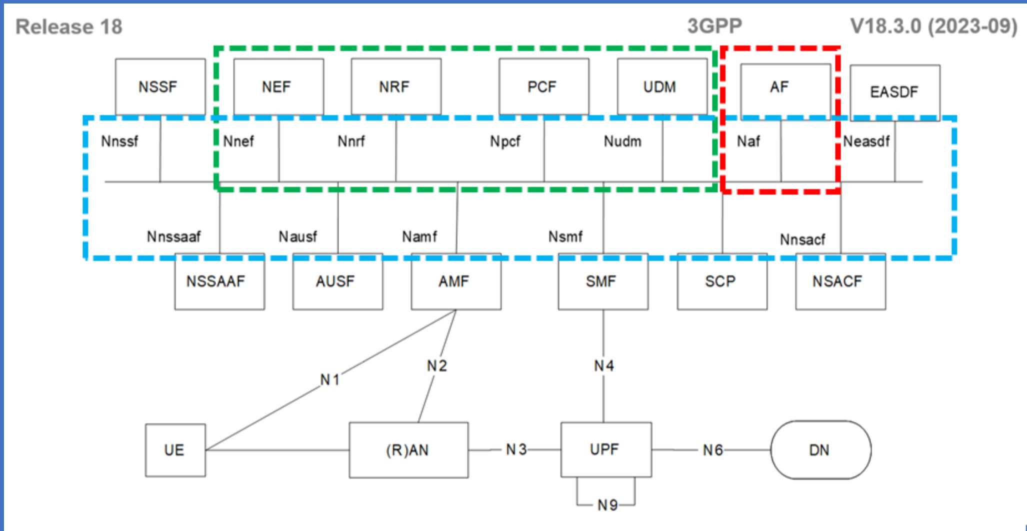


Figure: 5G System Non-Roaming Architecture

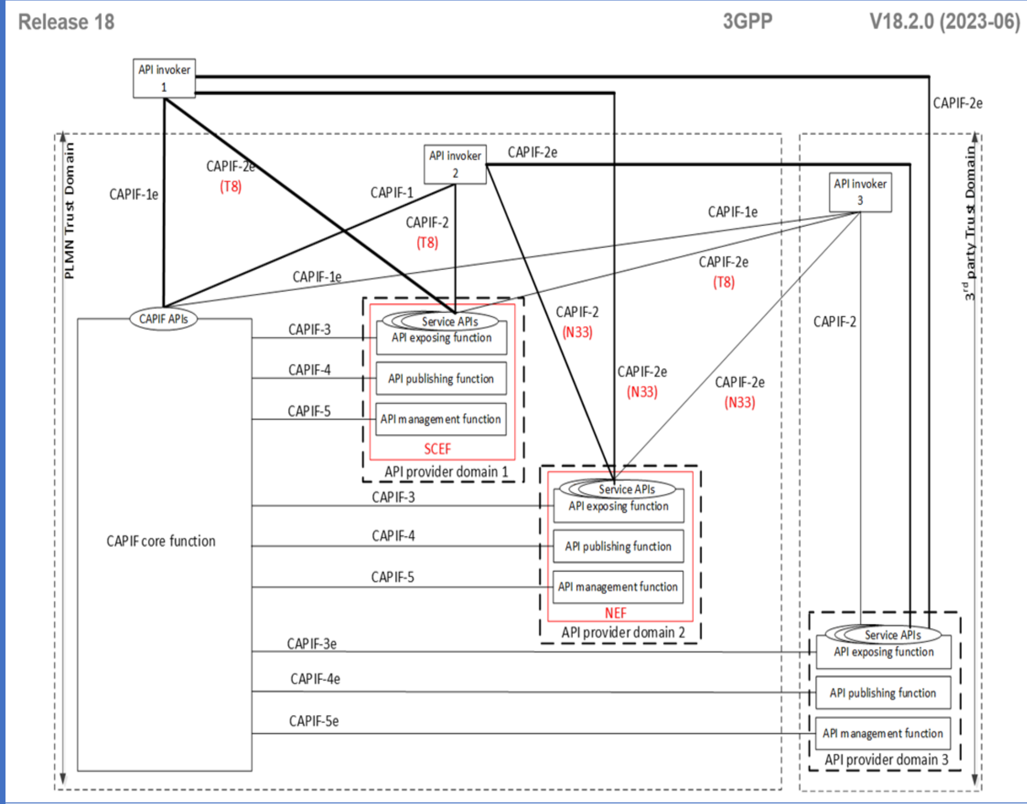


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

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

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

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

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

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

The **5G System** shall be able to:

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

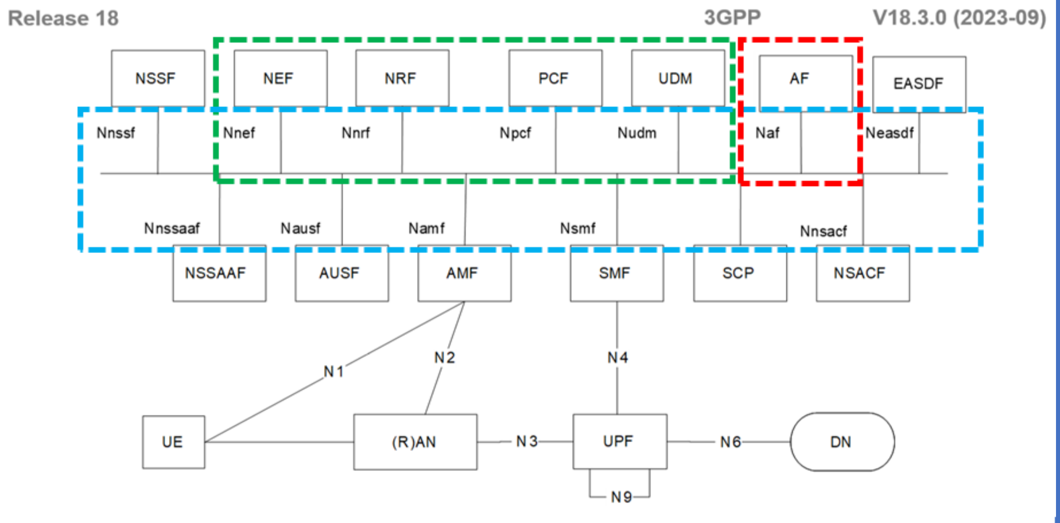


Figure: 5G System Non-Roaming Architecture

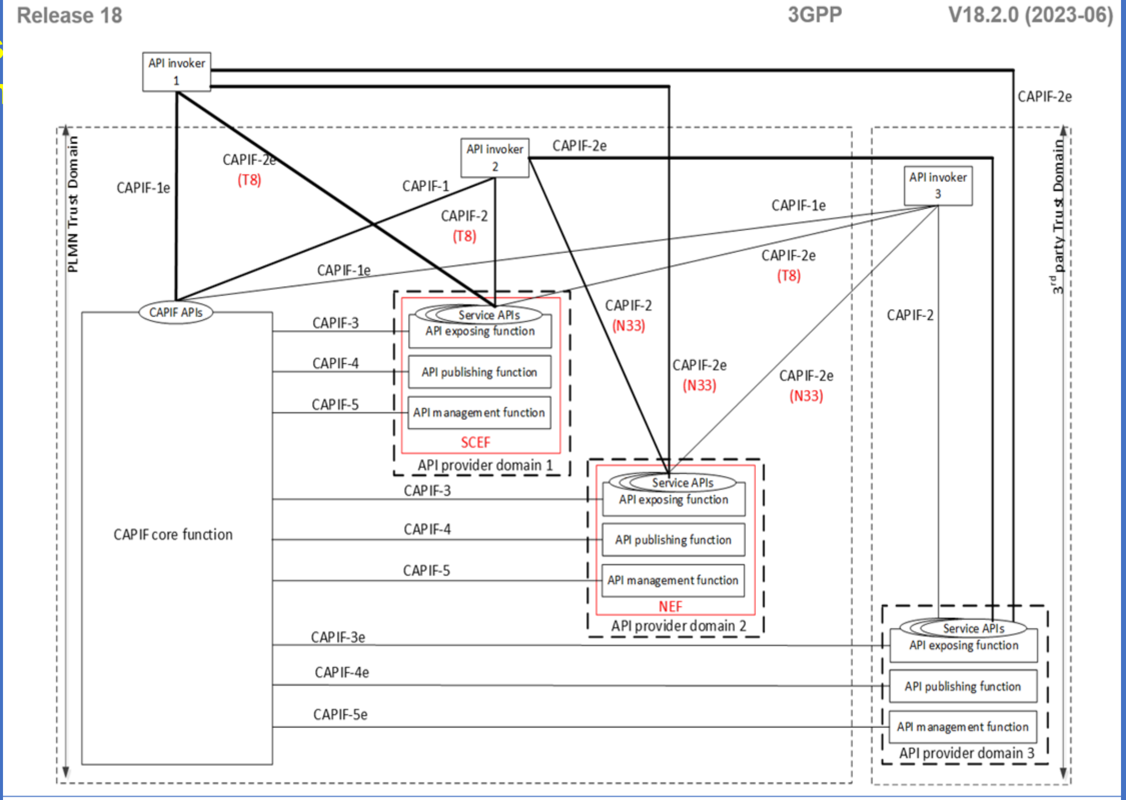


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

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

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

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

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

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

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

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

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

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

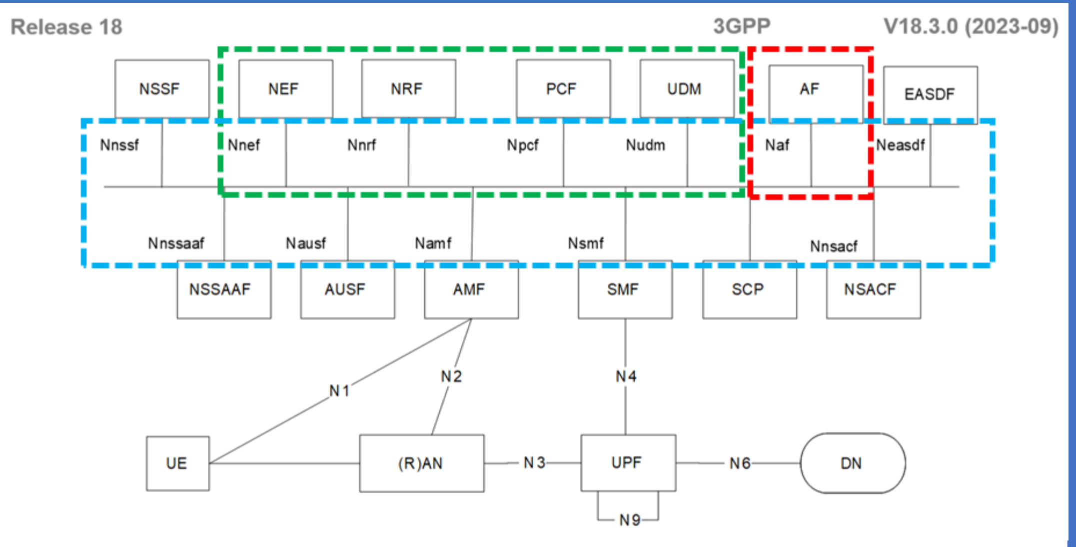


Figure: 5G System Non-Roaming Architecture

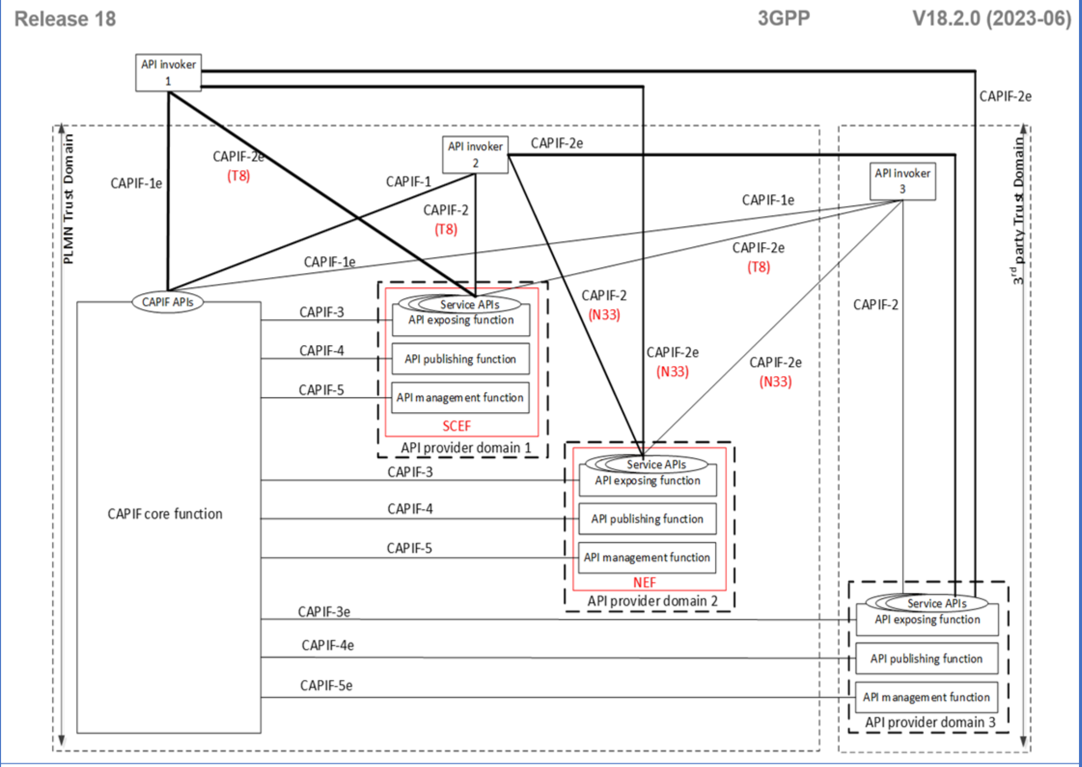


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

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

This solution addresses **the Business Relationship** between
- the User (UE),
- the AF and
- the Northbound API Provider in the AF-originated API Invocation scenario.

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

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

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

as the **API invoker** in the Figure can either be:
- **an Application on the UE** or
- **the AF.**

The API Invoker has Service Agreement with a CAPIF P9rovider, and the API Provider provides APIs associated with the Resource Owner.

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

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

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

Release 18 3GPP V18.1.0 (2023-03)

Solution #1: Business relationship in SNA

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

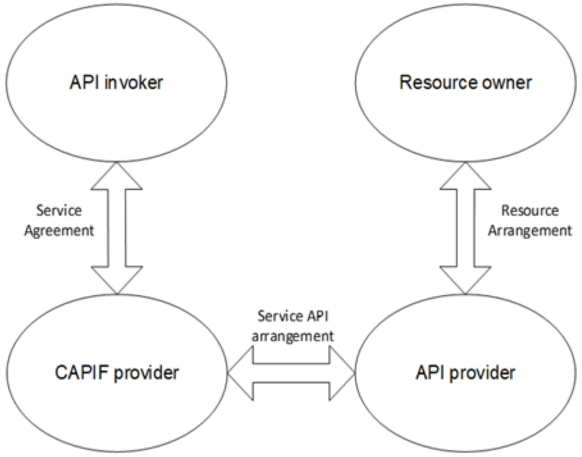


Figure: 5G Common API Framework (CAPIF) Business Relationships in Subscriber-aware Northbound API Access (SNA)

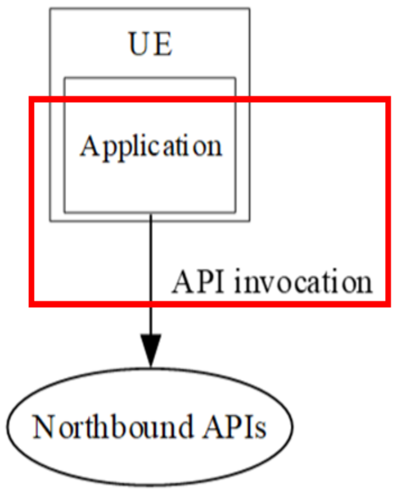


Figure: 5G UE-originated API invocation

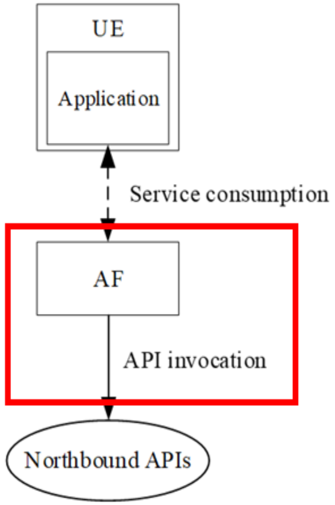


Figure: 5G AF-originated API invocation

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

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

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

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

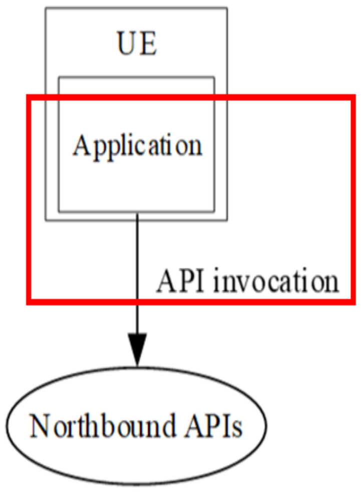


Figure: 5G UE-originated API invocation

2. AF-originated API invocation

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

The scenario is illustrated in the Figure.

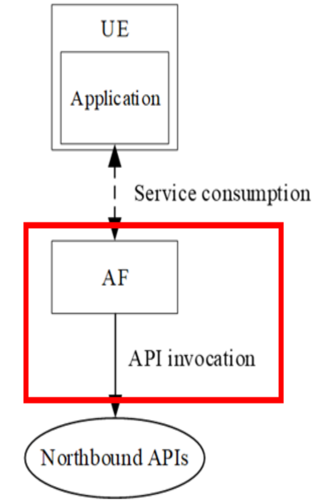


Figure: 5G AF-originated API invocation

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

Use case examples

AF-originated API invocation (Gaming)

General

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

Release 18 3GPP V18.1.0 (2023-03)

UE-originated API invocation (Location tracking)

General

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

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

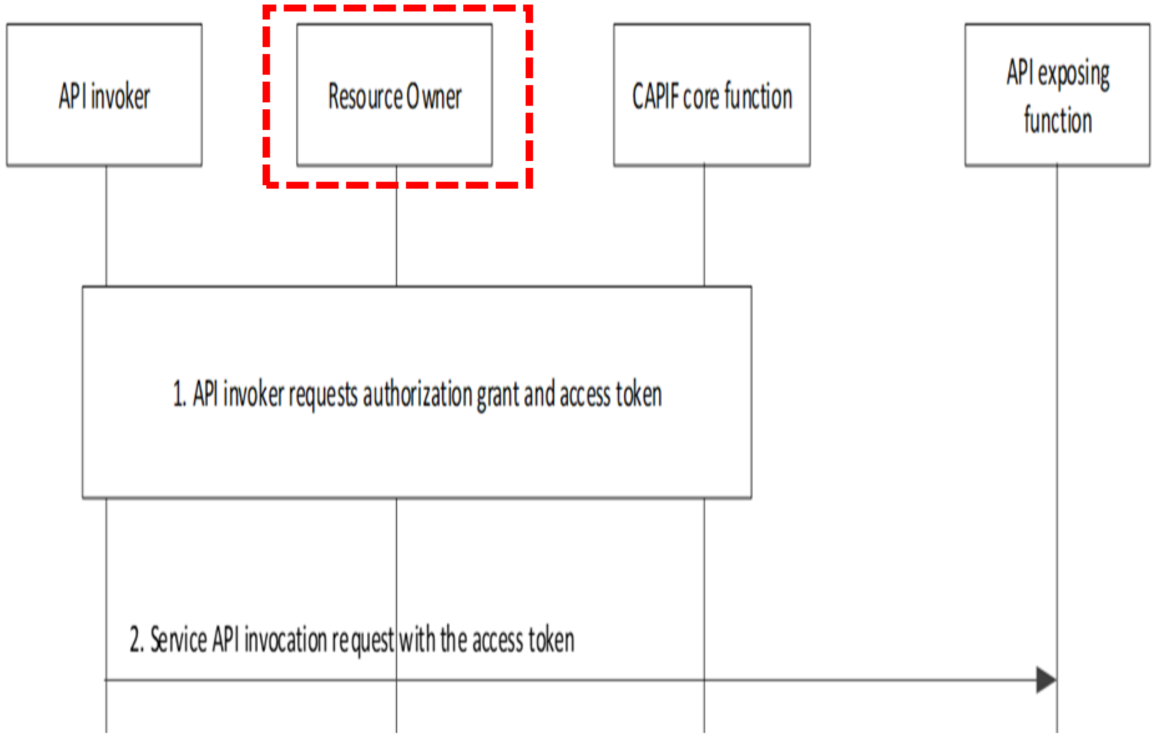


Fig.: 5G API Core Function procedure for API Invoker obtaining Resource owner Consent prior to the Service APIs Invocation

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

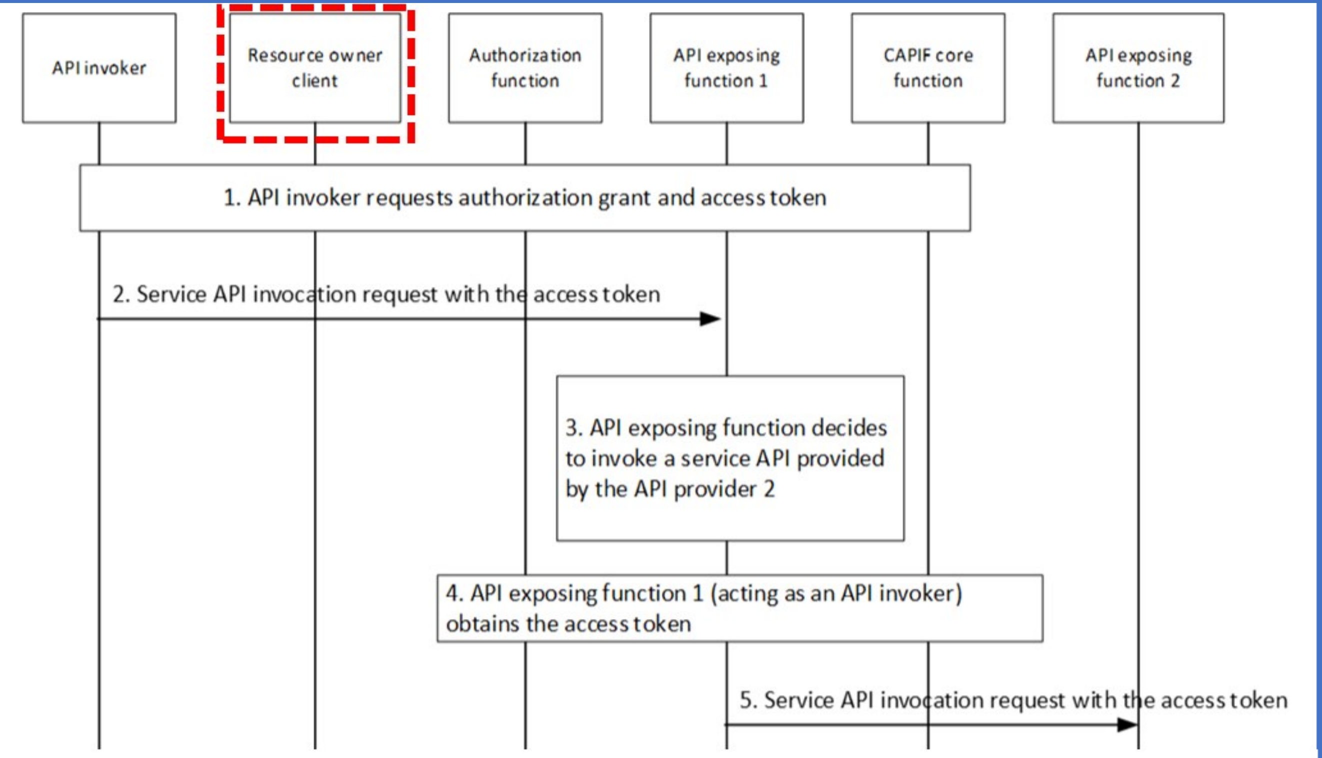


Fig.: 5G API Core Function Procedure for obtaining Resource owner Consent in a nested API Invocation

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

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

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

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

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

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

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

Release 18 3GPP V18.2.2 (2023-07)

Table : Information element contained in AF request

Information Name	Applicable for PCF or NEF (NOTE 1)	Applicable for NEF only	Category
Traffic Description	Defines the target traffic to be influenced, represented by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information.	The target traffic can be represented by AF-Service-Identifier, instead of combination of DNN and optionally S-NSSAI.	Mandatory
Potential Locations of Applications	Indicates potential locations of applications, represented by a list of DNAI(s).	The potential locations of applications can be represented by AF-Service-Identifier.	Conditional (NOTE 2)
Target UE Identifier(s)	Indicates the UE(s) that the request is targeting, i.e. one or a list of individual UE(s), a group of UE represented by Internal Group Identifier(s) (NOTE 3), or any UE accessing the combination of DNN, S-NSSAI and DNAI(s).	GPSI can be applied to identify the individual UE, or External Group Identifier(s) can be applied to identify a group of UE (NOTE 3). External Subscriber Category(s) (NOTE 5).	Mandatory
Spatial Validity Condition	Indicates that the request applies only to the traffic of UE(s) located in the specified location, represented by areas of validity.	The specified location can be represented by geographical area.	Optional
AF transaction identifier	The AF transaction identifier refers to the AF request.	N/A	Mandatory
N6 Traffic Routing requirements	Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation (NOTE 4).	N/A	Optional (NOTE 2)
Application Relocation Possibility	Indicates whether an application can be relocated once a location of the application is selected by the 5GC.	N/A	Optional
UE IP address preservation indication	Indicates UE IP address should be preserved.	N/A	Optional
Temporal Validity Condition	Time interval(s) or duration(s).	N/A	Optional
Information on AF subscription to corresponding SMF events	Indicates whether the AF subscribes to change of UP path of the PDU Session and the parameters of this subscription.	N/A	Optional
Information for EAS IP Replacement in 5GC	Indicates the Source EAS identifier and Target EAS identifier, (i.e. IP addresses and port numbers of the source and target EAS).	N/A	Optional
User Plane Latency Requirement	Indicates the user plane latency requirements	N/A	Optional
Information on AF change	N/A	Indicates the AF instance relocation and relocation information.	Optional
Indication for EAS Relocation	Indicates the EAS relocation of the application(s)	N/A	Optional
Indication for Simultaneous Connectivity over the source and target PSA at Edge Relocation	Indicates that simultaneous connectivity over the source and target PSA should be maintained at edge relocation and provides guidance to determine when the connectivity over the source	N/A	Optional
EAS Correlation indication	Indicates selecting a common EAS for the application identified by the Traffic Description for the set of UEs.		Optional
Common EAS IP address	the common EAS for the application identified by the Traffic Description for a set of UEs the AF request aims at.		Optional
Traffic Correlation ID	Identification of a set of UEs targeted at by the AF request, and accessing the application identified by the Traffic Description.		Optional
FQDN(s)	FQDN(s) used for influencing EASDF-based DNS query procedure as defined in TS 23.548 [130] (NOTE 6).		Optional

NOTE 1: When the AF request targets existing or future PDU Sessions of multiple UE(s) or of any UE and is sent via the NEF, as described in clause 6.3.7.2, the information is stored in the UDR by the NEF and notified to the PCF by the UDR.
NOTE 2: The potential locations of applications and N6 traffic routing requirements may be absent only if the request is for subscription to notifications about UP path management events only or request is for indication of seleting Common EAS for a set of UEs.
NOTE 3: Internal Group ID can only be used by an AF controlled by the operator and only towards PCF. If a list of Internal/External Group IDs is provided by the AF, the AF request applies to the UEs that belong to every one of these groups, i.e. a single UE needs to be a member of every group in the list of Internal/External Group IDs.
NOTE 4: The indication of traffic correlation can be used for 5G VN groups as described in clause 5.29.
NOTE 5: External Subscriber category(s) can be combined with External Group ID(s) or any UE. If a list of External Subscriber categories are provided by the AF, the AF request applies to the UEs that belong to every one of these Subscriber categories.
NOTE 6: FQDN(s) is used for influencing EASDF-based DNS query procedure as defined in clause 6.2.3.2.2 of [illegible]].

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

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

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

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

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

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

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

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

Release 18 3GPP V18.2.2 (2023-07)

Table : Information element contained in AF request

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

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

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

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

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

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

NOTE 6: FQDN(s) is used for influencing EASDF-based DNS query procedure as defined in clause 6.2.3.2.2 of [illegible]].

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

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

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

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

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

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

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

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

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

Release 18 3GPP V18.2.0 (2023-06)

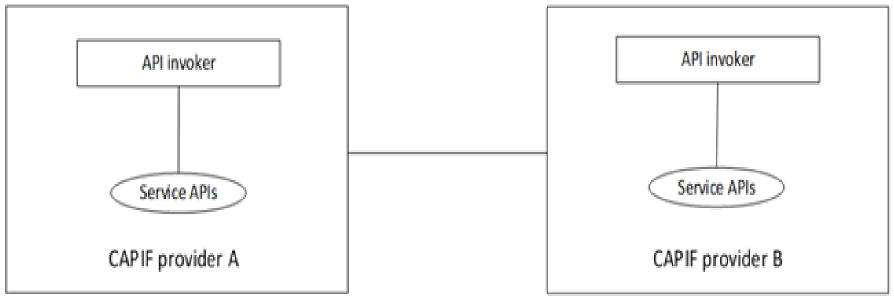


Figure: 5G CAPIF Interconnection between Common API Framework (CAPIF) Providers

Release 18 3GPP V18.2.0 (2023-06)

CAPIF business relationships for RNAA

Figure shows the CAPIF business relationships for the resource owner-aware northbound API access (RNAA).

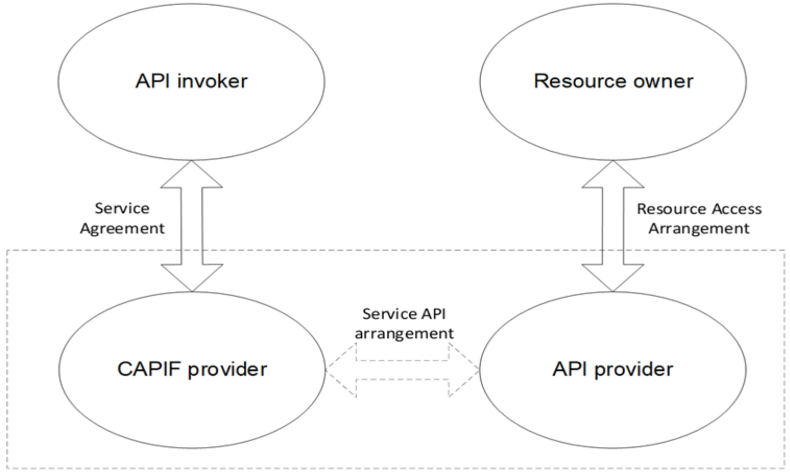


Figure: 5G Common API Framework (CAPIF) Business Relationships for Resource Owner-aware Northbound API Access (RNAA)

5G Common API Framework (CAPF) Functional Model description to support RNAA

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

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

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

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

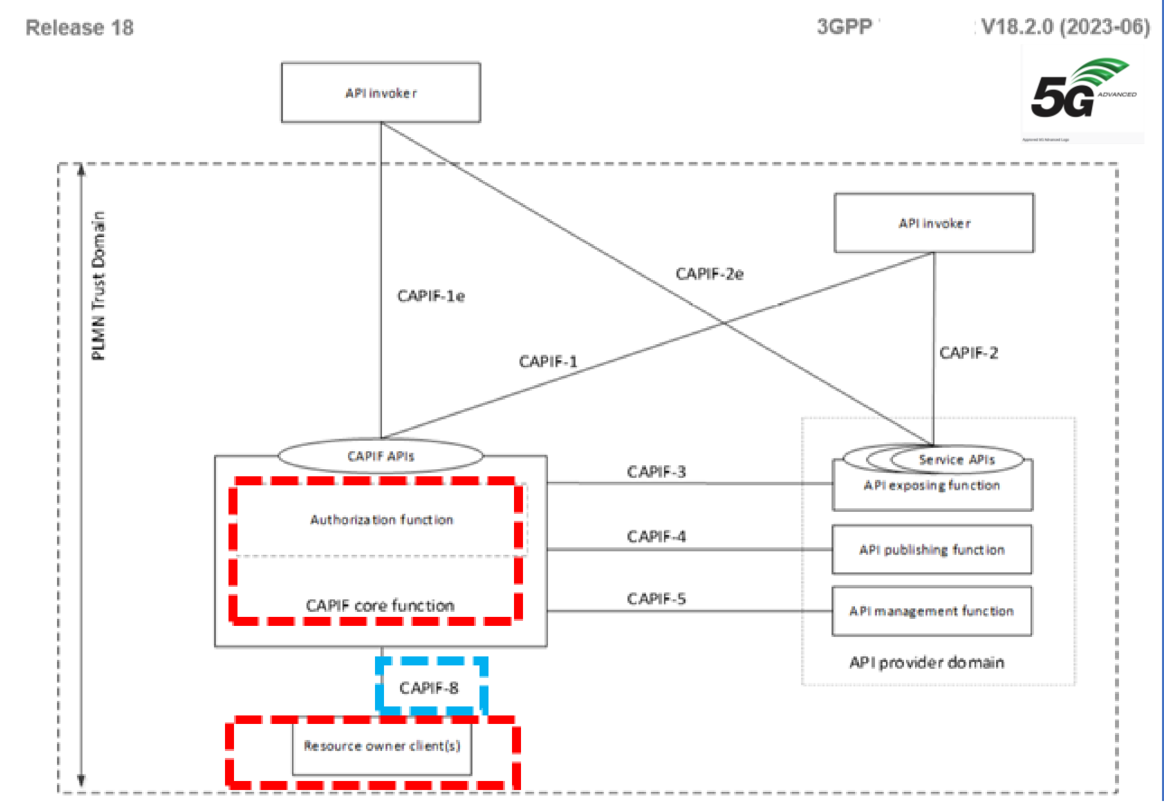


Figure: 5G Resource Owner-aware Northbound API Access (RNAA) Architecture support in 5G Common API Framework (CAPIF)

The API exposing function (e. g. NEF) acts as a Resource owner Consent Enforcement point as specified in 5GS and interacts with the Authorization Function via CAPIF-9.
The API Exposing Function can retrieve the Resource owner Consent Parameters from the Authorization function. The API invoker interacts with Authorization Function via CAPIF-10/CAPIF-10e.

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

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

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

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

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

5G Common API Framework (CAPIF) Business Relationships for Resource Owner-aware Northbound API Access (RNAA)

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

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

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

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

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

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

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

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

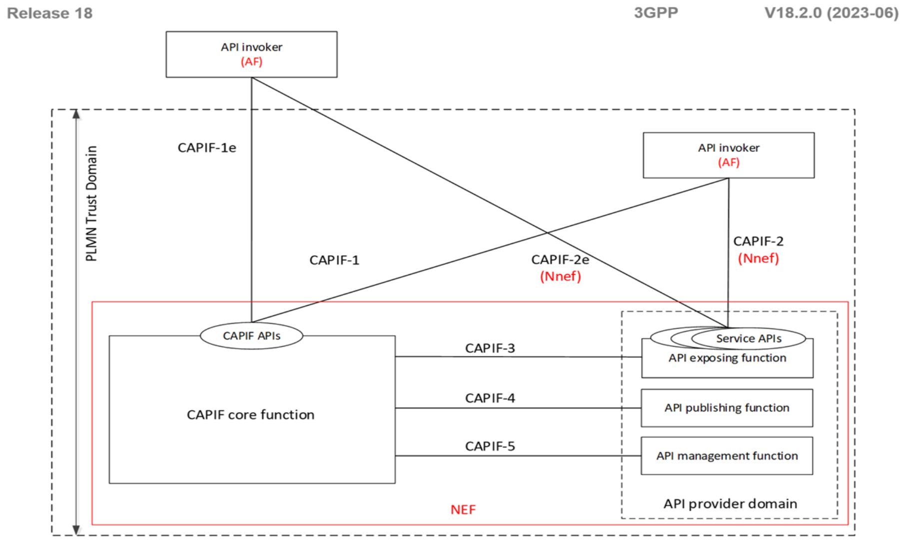


Figure: 5G CN NEF Implementation in the CAPIF Architecture

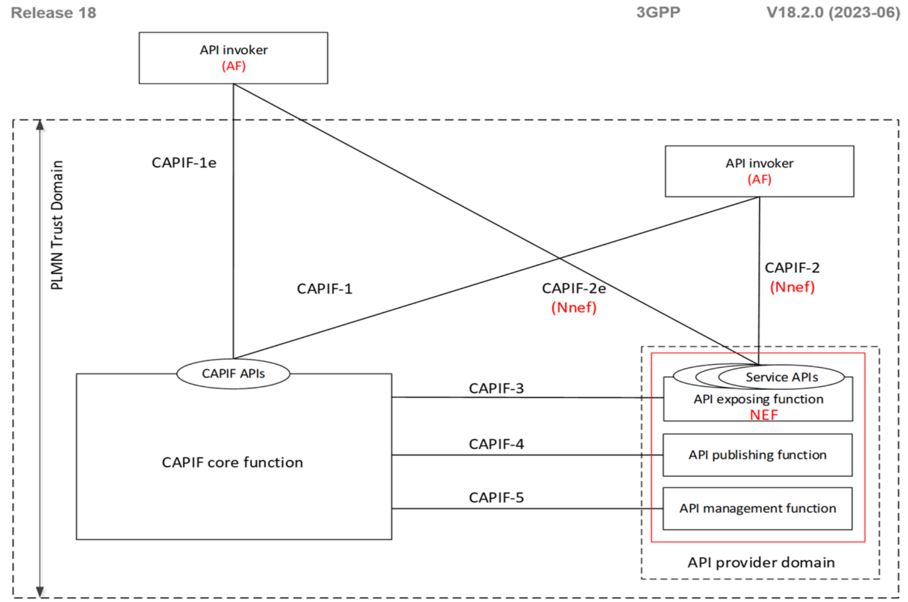


Figure: 5G CN NEF Implementation of the Service specific aspects compliant with the CAPIF Architecture

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

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

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

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

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

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

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

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

Release 18 3GPP V18.2.0 (2023-06)

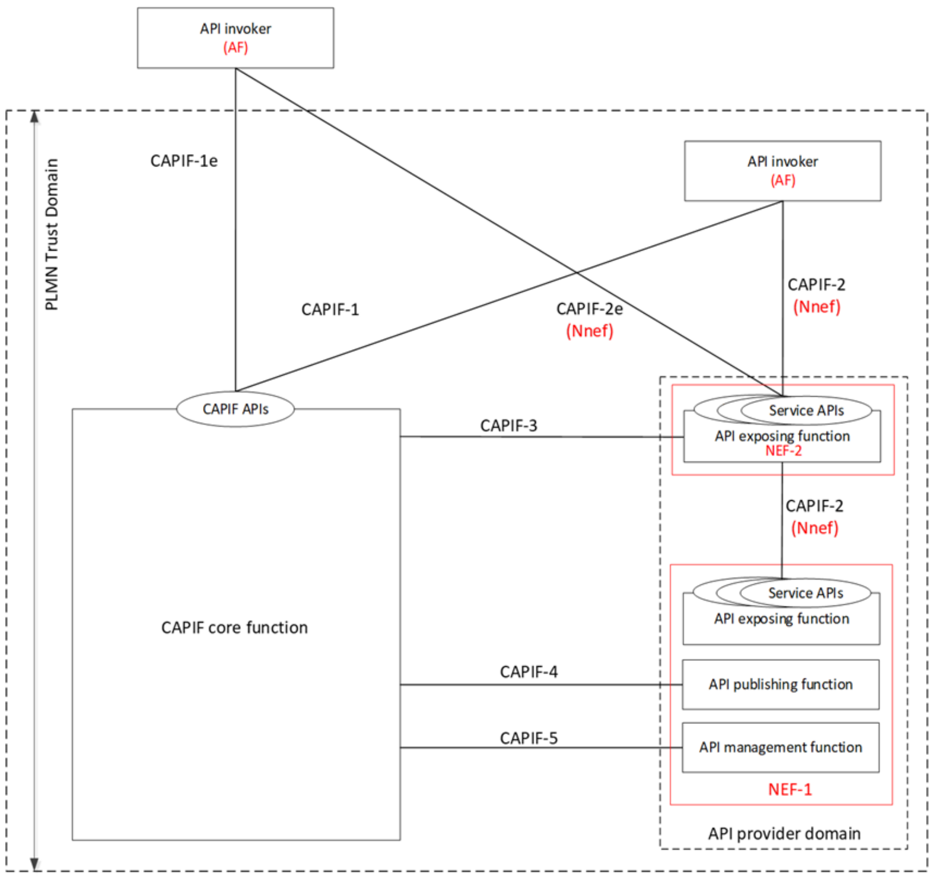


Figure: 5G NEF Distributed deployment compliant with the CAPIF Architecture

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

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

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

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

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

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

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

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

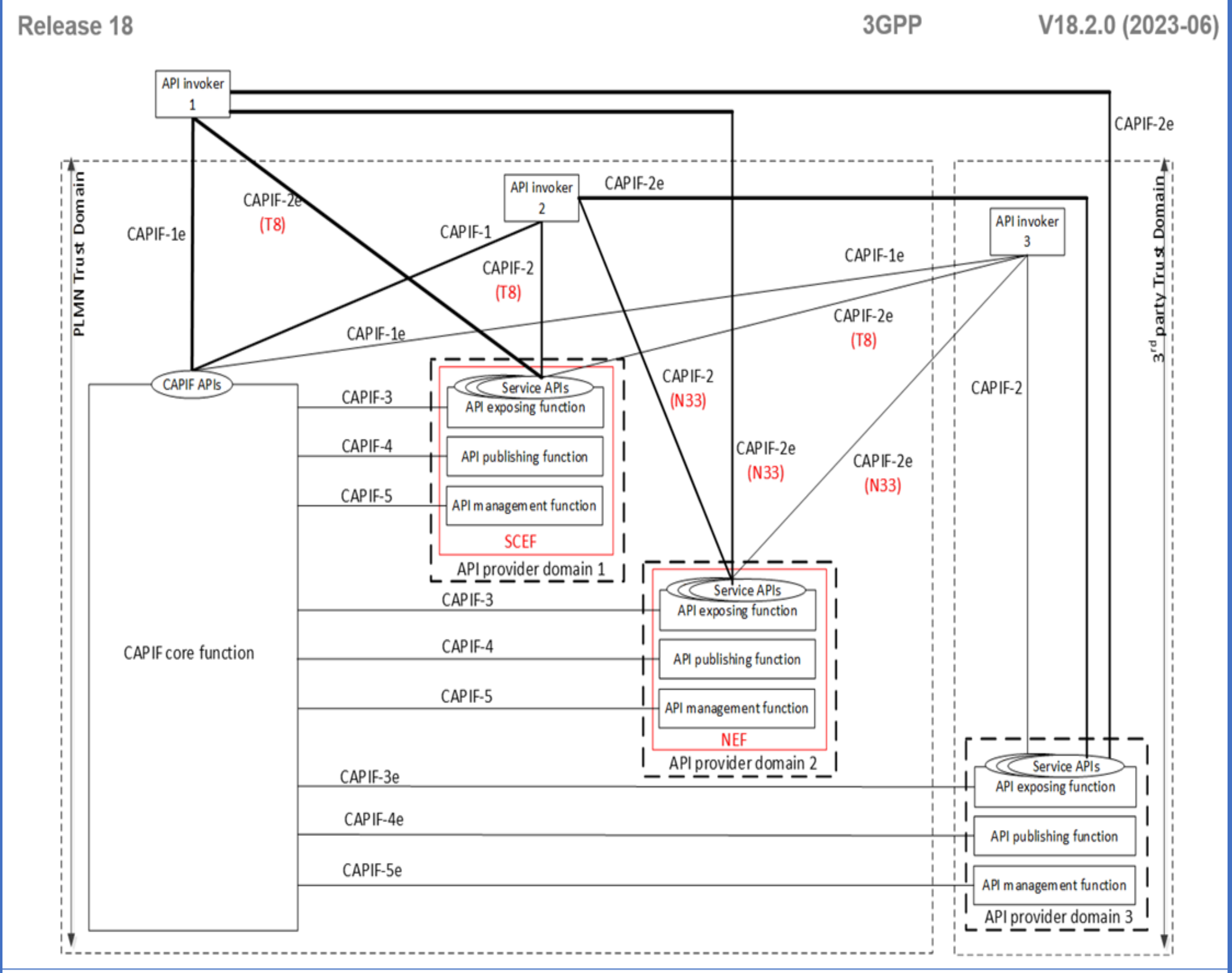


Figure: Integrated deployment of the 4G LTE SCEF and the 5G SA CN NEF with the CAPIF Architecture

1.7 5G CAPIF Role in Charging

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

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

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

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

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

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

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

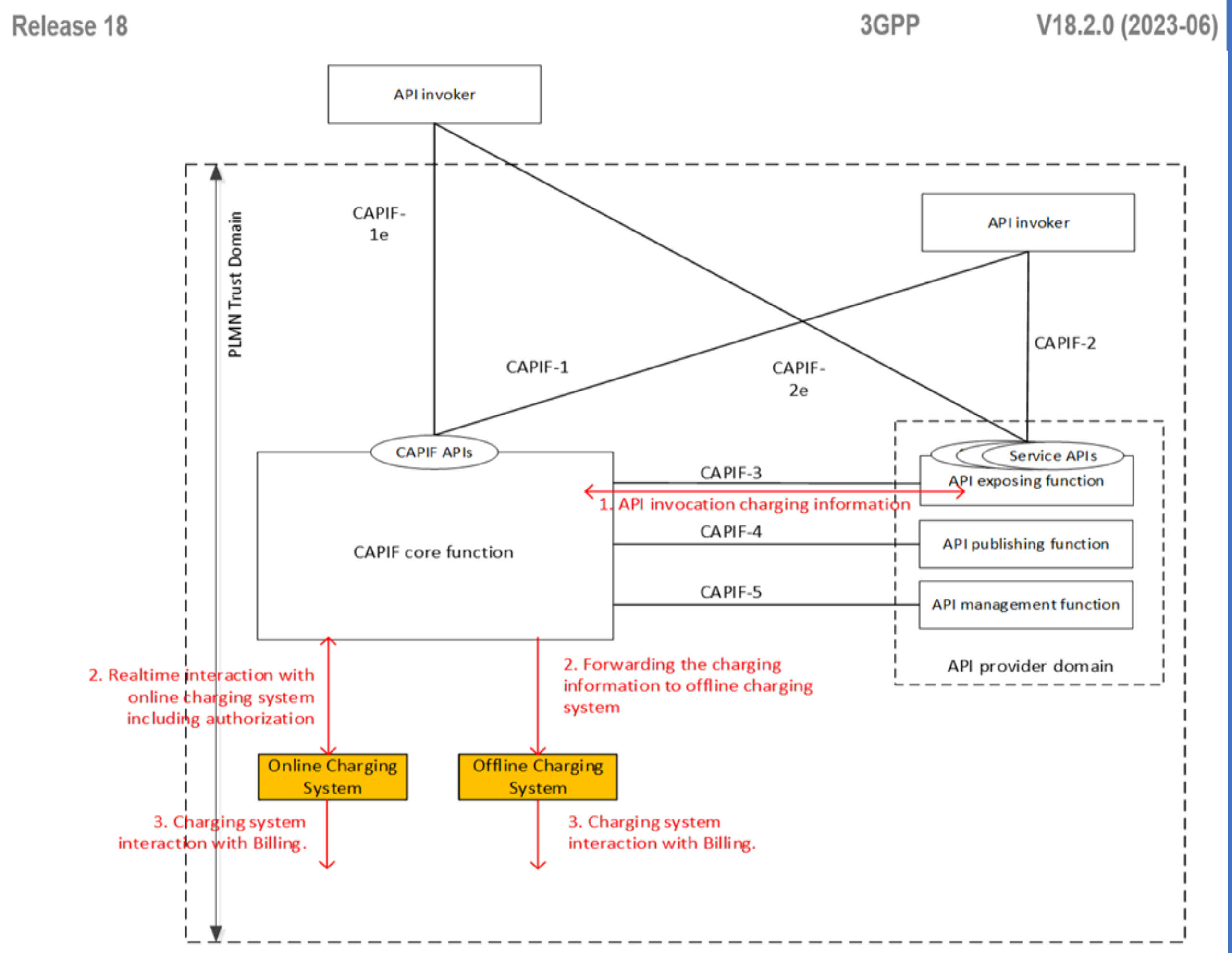


Figure: CAPIF role in Charging

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

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

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

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

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

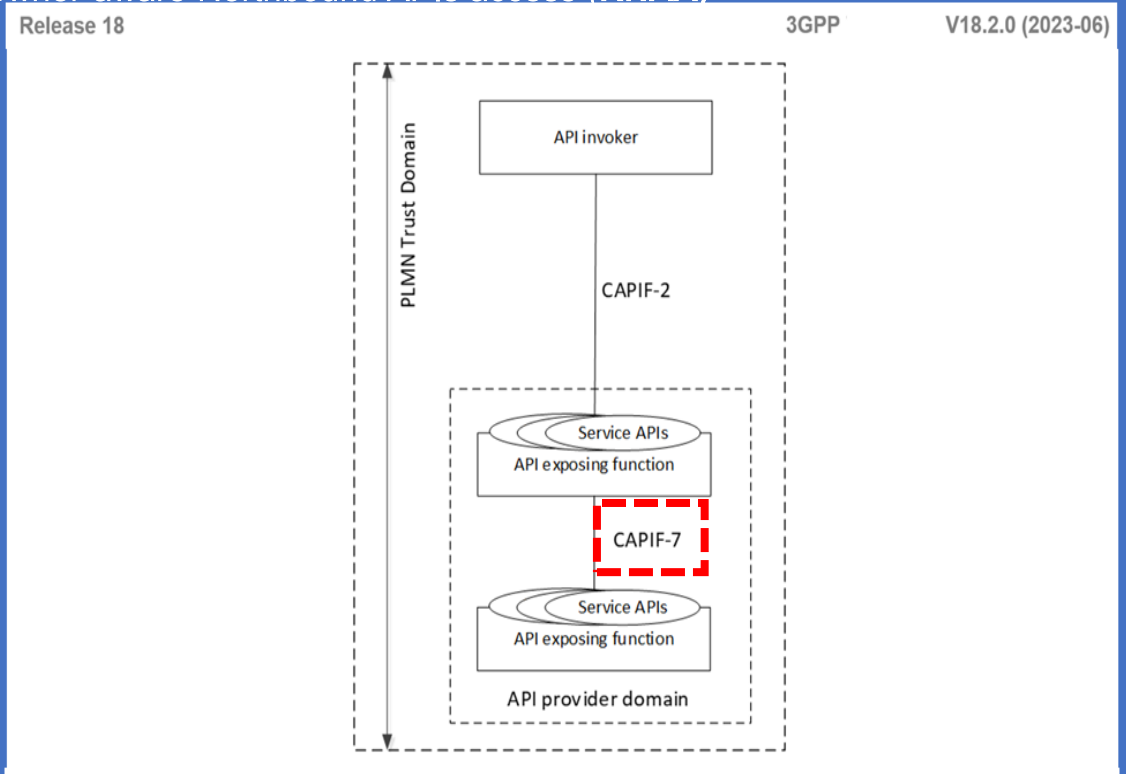


Figure: CAPIF Functional Model for Interactions between API Exposing Functions

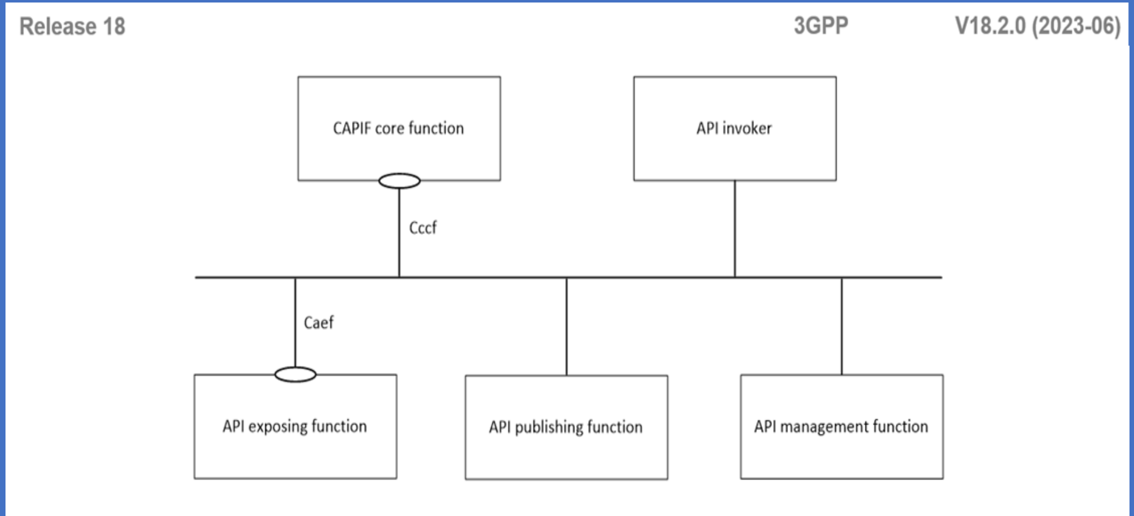


Figure: 5G CAPIF Functional Model Representation using Service-based Interfaces (SBIs)

CAPIF Functional Model description to support 3rd Party API Providers

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

The API invokers may exist within the PLMN Trust Domain, or within the 3rd party Trust Domain or outside of both the PLMN Trust Domain and the 3rd Party Trust Domain.

The API Provider Domain 1 offers the Service APIs from the PLMN Operator.

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

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

The API Invoker 2 within the PLMN Trust Domain interacts with the CAPIF Core Function (CCF) via CAPIF-1, and invokes the Service APIs in the PLMN Trust Domain via CAPIF-2 and invokes the Service APIs in the 3rd Party Trust Domain via CAPIF-2e.

The API Exposing Function (AEF), the API Publishing Function and the API Management Function of the API Provider Domain 1 within the PLMN Trust Domain interacts with the CAPIF core function via CAPIF-3, CAPIF-4 and CAPIF-5 respectively. The API exposing function, the API publishing function and the API management function of the API provider domain 2 within the 3rd party trust domain interacts with the CAPIF core function in the PLMN trust domain via CAPIF-3e, CAPIF-4e and CAPIF-5e respectively. The API Exposing Function within the PLMN trust domain and the 3rd party trust domain provides the service APIs to the API invoker, offered by the respective trust domains.
The interactions between the API Exposing Functions within the PLMN Trust Domain is via **CAPIF-7** (not shown in the Figure for simplicity).

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

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

Release 18 3GPP V18.2.0 (2023-06)

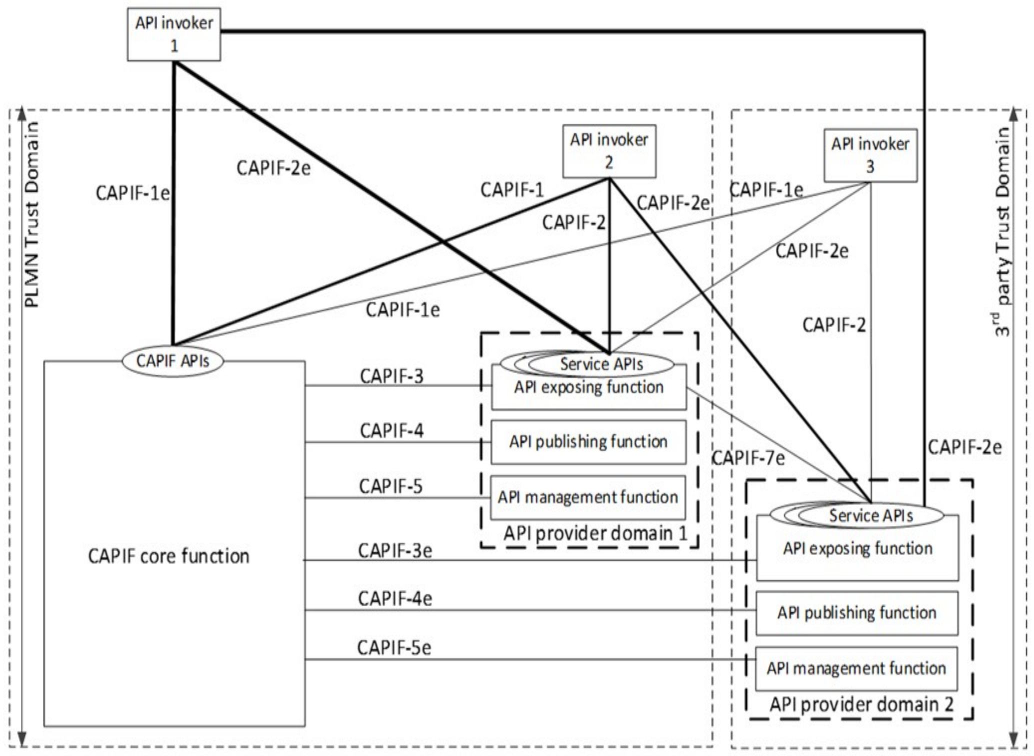


Figure: Functional Model for the CAPIF to support 3rd Party API Providers

1.9 Deployment Options of API Providers

Deployment of the 5G
- enhanced Common API Framework (CAPIF),
- Service APIs and
- Authorization APIs

by different Organizations within the PLMN Trust Domain

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

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

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

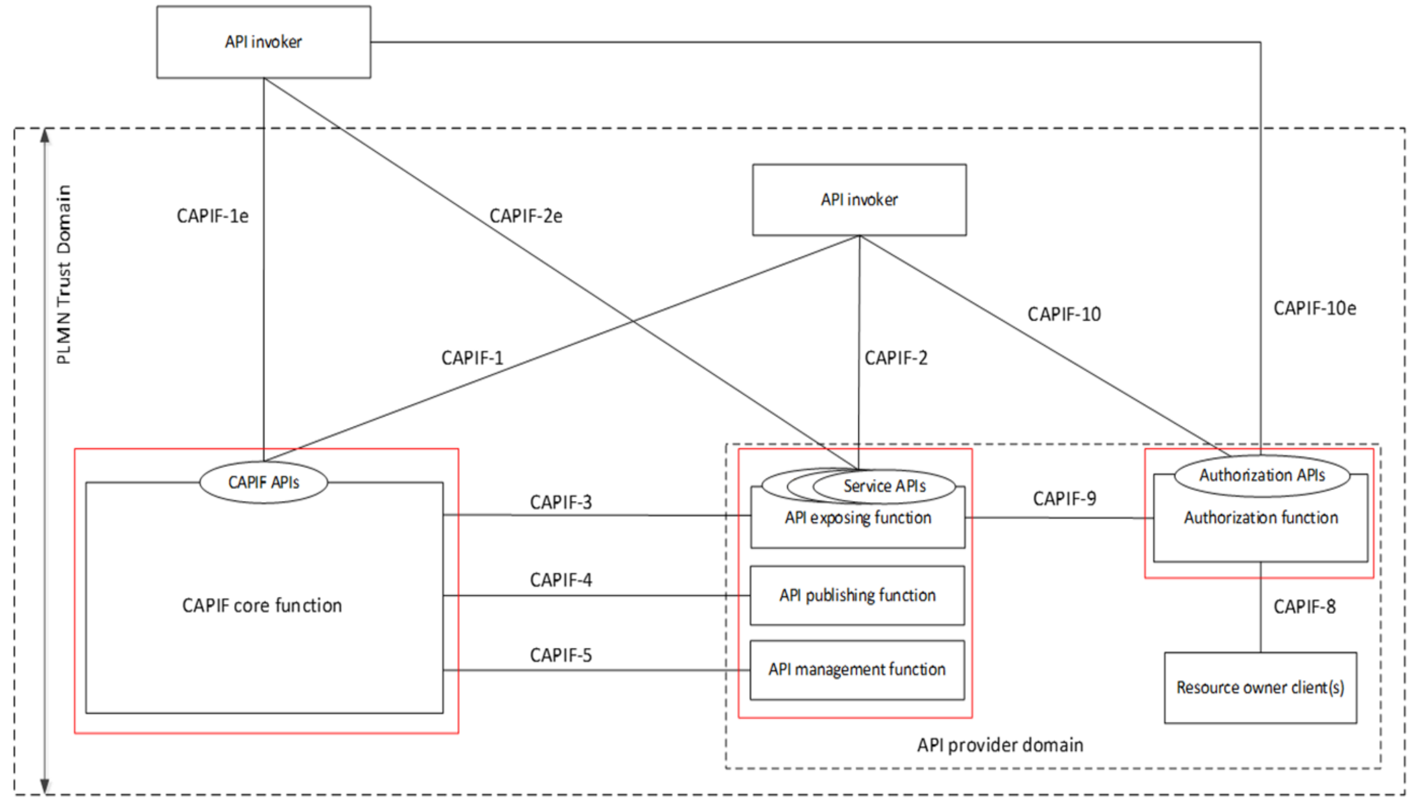


Figure: Deployment of the 5G enhanced Common API Framework (CAPIF), Service APIs and Authorization APIs by different Organizations within the PLMN Trust Domain

5G CAPIF Interconnection Model

CAPIF-6 and CAPIF-6e Reference Points connect two 5G Common API Framework Core Functions (CCFs) located in the same or different PLMN Trust Domains, respectively.

The reference points allows API invokers of a CAPIF Provider to utilize the Service APIs from the 3rd Party CAPIF Provider or another CAPIF Provider within trust domain.

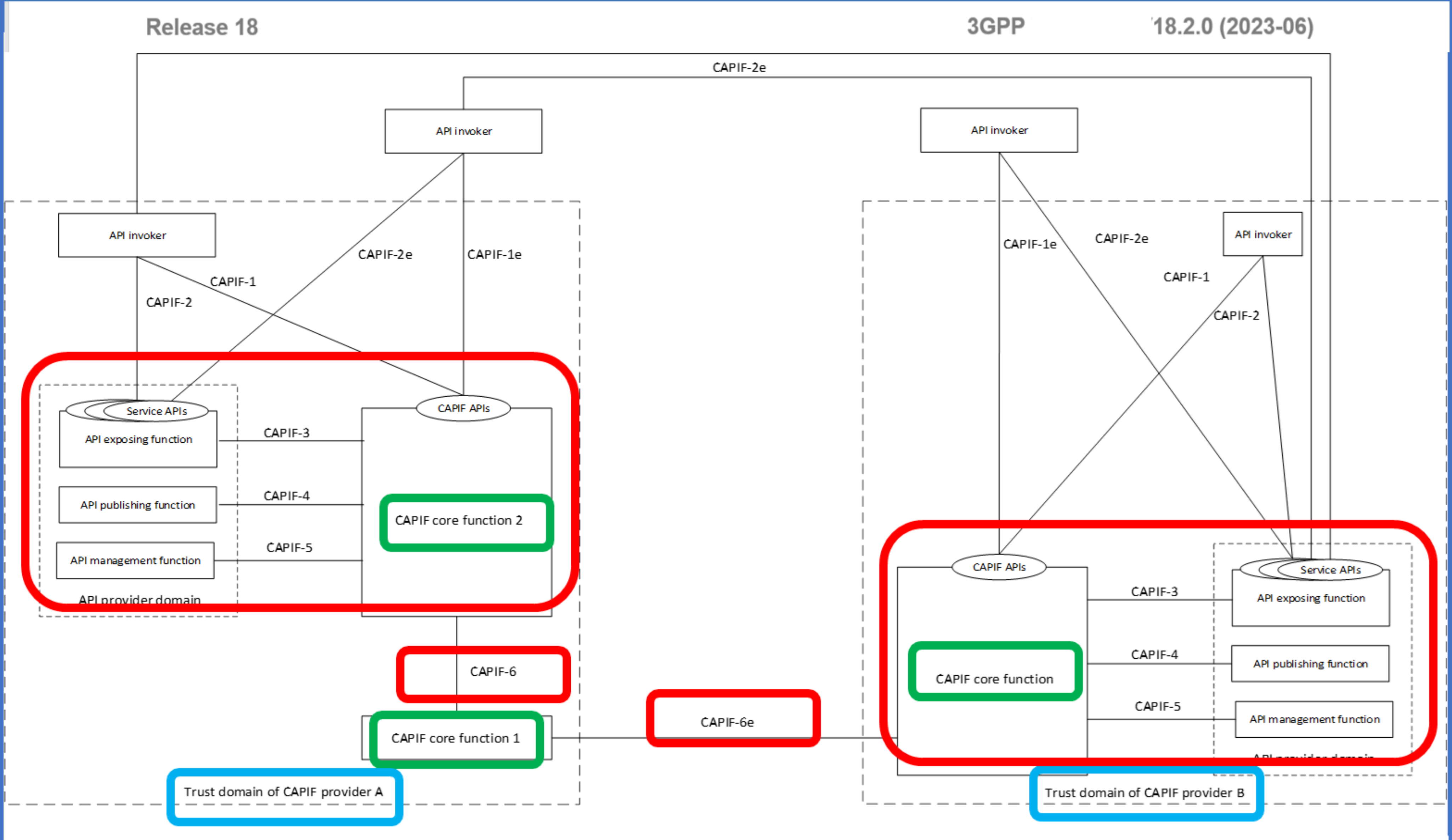


Figure: 5G Common API Framework Core Function (CCF) Interconnection Functional Model

The API Invoker supports several Capabilities as:

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

5G CAPIF Interconnection Model

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

The CAPIF provider A & CAPIF provider B host the CAPIF in their Trust Domains. A Business Relationship exists between the CAPIF Providers.
The CAPIF Providers in their respective Trust Domain hosts multiple CAPIF instances where each CAPIF instance consists of the CCF (local), the API Provider Domain and the API Invokers. All interactions within the CAPIF instance is according to the Functional Model as specified by 3GPP.
When multiple CAPIF instances are deployed by a CAPIF Provider there may be a hierarchy associated with the multiple CCF deployed which allows:
- the designated CCF of the CAPIF Provider A to interconnect with the designated CCF of the CAPIF provider B; and
- within CAPIF Provider A, one or more CCF interacts with the designated CCF 1

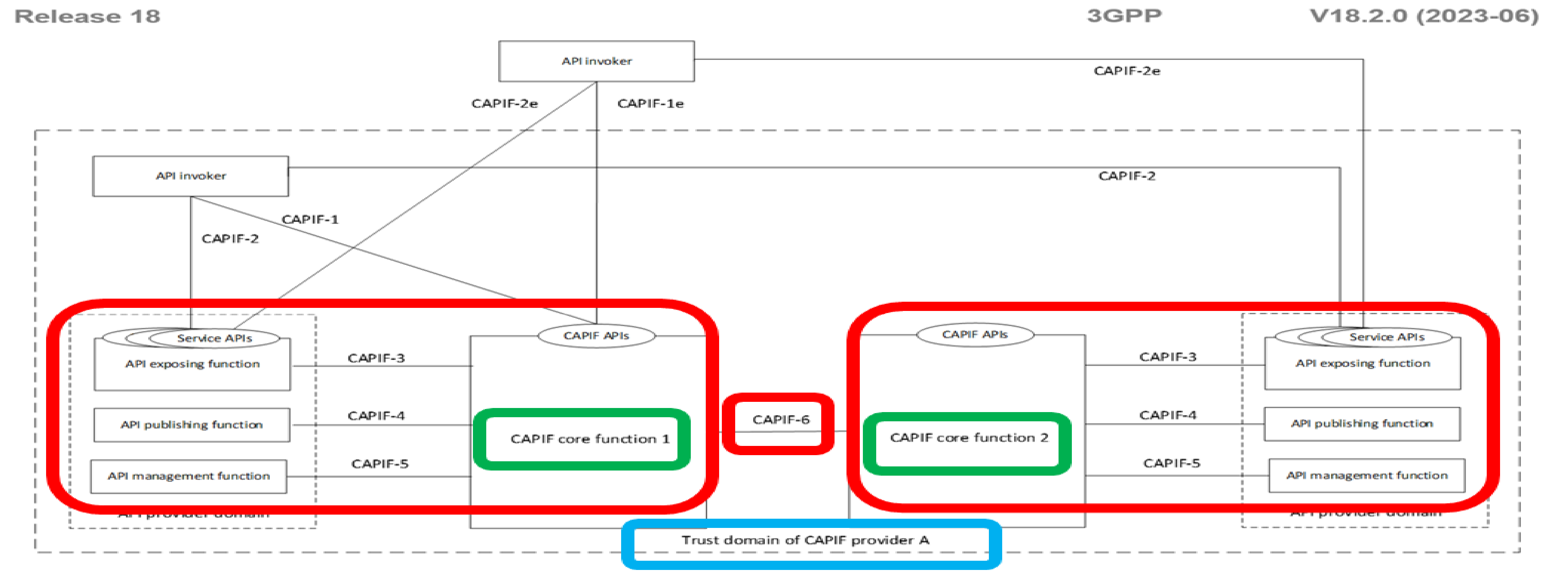


Figure: 5G Functional Architecture high-level for Common API Framework (CAPIF) Interconnection within a CAPIF Provider

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

Distributed CAPIF Core Functions (CCFs)

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

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

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

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

- the CAPIF Core Function (CCF) as specified in 5G Common API Framework to support onboarding of **EASs** (**API invokers**), Publish of Service APIs, Discovery of Service APIs and Charging of Service APIs invocations; and

- the API Exposing Function as specified in 5G Common API Framework to expose the **Service APIs from SCEF/NEF** to the EASs via Proxy or Gateway Function.

Centralized CAPIF Core Function (CCF)

The EES can support EAS (owned by **3rd Party** or by **PLMN Operator**) access to Northbound APIs exposed by **SCEF/NEF** by using centralized **CAPIF core functions (CCFs)** as shown in the Figure.
The EDNs reside outside the PLMN Trust Domain. In **EDN 2, the EAS and EES** are within the same **ECSP Ttrust Domain**. While **in EDN 1**, the **EES and the EAS** are in the **different ECSP Trust Domains**.

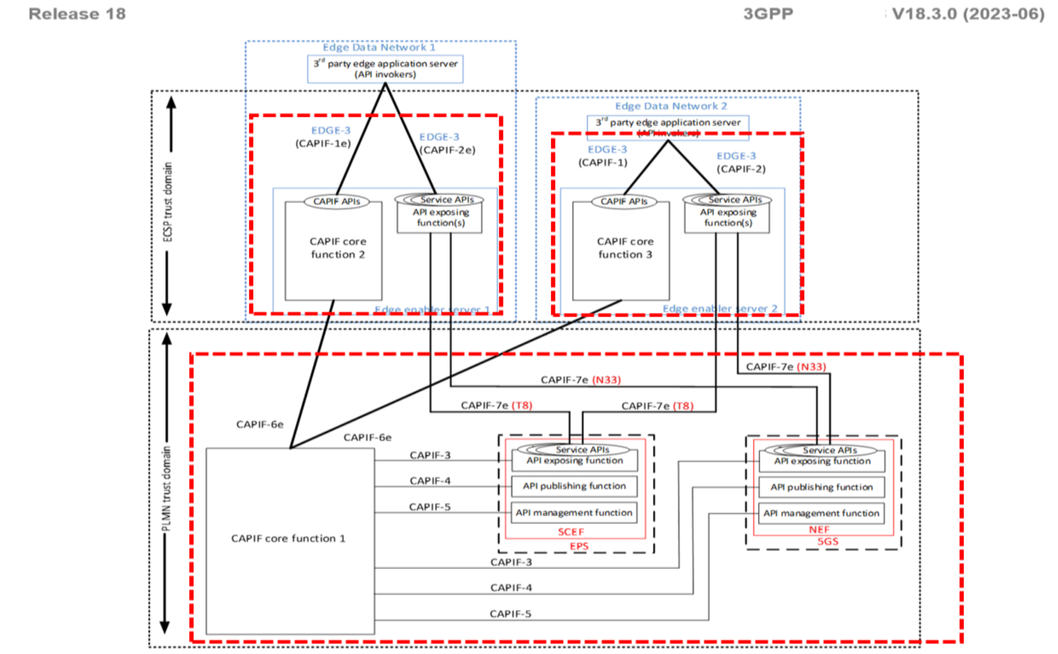


Figure: 5G Architecture enabling Edge Applications Edge Enabler Server (EES) supporting distributed 5G Common API Framework Core Function (CCF)

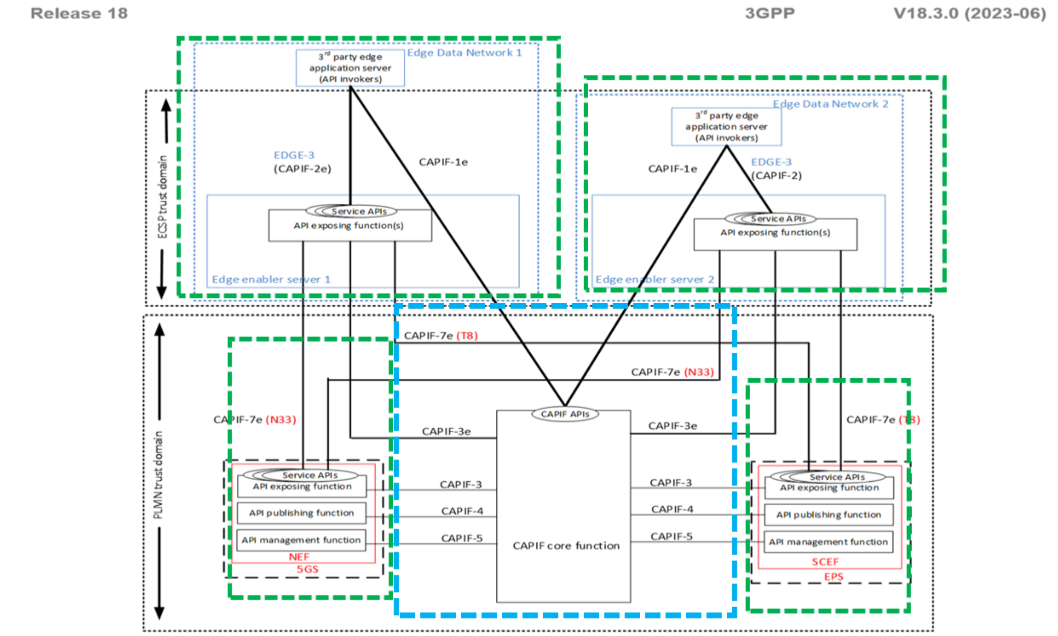


Figure: 5G Architecture enabling Edge Applications Edge Enabler Server (EES) supporting centralized 5G Common API Framework Core Function (CCF)

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

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

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

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

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

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

The **EES of an EDN** provides the following functions for exposure of EAS Service APIs:
- The CCF as specified in 5G Common API Framework to support:
- On-boarding of **EASs (API invokers)**,
- Publish of EAS Service APIs,
- Discovery of EAS Service APIs,
- Charging of EAS Service APIs Invocations.

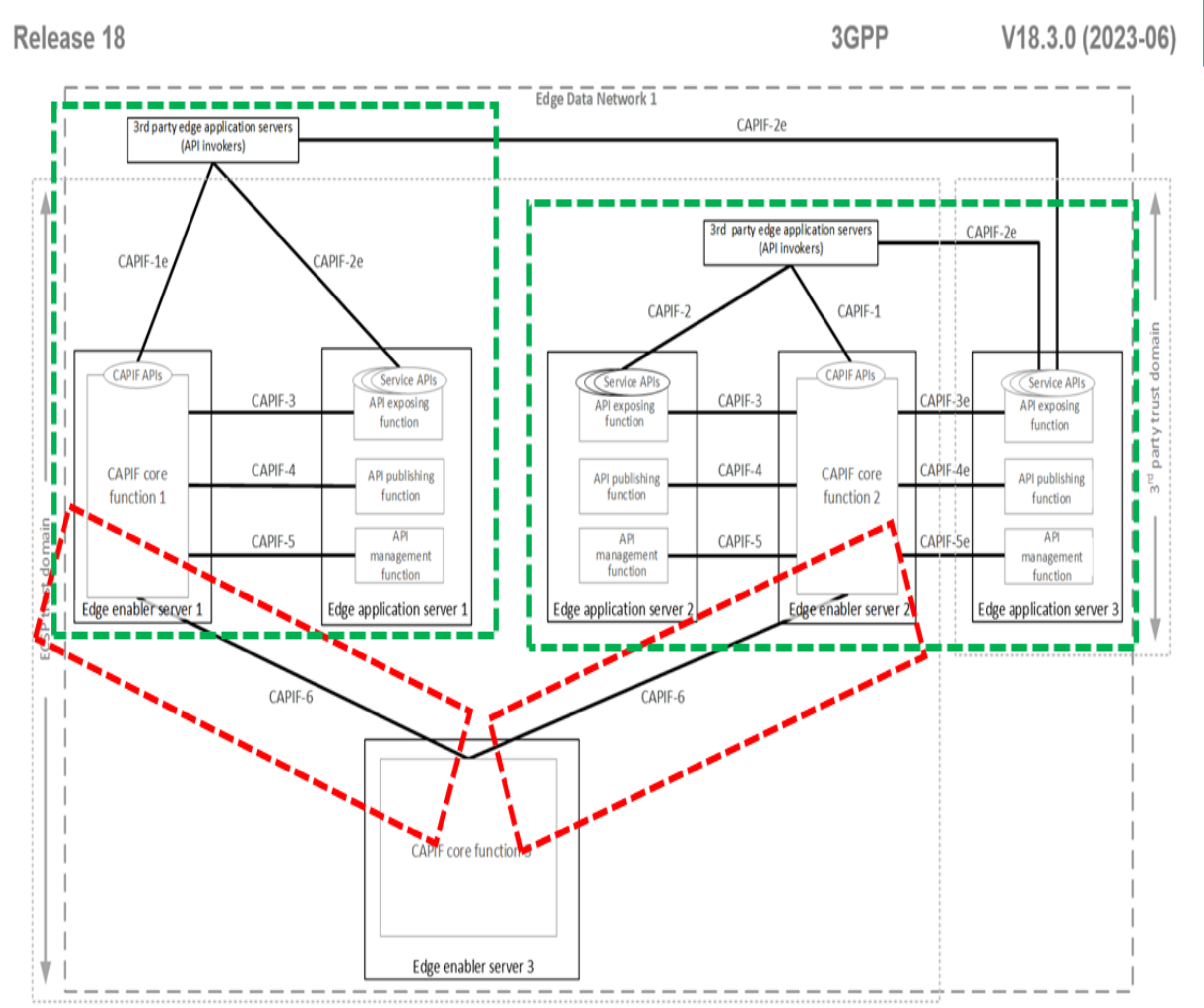


Figure: 5G Architecture enabling Edge Applications Edge Enabler Server (EES) supporting 5G Common API Framework Functions for exposure of EAS Service APIs

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

5G Architecture for enabling Edge Applications UE Identifier API

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

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

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

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

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

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

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

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

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

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

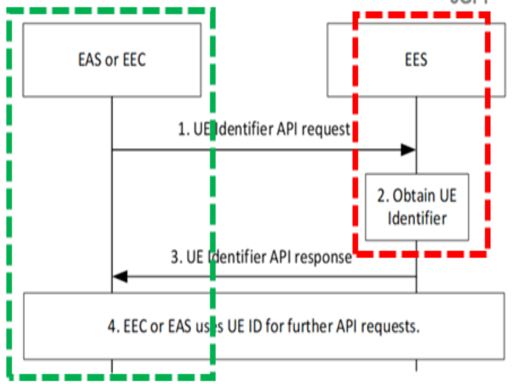


Figure: 5G Architecture for enabling Edge Applications UE Identifier API

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

Table : UE Identifier API request

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

Table : UE Identifier API response

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

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

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

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

EDGE-5 APIs include one-time Request/Response Operations for:
- **EAS discovery,**
- **Retrieval of UE ID and**
- **ACR Operations.**

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

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

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

EDGE-5 specified Procedures are:
- Registration;
- EAS discovery;
- ACR trigger request;
- EEC services subscription;
- UE ID request;

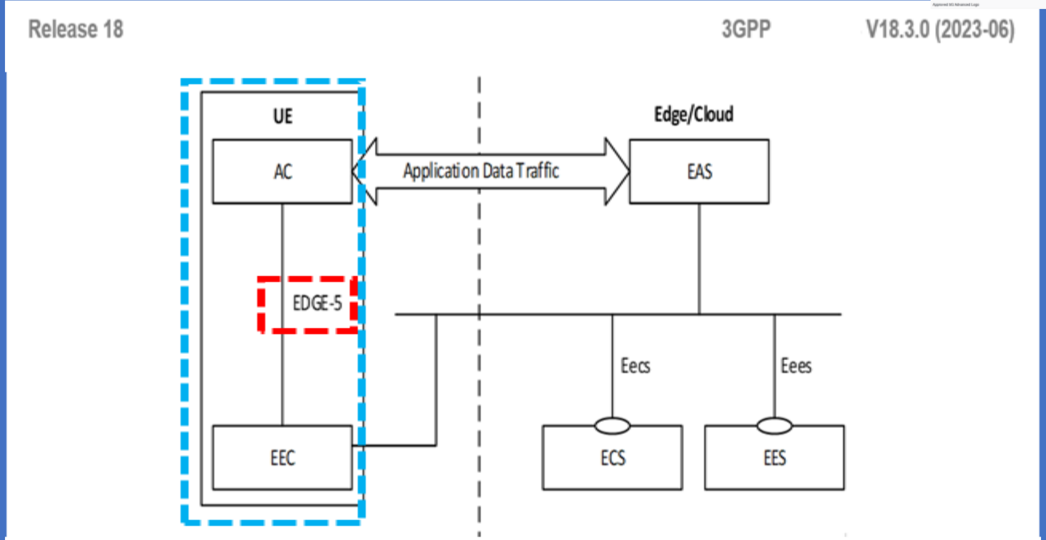


Figure: 5G Architecture for enabling Edge Applications - Service-based Representation

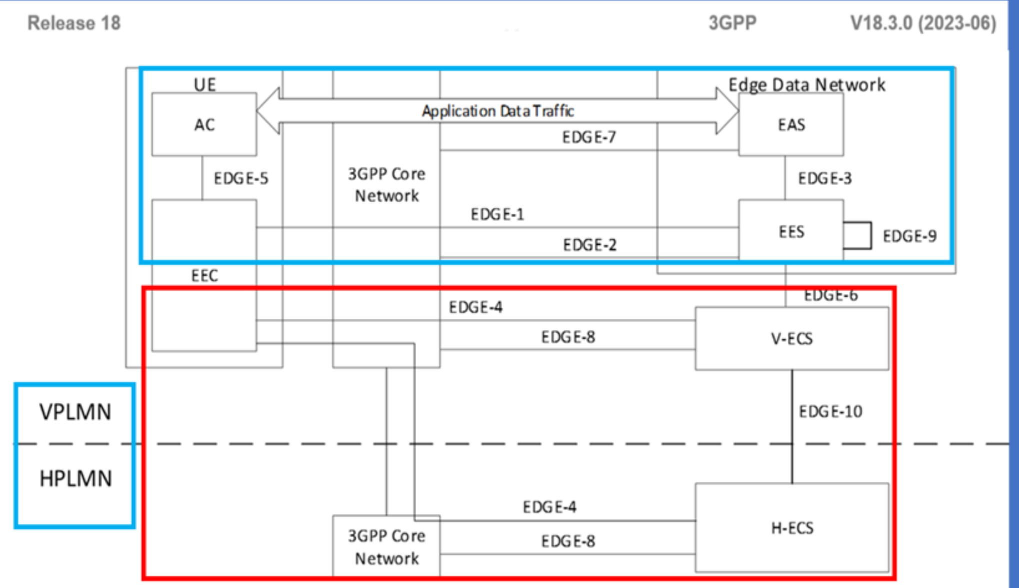


Figure: 5G Architecture for enabling Edge Applications (EDGEAPP) Services Roaming: Local breakout (LBO) for UE AC towards VPLMN EAS and EES over EDGE-1 and Home-Routed for UE EEC to H-ECS in HPLMN via V-ECS in VPLMN over EDGE-4

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

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

The Figure shows the Capability Exposure for enabling Edge Applications.

The Capability Exposure for enabling Edge Applications includes:

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

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

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

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

Table : APIs provided by the ECS

API Name	Known Consumers
Eecs_ServiceProvisioning	EEC
Eecs_EESRegistration	EES
Eecs_TargetEESDiscovery	EES

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

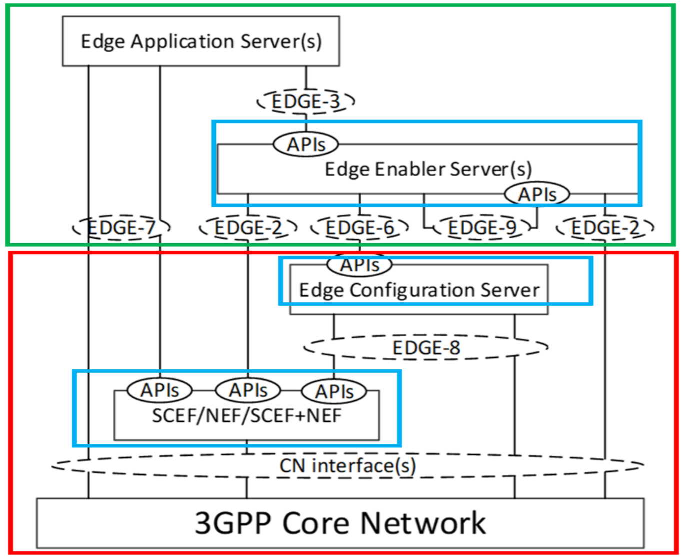


Figure: 5G Architecture Capability Exposure APIs for enabling Edge Applications

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

Table : APIs provided by the EES

API Name	Known Consumers
Eees_EECRegistration	EEC
Eees_EASRegistration	EAS
Eees_EASDiscovery	EEC
Eees_UELocation	EAS
Eees_ACRManagementEvent	EAS
Eees_AppClientInformation	EAS
Eees_UEIdentifier	EEC, EAS
Eees_SessionWithQoS	EAS
Eees_TargetEASDiscovery	EAS, EES
Eees_AppContextRelocation	EEC, EAS
Eees_ACREvents	EEC
Eees_EELManagedACR	EAS
Eees_EECContextPull	EES
Eees_EECContextPush	EES
Eees_SelectedTargetEAS	EAS
Eees_ACRStatusUpdate	EAS

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

This following slides present some of the enhancements to 5GS Architecture and related to it Procedure(s) and Flow(s), Policy and Charging Control for the 5G System as defined by 3GPP in the respective specifications in order to support Wireline Access Network and Fixed Wireless Access.

Network selection

The HPLMN is implicitly selected by Wired Physical Connectivity between 5G-RG (5G Residential Gateway) or FN-RG (Fixed Network RG) and W-AGF (Wireline-Access Gateway Function).

NOTE 1: *The 5G-RG or FN-RG can only connect to a Single Physical Wired Access W-5GAN to a W-AGF configured at line provisioning by the Operator, in addition no PLMN information is advertised by AS Protocols in W-5GAN, since the Network selection feature is not supported.*

In the case of 5G-RG connected via FWA the 5GS Architecture specification applies with the following difference:

- The PLMN selection defined in 5GS Architecture applies with the UE replaced by 5G-RG.

Release 18 3GPP V18.2.0 (2023-06)

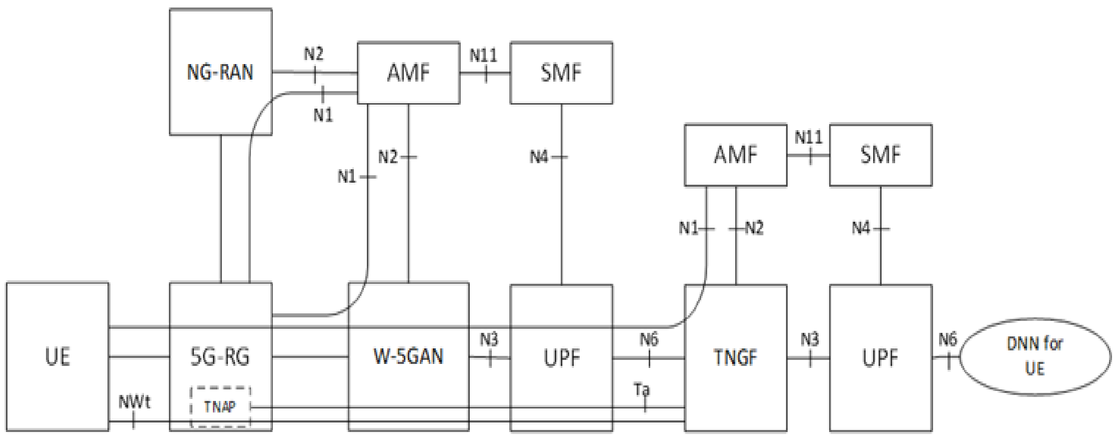


Figure: 5G System Non-Roaming Architecture for UE behind 5G-RG using Trusted N3GPP Access

Release 18 3GPP V18.2.0 (2023-06)

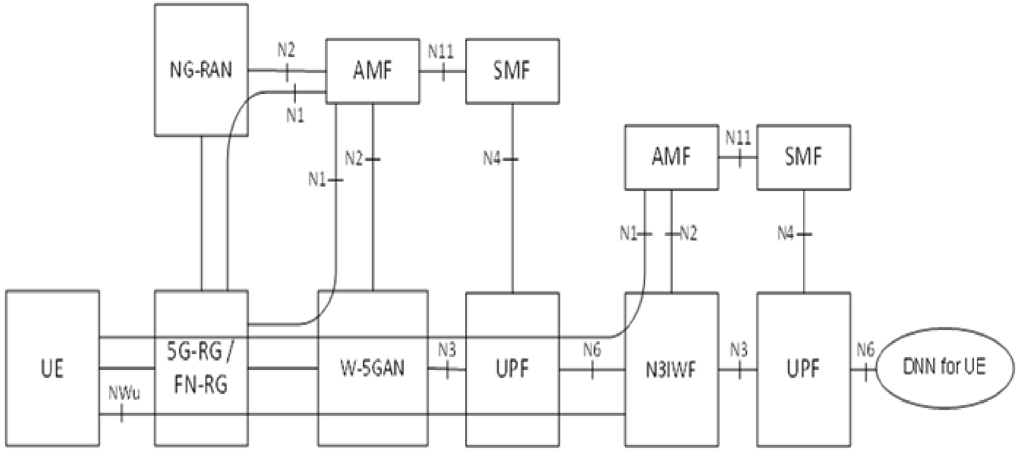


Figure: 5G System Architecture for UE behind 5G-RG and FN-RG using Untrusted N3GPP Access

1. 5G System Architecture enhancements on Wireless and Wireline Convergence Access support

Identification and Authentication

In the case of **5G-RG** *connected via* **W-5GAN or FWA**, the 5GS Architecture specification applies with the following difference:

- **UE** is replaced by **5G-RG.**

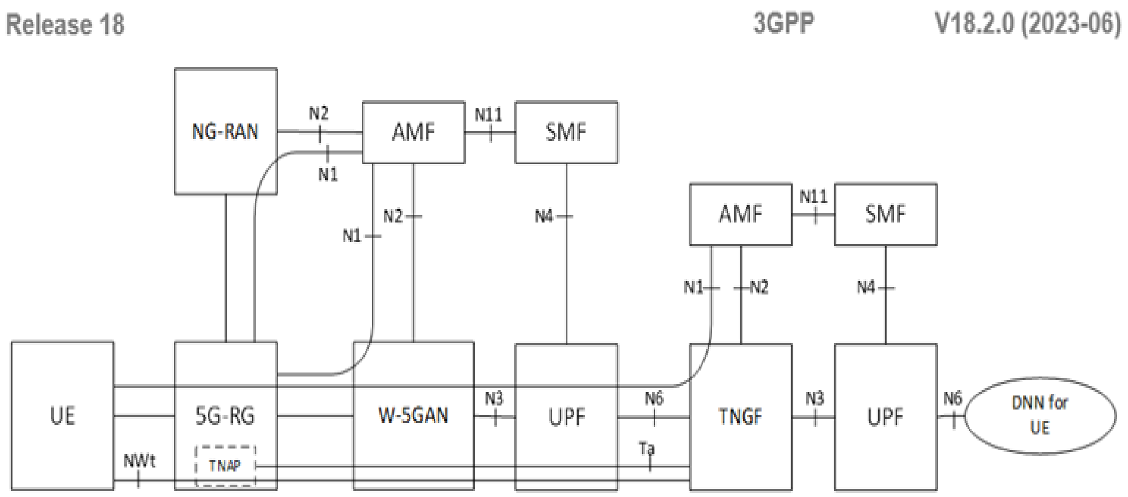


Figure: 5G System Non-Roaming Architecture for UE behind 5G-RG using Trusted N3GPP Access

In the case of **FN-RG** connected via **W-5GAN**, the 5GS Architecture specification applies with the following differences:

- UE is replaced by FN-RG.
- The W-AGF provides the NAS signalling connection to the 5GC on behalf of the FN-RG.
- The W-5GAN may authenticate the FN-BRG per BBF specifications. The W-5GAN may authenticate the FN-CRG per CableLabs DOCSIS MULPI.

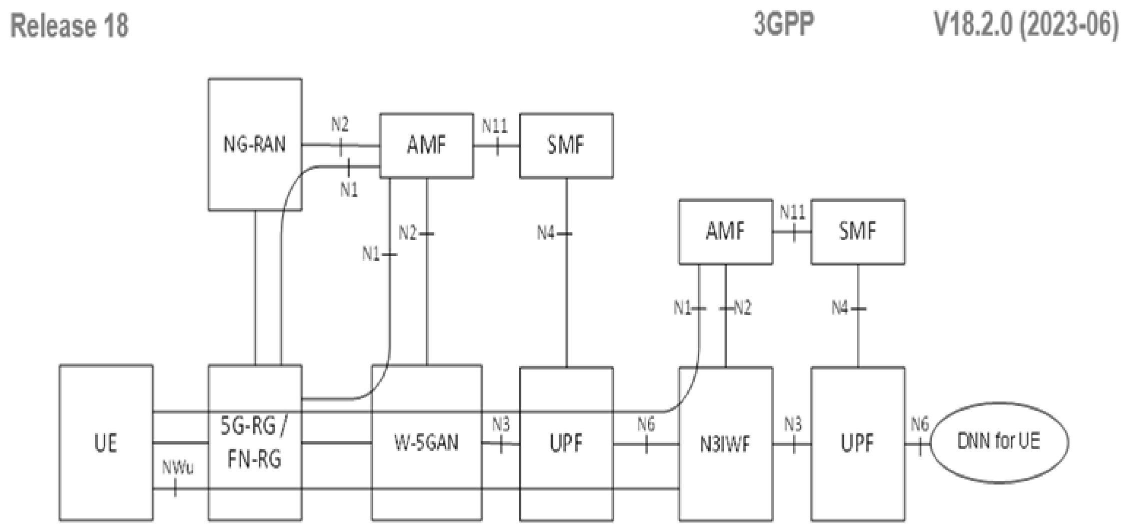


Figure: 5G System Architecture for UE behind 5G-RG and FN-RG using Untrusted N3GPP Access

Authorisation

In the case of **5G-RG** connected via **W-5GAN or FWA**, the 5GS Architecture specification applies with the following differences:

- UE is replaced by 5G-RG.

In the case of **FN-RG** connected via **W-5GAN**, the 5GS Architecture specification applies with the following differences:

- **UE** is replaced by **FN-RG**.
- **W-AGF** performs the **UE** Registration procedure on behalf of the **FN-RG**.

Access Control and Barring

In the case of **5G-RG** or **FN-RG** connected via **W-5GAN** the Access Control and Barring defined in the 5GS Architecture is not applicable.

In the case of **5G-RG** connected via **FWA** the 5GS Architecture specification applies with the following difference:
- UE is replaced by 5G-RG.

Release 18 3GPP V18.2.0 (2023-06)

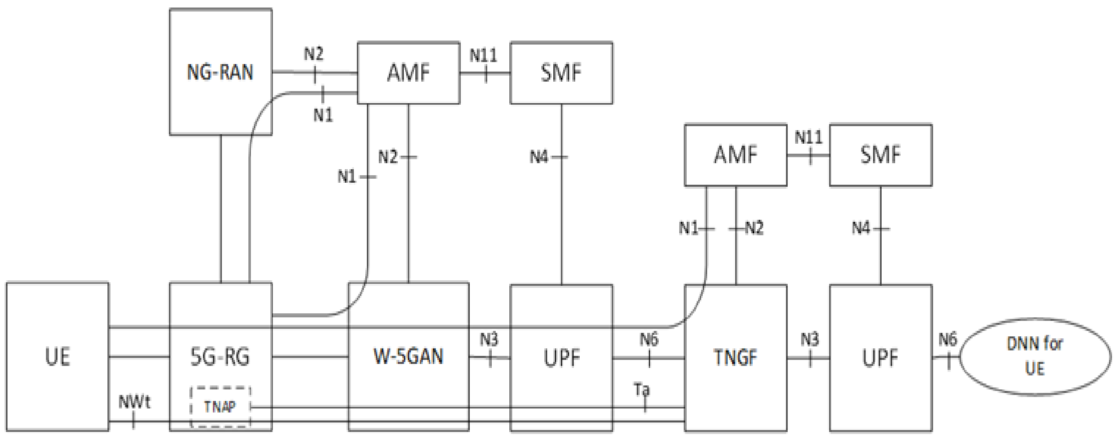


Figure: 5G System Non-Roaming Architecture for UE behind 5G-RG using Trusted N3GPP Access

Release 18 3GPP V18.2.0 (2023-06)

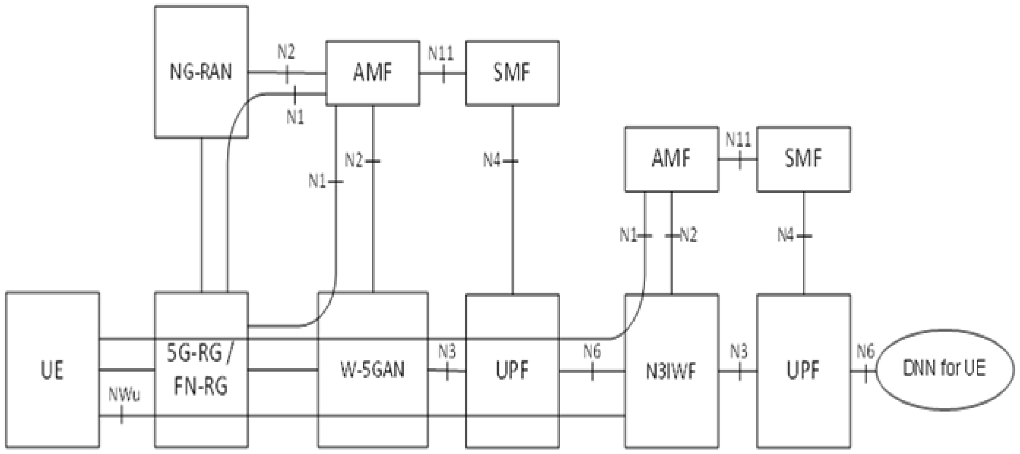


Figure: 5G System Architecture for UE behind 5G-RG and FN-RG using Untrusted N3GPP Access

Registration and Connection Management

Registration Management when **5G-RG or FN-RG** is connected to **5GC** via Wireline Access is described in the 5GS Architecture specification.

Registration Management when **5G-RG** is connected to **5GC** via **NG RAN A**ccess is described in the 5GS Architecture specification.

Connection Management when **5G-RG or FN-RG** is connected to **5GC** via Wireline Access is described in the 5GS Architecture specification.

Connection Management when **5G-RG** is connected to **5GC via NG RAN A**ccess is described in the 5GS Architecture specification.

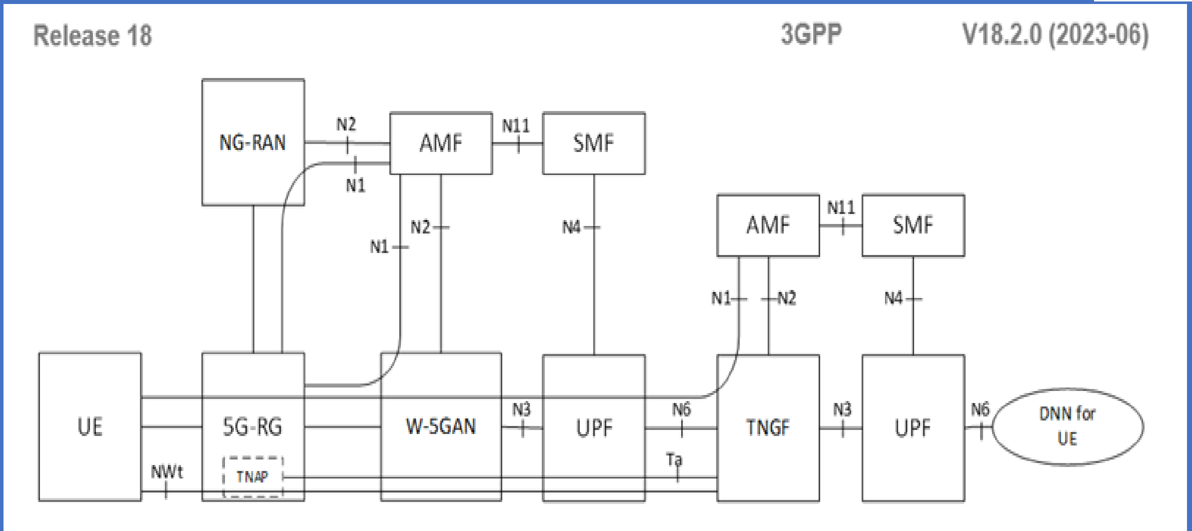


Figure: 5G System Non-Roaming Architecture for UE behind 5G-RG using Trusted N3GPP Access

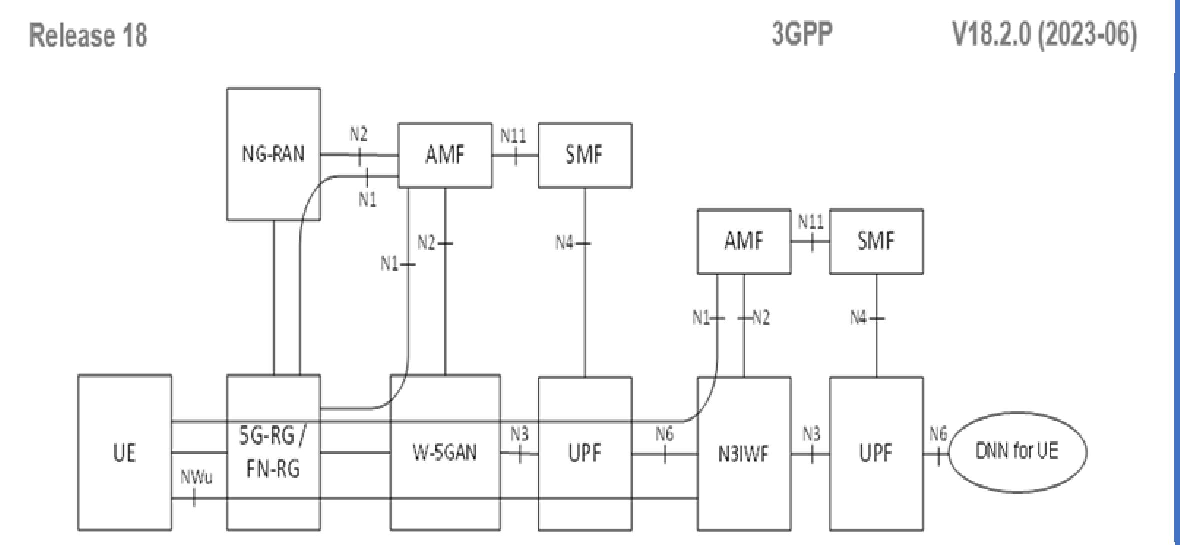


Figure: 5G System Architecture for UE behind 5G-RG and FN-RG using Untrusted N3GPP Access

1. 5G System Architecture enhancements on Wireless and Wireline Convergence Access support

Mobility Restrictions

Mobility Restrictions restrict Service Access of an 5G-RG depending on RG location.

For a **5G-RG connecting over NG-RAN**, the *Mobility Restriction* functionality as described in the 5GS Architecture applies.

For an **5G-RG** connecting over Wireline Access, the Mobility Restriction functionality is described in this clause.

Mobility Restrictions do not apply to scenarios with FN-BRG (Fixed Network Broadband RG).

NOTE 1: *Since Access to 5GC for FN-BRG Subscriptions are identified by a SUPI determined from the GLI as described. Such Subscriptions are by definition restricted to a specific location.*

NOTE 2: *For FN-CRG Subscriptions, HFC Node ID is used to identify the location of FN-CRG, thus Service Area restrictions for the FN-CRG can be identified by an HFC_Node ID, or by a list of HFC_Node ID.* Mobility Restrictions for Wireline Access consists of Forbidden Area & Service Area Restrictions, as described in the following clauses.

Management of Forbidden Area in Wireline Access

In a Forbidden Area, the 5G-RG, based on subscription, is not permitted by the 5GC to initiate any communication with the 5GC for this PLMN or SNPN.

The UDM stores the Forbidden Area for wireline access in the same way as for 3GPP access, with the following differences:
- For Subscriptions for 5G-BRG, GLI is used to describe the Forbidden Area.
- For subscriptions for 5G-CRG and FN-CRG, HFC Node IDs are used to describe the Forbidden Area (instead of TA).
- The Forbidden Area in UDM can be encoded as a "allow list" indicating the non-forbidden area. In this case all GLI or HFC_Node ID values not included in the list are considered forbidden.

NOTE: The use of "allow list" is to ensure an efficient Forbidden Area definition if only a small set of GLI / HFC Node ID values are not forbidden.

Forbidden Area is enforced by AMF, based on Subscription Data and the Location Information received from W-AGF.

The AMF rejects a Registration Request from a 5G-RG or the W-AGF acting on behalf of a FN-CRG in a Forbidden Area with a suitable cause code. The 5G-RG behaviour depends on the Network Response (cause code from AMF) that informs the RG that communication is forbidden.

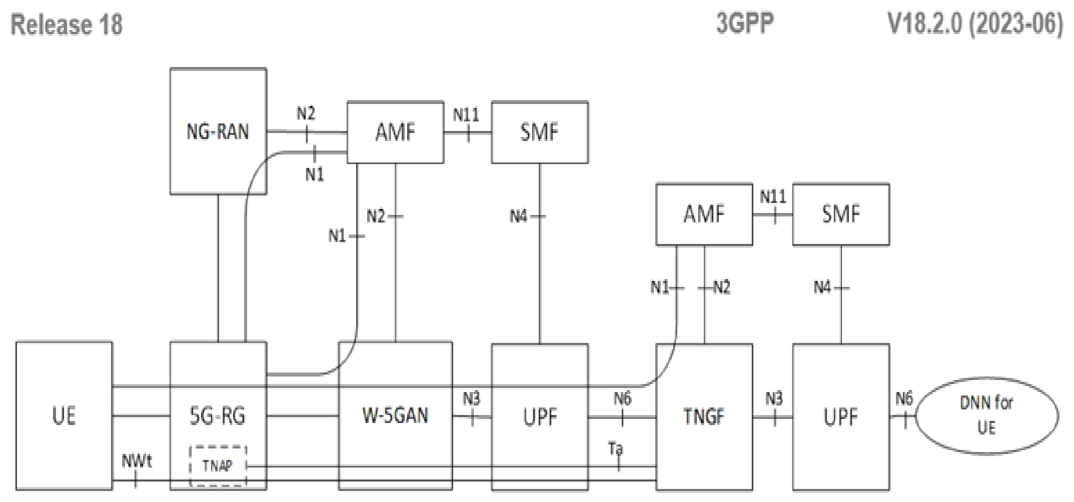


Figure: 5G System Non-Roaming Architecture for UE behind 5G-RG using Trusted N3GPP Access

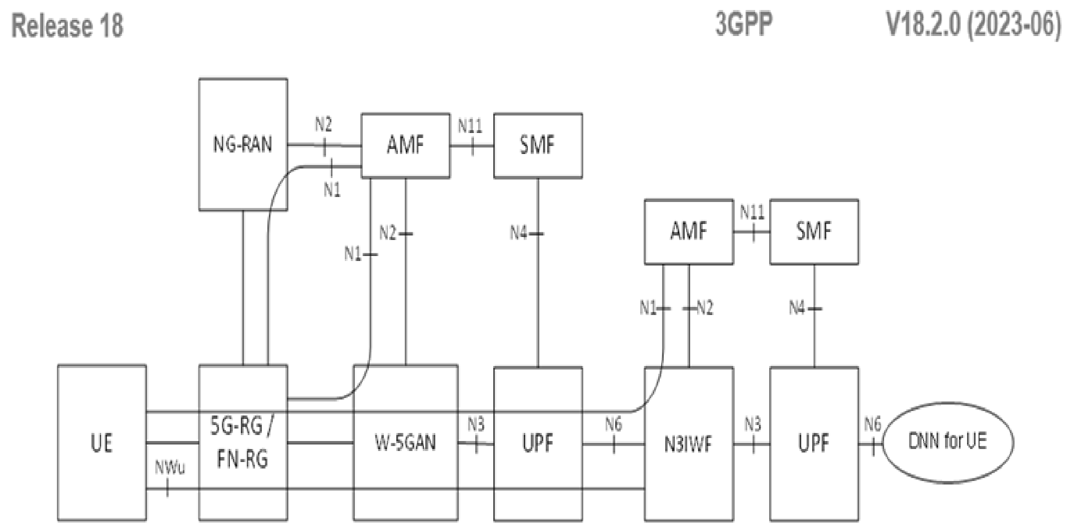


Figure: 5G System Architecture for UE behind 5G-RG and FN-RG using Untrusted N3GPP Access

Management of Service Area Restrictions in Wireline Access

The Subscription Data in the 5G CN for a 5G-BRG includes a Service Area Restriction which may contain either:
- Allowed or
- Non-Allowed Areas specified by using explicit GLI(s) and/or other Geographical Information (e.g., Longitude/Latitude, Zip Code, etc.).'

The Subscription Data in the 5G CN for a 5G-CRG and FN-CRG includes a Service Area Restriction which may contain either Allowed or Non-Allowed Areas specified by using explicit HFC Node IDs and/or other geographical information (e.g., longitude/latitude, zip code, etc.).

The Geographical Information used to specify Allowed or Non-Allowed Area is only managed in the Network, and the Network will map it to a List of GLI(s) or HFC Node IDs before sending Service Area Restriction information to the 5G CN Policy Node.

The 5G CN Node stores the Service Area Restrictions for the 5G-RG or FN-CRG as part of the Subscription Data.

The 5G CN Policy Node in the Serving Network may (e.g. due to varying conditions such as 5G-RG's Location, Time & Date) further adjust Service Area Restrictions of a 5G-RG, either by expanding an allowed Area or by reducing a Non-Allowed Area.

The 5G CN and the Policy Node may update the Service Area Restrictions of a 5G-RG or a FN-CRG at any time.

Upon change of serving AMF due to Mobility, the old AMF may provide the new AMF with the Service Area Restrictions of the 5G-RG that may be further adjusted by the 5G CN Policy node.

Release 18 3GPP V18.2.0 (2023-06)

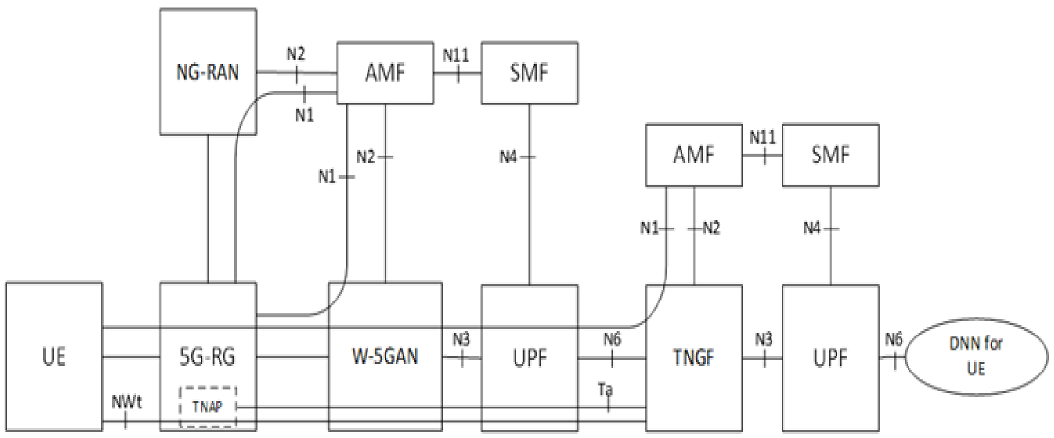


Figure: 5G System Non-Roaming Architecture for UE behind 5G-RG using Trusted N3GPP Access

Release 18 3GPP V18.2.0 (2023-06)

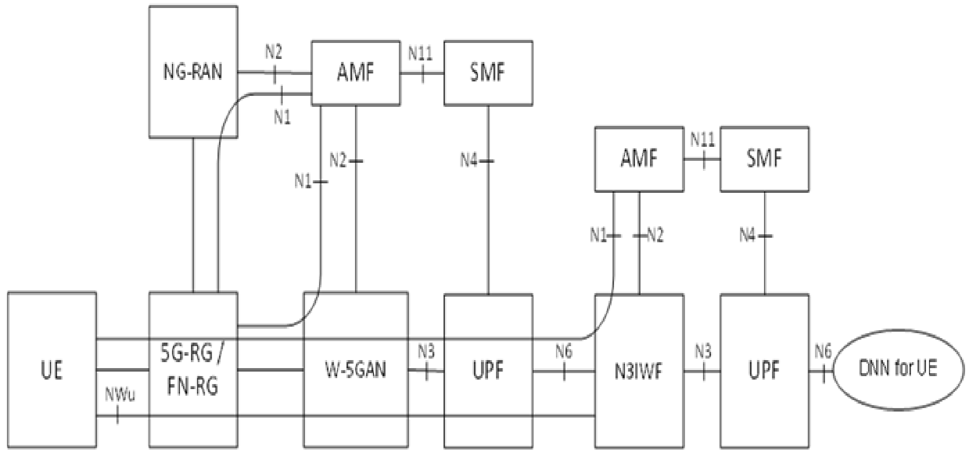


Figure: 5G System Architecture for UE behind 5G-RG and FN-RG using Untrusted N3GPP Access

UE behind 5G-RG and FN-RG

An RG connecting via W-5GAN or NG-RAN Access towards 5GC can provide Connectivity for a UE behind the RG to access an N3IWF or TNGF.

It is assumed that the UE is 5GC capable, i.e. supports un-trusted Non-3GPP Access and/or Trusted Non-3GPP Access.

This allows the RG, W-5GAN and the RG's Connectivity via 5GC to together act as Un-trusted/Trusted N3GPP Access to support UEs behind the RG.

When FN-RG/5G-RG is serving a UE, the Control (CP) & User Plane (UP) Packets of the UE is transported using a FN-RG/5G-RG IP PDU session and then from PSA UPF of that PDU session to an IWF.

A single FN-RG/5G-RG IP PDU session can be used to serve multiple UEs.

The Figure shows the Non-Roaming Architecture for a UE, behind a 5G-RG, accessing the **5GC via TNGF** where the combination of **5G-RG, W-5GAN and UPF serving the 5G-RG is acting as a trusted Non-3GPP access network**.

NOTE 1: *FN-RG and W-5GAN acting as trusted Non-3GPP access is not considered in this specification as it is assumed that FN-RG does not support EAP-5G.*

Release 18 3GPP V18.2.0 (2023-06)

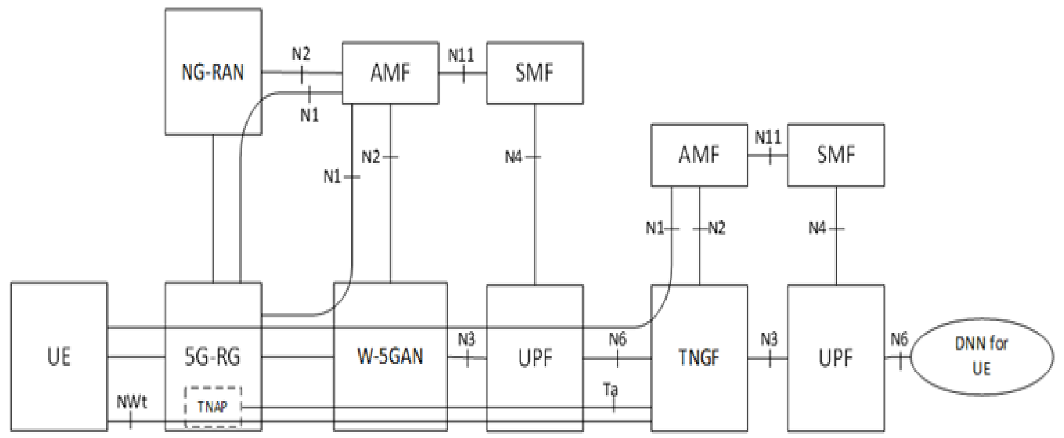


Figure: 5G System Non-Roaming Architecture for UE behind 5G-RG using Trusted N3GPP Access

Release 18 3GPP V18.2.0 (2023-06)

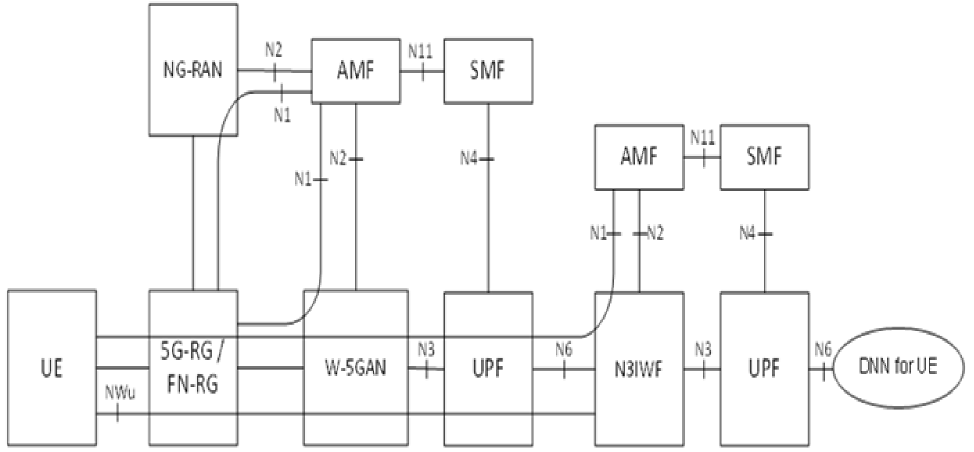


Figure: 5G System Architecture for UE behind 5G-RG and FN-RG using Untrusted N3GPP Access

Non-5G Capable Device behind **5G-CRG** (*5G Cable Residential Gateway*) and **FN-CRG** (*Fixed Network Cable RG*)

For isolated 5G Networks (i.e. Roaming is not considered) with Wireline Access, *Non-5G Capable* (**N5GC**) Devices connecting via **W-5GAN** (*Wireline 5G Access Network*) can be authenticated by the 5GC using EAP based Authentication method(s) as defined in 5GS Security Architecture & Procedure.

In the Figure, the following Call Flow describes the overall Registration procedure of such a Device.

Roaming is not supported for N5GC Devices.

The usage of N5GC Device correspond to a Subscription record in the 5G CN that is separate from that of the CRG.

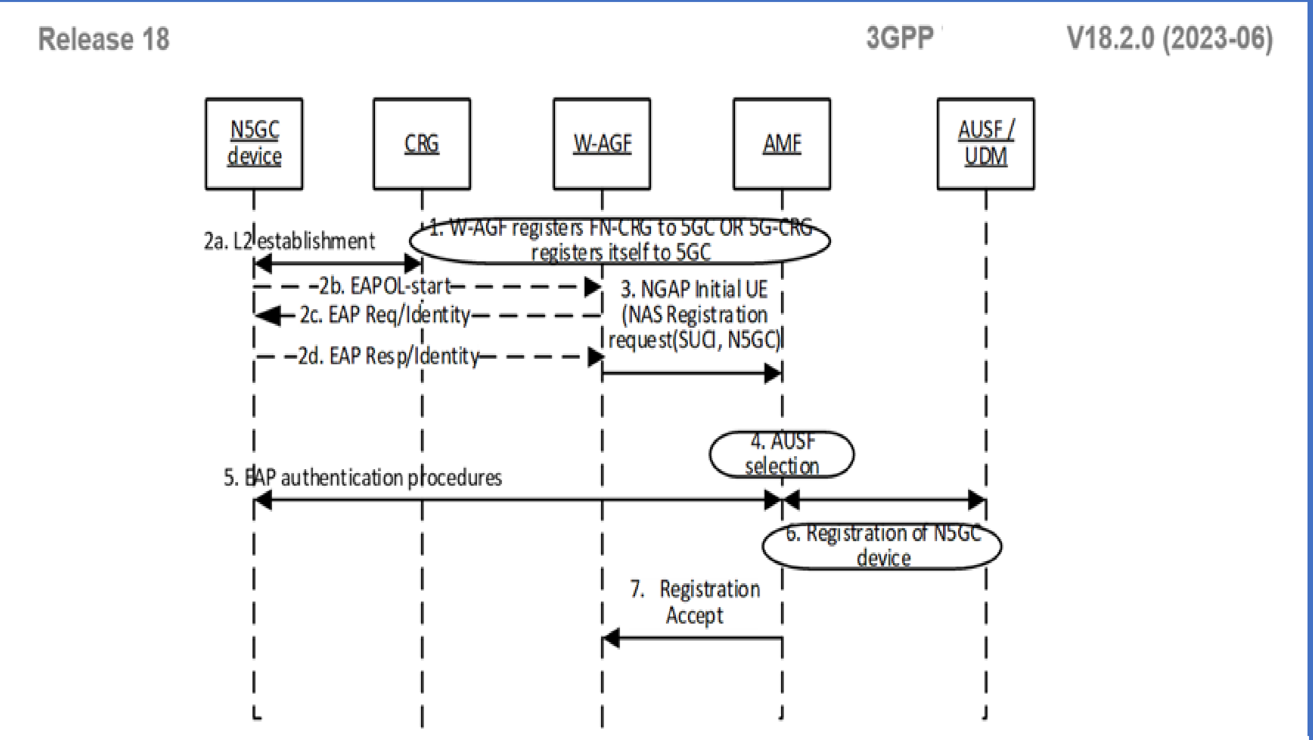


Figure: 5G Core registration of Non-5GC device

Differentiated services for NAUN3 (Non Authenticable Non-3GPP) Devices behind 5G-RG

NAUN3 Devices cannot be authenticated by 5GC, but may e.g. be locally authenticated by the 5G-RG using pre-shared secret.

Differentiated Services (QoS, Network Slicing) may be provided for NAUN3 Devices as defined.

NAUN3 Devices may be associated with "Connectivity Group IDs" where each Connectivity Group ID corresponds to a separate Physical or Virtual Port on the 5G-RG.

These ports could, e.g. refer to separate Physical Ethernet Ports and/or to Separate WLAN SSIDs &/or to a separate VLAN.

The devices that connect to a certain logical port are considered part of the same Connectivity Group ID.

Each Connectivity Group ID is then mapped to a separate PDU Session that is established by the 5G-RG based on the procedures defined. The overall Architecture is illustrated in the Figure.

The 5G-RG is configured with the (Virtual) Port Information (e.g. VLANs & SSIDs). The URSP rules can be provided to the RG to indicate how to map Connectivity Group ID to the Parameters of the PDU Session used to carry the traffic of corresponding Devices e.g. DNN, S-NSSAI, etc.

NOTE: *In addition, the mapping between a "virtual port" and DNN/S-NSSAI can be configured.*

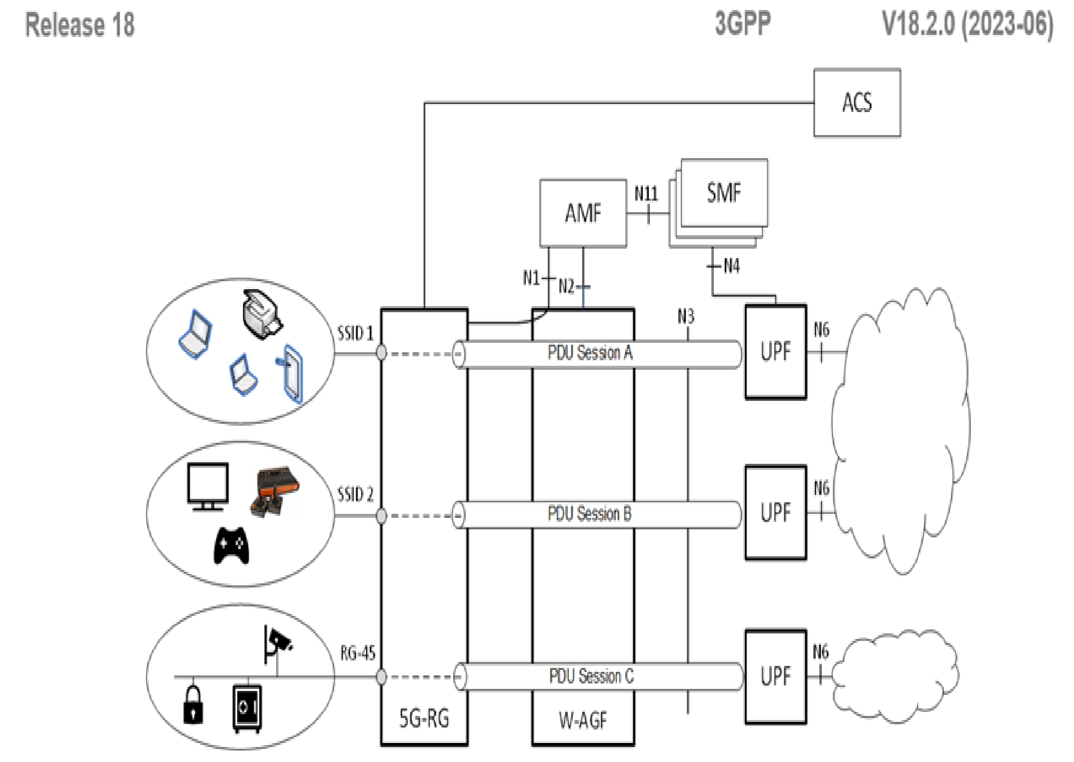


Figure: 5G System Architecture example for NAUN3 devices behind 5G-RG based on Connectivity Groups

1. 5G System Architecture enhancements on Wireless and Wireline Convergence Access support

Authenticable Non-3GPP **(AUN3)** ***Devices*** **behind 5G-RG**

- Each AUN3 Device has its own 5G CN Subscription Data including its own SUPI & Policy Control Subscription Data.

- In order to serve the AUN3 Device in 5GC, a 5G-RG issues a NAS register & handles RM & CM related Signalling on behalf of an AUN3 Device that it is requesting to be served and relays EAP signalling between the AUN3 Device & the 5GC.

- A 5G-RG serving an AUN3 Device establishes a single PDU Session on behalf on this AUN3 Device.

- A 5G-RG shall be connected to the 5GC (be in RM-REGISTERED & CM-CONNECTED mode) over Wireline Access to serve an AUN3 Device: the 5G-RG shall not issue a NAS register or Service request on behalf of an AUN3 Device if it is itself not registered & connected to the 5GC.

- The 5G-RG is configured with URSP for each AUN3 Devices it serves.

- The AUN3 devices and the 5G-RG belong to the same PLMN.

- There shall be a separate N2 connection per AUN3 Device that is in state CM-CONNECTED.

- The W-CP & W-UP Protocols shall be able to manage Multiple Separate Registrations & PDU Sessions for different SUPIs between the same pair of 5G-RG & W-AGF. In particular, W-CP needs to be able to differentiate NAS messages related to a 5G-RG & to each different AUN3 Device served by this 5G-RG & W-UP needs to distinguish between UP Packets for a 5G-RG & each different AUN3 Device served by this 5G-RG.

- When the registration of an AUN3 Device has successfully completed, the 5G-RG establishes a PDU Session on behalf of the AUN3 Device. This PDU Session is handled by 5GC as part of the AUN3 Subscription & is associated with the SUPI of AUN3 Device. An AUN3 Device can at a given time only use a single PDU Session. The parameters to establish this PDU session are based on the URSP (if any) for the AUN3 device.

- Different QoS Parameters may apply to PDU sessions of different AUN3 Devices.

- Roaming is not applicable to Subscriptions for AUN3 Devices.

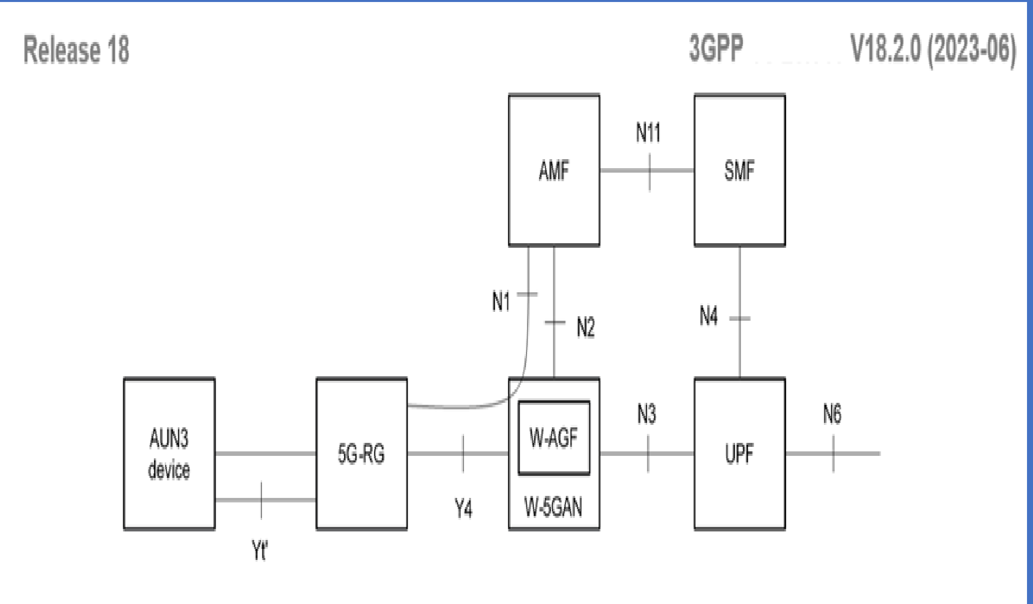


Figure: 5G System Architecture AUN3 Device behind 5G-RG

Non-3GPP Device behind 5G-RG based on 5G System Exposure

The Solution consists of three (3) parts that are used to provide a working End-to-End (E2E) Solution:

1. Example for how non-3GPP device information can be created in an AF.

2. Enhancements to the NEF Exposure Services to provide the non-3GPP Device
   information to 5GC.

3. Description for How the Traffic from Non-3GPP Devices can be identified in the 5GC to
   provide differentiated Charging & QoS.

The overall 5GS Architecture is shown in the Figure. Only the relevant NFs are shown.

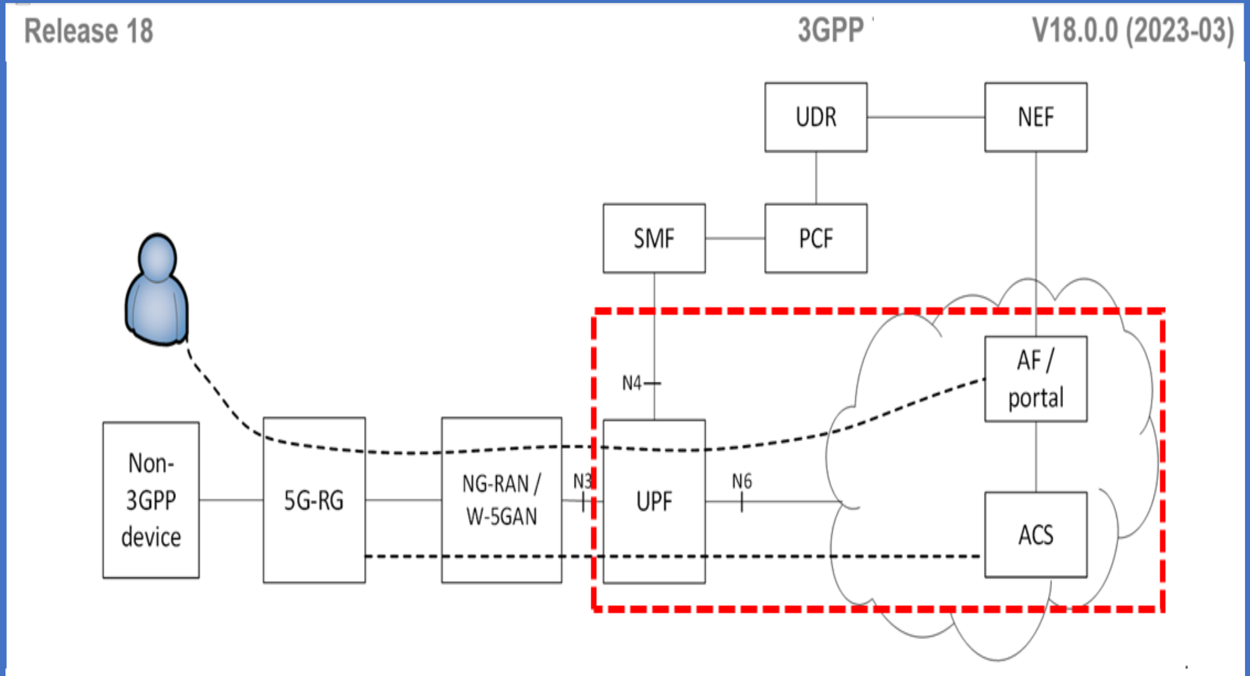


Figure: 5G System Architecture for Non-3GPP Device behind 5G-RG based on 5GS exposure

1. 5G System Architecture enhancements on Wireless and Wireline Convergence Access support

Non-3GPP Device behind 5G-RG based on 5G System Exposure

Providing Non-3GPP Device information to AF

In this solution, the AF is assumed to have access to Information about the Non-3GPP Devices that are or have been connected behind the RG.

Based on existing BBF specifications, the Auto-Configuration Server (ACS) can retrieve Information about the Non-3GPP Devices from the 5G-RG.

This Information can e.g. contain the Host Table from the DHCP Server in the RG, or Device List gathered by other means, & typically includes for each Device such as:

- Host Name,
- MAC Address of the Device
- IP Address allocated to the Device.

Release 18 3GPP V18.0.0 (2023-03)

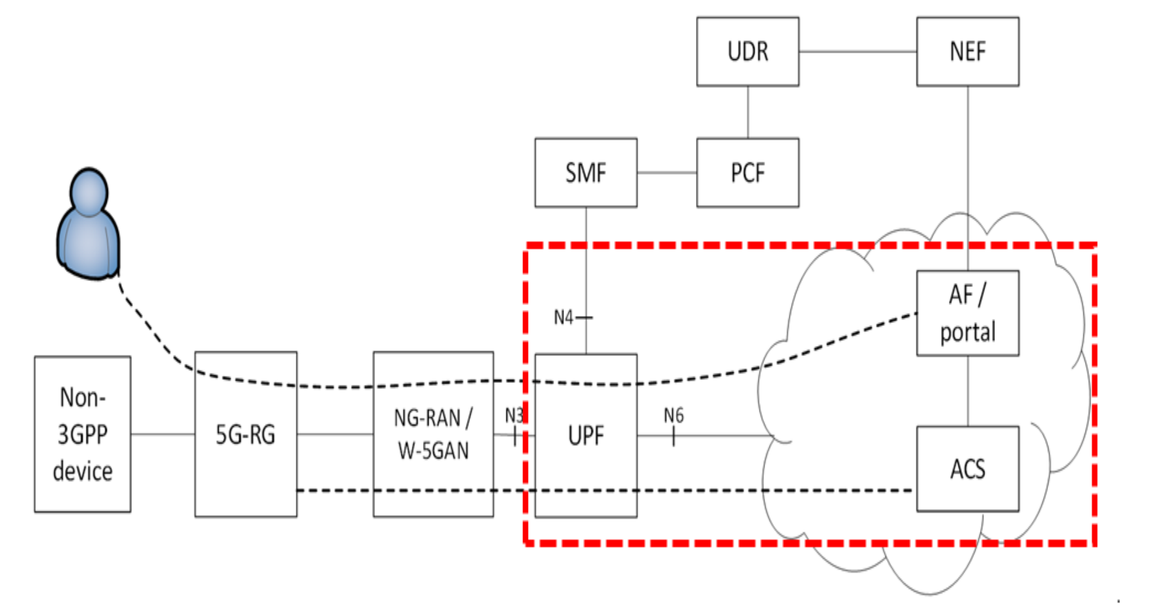


Figure: 5G System Architecture for Non-3GPP Device behind 5G-RG based on 5GS exposure

An example of IPv6 LAN Devices Host Table is shown in the Figure.

Release 18 3GPP V18.0.0 (2023-03)

```
IPv6 LAN Devices List
---------------------------------------------------------------------
Hostname                          MAC Address       IPv6 Address
E-5CG1475XFN                      f4:7b:09:b0:35:c9 2001:b030:2309:0:68d5:35ca:7691:9bb9
Galaxy-S21-5G                     46:15:0f:b6:85:b7 2001:b030:2309:0:4846:9efb:90e5:2466
LAPTOP-8PP10Q5G                   00:f4:8d:d6:34:a7 2001:b030:2309:0:f8f1:e3c5:72e9:233d
Apple-TV                          04:4b:ed:a8:9a:b1 2001:b030:2309:0:ec69:b99d:3260:87f3
Galaxy-Tab-S2                     c0:d3:c0:b9:4d:73 2001:b030:2309:0:b8e2:cc2f:dde2:d0f3
Stefan--iPhone                    c6:71:15:15:97:71 2001:b030:2309:0:987:7bf7:9993:dd97
```

Figure: Example of IPv6 LAN Devices Host Table from 5G-RG

In the case of IPv4 traffic, the routed RG typically has NAT functionality. The IPv4 addresses in the list of Non-3GPP Devices received from the RG would thus correspond to the Private IPv4 addresses.

1. 5G System Architecture enhancements on Wireless and Wireline Convergence Access support

Non-3GPP Device behind 5G-RG based on 5G System Exposure

Providing Non-3GPP Device information to AF

The existing 5G CN NEF Service Parameter Service is enhanced with a new Service Description to allow an AF to provide the Non-3GPP Device information to 5GC.

This information will be used by 5GC to detect the Traffic to/from a Non-3GPP Device & also to provide Differentiated QoS &/or Charging.

The information provided by the AF via the Nef_ServiceParameter Service contains:
- GPSI of the RG.
- List of Non-3GPP Devices, containing for each device:
- IPv6 Address or IPv4 & the Port number of the Device.
- Device Profile ID.

The 5G CN NEF maps the RG's GPSI to the RG's SUPI & stores the Non-3GPP Device information in 5G CN as Application Data, as currently defined for Nnef_ServiceParameter Service in 5GS Architecure Procedures.

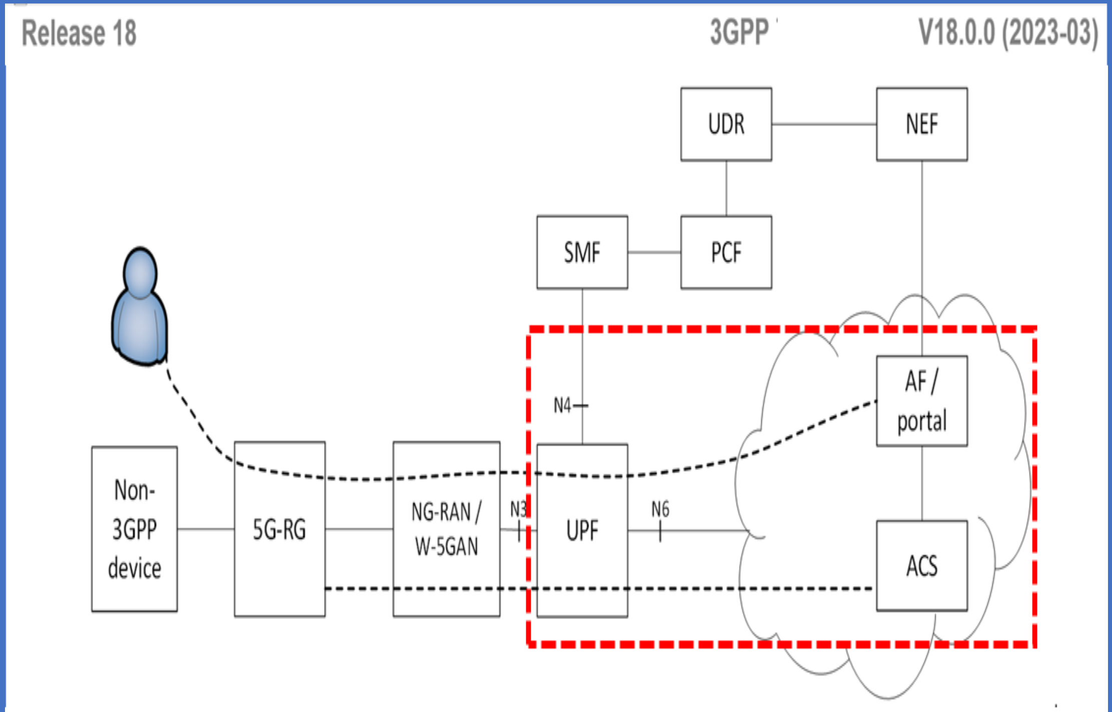


Figure: 5G System Architecture for Non-3GPP Device behind 5G-RG based on 5GS exposure

Non-3GPP Device behind 5G-RG based on 5G System Exposure

Providing Non-3GPP Device information to AF

Differentiated Services per Non-3GPP Device

When a PDU Session for an RG is established, the PCF contacts the UDR to subscribe to Application Data that may be available, as per existing procedure for Service specific Parameter Provisioning.

The PCF thus receives the Non-3GPP Device Information from UDR corresponding to the RG's SUPI.

The PCF takes the Service Parameters as well as other information (e.g. RG's Subscribed QoS & RG's Policy Subscription Data in UDR) into account for Policy decisions, e.g. to determine QoS & Charging Parameters for the Non-3GPP Device's Traffic.

The PCF may provide PCC rules to SMF that are specific for individual Non-3GPP Devices, containing SDF Filter with the IPv6 address or IPv4 and the Port number of the Device, and corresponding QoS & Charging related parameters.

The PCF may provide different PCC rules for different Services, as per existing Standards.

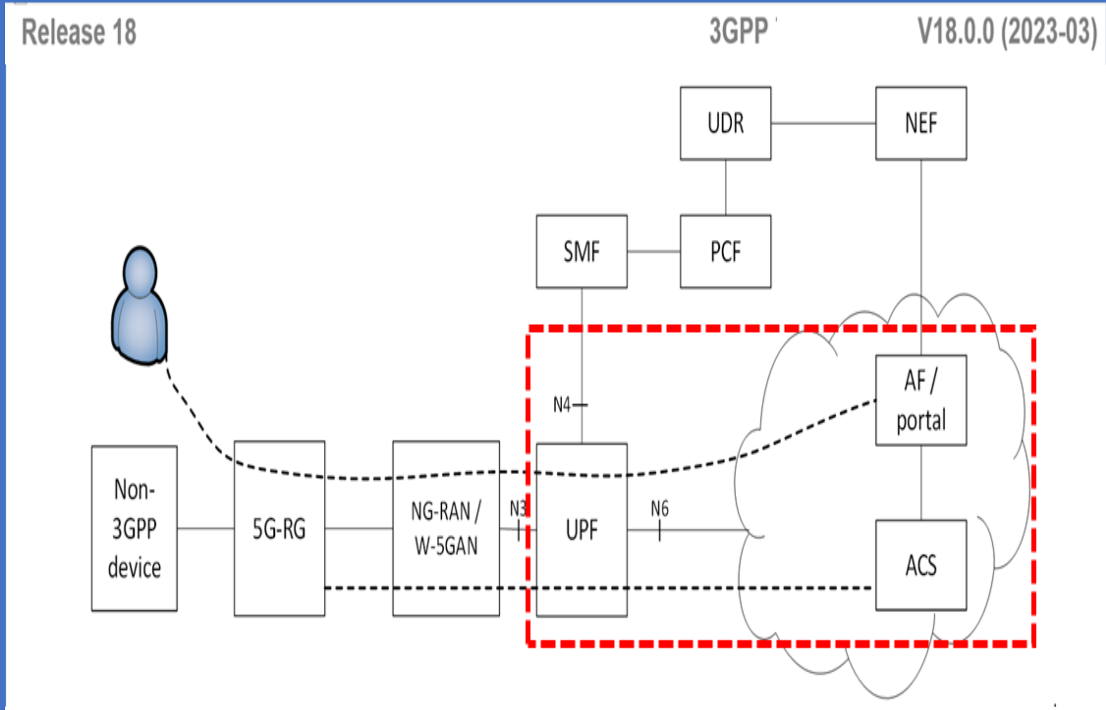


Figure: 5G System Architecture for Non-3GPP Device behind 5G-RG based on 5GS exposure

Control Plane (CP) Protocol Stacks for W-5GAN (Wireline 5G Access Network)

Control Plane Protocol Stacks between the 5G-RG and the 5GC AMF is shown in the Figure.

For W-5GBAN, the W-CP Protocol stack between 5G-BRG & W-AGF is defined by BBF.

For W-5GCAN, the W-CP protocol stack between 5G-CRG and W-AGF is defined in WR-TR-5WWC-ARCH.

The Protocol Stack between 5GC/AMF & W-AGF is defined in the 5GS Architecture.

The W-CP Protocol Stack:
- supports transfer of NAS signalling between the 5G-RG & the W-AGF;
- supports to carry AS Parameters (e.g. SUCI or 5G-GUTI, Requested NSSAI & Establishment Cause) and NAS packets;
- supports the setup, modification and removal of at least one W-UP Resource per PDU session;
- may support the Setup, Modification & Removal of Multiple W-UP Resources per PDU session.

For the 5G-RG connected via NG-RAN the Protocol Stack defined in the 5GS Architecture applies with UE corresponding to 5G-RG.

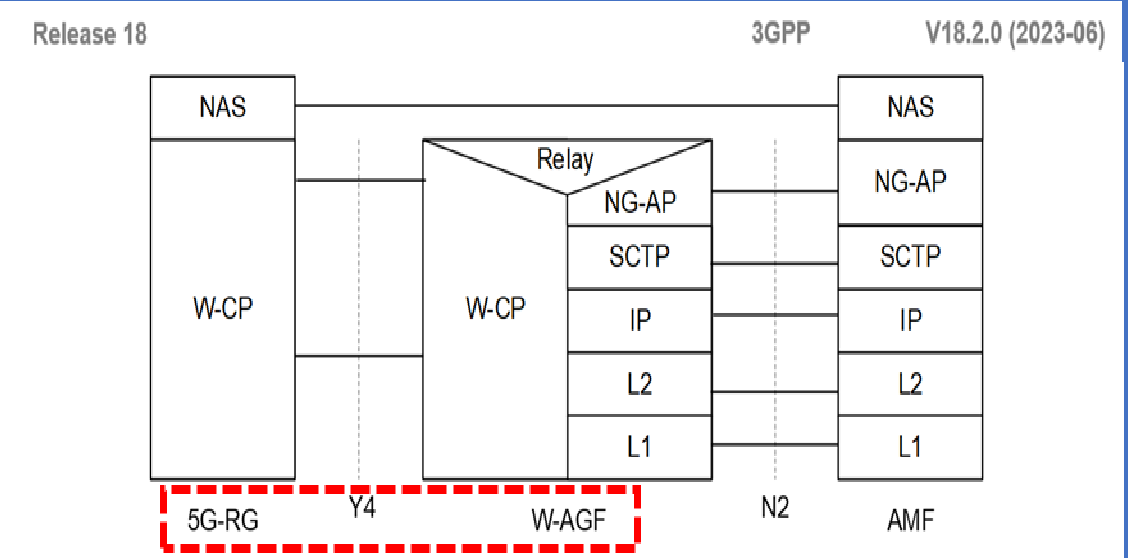


Figure: 5G System Architecture Control Plane (CP) stack for W-5GAN for 5G-RG

Control Plane (CP) Protocol Stacks between the FN-RG and the 5GC

The CP Protocol Stack between FN-RG & AMF is shown in the Figure.

The W-AGF acts as an N1 termination point on behalf of FN-RG.
For W-5GBAN, the L-W-CP Protocol Stack, between FN-BRG & W-AGF is defined by BBF.

For W-5GCAN, the L-W-CP Protocol Stack between FN-CRG & W-AGF is defined in WR-TR-5WWC-ARCH.

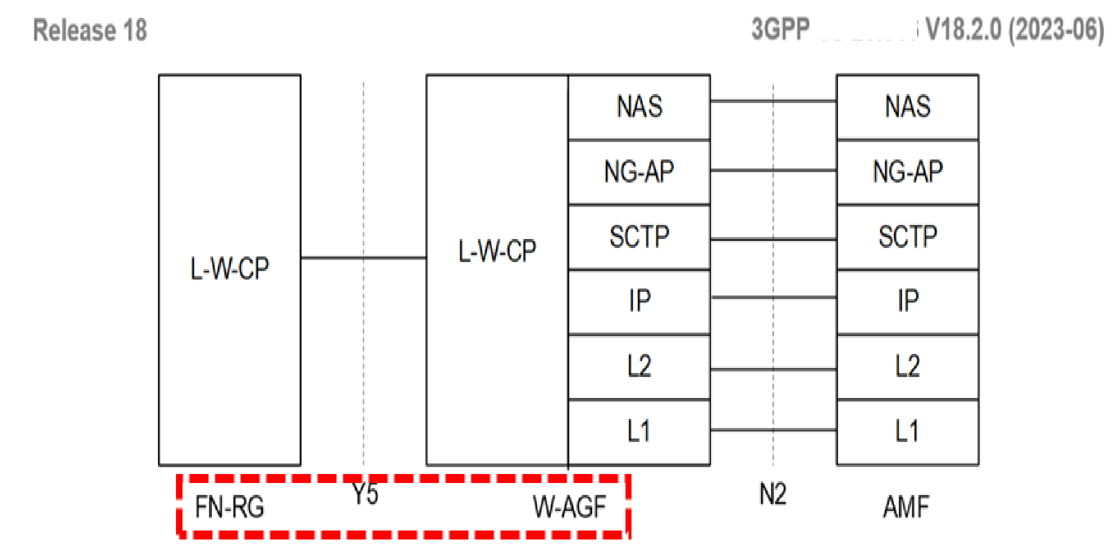


Figure: 5G System Architecture Control Plane (CP) stack for W-5GAN for FN-RG

User Plane Protocol Stacks for W-5GAN (Wireline 5G Access Network)

User Plane (UP) Protocol Stacks between the 5G-RG and the 5GC UPF is shown in the Figure.

For W-5GBAN, the W-UP protocol stack between 5G-BRG and W-AGF is defined by BBF.

For **W-5GCAN** (*Wireline 5G Cable Access Network*), the W-UP Protocol Stack between 5G-CRG & W-AGF is defined in WR-TR-5WWC-ARCH.

The Protocol Stack between 5GC/UPF & W-AGF is defined in the 5GS Architecture.

For the W-UP Protocol Stack:

- W-UP supports at least one (1) W-UP Resource per PDU session. This will be the default W-UP resource.
- W-UP may support multiple W-UP resources per PDU session and associate different QoS profiles (QFIs) to different W-UP resources.
- W-UP supports transmission of Uplink (UL) & Downlink (DL) PDUs.
- W-UP supports Access specific QoS Parameters that can be mapped from 3GPP QoS Parameters (e.g.5QI, RQI) received from the 5GC.

For the 5G-RG connected via NG-RAN the protocol stack defined in the 5GS Architecture applies with 5G-RG replacing the UE.

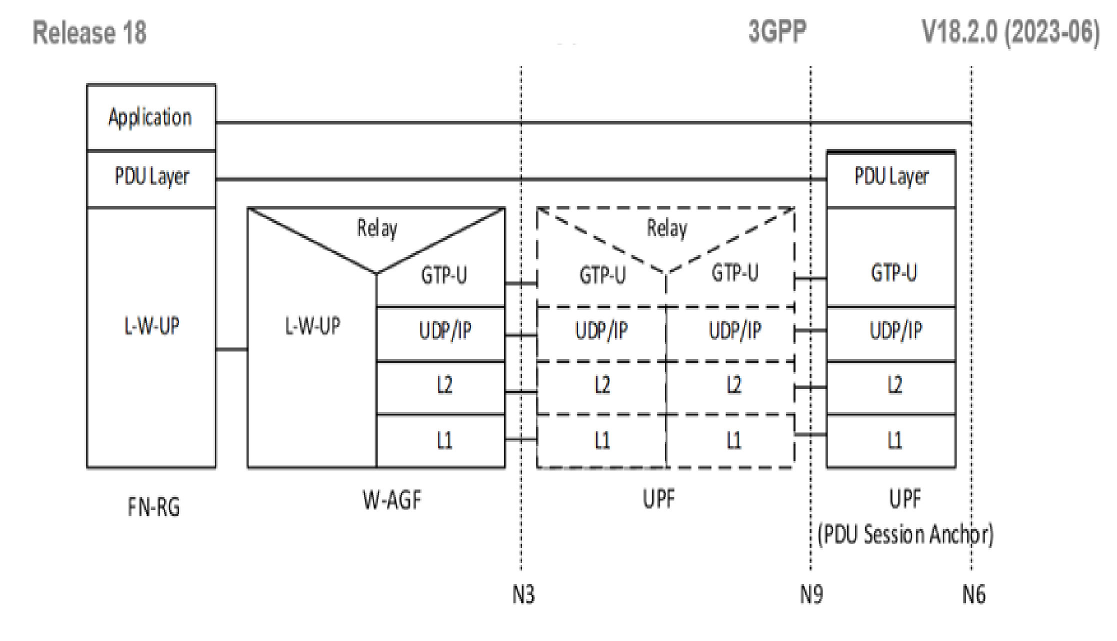


Figure: 5G System Architecture User Plane (UP) stack for W-5GAN for FN-RG

Annex 1- 5G PINs (Personal IoT Networks): Definition

Personal IoT Network: A configured and managed group of PIN Element that are able to communicate each other directly or via PIN Elements with Gateway Capability (PEGC), communicate with 5G network via at least one PEGC, and managed by at least one PIN Element with Management Capability (PEMC).

PIN Element (PINE): A UE or Non-3GPP device that can communicate within a PIN (via PIN "direct" connection, via PEGC, or via PEGC and 5GC), or outside the PIN via a PEGC and 5GC.

PIN Element with Gateway Capability: A PIN Element with the ability to provide connectivity to & from the 5G Network for other PIN Elements, or to provide "relay" for the communication between PIN Elements.

PIN Element with Management Capability: A PIN Element with capability to manage the PIN.

NOTE: A PIN Element can have both PIN Management Capability and Gateway Capability

PINE-to-PINE communication: communication between two PINEs which may use PINE-to-PINE direct communication or PINE-to-PINE indirect connection.

PINE-to-PINE direct connection: the connection between two PIN Elements without PEGC, any 3GPP RAN or core network entity in the middle.

PINE-to-PINE indirect connection: the connection between two PIN Elements via PEGC or via UPF.

PINE-to-PINE routing: the traffic is routed by a PEGC between two PINEs, the two PINEs direct connect with the PEGC via non-3GPP access.

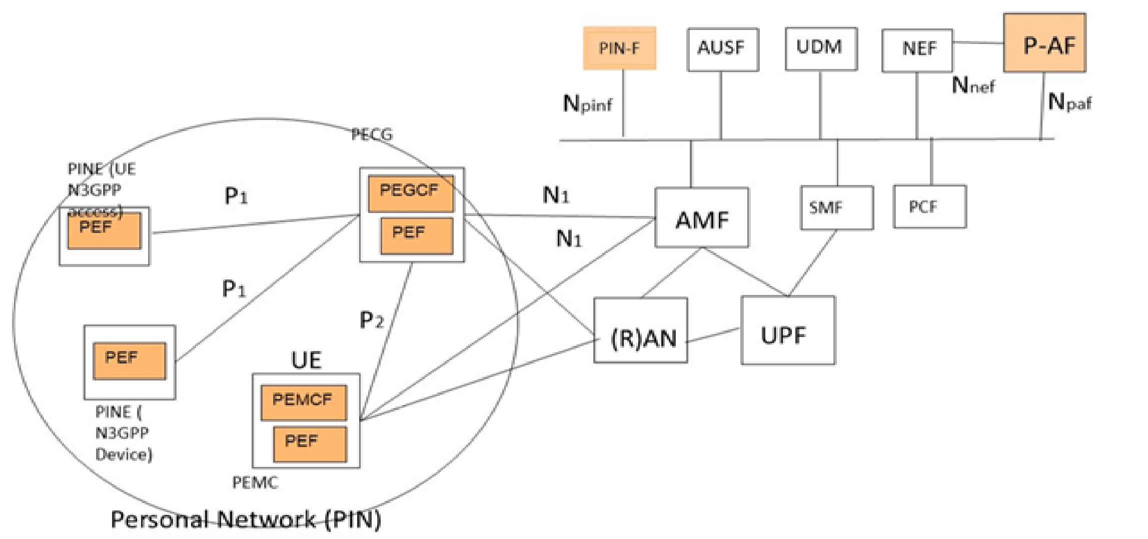
PINE-to-Network routing: the traffic is routed by a PEGC between PINE and 5GS, the PINE direct connects with the PEGC via non-3GPP access separately.

Network local switch for PIN: the traffic is routed by UPF(s) between two PINEs, the two PINEs direct connect with two PEGCs via non-3GPP access separately.

Abbreviations

PIN	Personal IoT Networks
PINE	PIN Element
PEGC	PIN Elements with Gateway Capability
PEMC	PIN Elements with Management Capability
P2P	PINE-to-PINE
P2N	PINE-to-Network
NLSP	Network Local Switch for PIN

Note 1: The AF relies on PIN signaling between the PINE/PEGC/PEMC and the PIN AF, which is transferred via UP transparently to the 5G System, to determine the need for a QoS modification.



5G System PIN Solution Reference Architecture

Annex 1- 5G System (5GS) enhancements to support **Personal IoT Networks (PINs).**

- Management of PIN,
- Access of PIN via PIN Element (PINE) with Gateway Capability (PEGC), and
- Communication of PIN (e.g. PINE (e.g. a UE) communicates with
  - other PINE (UE) "directly" or
  - via PEGC or
  - via PEGC and 5GS.

- Security related when identifying PIN and the PINE when:
  - How to identify PIN and the PINEs in the PIN at 5GC level to serve for Authentication& Authorization
  - Management as well as Policy and Routing Control enforcement:

- Management of a PIN.
- PIN & PINE Discovery

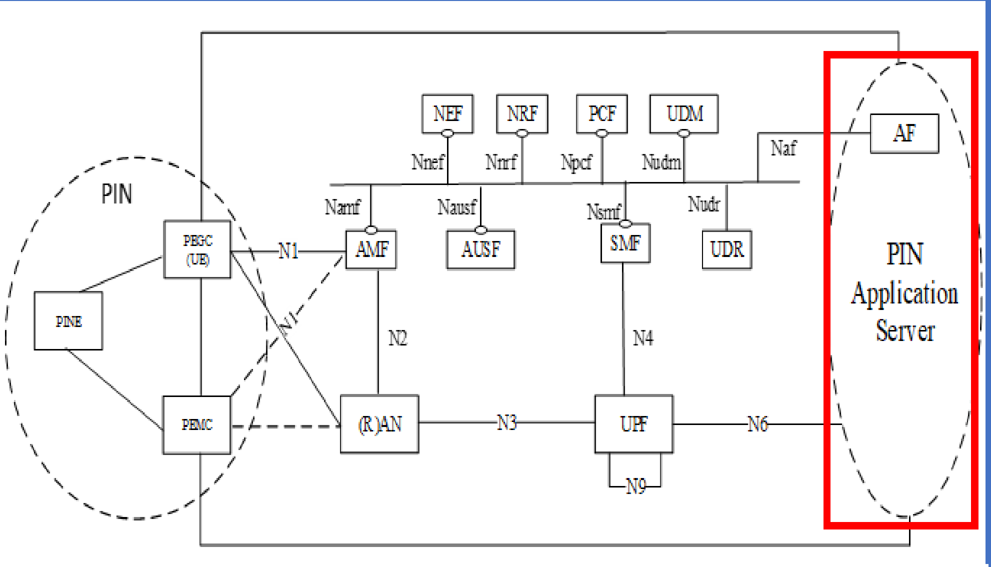


Figure: 5GS PIN Personal IoT Network Reference Architecture

A **Personal IoT Network (PIN**) in **5GC** consists of:

- 1 (one) or more Devices providing Gateway/Routing Functionality known as **the PIN Element with Gateway Capability (PEGC**), and

- 1 (one) or more Devices providing PIN Management Functionality known as the **PIN Element with Management Capability (PEMC**) to manage the Personal IoT Network; and

- Device(s) called the PIN Elements (PINE). A PINE can be a non-3GPP Device.

The PIN can also have a PIN Application Server (AS) that includes an AF (Application Function) functionality.

The AF can be deployed by Mobile Operator or by an Authorized Third (3rd) Party.

When the AF is deployed by 3rd Party, the interworking with 5GS is performed via the NEF.

The PEMC and PEGC communicates with the PIN Application Server (AS) at the Application Layer over the User Plane. The PEGC and PEMC can communicate with each other via "Direct" Communication

Only a 3GPP UE can act as PEGC and/or PEMC.

Annex 1: 5G PINs (Personal IoT Networks) and 5G CPNs (Customer Premises Networks)

Personal IoT Networks (PINs) and Customer Premises Networks (CPNs) provide local connectivity between UEs and/or Non-3GPP Devices.

The CPN via an eRG, or in 5G PINs with PIN Elements (PINEs) via a PIN Element with Gateway Capability (PEGC) can provide access to 5G Network Services for the UEs and/or Non-3GPP Devices on the CPN or PIN.

CPNs and PINs have in common that, in general, they are:
- owned, Installed and/or (at least partially) Configured by a Customer of a Public Network Operator.

A Customer Premises Network (CPN) is a Network located within
- a Premises (e.g. a Residence, Office or Shop).
- via an evolved Residential Gateway (eRG), the CPN provides connectivity to the 5G Network. The eRG can be connected to the 5G Core Network via wireline, wireless, or hybrid access.
- A *Premises Radio Access Station* (**PRAS**) is a Base Station installed in a CPN. Through the PRAS, UEs can get Access to the CPN and/or 5G Network Services.

The **PRAS** can be configured to use
- Licensed,
- Unlicensed, or
- Both Frequency bands.

Connectivity between the **eRG** and the **UE**, **non-3GPP Device**, or **PRAS** can use any suitable **Non-3GPP Technology** (e.g. **Ethernet, optical, WLAN).**

A Personal IoT Network (PIN) consists of **PIN Elements (PINEs)** that communicate using PIN
- "Direct Connection" or
- "Direct Network Connection

and is managed locally using a PIN Element (PINE) with Management Capability (PEMC).

Examples of PINs include Networks of Wearables and Smart Home / Smart Office Equipment.

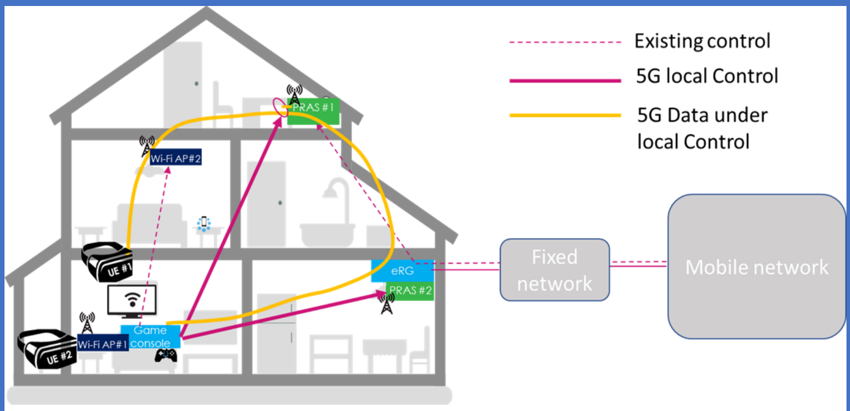


Figure: 5G Local Control of Premise Radio Access Stations (PRASs) for UE to access CPN Device

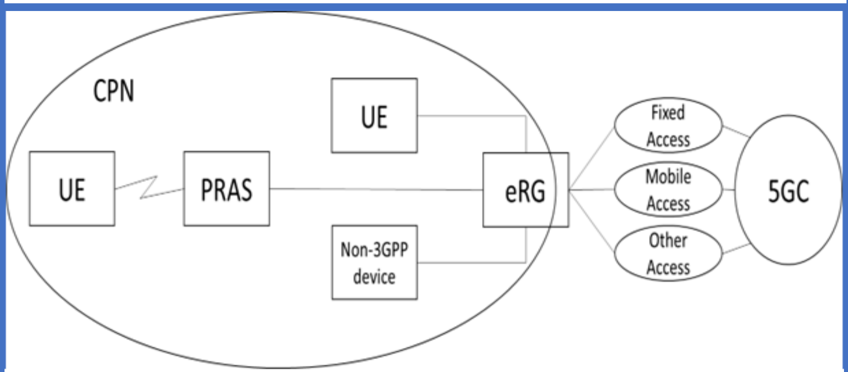


Figure: Customer Premises Network (CPN) connected to 5GC

Vodafone unveils Open RAN 5G network-in-a-box

Feb 17, 2023

Vodafone's Yago Tenorio shows off the operator's 5G network-in-a-box.

- Vodafone has unveiled a new mini 5G network the size of a Wi-Fi router
- It has a core and radio software, a mini computer and a software-defined radio chipset
- It is just a prototype currently
- But if offered as a product could revolutionise the 5G private network sector

Annex 2: 3GPP 5G Advanced Release specification for NPNs/SNPNs (Non-Public Network(s)/Stand-alone NPNs)

3GPP decision in 2018 to "delete" the term "Private Network" in the 5G Service Requirements specification & replace it with the term "Non-Public Network" (NPN) to avoid confusion

3GPP TSG-SA WG1 Meeting #84 **S1-183121**
Spokane, WA, USA, 12 - 16 November 2018 *(revision of S1-18xxxx)*

CR-Form-v11.2

CHANGE REQUEST

	CR	**0315**	**rev**	**-**	**Current version:**	**16.5.0**

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

Proposed change affects: UICC apps [ ] ME [X] Radio Access Network [X] Core Network [X]

Title:	Replacing private network with non-public network
Source to WG:	ETRI
Source to TSG:	S1
Work item code:	cyberCAV
Date:	2018-11-01
Category:	F
Release:	Rel-16

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-12 (Release 12)
Rel-13 (Release 13)
Rel-14 (Release 14)
Rel-15 (Release 15)
Rel-16 (Release 16)

Reason for change:	In the last SA1 #83 meeting, the definition and requirements of non-public network were agreed and added. As the result, we now have two terminologies, non-public network and private network, for the network that is intended for the sole use of a private entity such as an enterprise.
Summary of change:	To integrate two terms to one term, non-public network. - Delete the term "private network" from 3.1 Definitions - Replace private network with non-public network in the context.
Consequences if not approved:	Duplicated terms, non-public network and private network could make a confusion.

3GPP TSG-SA1 Meeting #97-e ***S1-220219***
Online, , 14th Feb 2022 - 24th Feb 2022

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

Annex 2: 3GPP 5G Advanced Release specification for NPNs/SNPNs (Non-Public Network(s)/Stand-alone NPNs)

5G NPNs/SNPNs 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

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

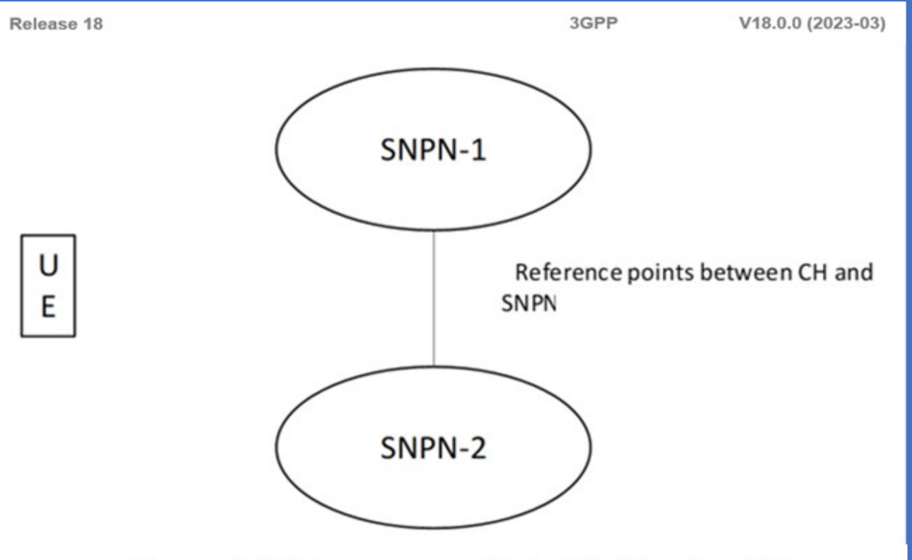


Figure: 5G UE accesses multiple SNPNs using CH

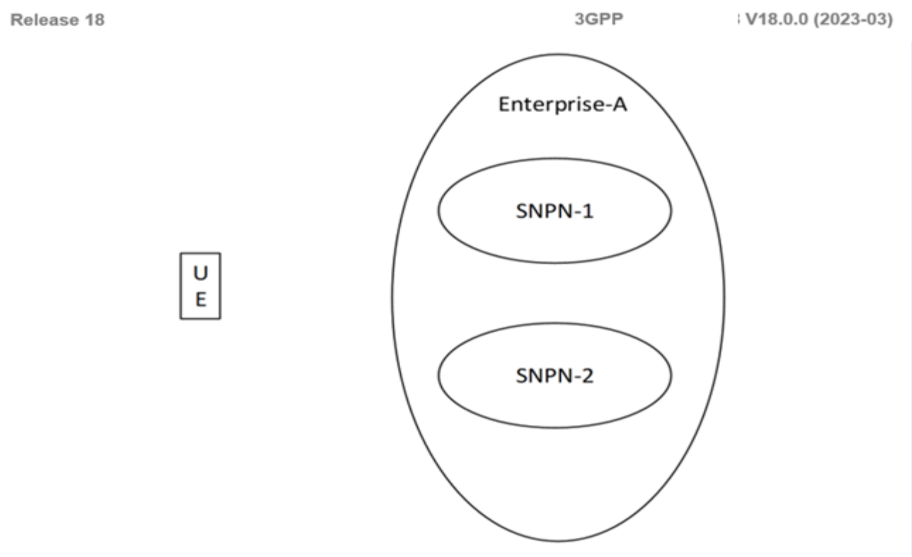


Figure: 5G UE accesses multiple SNPNs belonging to the same Administrative Entity

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* (**NFs**) provided by a **PLMN**,

   or

2. a *Public Network Integrated NPN* (**PNI-NPN**), i.e. a *Non-Public Network* (***NPN***) 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 & Trusted Non-3GPP Access *(Figures on the slide) for access to SNPN Services via a PLMN*

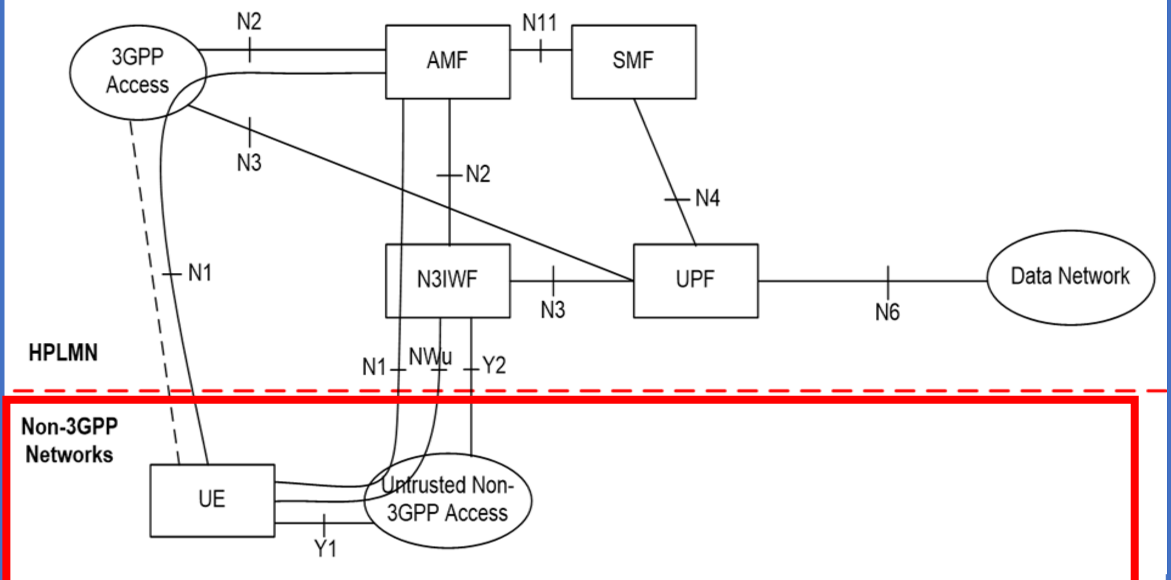


Fig. Non-Roaming Architecture for 5G Core Network with Untrusted Non-3GPP Access

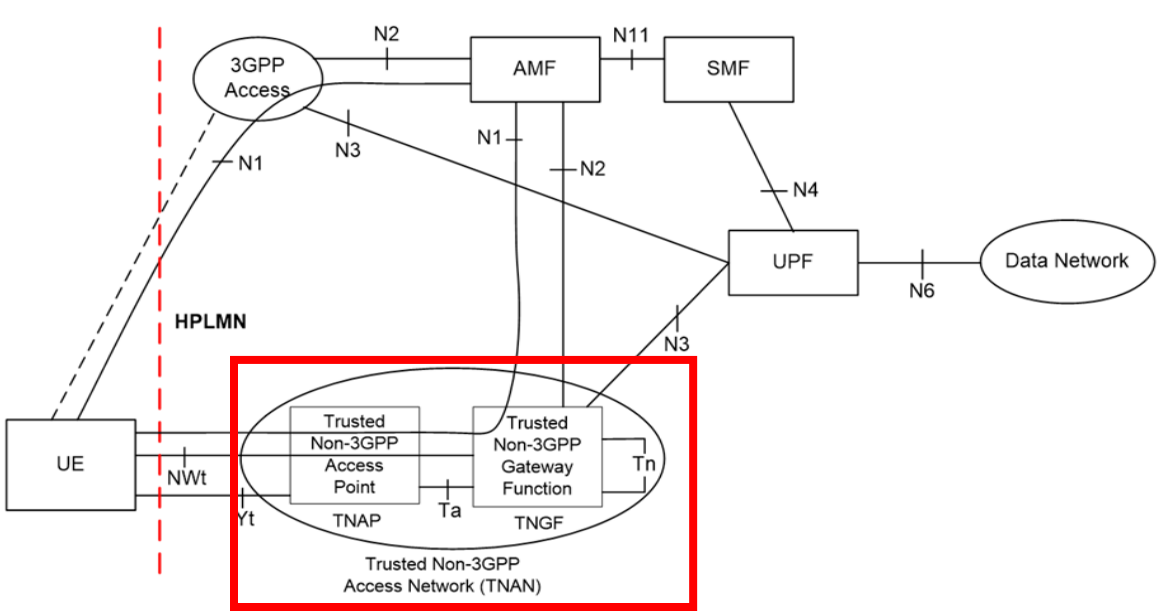


Fig. Non-Roaming Architecture for 5G Core Network with Trusted Non-3GPP Access

PLMN and NPN/SNPN Network Configurations Definitions:

***"Overlay Network"*:**

When UE is accessing SNPN Service via "Nwu" using User Plane (UP) established in PLMN,
SNPN is the "Overlay Network".

When UE is accessing PLMN Services via "Nwu" using User Plane (UP) established in SNPN,
PLMN is the "Overlay Network".

Release 18 3GPP V18.2.2 (2023-07)

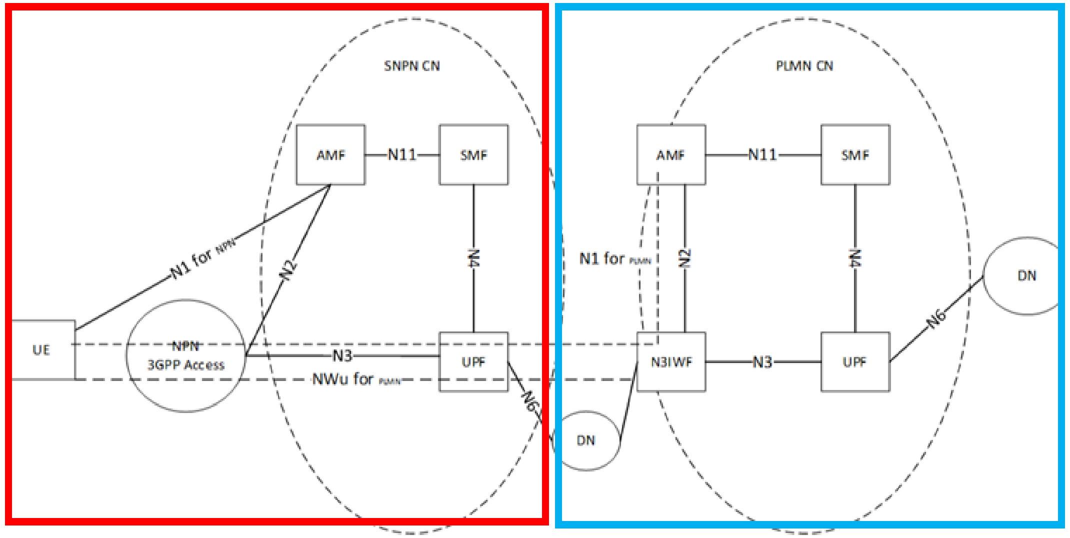


Figure: 5G System Access to PLMN Services via Stand-alone Non-Public Network (SNPN)

"Underlay Network":

When UE is accessing SNPN Service via NWu using User Plane established in PLMN,
PLMN is the "Underlay Network".

When UE is accessing PLMN Services via NWu using User Plane (UP) established in SNPN,
SNPN is the "Underlay Network".

Release 18 3GPP V18.2.2 (2023-07)

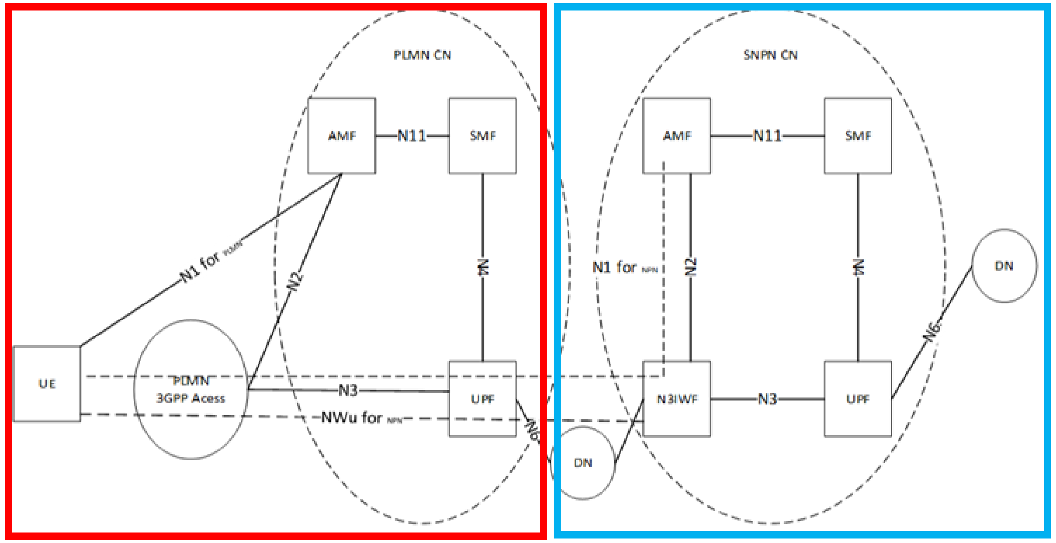


Figure: 5G System Access to Stand-alone Non-Public Network (SNPN) Services via PLMN

5G System Stand-alone Non-Public Networks specified configuration foreseen deployments are based on:

- the Architecture (s) depicted in the Figure(s) on this slide
- the Architecture for 5GC with Untrusted non-3GPP access (*previous slides*) for either access to SNPN services via a PLMN (& vice versa) or for direct access to SNPN via non-3GPP access;
- the Architecture for 5GC with Trusted Non-3GPP access (*previous slides*); and
- the additional functionality covered in this clause

Alternatively, a Credentials Holder (CH) may authenticate & authorize access to an SNPN separate from the Credentials Holder based on the Architecture specified.

- Idle & Connected mode Mobility is supported as defined
- It is hereby specified the common SNPN aspects applicable to both 3GPP & Non-3GPP Access, except where stated differently.
- Aspects specific to Untrusted Non-3GPP Access for SNPN are specified
- Aspects specific to Trusted Non-3GPP access for SNPN are specified
- Aspects specific to N5CW Devices accessing SNPN Services are specified

Release 18 3GPP V18.2.2 (2023-07)

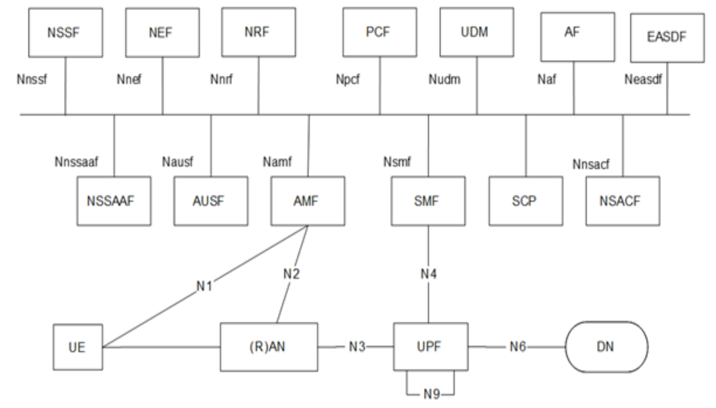


Figure : Non-Roaming 5G System Architecture

Release 18 3GPP V18.2.2 (2023-07)

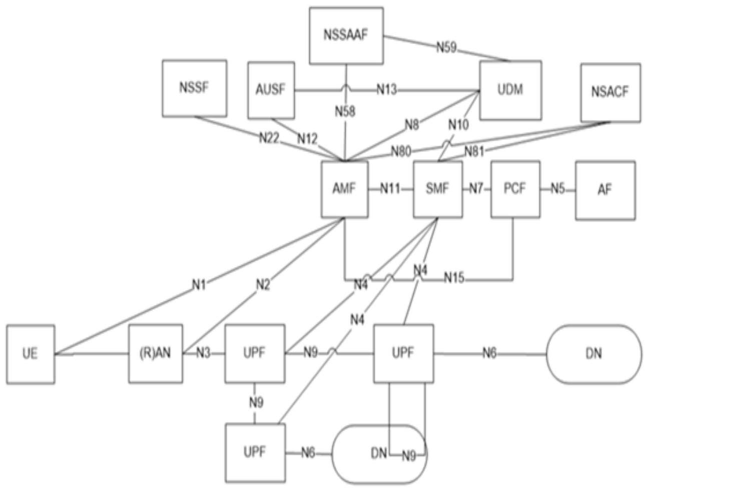


Figure: Applying Non-Roaming 5G System Architecture for concurrent Access to two (e.g. Local and Central) Data Networks (Single PDU Session option) in Reference Point Representation

Annex 2: 5G NPNs/SNPNs evolvement in 3GPP Rel-18 (5G Advanced) exemplifying the 100% shift in selected/specified KIs (Key Issues) & (KIs) Solutions

5G System Stand-alone Non-Public Networks specified configuration foreseen deployments are based on the following 5GS Features and Functionalities are not supported for SNPNs:

- Interworking with EPS.
- Also, Emergency Services when the UE accesses the SNPN over NWu via a PLMN.

- Roaming, e.g. Roaming between SNPNs. *However, it is possible for a UE to access an SNPN with credentials from a CH as described and to move between "equivalent" SNPNs.*

- Handover between SNPN and PLMN or PNI NPN.
- CIoT 5GS optimizations.
- CAG.
- Proximity based Services (ProSe) as defined by 3GPP for 5G
- 5G NSWO (*Non-Seamless WLAN Offload*).

- 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 as described in 5GS Architecture.

- 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.

NPNs/SNNs Identifiers

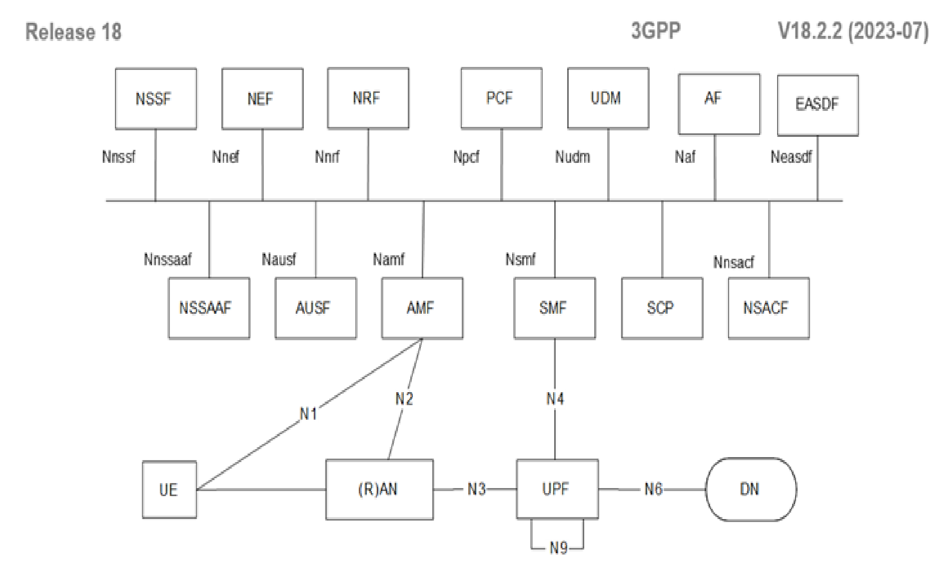


Figure : Non-Roaming 5G System Architecture

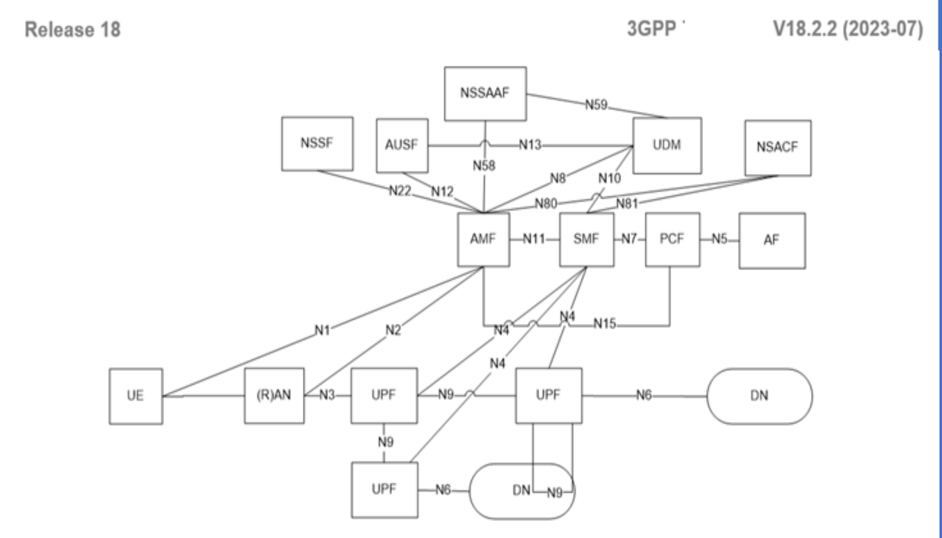


Figure: Applying Non-Roaming 5G System Architecture for concurrent Access to two (e.g. Local and Central) Data Networks (Single PDU Session option) in Reference Point Representation

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.

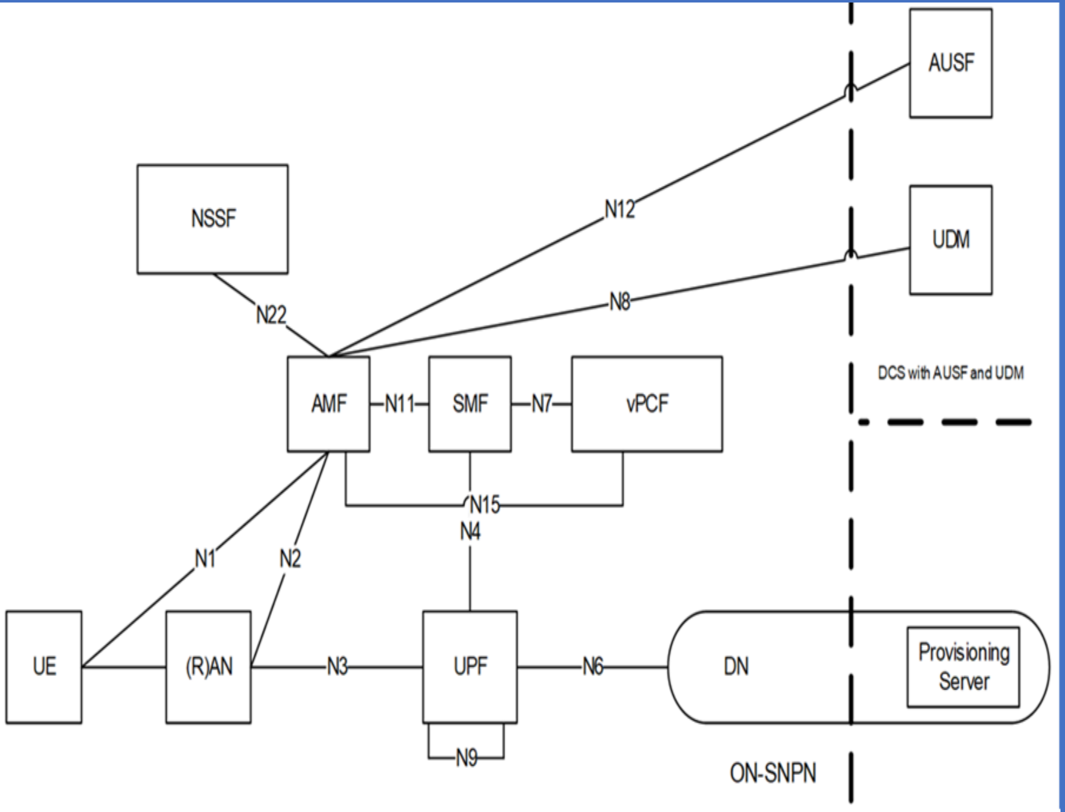


Fig.: Architecture for UE Onboarding in ON-SNPN when DCS includes AUSF and a UDM

5G NPNs/SNPNs Identifiers - the combination of a PLMN ID & 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 (**NFs**) provided by the PLMN.*

The NID shall support two (2) assignment Models:

A) 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 co-ordinated assignment NIDs as defined by 3GPP.

B) Coordinated assignment: NIDs are assigned using one of the following two (2) 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.

NOTE: *The use of SNPN with Self-assignment Model NID such that the combination of PLMN ID and NID is not globally unique is not assumed for the Architecture described and for SNPN - SNPN Mobility as described*

The **GIN** *(Group ID for Network Selection)* shall support two (2) Assignment Models:
- Self-assignment: GINs are chosen individually and may therefore not be unique. It is defined by 3GPP.
- Coordinated assignment: GIN uses a combination of PLMN ID and NID and is assigned using one of the following two (2) options as defined:
1. The GIN is assigned such that the NID is Globally Unique (e.g. using IANA Private Enterprise Numbers) independent of the PLMN ID used; or
2. The GIN is assigned such that the combination of the NID and the PLMN ID is Globally Unique.
An optional Human-Readable Network Name helps to identify an SNPN during Manual SNPN Selection. The Human-Readable Network Name and how it is used for SNPN Manual Selection is specified in 5G Service Requirements

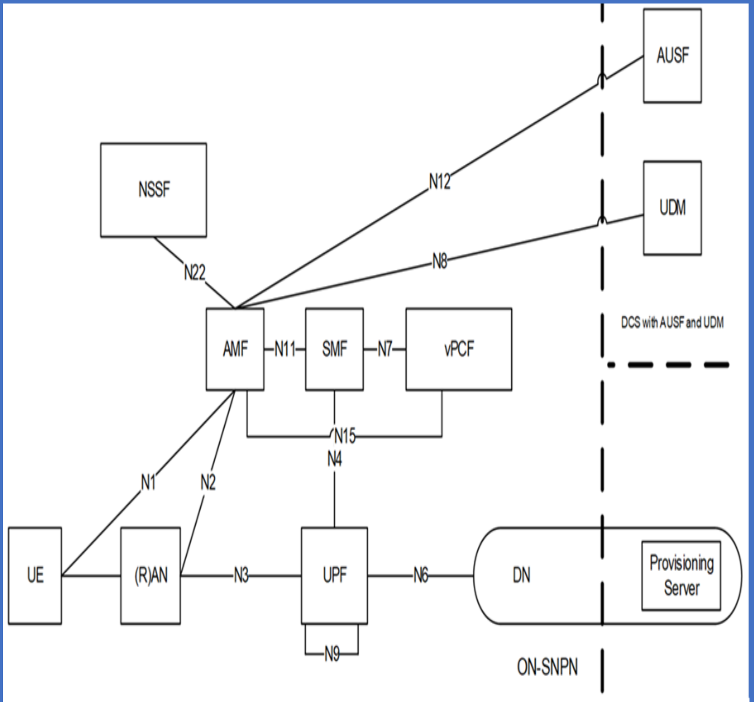


Fig.: Architecture for UE Onboarding in ON-SNPN when DCS includes AUSF and a UDM

5G NPNs/SNPNs UE Configuration and Subscription aspects - 1

An SNPN-enabled UE is configured with the following information for each Subscribed SNPN:
- PLMN ID and NID of the subscribed SNPN;
- Subscription identifier (SUPI) and Credentials for the subscribed SNPN;
- Optionally, an N3IWF FQDN and the MCC of the country where the configured N3IWF is located;
- Optionally, if the UE supports access to an SNPN using credentials from a Credentials Holder:
- User controlled prioritized list of preferred SNPNs;
- Credentials Holder controlled prioritized list of preferred SNPNs;
- Credentials Holder controlled prioritized list of GINs;
- Optionally, if the UE supports access to an SNPN using credentials from a Credentials Holder and access to an SNPN providing access for Localized Services:
- User controlled prioritized list of preferred SNPNs;
- Credentials Holder controlled prioritized list of preferred SNPNs for accessing Localized Services, each entry of the list includes:
- an SNPN identifier;
- validity information; and
- optionally, location assistance information;
- Credentials Holder controlled prioritized list of GINs for accessing Localized Services, each entry of the list includes:
- a GIN;
- validity information; and
- optionally, location assistance information;
- Protection scheme for concealing the SUPI as defined

NOTE 1: Additionally the UE can be configured with indication to use anonymous SUCI as defined

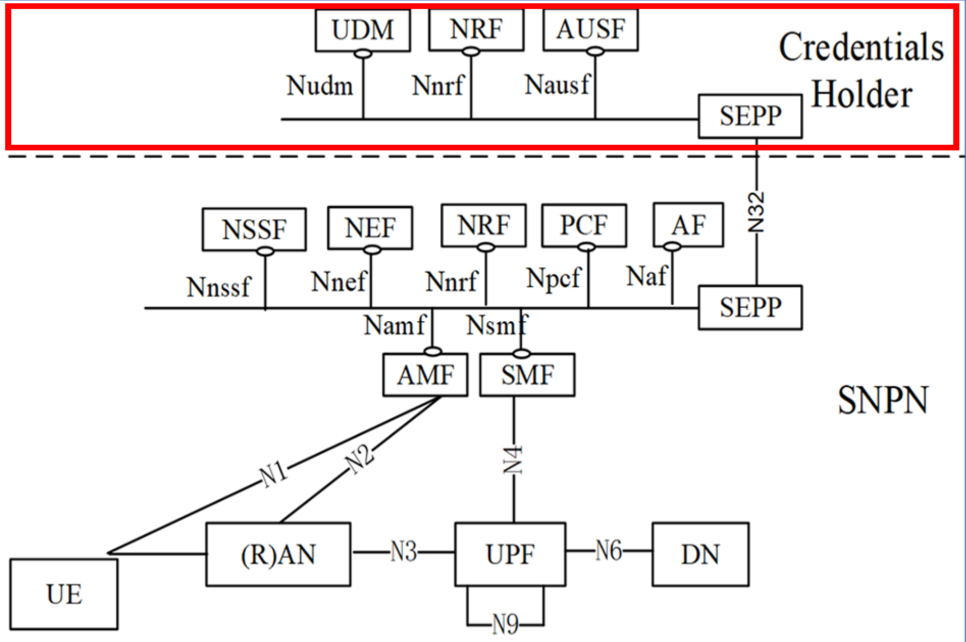


Fig. 5G System Architecture with Access to SNPN using credentials from Credentials Holder using AUSF and UDM

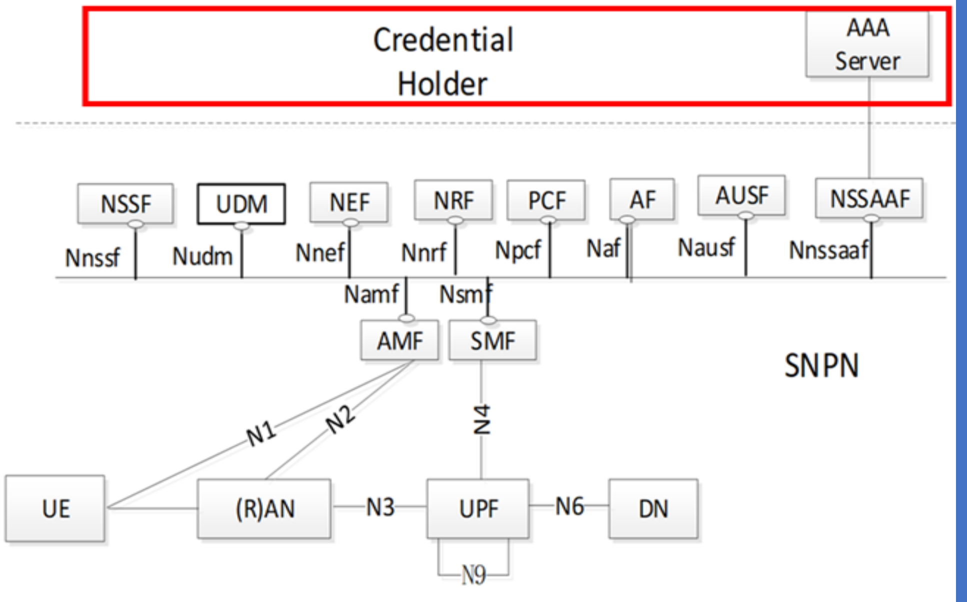


Fig. 5G System Architecture with Access to SNPN using credentials from Credentials Holder using AAA Server

5G NPNs/SNPNs UE Configuration and Subscription aspects - 2

Validity information consists of:

- Time validity information, i.e. time periods (defined by start & end times) when access to the SNPN for accessing Localized Services is allowed; and/or Location assistance information consisting of:

- Geolocation information, &/or,
- Tracking Area information of serving networks, i.e. lists of TACs per PLMN ID or per PLMN ID and NID.

For an SNPN-enabled UE with SNPN Subscription, the Credentials Holder controlled Prioritized Lists of Preferred SNPNs & GINs, or Credentials Holder controlled prioritized lists of preferred SNPNs and GINs for accessing Localized Services may be updated by the Credentials Holder using the Steering of Roaming (SoR) procedure as defined.

A Subscription of an SNPN is either:
- identified by a SUPI containing a Network-specific identifier that takes the form of a Network Access Identifier (NAI) using the NAI based User identification as defined. The realm part of the NAI may include the NID of the SNPN; or
- identified by a SUPI containing an IMSI.

An SNPN-enabled UE that supports Access to an SNPN using Credentials from a Credentials Holder and that is equipped with a PLMN Subscription may additionally be configured with the following information for SNPN selection and registration using the PLMN subscription in SNPN access mode:

- User controlled Prioritized List of Preferred SNPNs;
- Credentials Holder controlled Prioritized List of Preferred SNPNs;
- Credentials Holder controlled Prioritized List of Preferred GINs.

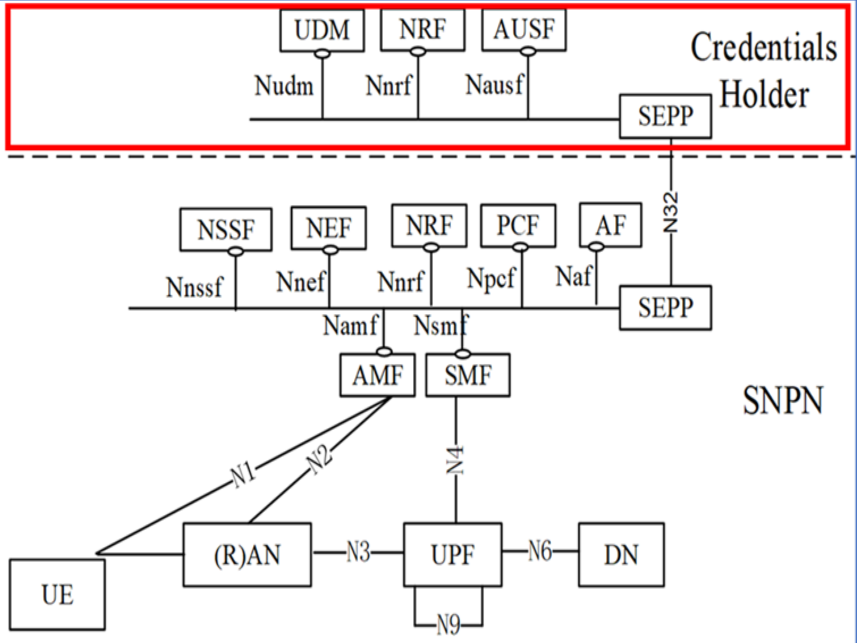


Fig. 5G System Architecture with Access to SNPN using credentials from Credentials Holder using AUSF and UDM

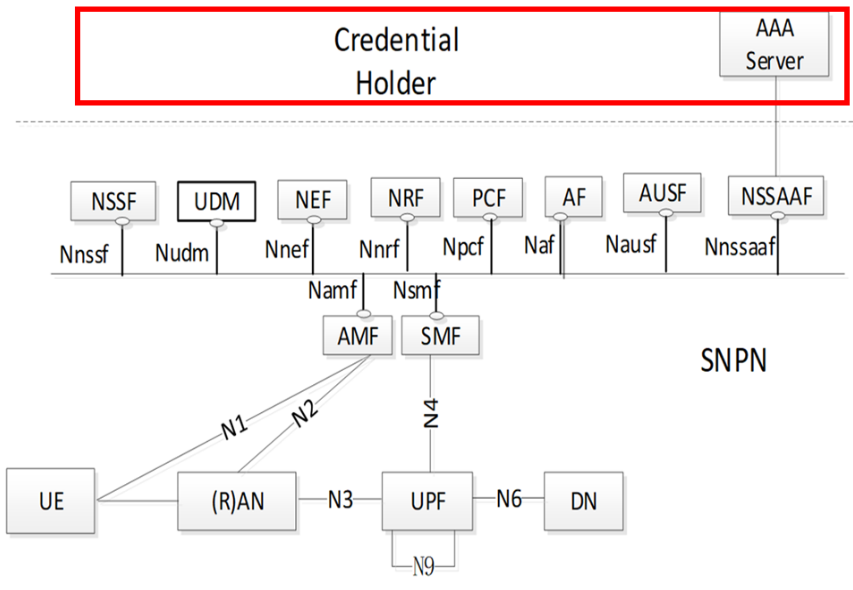
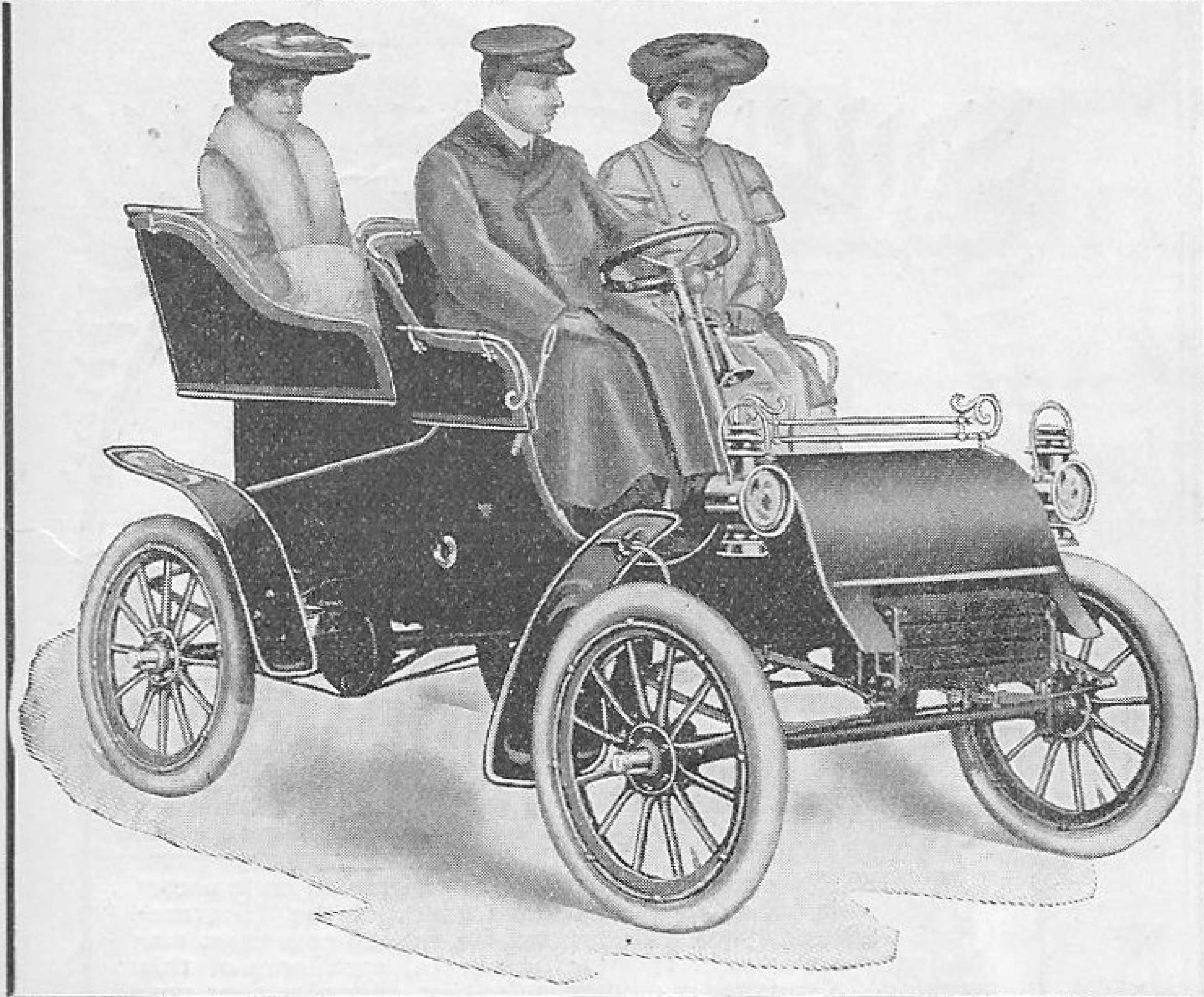


Fig. 5G System Architecture with Access to SNPN using credentials from Credentials Holder using AAA Server

Annex 3 - Self-driving vehicles in B5G and 6G Networks - 1



The Advance of
The Ford

All the *best* things in this world are usually worth even more than the price you pay for them. A *cheap* automobile is dear at any price, but a car like the Ford is a bargain at any reasonable figure.

The advanced and improved construction, the higher grade of materials used in building the machinery and body, and the addition of heavy 3 in. detachable tires to its equipment compel us to make the price of the **1904 Ford**

$900 with Tonneau $800 as a Runabout.

Lamps, Horn and Brass Trimmings Extra.

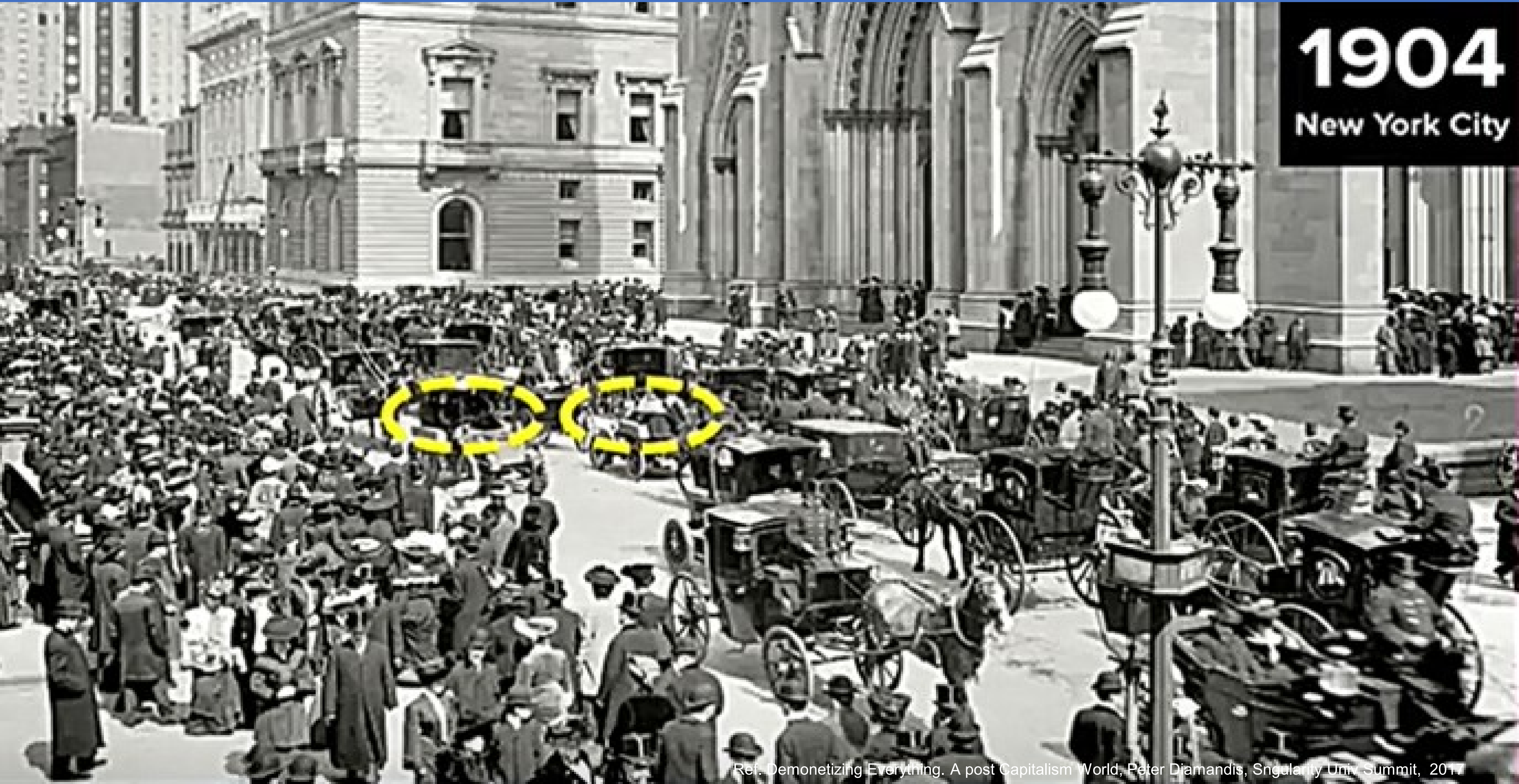
Mr. Ford made the first automobile in Detroit and the third in the United States. THE FORD MOTOR CAR of today represents the most advanced type of automobile construction.

WE agree to assume all responsibility in any action the Trust may take regarding alleged infringement of the Selden Patent to prevent you from buying the Ford, "The car of satisfaction."

Write for full information and Illustrated Catalogue to

FORD MOTOR CO. Detroit, Mich.

Annex 3 - Self-driving vehicles in B5G and 6G Networks - 2

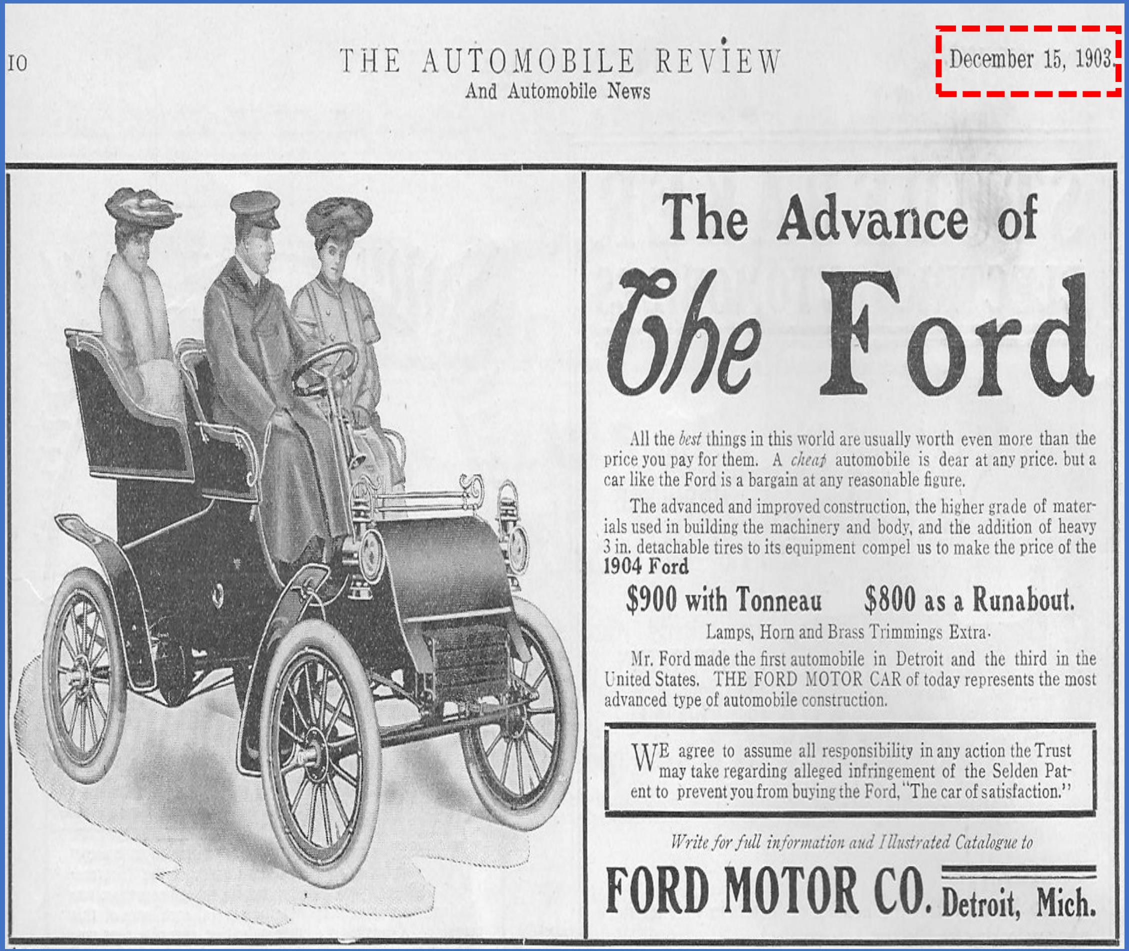


Ref. Demonetizing Everything. A post Capitalism World, Peter Diamandis, Sngularity Univ Summit, 2017

Annex 3 - Self-driving vehicles in B5G and 6G Networks - 3

Ref. Demonetizing Everything. A post Capitalism World, Peter Diamandis, Sngularity Univ Summit, 2017

Annex 3 - Self-driving vehicles in B5G and 6G Networks - 4



10 THE AUTOMOBILE REVIEW December 15, 1903

And Automobile News

The Advance of

The Ford

All the *best* things in this world are usually worth even more than the price you pay for them. A *cheap* automobile is dear at any price, but a car like the Ford is a bargain at any reasonable figure.

The advanced and improved construction, the higher grade of materials used in building the machinery and body, and the addition of heavy 3 in. detachable tires to its equipment compel us to make the price of the 1904 Ford

$900 with Tonneau $800 as a Runabout.

Lamps, Horn and Brass Trimmings Extra.

Mr. Ford made the first automobile in Detroit and the third in the United States. THE FORD MOTOR CAR of today represents the most advanced type of automobile construction.

WE agree to assume all responsibility in any action the Trust may take regarding alleged infringement of the Selden Patent to prevent you from buying the Ford, "The car of satisfaction."

Write for full information and Illustrated Catalogue to

FORD MOTOR CO. Detroit, Mich.

Ford 1921 T-Model

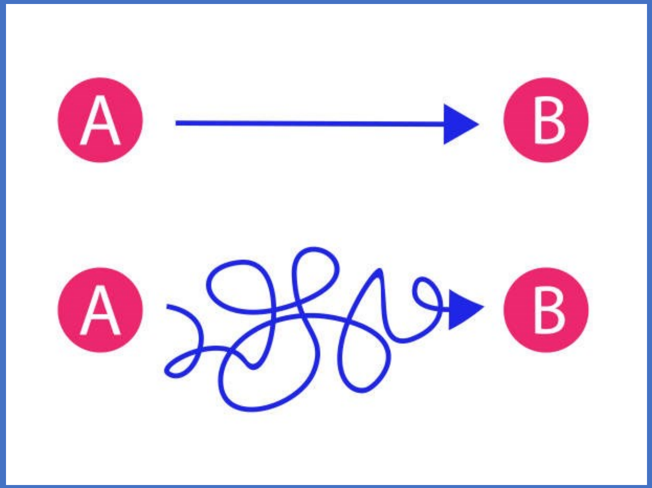
Ref. Demonetizing Everything. A post Capitalism World, Peter Diamandis, Sngularity Univ Summit, 2017

Annex 3 - Self-driving vehicles in B5G and 6G Networks - 6

Ref. Demonetizing Everything. A post Capitalism World, Peter Diamandis, Sngularity Summit, 2017

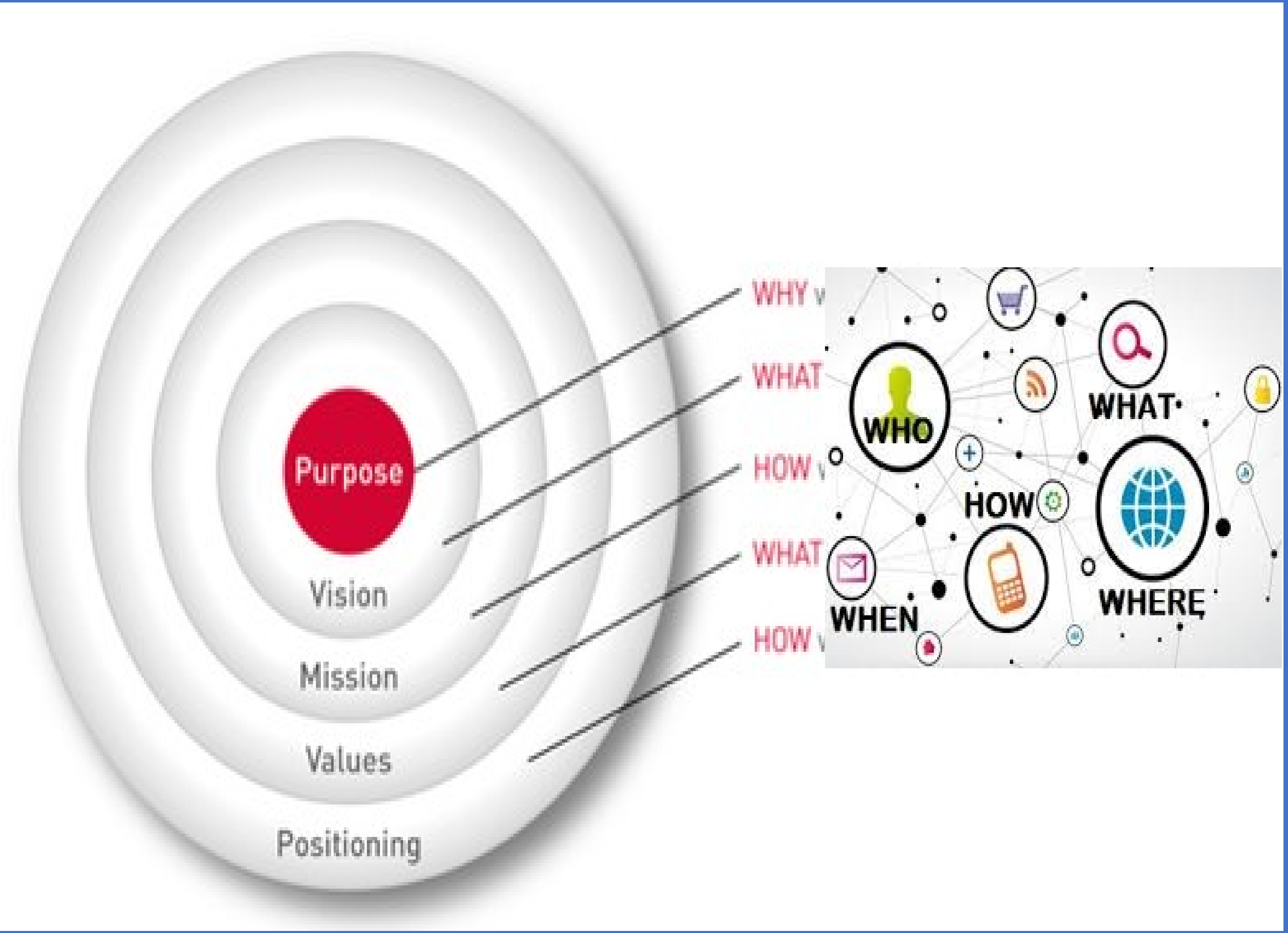
Annex 3 - Self-driving vehicles in B5G and 6G Networks - 7

Destination from point "A" to point "B" - Car design type and use since Ford T-Model since 1908 in the last 100 years



Annex 3 - Self-driving vehicles in B5G and 6G Networks - 8

Shift to importance & focus on "Purpose" in the Vehicle use & design type in the self-driving B5G Connected Vehicles set to be 7/24 "Connected" to drive on "pre-defined"/"set"/"pre-configured" route as a Network Slice (SST V2X) and/or NPN/SNPN (Stand-alone Non-Public Network)



5GS QoS handling for V2X Communication PQI (PC5 5QI (5G QoS Identifier)) with 5G SST (Slice/Service Type) Standardized Values

Release 18 3GPP V18.1.0 (2023-09)

Figure: 5G System Architecture V2X Standardized PQI (PC5 5QI 5G QoS Identifier) to QoS Characteristics Mapping

PQI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Maximum Data Burst Volume	Default Averaging Window	Example Services
21	GBR	3	20 ms	10^{-4}	N/A	2000 ms	Platooning between UEs – Higher degree of automation; Platooning between UE and RSU – Higher degree of automation
22	(NOTE 1)	4	50 ms	10^{-2}	N/A	2000 ms	Sensor sharing – higher degree of automation
23		3	100 ms	10^{-4}	N/A	2000 ms	Information sharing for automated driving – between UEs or UE and RSU - higher degree of automation
55	Non-GBR	3	10 ms	10^{-4}	N/A	N/A	Cooperative lane change – higher degree of automation
56		6	20 ms	10^{-1}	N/A	N/A	Platooning informative exchange – low degree of automation; Platooning – information sharing with RSU
57		5	25 ms	10^{-1}	N/A	N/A	Cooperative lane change – lower degree of automation
58		4	100 ms	10^{-2}	N/A	N/A	Sensor information sharing – lower degree of automation
59		6	500 ms	10^{-1}	N/A	N/A	Platooning – reporting to an RSU
90	Delay Critical GBR	3	10 ms	10^{-4}	2000 bytes	2000 ms	Cooperative collision avoidance; Sensor sharing – Higher degree of automation; Video sharing – higher degree of automation
91	(NOTE 1)	2	3 ms	10^{-5}	2000 bytes	2000 ms	Emergency trajectory alignment; Sensor sharing – Higher degree of automation
NOTE 1: GBR and Delay Critical GBR PQIs can only be used for unicast PC5 communications.							

NOTE 1: For Standardized PQI to QoS characteristics mapping, the table will be extended/updated to support service requirements for other identified V2X services.

NOTE 2: The PQIs may be used for other services than V2X.

NOTE 3: A PQI may be used together with an application indicated priority, which overrides the Default Priority Level of the PQI.

Release 18 3GPP V18.3.0 (2023-09)

Table: 5G System Architecture 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.
HDLLC	6	Slice suitable for the handling of High Data rate and Low Latency Communications.

Annex 3 - Self-driving vehicles in B5G and 6G Networks - 10

Use Case (UC) on Sensing Assisted Automotive Manoeuvring and Navigation

To support Smart Transportation and Autonomous Driving, more Vehicle and Devices are equipped with Sensing Technologies, e.g. Cameras, Radar, and Lidar Systems are the most used Sensors by the Automotive Industry to maintain the perception for Autonomous Vehicles at various Levels of Autonomy.

Accurate Sensing results are crucial to enable the safe and reliable Control of the Vehicles.

Due to the mounting position of the sensors (e.g., 3GPP based Sensors) Information Collected from a Single Vehicle's Sensors can not be sufficient or accurate enough to satisfy the Advanced Automotive Use Cases, e.g., Autonomous Driving, Co-ordinated Maneuver, etc.

Therefore, the 5G System could co-ordinate Sensing to get Sensing Data from various sources and generate Sensing Results which could be consumed at the Vehicle and used for the Vehicular Control and Driver Assistance, e.g., feed into the Automated Driving System (ADS) in the Car.

The 3GPP Sensing Data Collected by the UE can be sent alongside relevant Sensing Information to other Sensing Entities (including other Vehicles, Roadside Units, and Network) for further processing (if required) before sharing with a 3rd-Party Application as shown in the Figure.

The Network facilitated NR based Sensing described above could significantly improve the Sensing Reliability and Quality, enabling New and Advanced Automotive Use Cases.

In this UC, Joe and Bob's Vehicles are equipped with 3GPP-based Sensing Technology. Non-3GPP Sensors like Radar, Camera and Lidar Sensors could also be available in the Vehicles. Additionally, the Vehicles are Capable of 5G Communications, including Direct Communication with other Vehicles, Communication with 5G system via RAN entities.

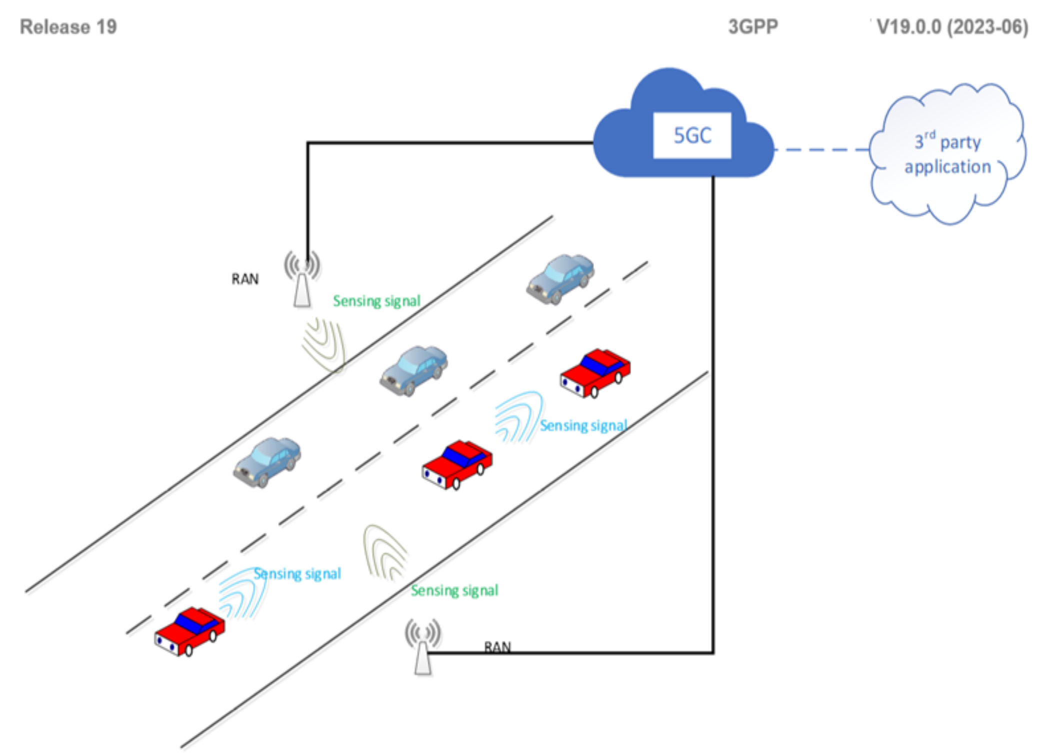


Figure: 5G System Assisted Automotive Manoeuvring and Navigation with Network support for Sensing equipped Sensors

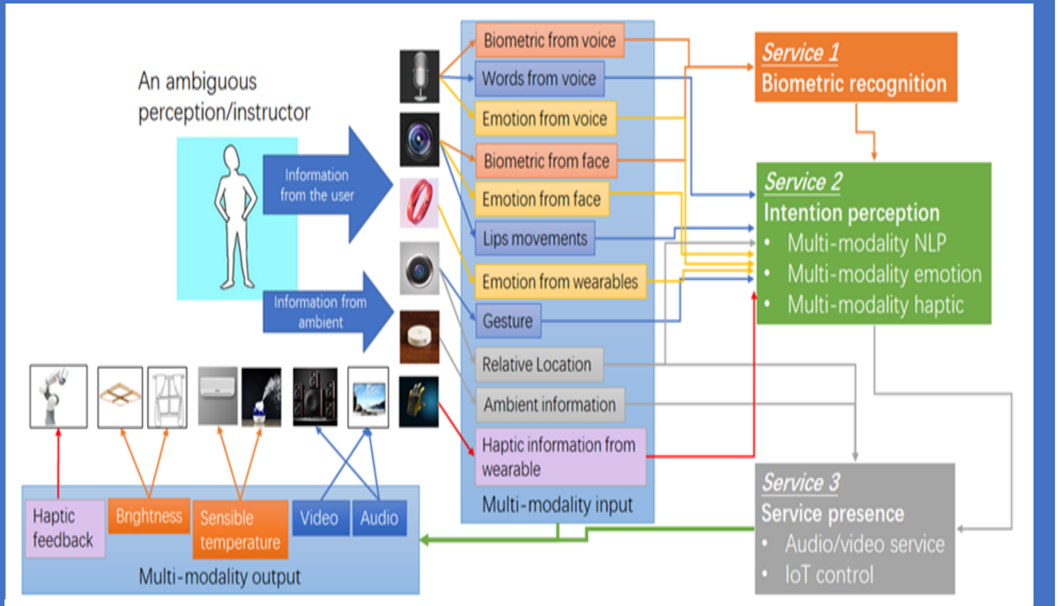


Figure: 5G Multi-modal Interactive System for Tactile and Multi-modal Communication Service

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.		

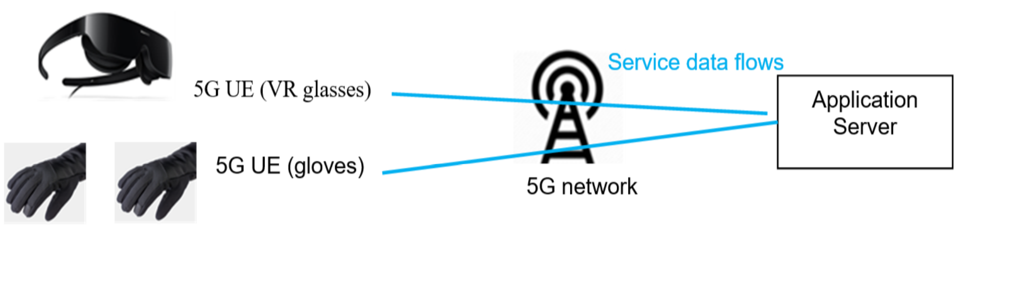


Figure . Immersive multi-modal VR application with multiple 5G UEs directly connected to 5G network

Release 19 3GPP V19.2.0 (2023-03)

Overview

Unlike previous 3GPP systems that attempted to provide a 'one size fits all' system, the 5G system is expected to be able to provide optimized support for a variety of different services, different traffic loads, and different end user communities. Various industry white papers, most notably, the NGMN 5G White Paper [2], describe a multi-faceted 5G system capable of simultaneously supporting multiple combinations of reliability, latency, throughput, positioning, and availability. This technology revolution is achievable with the introduction of new technologies, both in access and the core, such as flexible, scalable assignment of network resources. In addition to increased flexibility and optimization, a 5G system needs to support stringent KPIs for latency, reliability, throughput, etc. Enhancements in the radio interface contribute to meeting these KPIs as do enhancements in the core network, such as network slicing, in-network caching and hosting services closer to the end points.

A 5G system also supports new business models such as those for IoT and enterprise managed networks. Drivers for the 5G KPIs include services such as Uncrewed Aerial Vehicle (UAV) control, Augmented Reality (AR), and factory automation. Network flexibility enhancements support self-contained enterprise networks, installed and maintained by network operators while being managed by the enterprise. Enhanced connection modes and evolved security facilitate support of massive IoT, expected to include tens of millions of UEs sending and receiving data over the 5G network.

Flexible network operations are the mainstay of the 5G system. The capabilities to provide this flexibility include network slicing, network capability exposure, scalability, and diverse mobility. Other network operations requirements address the necessary control and data plane resource efficiencies, as well as network configurations that optimize service delivery by minimizing routing between end users and application servers. Enhanced charging and security mechanisms handle new types of UEs connecting to the network in different ways. The enhanced flexibility of the 5G system also allows to cater to the needs of various verticals. For example, the 5G system introduces the concept of non-public networks providing exclusive access for a specific set of users and specific purpose(s). Non-public networks can, depending on deployment and (national) regulations, support different subsets of 5G functionality. In this specification 5G network requirements apply to both NPNs and PLMNs, unless specified otherwise. Additionally, there are specific requirements dedicated only to NPNs or PLMNs, which are indicated accordingly.

Mobile Broadband (MBB) enhancements aim to meet a number of new KPIs. These pertain to high data rates, high user density, high user mobility, highly variable data rates, deployment, and coverage. High data rates are driven by the increasing use of data for services such as streaming (e.g. video, music, and user generated content), interactive services (e.g. AR), and IoT. These services come with stringent requirements for user experienced data rates as well as associated requirements for latency to meet service requirements. Additionally, increased coverage in densely populated areas such as sports arenas, urban areas, and transportation hubs has become essential for pedestrians and users in urban vehicles. New KPIs on traffic and connection density enable both the transport of high volumes of data traffic per area (traffic density) and transport of data for a high number of connections (e.g. UE density or connection density). Many UEs are expected to support a variety of services which exchange either a very large (e.g. streaming video) or very small (e.g. data burst) amount of data. The 5G system will handle this variability in a resource efficient manner. All of these cases introduce new deployment requirements for indoor and outdoor, local area connectivity, high user density, wide area connectivity, and UEs travelling at high speeds.

Another aspect of 5G KPIs includes requirements for various combinations of latency and reliability, as well as higher accuracy for positioning. These KPIs are driven by support for both commercial and public safety services. On the commercial side, industrial control, industrial automation, UAV control, and AR are examples of those services. Services such as UAV control will require more precise positioning information that includes altitude, speed, and direction, in addition to horizontal coordinates.

Support for Massive Internet of Things (MIoT) brings many new requirements in addition to those for the enhanced KPIs. The expansion of connected things introduces a need for significant improvements in resource efficiency in all system components (e.g. UEs, IoT devices, radio, access network, core network).

The 5G system also aims to enhance its capability to meet KPIs that emerging V2X applications require. For these advanced applications, the requirements, such as data rate, reliability, latency, communication range and speed, are made more stringent.

Release 19 3GPP V19.0.0 (2023-03)

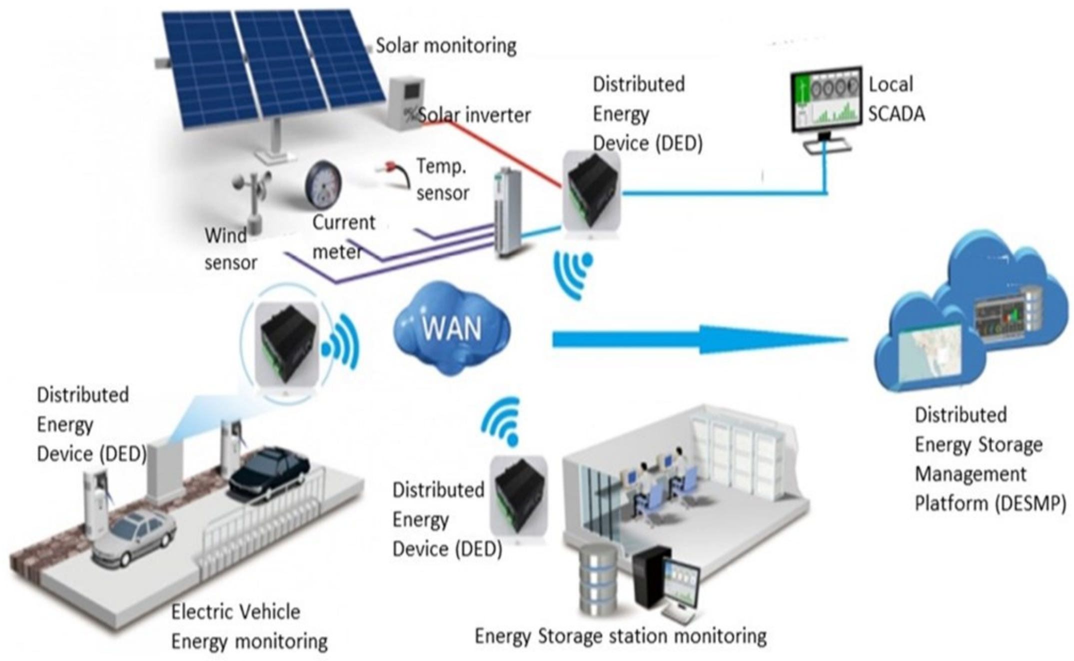


Figure: 5G Vertical Example of Distributed-Energy Storage Grid Domain

Release 19 3GPP V19.0.0 (2023-03)

Table : Key Performance for uninterrupted MTC service availability

Characteristic parameter (KPI)				Influence quantity				
Communication service availability: target value	Communication service reliability: mean time between failures	Max Allowed End-to-end latency (note 1; (note 2)	Service bit rate: user-experienced data rate (note 2)	Message size [byte]	Survival time	UE speed	# of UEs	Service Area
99.999 9 %	–	100 ms	< 1 kbit/s per DER	–	–	Stationary	–	–

NOTE 1: Unless otherwise specified, all communication includes 1 wireless link (UE to network node or network node to UE) rather than two wireless links (UE to UE).
NOTE 2: It applies to both UL and DL unless stated otherwise.

Release 19 3GPP V19.0.0 (2023-03)

Overview

For the purpose of this document, a vertical domain is a particular industry or group of enterprises in which similar products or services are developed, produced, and provided. Automation refers to the control of processes, devices, or systems in vertical domains by automatic means. The main control functions of automated control systems include taking measurements, comparing results, computing any detected or anticipated errors, and correcting the process to avoid future errors. These functions are performed by sensors, transmitters, controllers, and actuators.

In the context of this document, cyber-physical systems are referred to as systems that include engineered, interacting networks of physical and computational components. Cyber-physical control applications are to be understood as applications that control physical processes. Cyber-physical control applications in automation follow certain activity patterns, which are open-loop control, closed-loop control, sequence control, and batch control

Communication services supporting cyber-physical control applications need to be ultra-reliable, dependable with a high communication service availability, and often require low or (in some cases) very low end-to-end latency.

Communication in automation in vertical domains follows certain communication patterns. The most well-known is periodic deterministic communication, others are aperiodic deterministic communication and non-deterministic communication (see Clause 4.3).

Communication for cyber-physical control applications supports operation in various vertical domains, for instance industrial automation and energy automation. This document addresses service requirements for cyber-physical control applications and supporting communication services from the vertical domains of factories of the future (smart manufacturing), electric power distribution, and central power generation. Service requirements for cyber-physical control applications and supporting communication services for rail-bound mass transit are addressed

Control systems and related communication patterns

There are preferences in the mapping between the type of control and the communication pattern. Open-loop control is characterised by one or many messages sent to an actuator. These can be sent in a periodic or an aperiodic pattern. However, the communication means used need to be deterministic since typically an activity response from the receiver and/or the receiving application is expected.

Closed-loop control produces both periodic and aperiodic communication patterns. Closed-loop control is often used for the control of continuous processes with tight time-control limits, e.g., the control of a printing press. In this case, one typically relies on periodic communication patterns. Note that in both the aperiodic and periodic case, the communication needs to be deterministic.

Logging of device states, measurements, etc. for maintenance purposes and such typically entails aperiodic communication patterns. In case the transmitted logging information can be time-stamped by the respective function, determinism is often not mandatory.

In practice, vertical communication networks serve a large number of applications exhibiting a wide range of communication requirements. In order to facilitate efficient modelling of the communication network during engineering and for reducing the complexity of network optimisation, traffic classes or communication patterns have been identified [6]. There are three typical traffic classes or communication patterns in industrial environments [6], i.e.,

- deterministic periodic communication: periodic communication with stringent requirements on timeliness of the transmission.
- deterministic aperiodic communication: communication without a preset sending time. Typical activity patterns for which this kind of communication is suitable are event-driven actions.
- non-deterministic communication: subsumes all other types of traffic, including periodic non-real time and aperiodic non-real time traffic. Periodicity is irrelevant in case the communication is not time-critical.

Some communication services exhibit traffic patterns that cannot be assigned to one of the above communication patterns exclusively (mixed traffic).

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

Figure Localized Mobile Metaverse Services offering relevant information

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

Figure Example of Smart Transport Metaverse

Figure: Service offering relevant information are anchored in Space

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

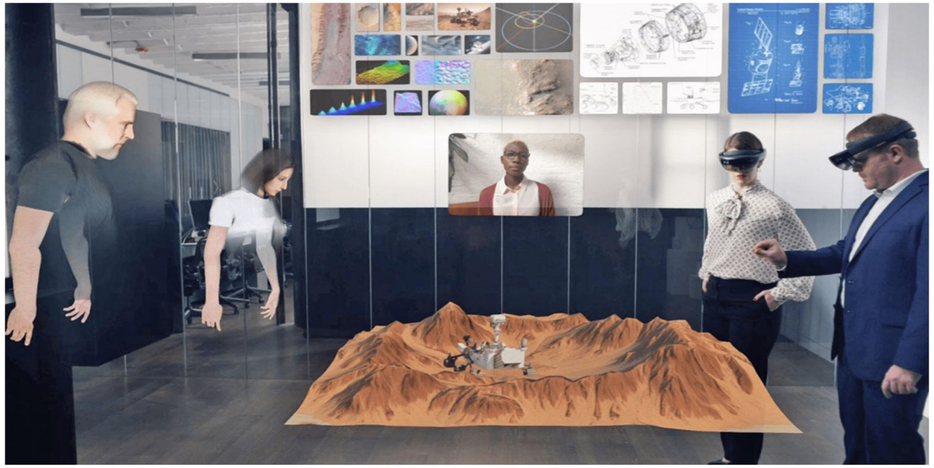


Figure XR enabled collaborative and concurrent engineering in product design

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

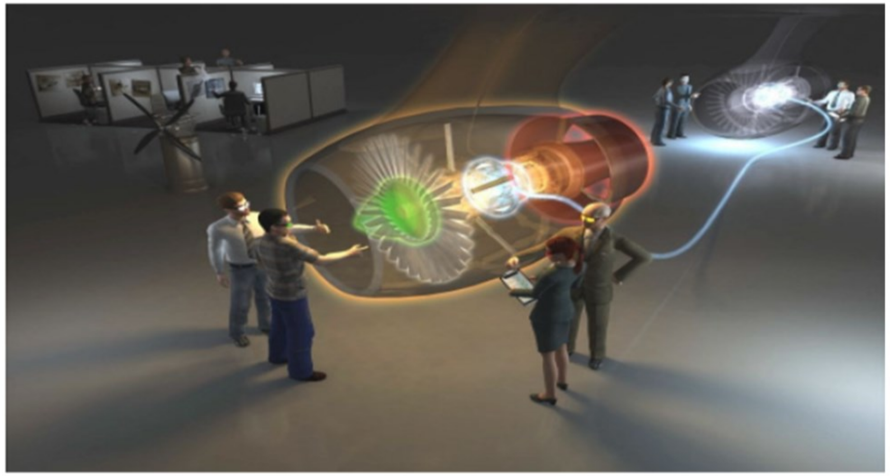


Figure : Illustration of Collaborative Workspace (Source: ESI-Icido GmbH)

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/km² (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 km² (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.

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 km^2 (note 3)	Haptic feedback
	5 ms	< 1Mbit/s	[99.99%]	MTU	-	Stationary or Pedestrian	typically < 100 km^2 (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 km^2 (note 3)	Video
	10 ms	5-512 kbit/s	[99.9%]	50	-	Stationary or Pedestrian	typically < 100 km^2 (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 km^2 (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.

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.

1. Automotive: A USD 23 Billion Market Opportunity

Tele-Operated Driving alone is a USD 300 million Near-term Opportunity

Ref.: Ericsson, Network Slicing: Top 10 UCs to target, reports, May & June 2021

Segment overview

Automotive

Segment scope
Manufacturing, maintenance, and services for connected vehicles

Typical CSP customers
Fleet operators

Key slicing cases:

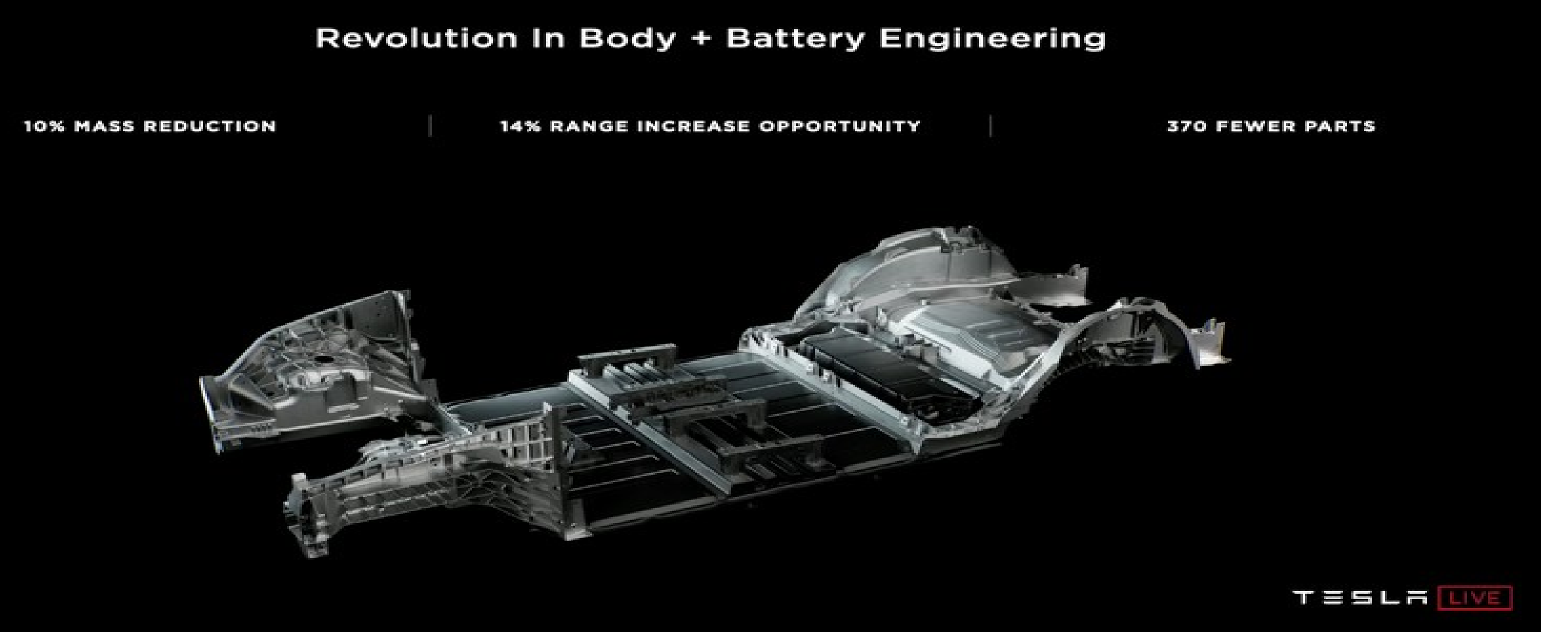
Tele-operated driving Low Latency	**Platooning** Low Latency
Automated lane change Availability	**Real-time-situational awareness** Availability

Future Tesla Cars Will Use Batteries for Shell Structure (Sept 22, 2020)

To Increase Range & Reduce Cost, Tesla Battery Packs will become Structurally Integral.

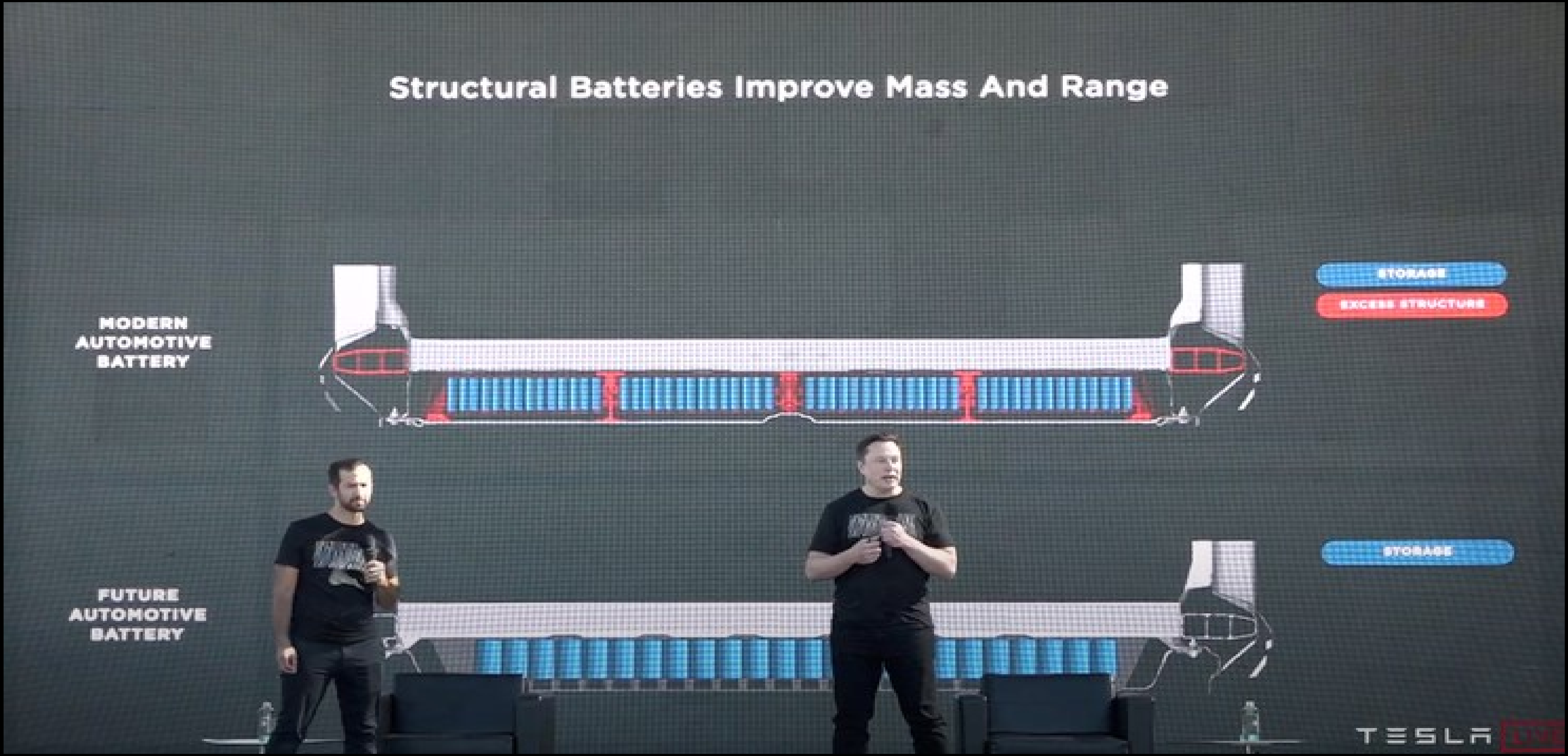
Battery Packs in current Tesla's are mounted in the floor of the Cars, but they're not structural parts of the Chassis.

The cells will be adhered to top and bottom "sheets" with a flame-retardant structural adhesive, which Musk says provides incredible rigidity. So much rigidity that if you were to build a convertible based around this sort of chassis, it'd be stiffer than a conventional car.
This New Approach to Chassis design is part of Tesla's goal of reducing cost per kilowatt hour of battery capacity by half.

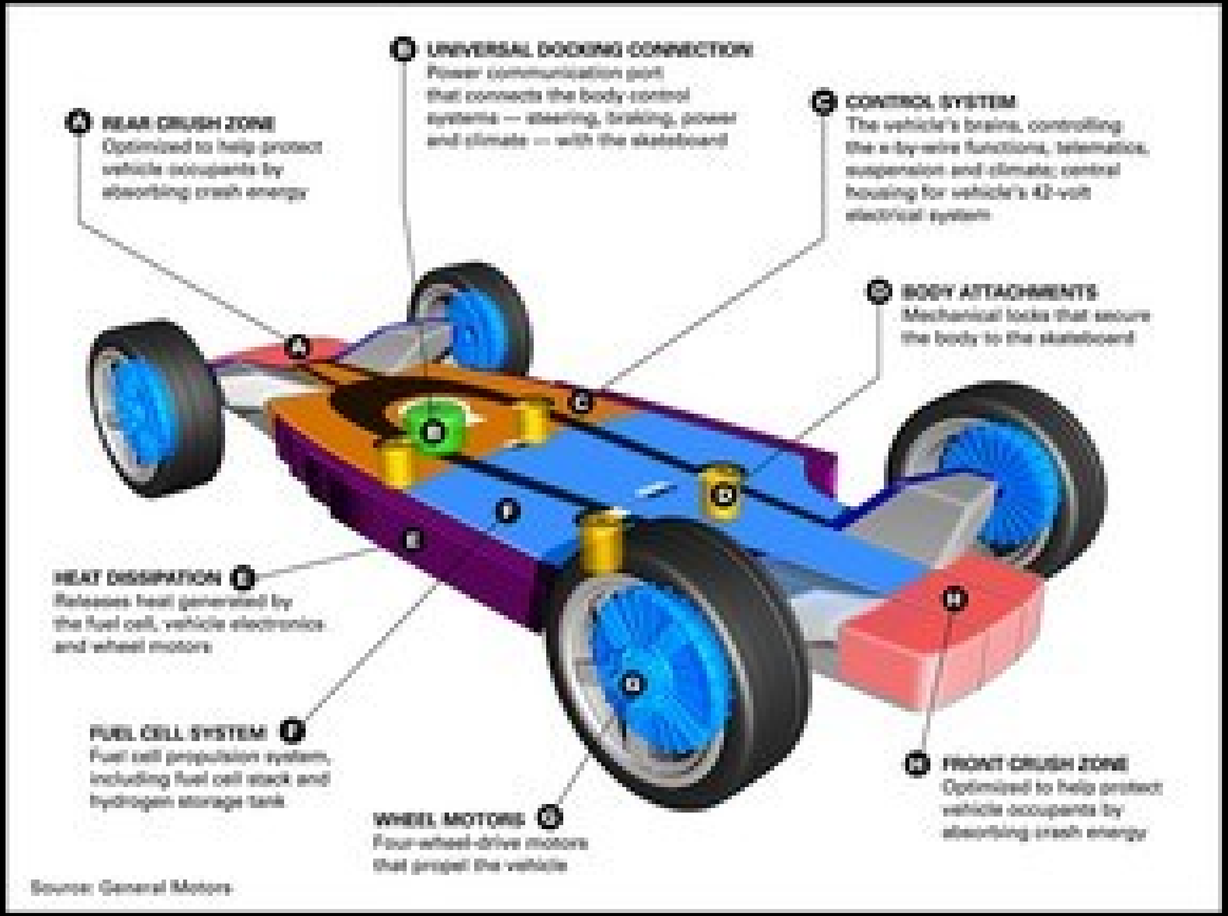


Future Tesla Cars Will Use Batteries for Shell Structure

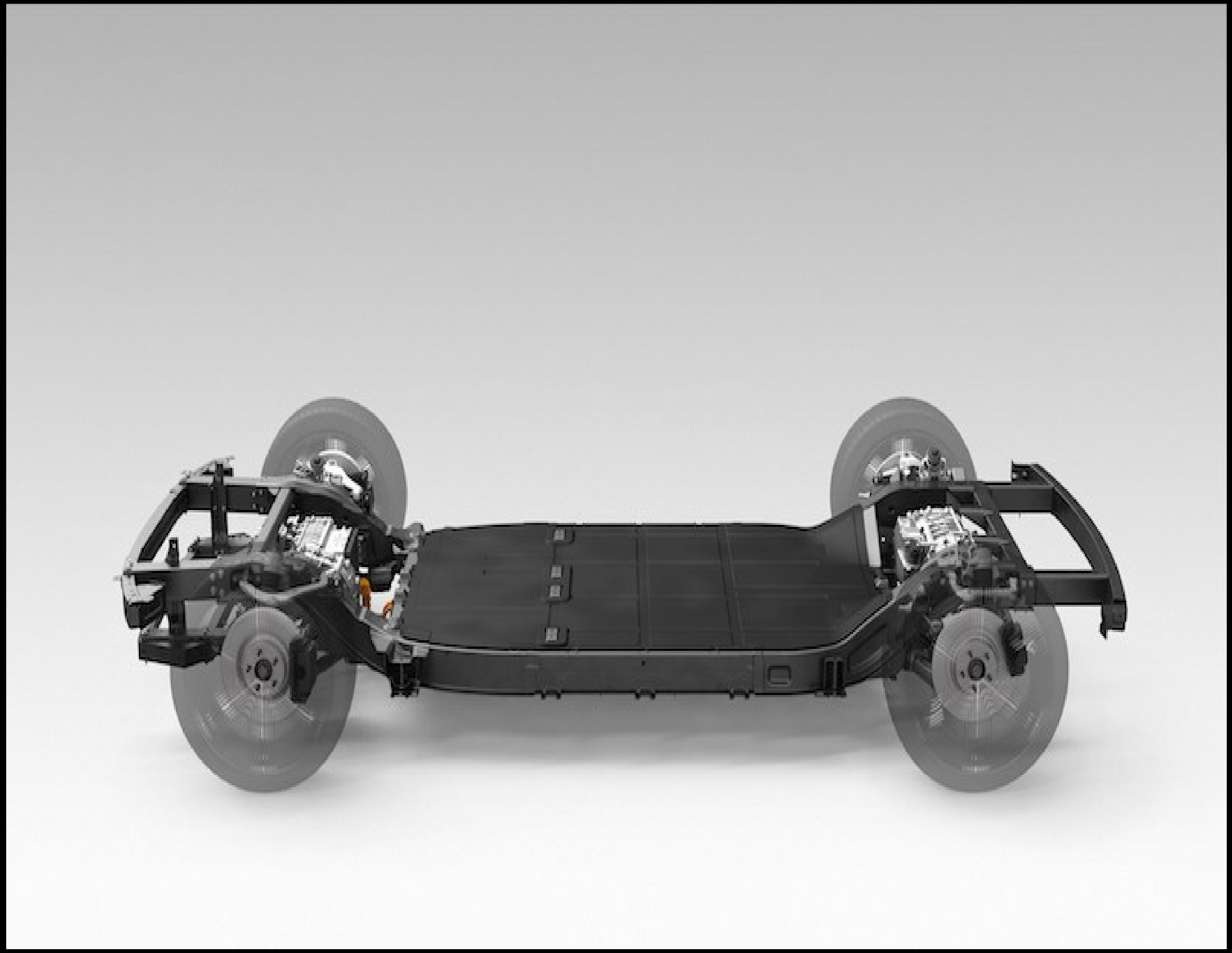
To increase range and reduce cost, Tesla battery packs will become structurally integral (in the chassi).



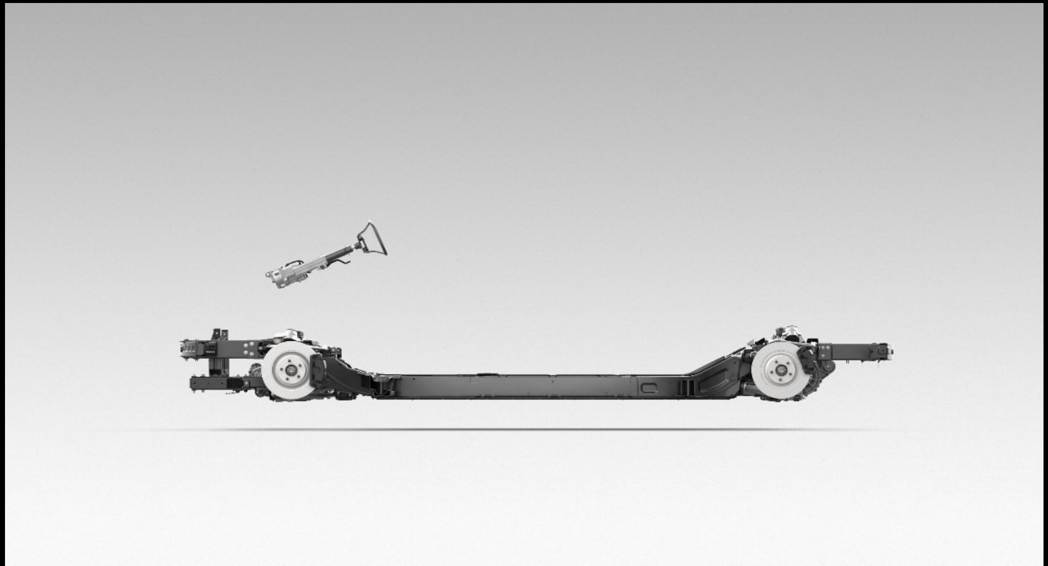
EV Electric Vehicle Skateboard Chassis - GM

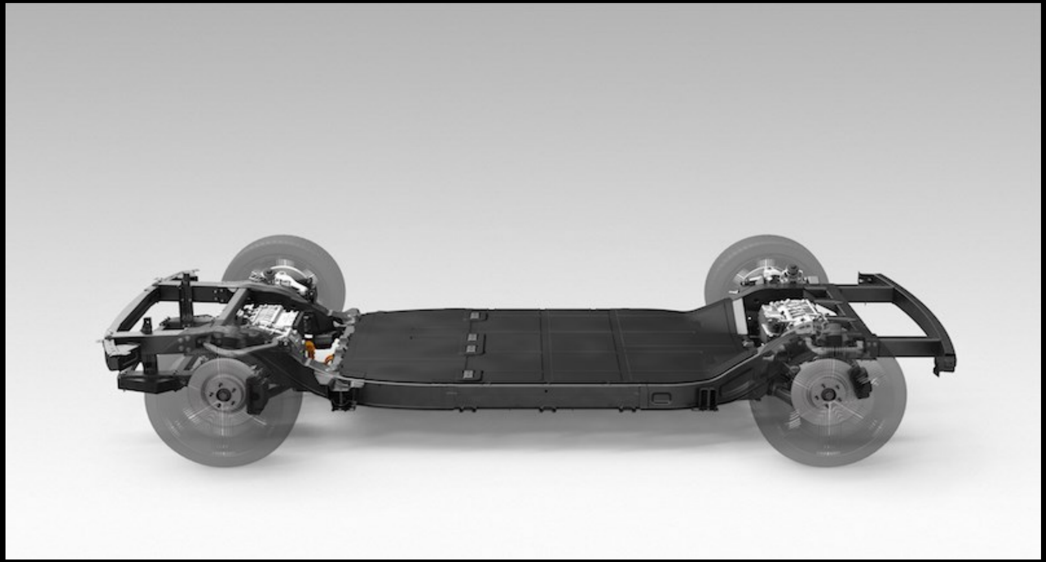


EV Electric Vehicle Skateboard Chassis - Canoo

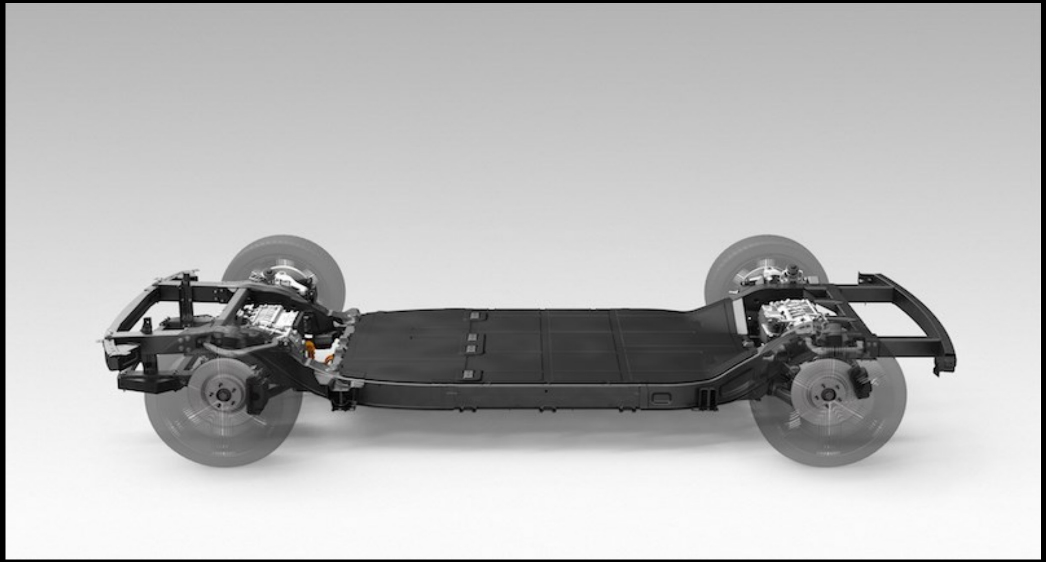


EV Electric Vehicle Skateboard Chassis - Canoo





EV Electric Vehicle Skateboard Chassis - Canoo



Annex 4

6G selected Architecture Themes

Sensing Networks 3GPP Core RAN Synergy (& Cell Free Wireless Network Solution)

to

LF Edge Akraino TSC

Ike Alisson

LF Edge Akraino Documentation Sub-committee TSC Chair

2021-06-29

Rev PA10

Table of Contents

European 6G Vision

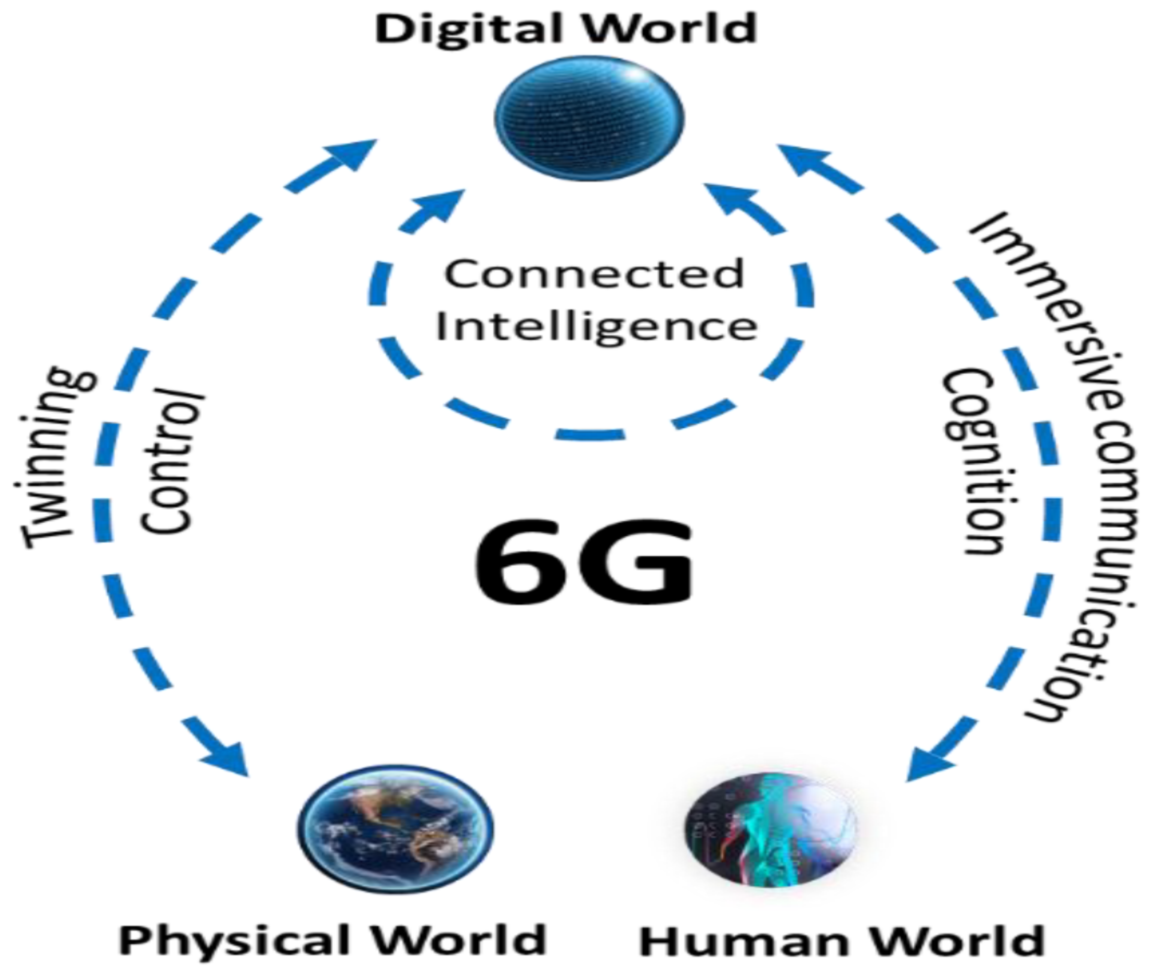
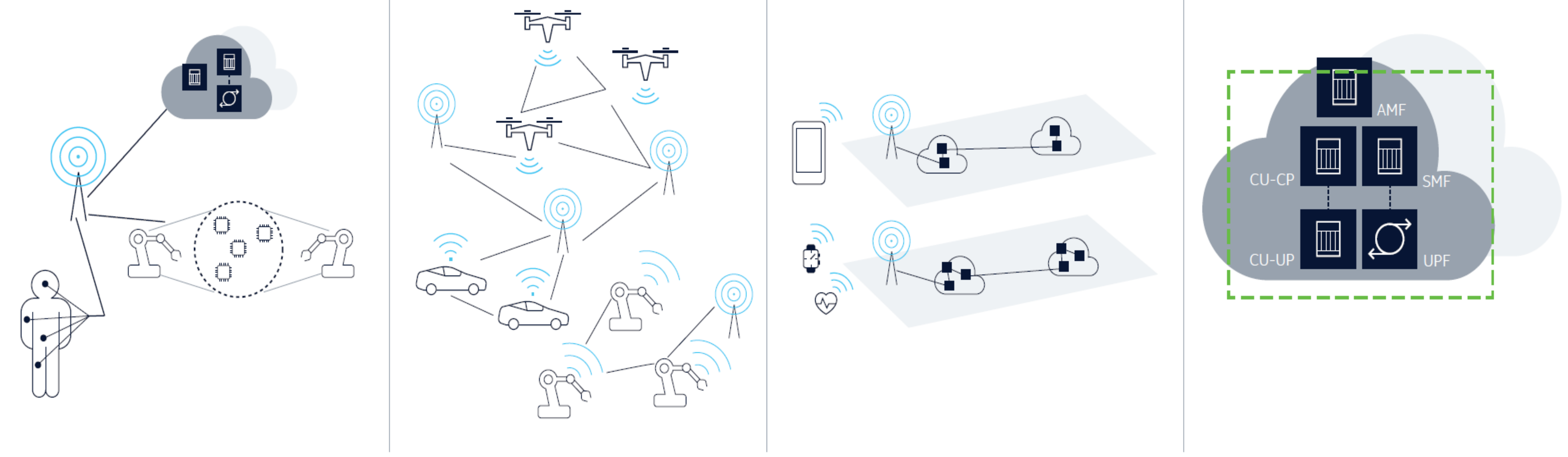


Figure 3.1: Convergence of digital, physical, and personal domains.

Ref. 5G IA, Europan Vision for the 6G Network Ecosystem, June 2021: 9

1

6G Architecture Themes



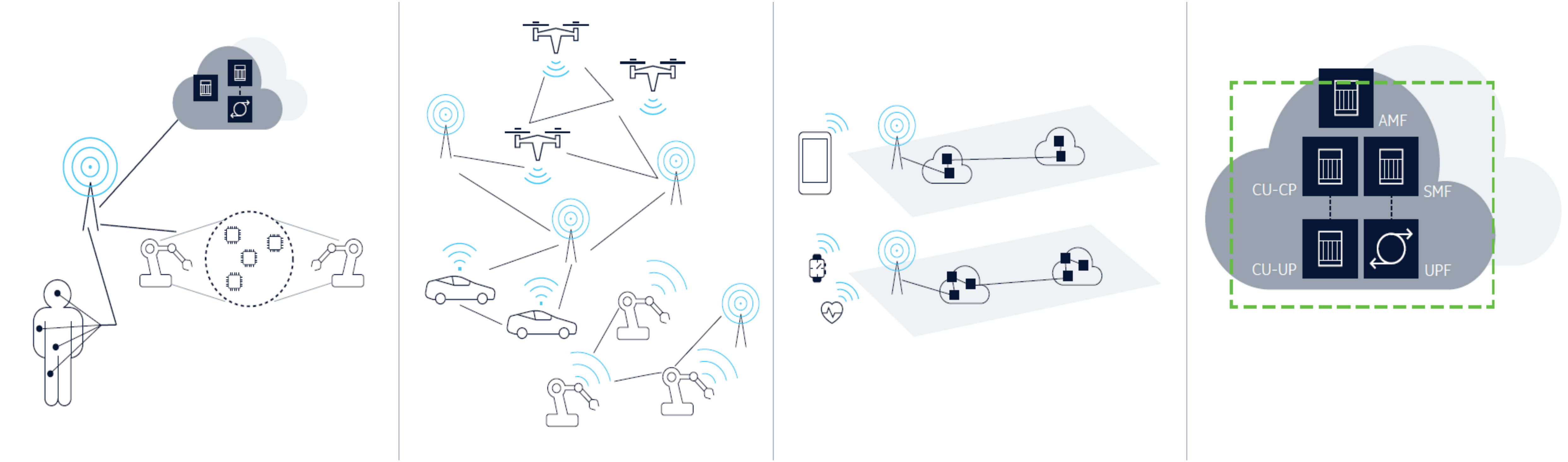
End point is a network | Cell free/mesh | Hyper-specialized slicing | RAN-Core convergence

Ref., Nokia, Communications in the 6G Era, WP, Aug., 2020:15

1

2

6G Architecture Themes



End point is a network | Cell free/mesh | Hyper-specialized slicing | RAN-Core convergence

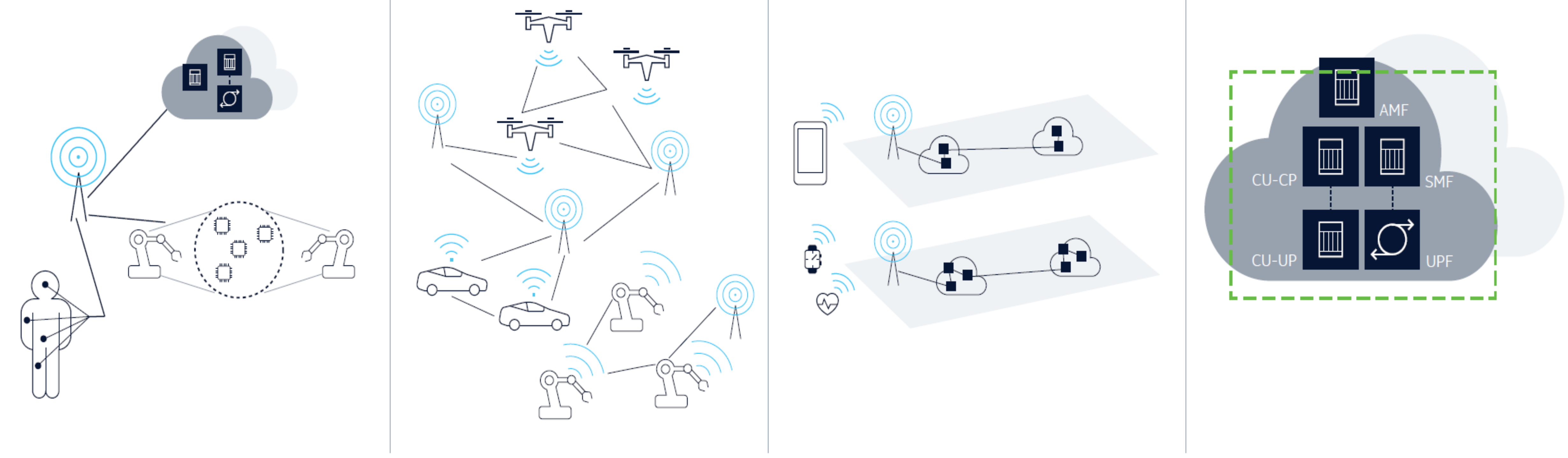
Ref., Nokia, Communications in the 6G Era, WP, Aug., 2020:15

1

3

2

6G Architecture Themes



End point is a network

Cell free/mesh

Hyper-specialized slicing

RAN-Core convergence

Ref., Nokia, Communications in the 6G Era, WP, Aug., 2020:15

European 6G Vision

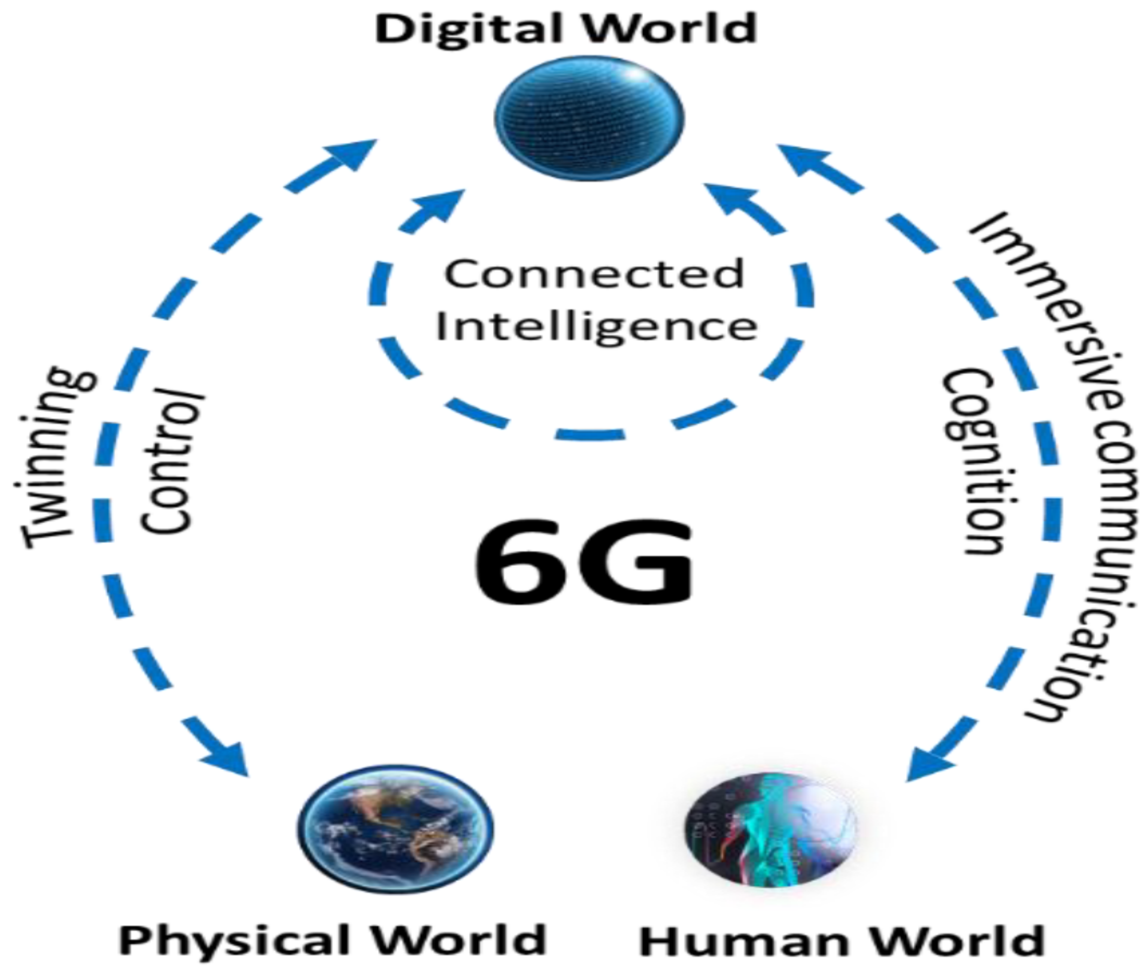
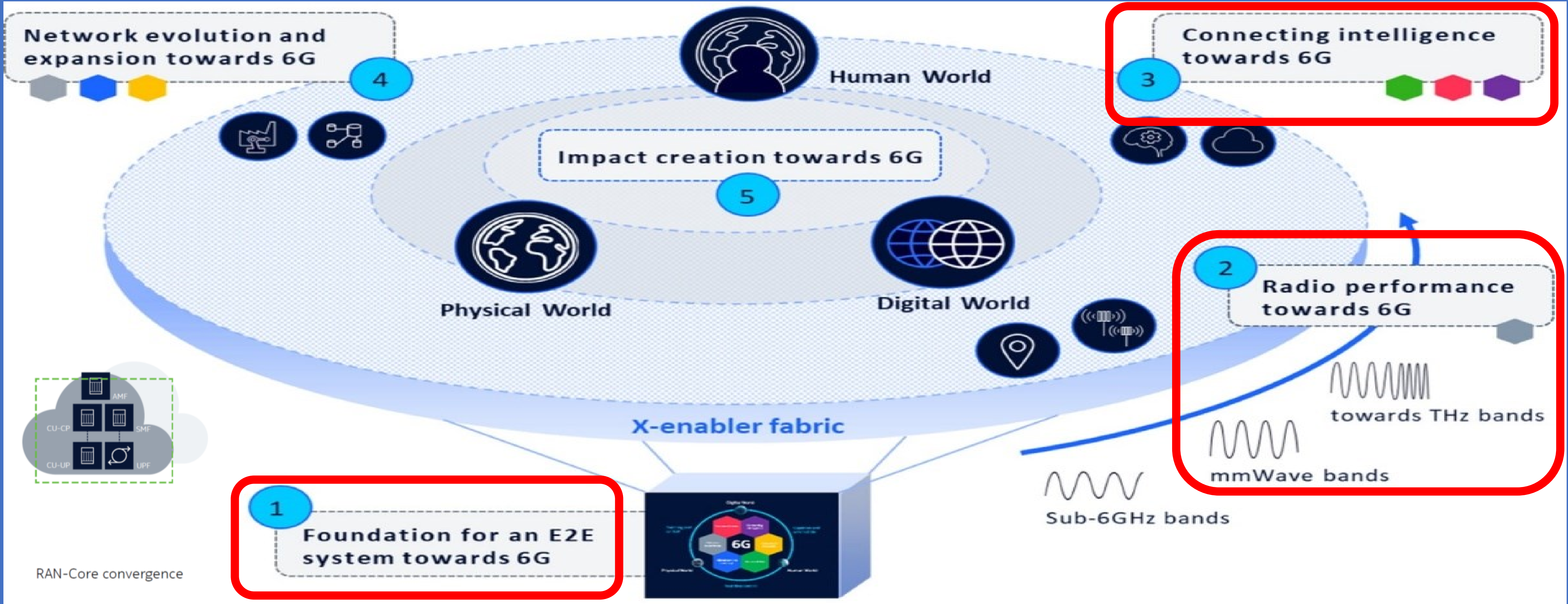


Figure 3.1: Convergence of digital, physical, and personal domains.

Ref. 5G IA, Europan Vision for the 6G Network Ecosystem, June 2021: 9

Network Evolution & Expansion

Enablers for an **Intelligent Network of Networks**, through Network disaggregation & dynamic dependability, forming the backbone of the 6G system. Through specialized and Flexible Networks such as Mesh Networks, NTNs, D2D, Cell-Free MIMO & Local Device Networks the requirements of both Extreme Performance & Global Service coverage can be met. Service-based Networks will be taken further with solutions for fully Cloud-Native RAN & CN Network Functions (NFs) using Common Platform Functions & Distributed Cloud Infrastructure.



Ref. Ericsson, "Hexa X-The Joint European Initiative to shape 6G", Vetter P., Nokia & Frodigh, M, Ericsson, June 2021,

European 6G Vision

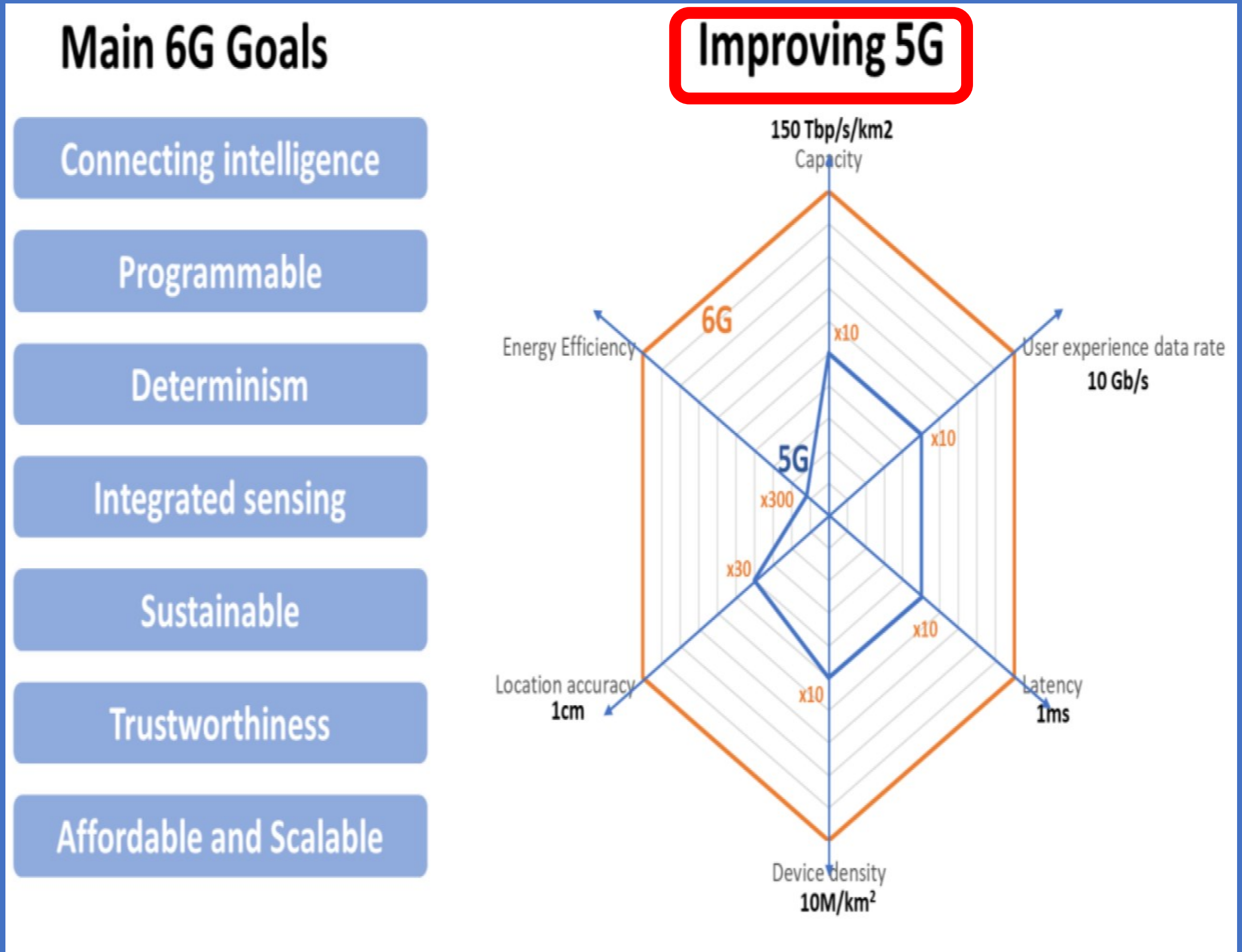


Figure 3.3: 6G goals.

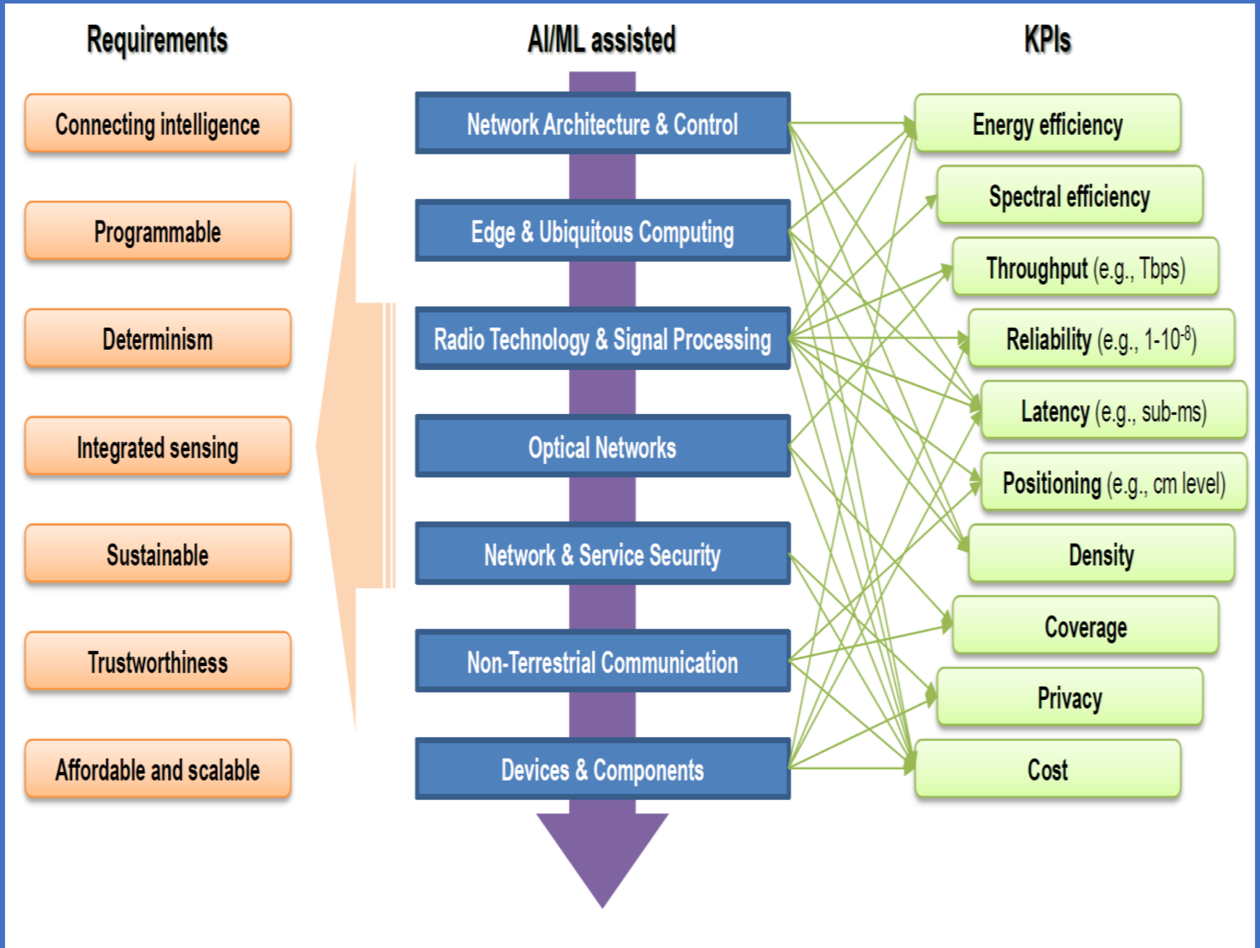


Figure 4.1: Technology areas with strong impact on different 6G requirements and KPIs.

Ref. 5G IA, Europan Vision for the 6G Network Ecosystem, June 2021: 13, 14

Table 3. A comparative analysis of 5G, B5G, and 6G.

Description	5G	Beyond 5G	6G
Frequency bands	■ Sub-6GHz ■ mmWave for fixed access	■ Sub-6GHz ■ mmWave for fixed access	■ Sub-6GHz ■ mmWave for mobile access ■ Exploration of higher frequency and THz bands (above 300 GHz) ■ Non-RF (optical, VLC)
Rates requirements	20 Gb/s	100 Gb/s	1 Tb/s
Radio only delay requirements	100 ns	100 ns	10 ns
End-to-End delay(latency) requirements	5 ms	1 ms	<1 ms
Processing delay	100 ns	50 ns	10 ns
Device types	■ Sensors ■ Smartphones ■ Drones	■ Sensors ■ Smartphones ■ Drones ■ XR equipment	■ Sensors and DLT ■ CRAS ■ XR and BCI ■ Smart implants
Architecture	■ Dense sub-6 GHz small base stations with umbrella macro stations. ■ mmWave small cells of about 100 m (about fixed access).	■ Denser sub-6 GHz small cells with umbrella macro base stations. ■ <100 m tiny and dense mmWave cells.	■ Cell-free smart surfaces at high frequency supported by mmWave tiny cells for mobile and free access. ■ Temporary hotspots are served by drone-carrier base stations or tethered balloons. ■ Trials of tiny THz cells.
Services	■ eMBB ■ URLLC ■ mMTC	■ Reliable eMBB ■ URLLC ■ mMTC ■ Hybrid (URLLC + eMBB)	■ HCS ■ MPS ■ MBRLLC ■ mURLLC

5G and 6G KPIs Comparison

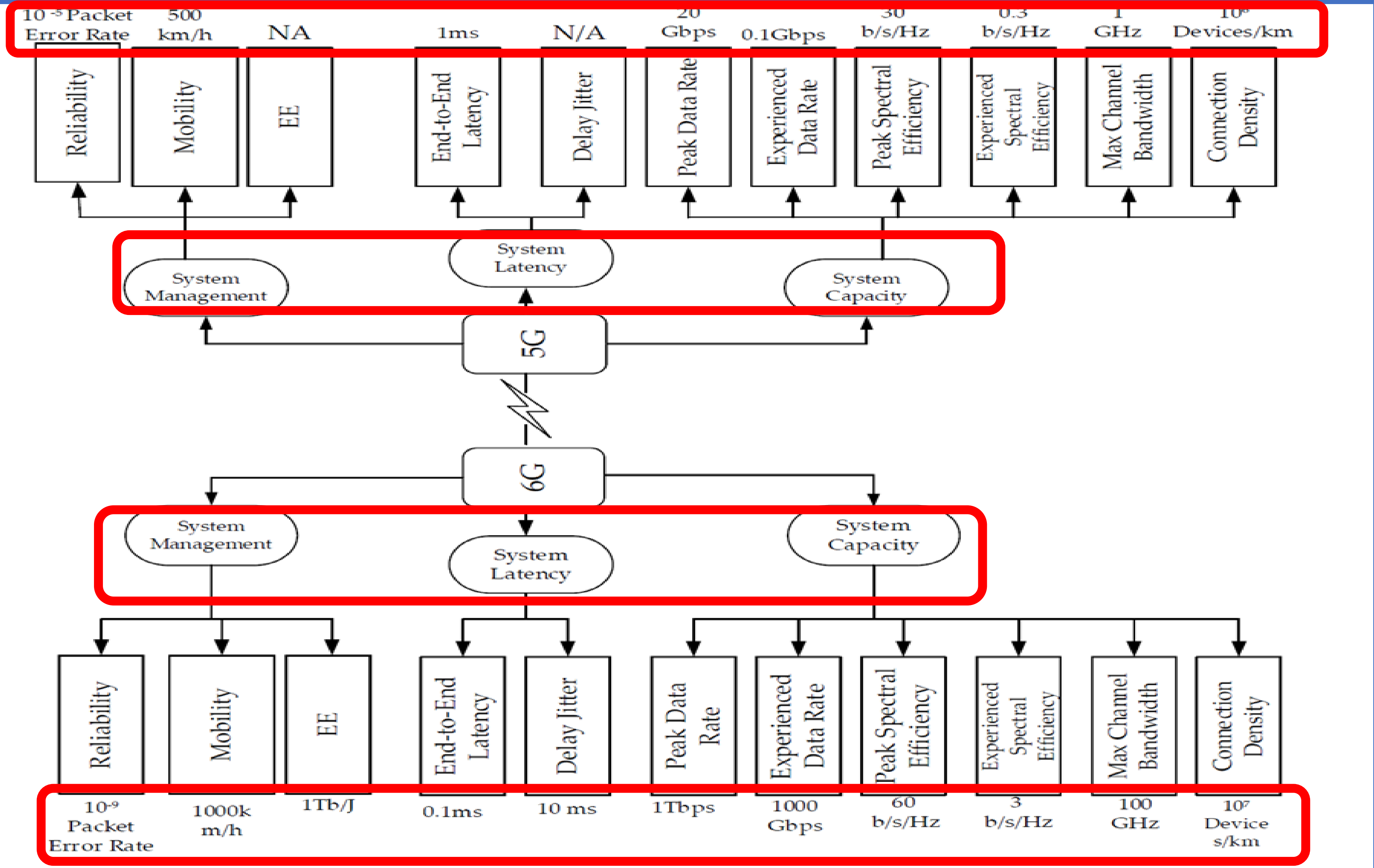


Figure 2. Comparative Analysis of 5G and 6G Key Performance Indicators.

Ref Sensors, 6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, & Research Roadmap, March 2021: 11

Trends towards 6G

Table 6. A summary of the driving trends towards 6G wireless networks.

Driving Trends	Description
The convergence of Communications, Computing, Control, Localization, and Sensing (3CLS).	Provides computing, control, localization, and sensing in addition to Wireless Communication that previous generations provided. Supports applications such as XR, CRAS, DLS.
The emergence of Smart Reflective Surfaces and Environments.	Driven by smart reflective surfaces that serve as walls, roads, doors, and entire buildings, help maintain a line of sight and obtain a quality signal with minimal loss.
Massive Availability of Small Data.	The shift from centralized big data to massive distributed small data.
More bits, More spectrum, and More Reliability.	Exploring higher frequency spectrum (THz), which is proposed to facilitate the actualization of 1 Tb/s.
From Self-Organizing Networks to Self-Sustaining Networks.	AI is proposed to facilitate intelligent wireless networks that are self-sustaining.
Ubiquitous connectivity that encompasses air, ground, and undersea.	6G is envisioned to integrate space-air-ground-sea mode to facilitate wireless communication in flying vehicles, XR, BCI, and more.
The emergence of Haptics and the End of Smartphone era.	The pervasive use of wearables and implants, supported by BCI and XR.

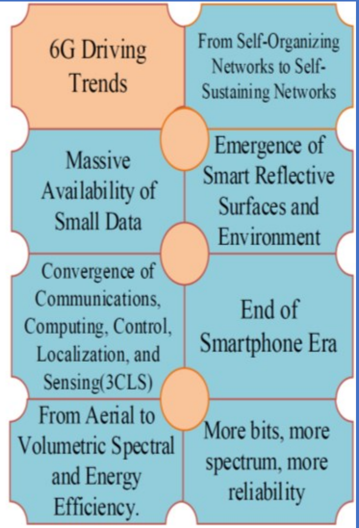


Figure 3. 6G Driving Trends.

Ref Sensors, 6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, & Research Roadmap, March 2021: 12

Samsung's 6G Vision

Today’s exponential growth of advanced Technologies such as AI, Robotics, & Automation will usher in unprecedented paradigm shifts in the Wireless Communication.

These circumstances lead to four (4) major Megatrends advancing toward 6G:

1. Connected Machines,
2. Use of AI for the Wireless Communication,
3. Openness of Mobile Communications, and
4. Increased contribution for achieving Social Goals.

Figure 1

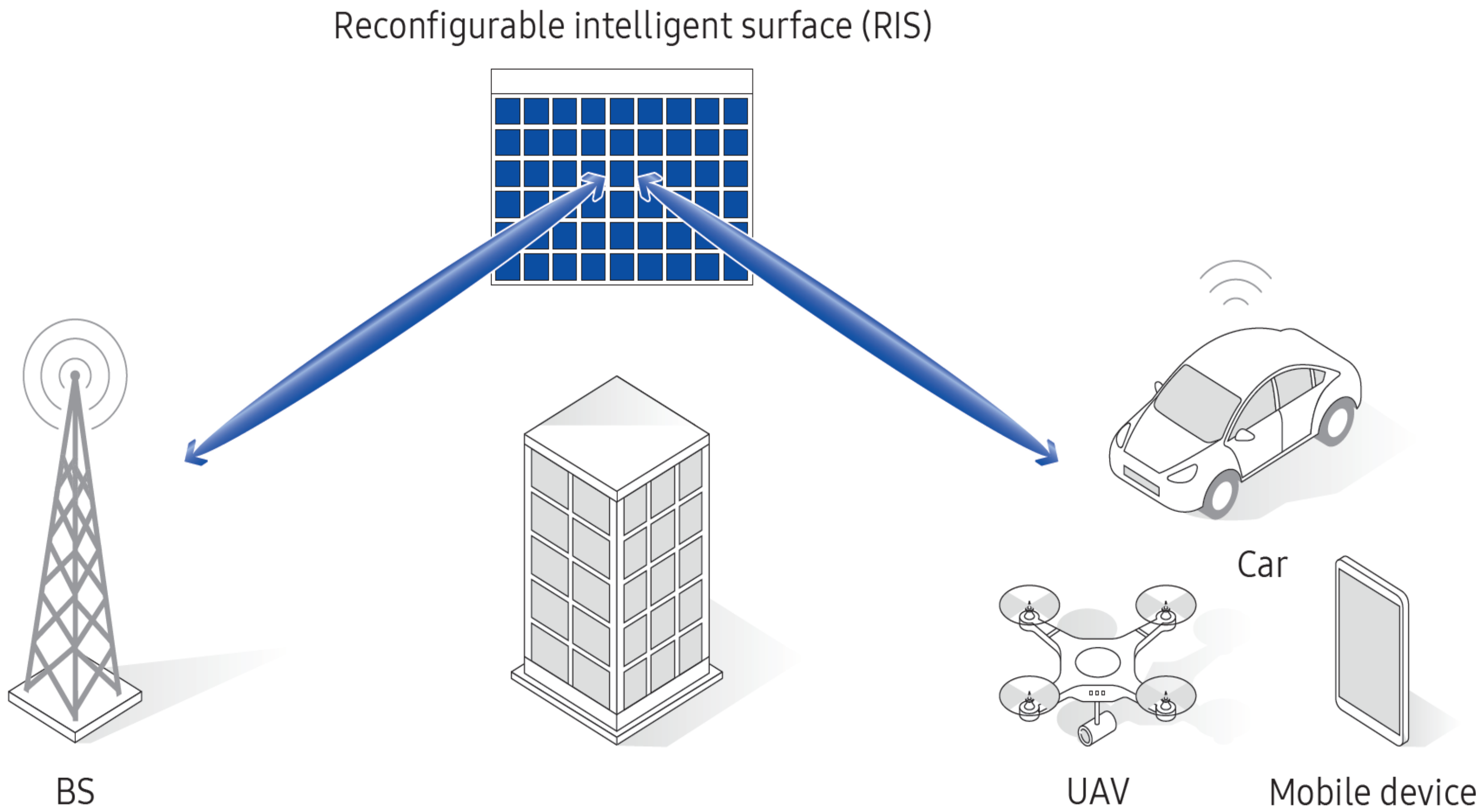
Evolution of mobile devices and connected machines.

Ref. Samsung 6G Vision July 2020: 9 - 10

- *Reconfigurable intelligent surface (RIS)* can be used to provide a propagation path where no LoS link exists [25]. An example of signal reflection via RIS is illustrated in Figure 12.

Figure 12

RIS-aided communication between a BS and a mobile user, where the LoS path is blocked.



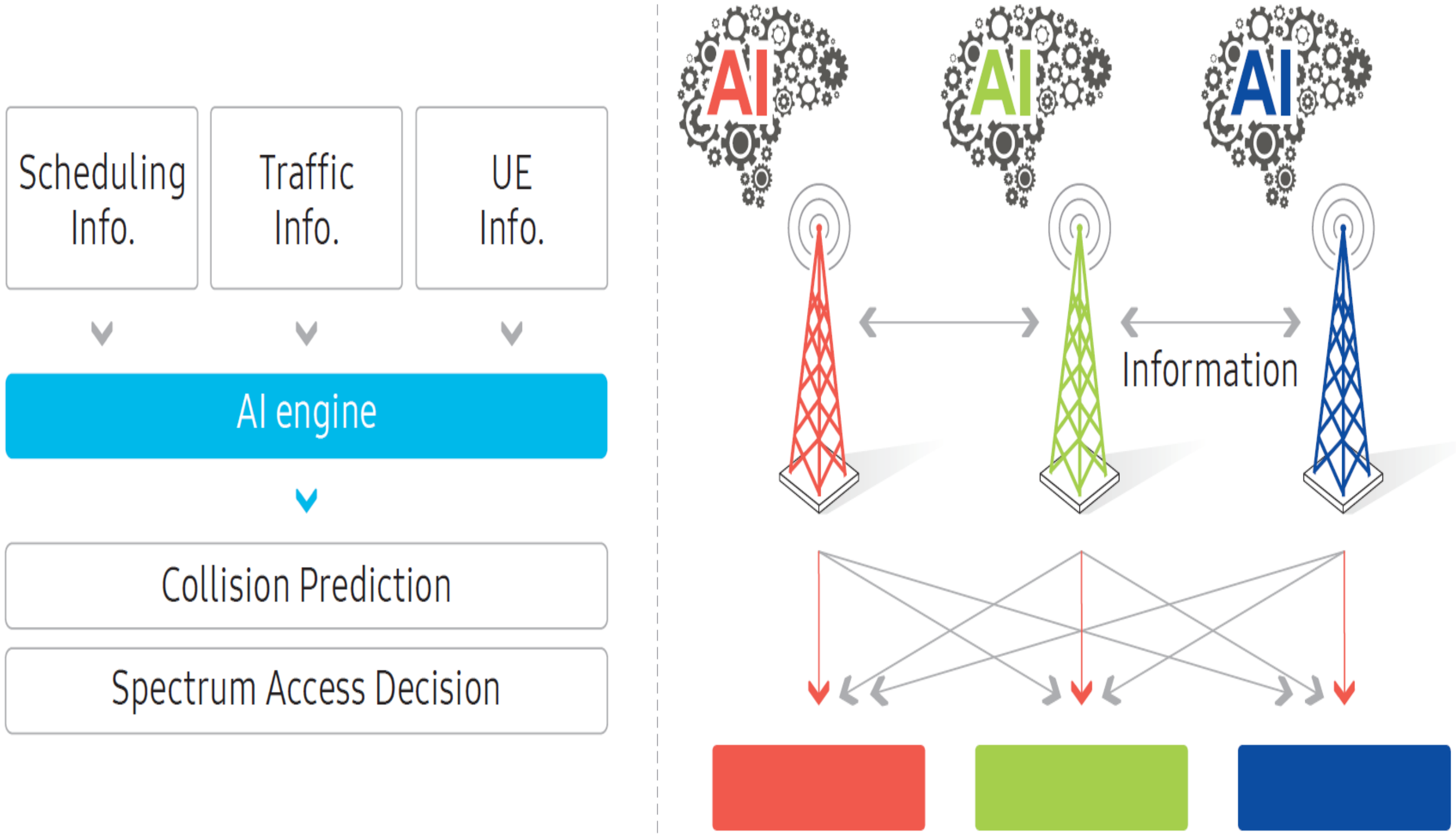
Ref. Samsung 6G Vision July 2020: 24

Evolution of Duplex Technology (DSS)

The main challenge of the Dynamic Spectrum Sharing (DSS) is avoiding (or minimizing) collision of spectrum usage among different entities while allowing them to access spectrum in a dynamic manner. Theoretically, to prevent such collisions, network operators could exchange all relevant spectrum access information. In practice, however, this would not be possible because acquiring all required information for every entity in real time would impose an enormous communication overhead. AI could avoid collisions by predicting the spectrum usage of other entities with a limited amount of information exchanged, as illustrated in Figure 18.

Figure 18

Intelligent spectrum sharing.



Ref. Samsung 6G Vision July 2020: 30 - 32

Comprehensive AI

AI receives much attention as a tool to solve problems that were previously deemed intractable due to their tremendous Complexity or the Lack of the necessary Model and Algorithm.

A comprehensive AI System to optimize the overall System Performance and Network Operation.

An overall Network Architecture consists of four (4) Tiers of Entities:

1. UE,
2. BS (BTS)
3. Core Network (CN), and
4. Application Server (AS).

Application of AI can be categorized into three (3) Levels (Fig. 19):

1) Local AI,
2) Joint AI,
3) E2E AI

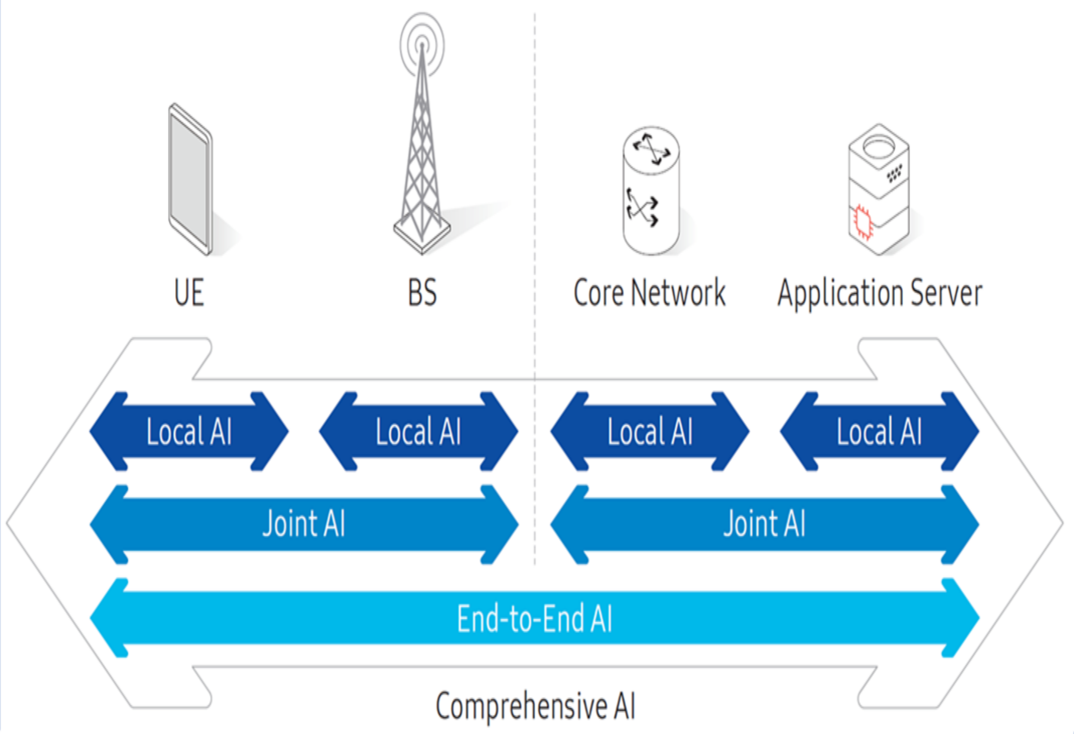


Fig. 19 Comprehensive AI System Model

There are ongoing efforts to introduce support for AI in standards.
The 3GPP) has standardized Network Data Analytics Function (NWDAF) for Data Collection & Analytics in Automated Cellular Networks.

In addition to 3GPP, the O-RAN Alliance ushers in an open & efficient RAN leveraging AI Technologies.

This effort, as we progress towards 6G, will result in Native Support of a Comprehensive AI System to realize more efficient, more reliable, & low cost communication systems.

Ref. Samsung 6G Vision July 2020: 32

Split Computing

Future applications, such as truly immersive XR, mobile holograms, and digital replica, require extensive computation capabilities to deliver real-time immersive user experience. However, it would be challenging to meet such computational requirements solely with mobile devices, especially, given that many of future mobile devices will tend to become thinner and lighter. For example, AR glasses should be as light, thin, and small as regular glasses to meet the user's expectations.

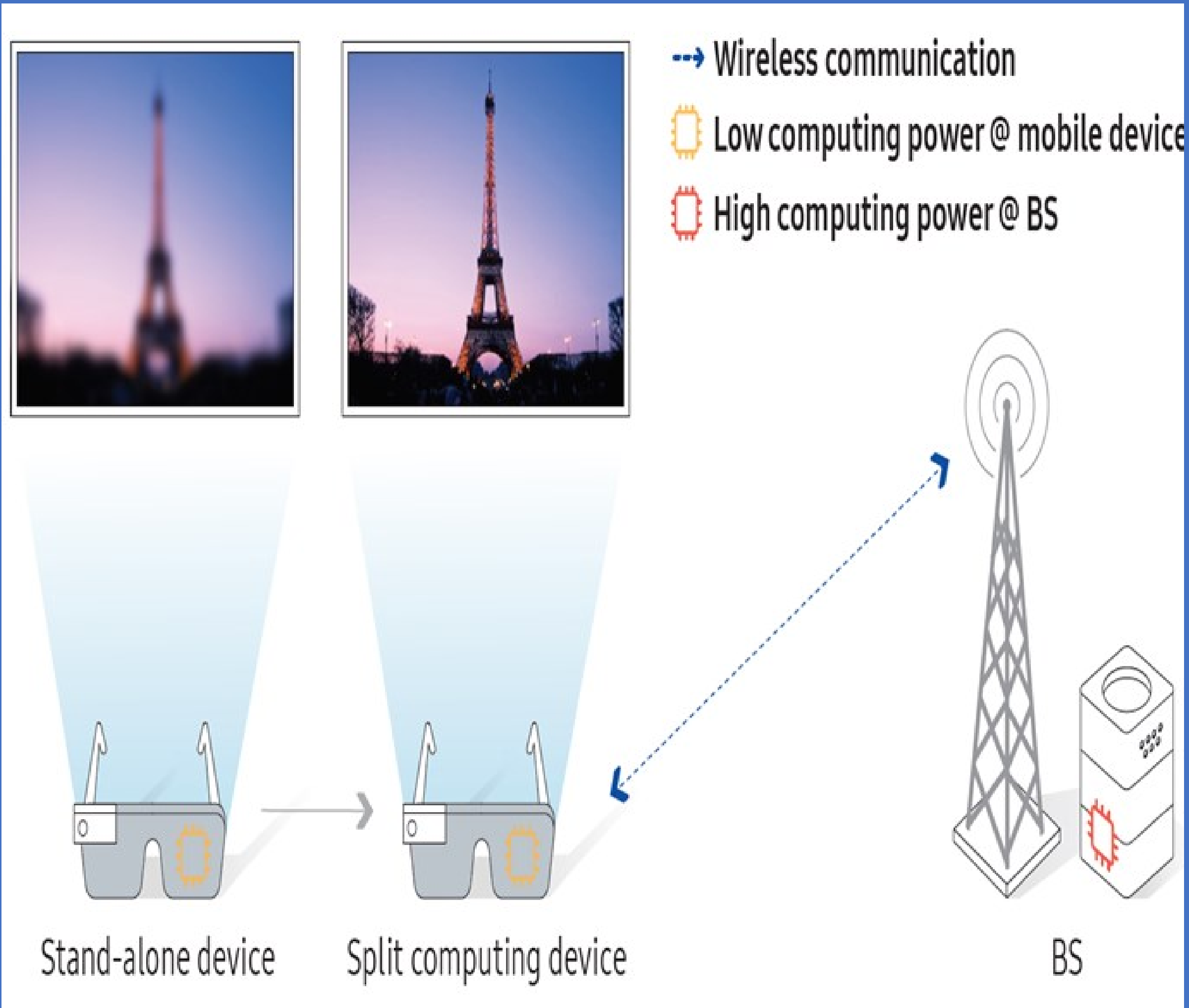


Figure 20 Split Computing

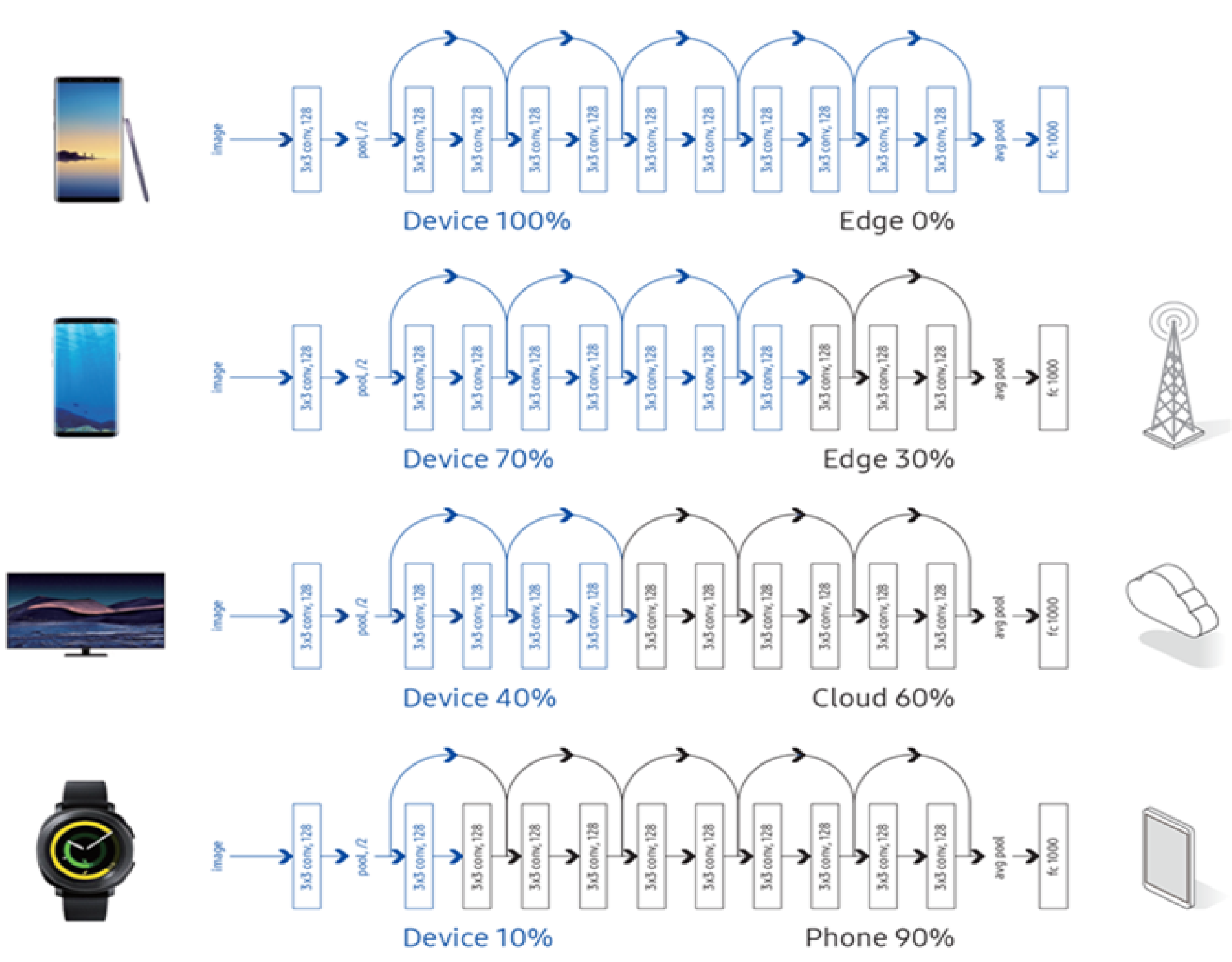
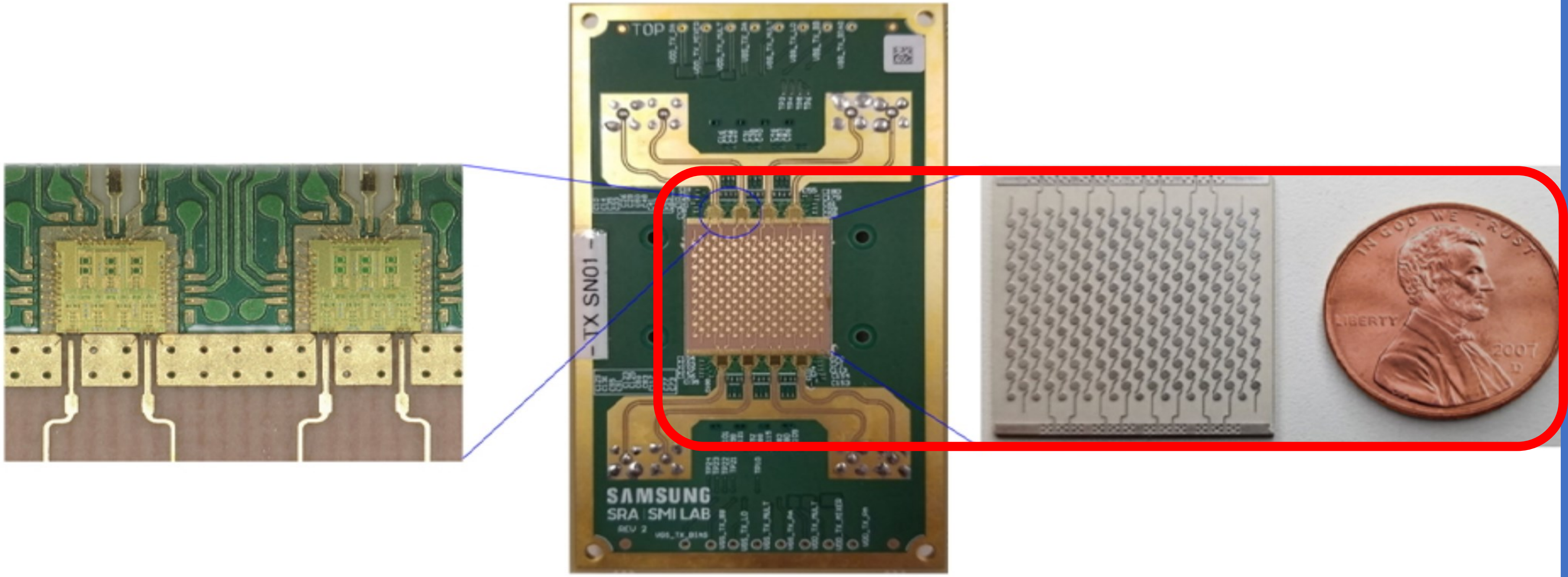


Figure 21 Examples of Split Computing by Various Devices

6G Terahertz Wireless Communication Prototype - Samsung Electronics &UCB Demonstrate

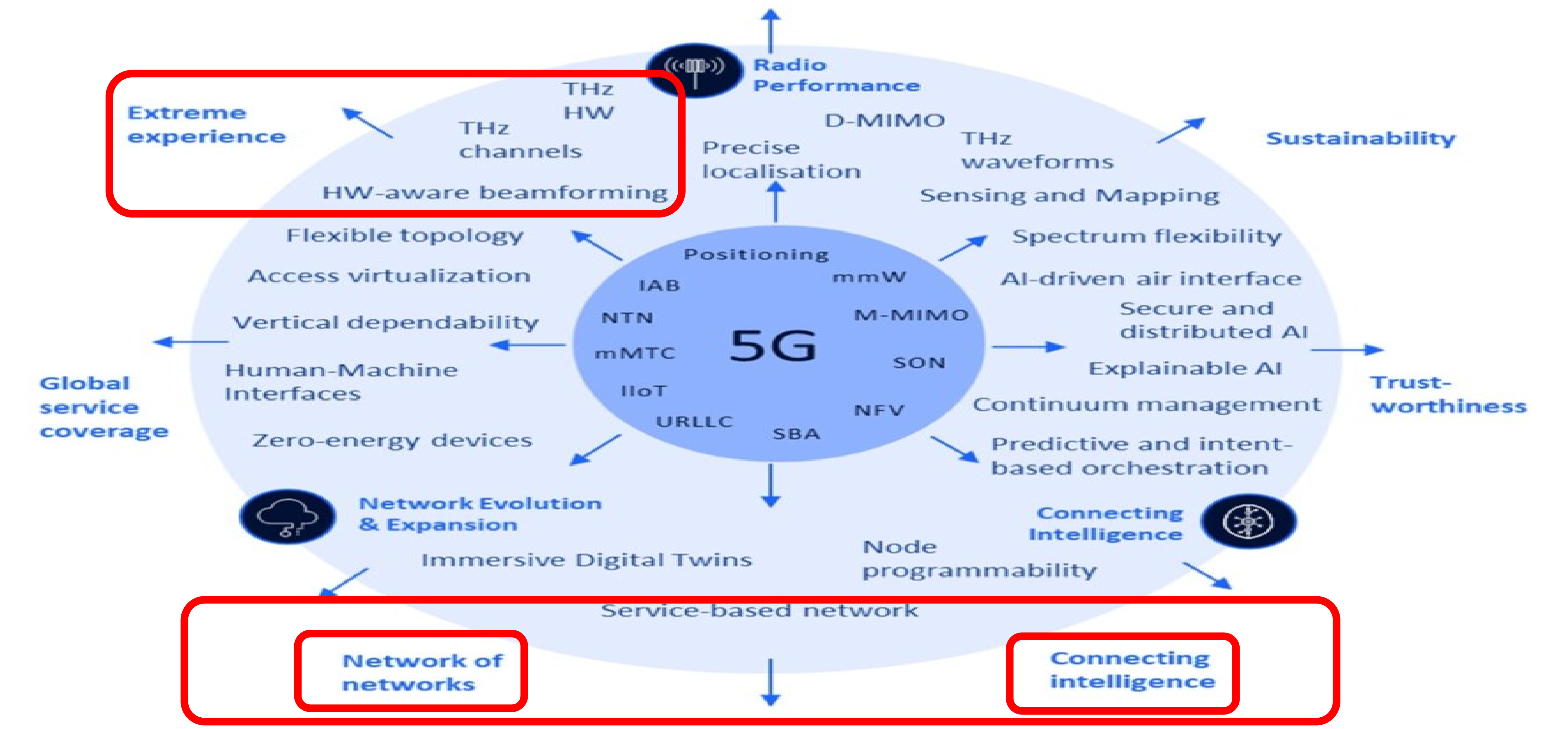
Samsung Newsroom

CORPORATE | PRODUCTS | PRESS RESOURCES | VIEWS | A



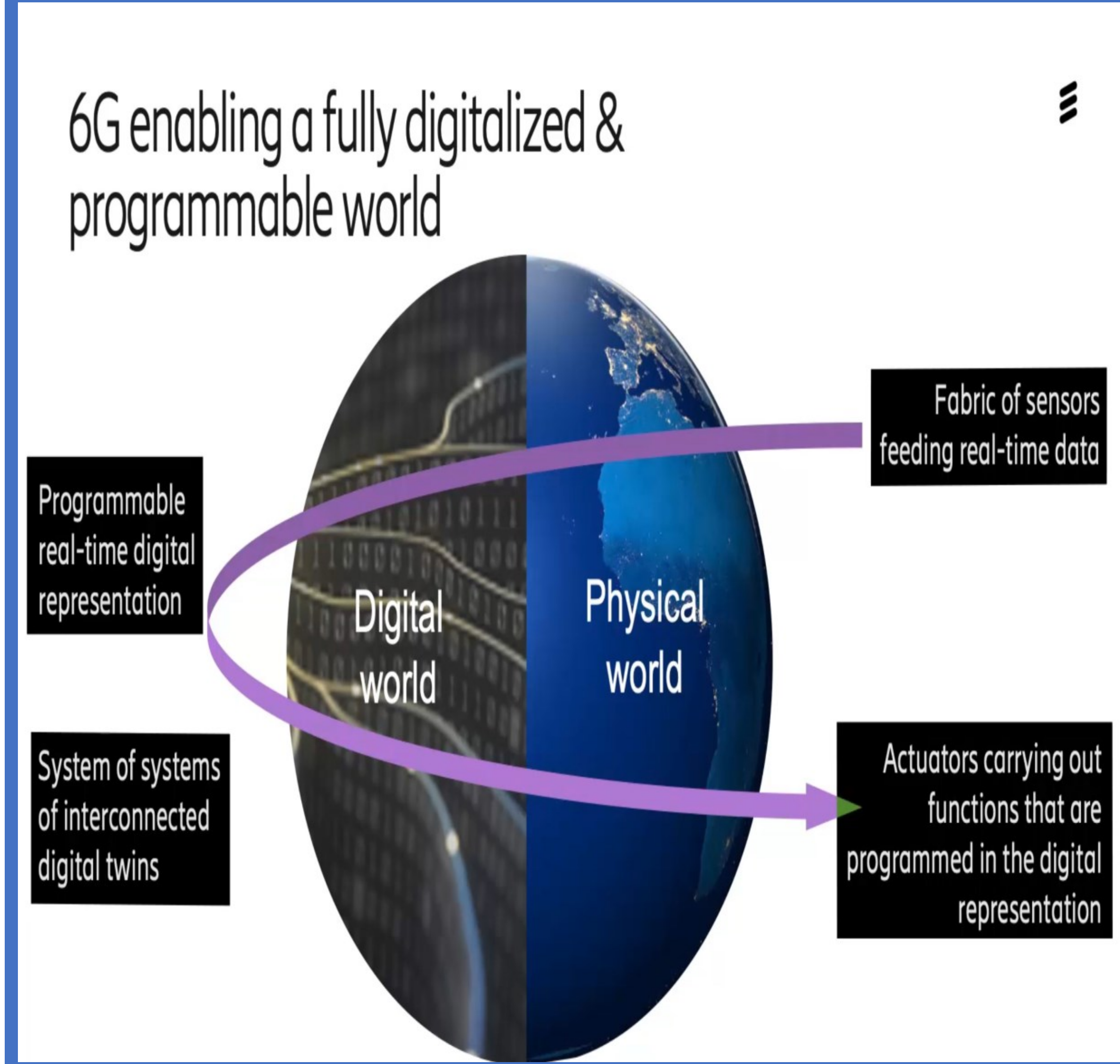
△ 16-channel 140GHz phased-array module (middle), dual-channel 140GHz RFICs (left), 128-element antenna array (right)

Technical areas to be studied



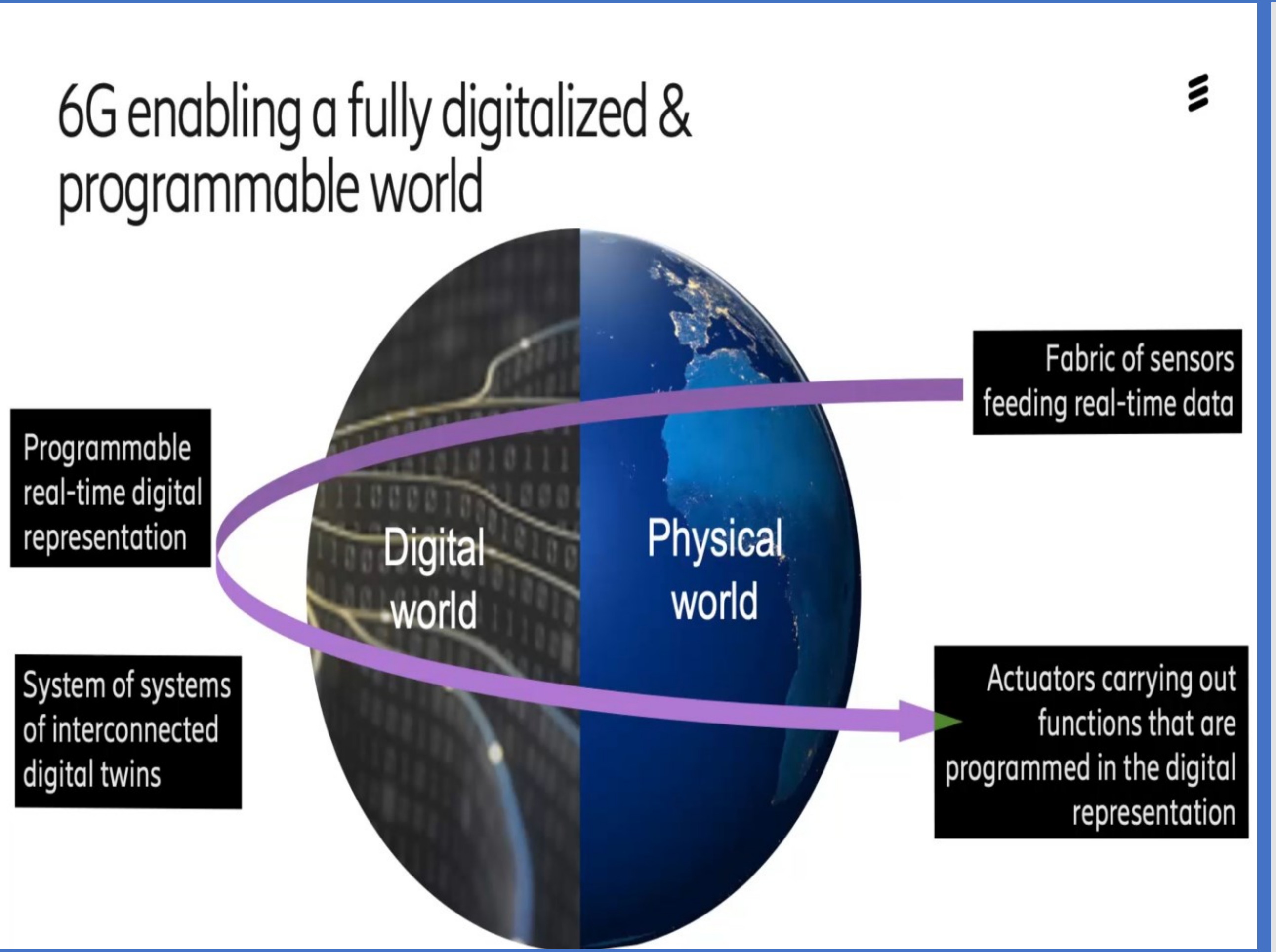
Ref. Ericsson, "Hexa X-The Joint European Initiative to shape 6G", Vetter P., Nokia & Frodigh, M, Ericsson, June 2021,

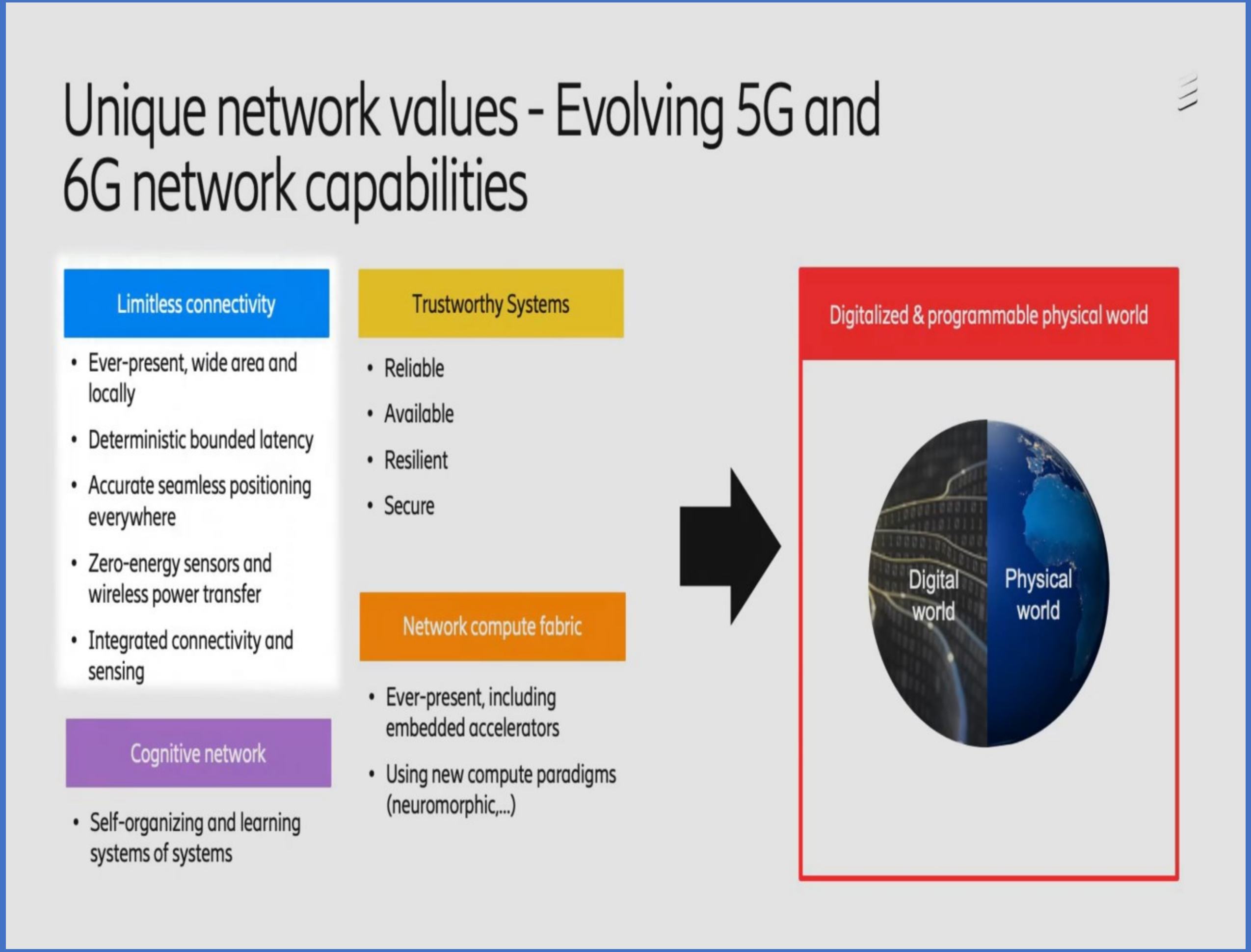
6G Vision - 1



Ref. 5G++ Summit in Drezden, Magnus Frodigh Keynotes, May 2021

Ericsson 6G Vision - 2





Ref. 5G++ Summit in Drezden, Magnus Frodigh Keynotes, May 2021

5G System as a DetNet Node: 5G Advanced for 5G System interworking with IETF DetNet (Deterministic Networking) Architecture specification

5G Advanced release proposes an enhanced Architecture that supports the interworking between 5G System (5GS) & IETF specified DetNet (Deterministic Networking) Architecture with the goal to achieve Deterministic Forwarding Mechanism in 5G Mobile Network. The 5GS supports IETF DetNet by abstracting the whole 5GS as a "DetNet Node" (shown below). The Architecture is based on 5GS QoS Framework, & maps the DetNet flow (through DetNet YANG model) to 5GS QoS flow (shown in Fig. below). It supports DetNet IP Data Plane & Forwarding Sub-Layer Operations with specific QoS & Management Capabilities that are exposed to DetNet Controller. No UE impact is required. While the UE is logically part of the 5GS DetNet Node, the Device including the UE may also act as a separate DetNet Capable IP Router Node. The 5GS supports the DetNet Node Functions & DetNet Forwarding Sub-Layer related Functions except for Service Sub-Layer Functions. It uses DetNet Flow-Related Parameters from the DetNet Controller as DetNet Configuration Parameters for DetNet Traffic. DetNet Controller determines the E2E Path & ensures the E2E Requirements of the DetNet flow & 5GS should strictly ensure the Requirements as e.g. - The DetNet IP flow description identifies the DetNet flow & can be mapped to Packet Filter Set under 5GS QoS Framework (extended in TSCTSF) & using the following methods: - The Minimum Guaranteed Bandwidth is mapped to GFBR in QoS Profile. - The Maximum Delay is mapped to 5QI-PDB in QoS profile. - The Maximum Packet Loss is mapped to 5QI-Error Rate in QoS Profile. The TSCTSF converts DetNet Configuration Parameters for DetNet Traffic into 5GS QoS Parameters & TSCAI, such as Interval into Periodicity & MaxPacketsPerInterval & MaxPayloadSize combined into MDBV. Due to the lack of any minimum values for Payload Size or Packets in the 5GS, MinPayloadSize & MinPacketsPerInterval cannot currently be mapped into 5G Parameters. In DnFlowRequirements, the MaxLatency, MaxLatencyVariation, MaxLoss, MaxConsecutiveLossTolerance, & MaxMisordering attributes specify Requirements not in a Single DetNet Node but throughout the DetNet Flow Path. 5GS provisions & enables DetNet Node DnFlowRequirements as specified in IETF DetNet Architecture. Currently, the 5GS may allow for the translation of MinBandwidth to GFBR, MaxLatency to PDB, & MaxLoss to PER.

DetNet defines the Packet Replication, Elimination, & Ordering Functions (PREOF) as a way to provide Service protection (through) 4 Capabilities, such as: 1. Sequencing information, by adding a Sequence Nr or Time Stamp as part of DetNet (typically done once, at or near the Source). 2. Replicating Packets into Multiple DetNet Member Flows, & sending them along Multiple Different Paths to the Destination(s). 3. Eliminating Duplicate Packets of a DetNet Flow based on the Sequencing Information & a History of Received Packets. 4. Reordering DetNet Flow's Packets that are received out of order. Packet (Hybrid) ARQ, Replication, Elimination and Ordering (PAREO) is a superset of DetNet's PREOF, defined in RAW (Reliable & Available Wireless), that includes Radio-specific Techniques such as Short-range Broadcast, MU-MIMO, Constructive Interference & Overhearing, which can be leveraged separately or combined to increase the Reliability. There multiple Scenarios & UCs that might involve Multiple Technologies &/or Administrative Domains in DetNet & RAW, e. g. several UCs, where Service "Reliability" & "Availability" are imperative.

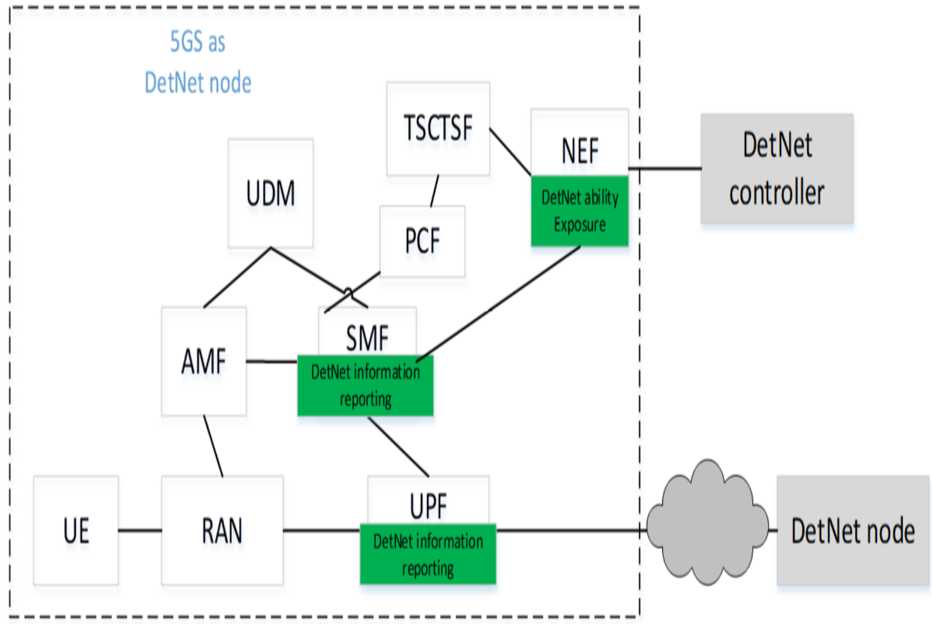


Figure: 5G System (as DetNet Node) Enhanced Architecture and Network Function (NF)

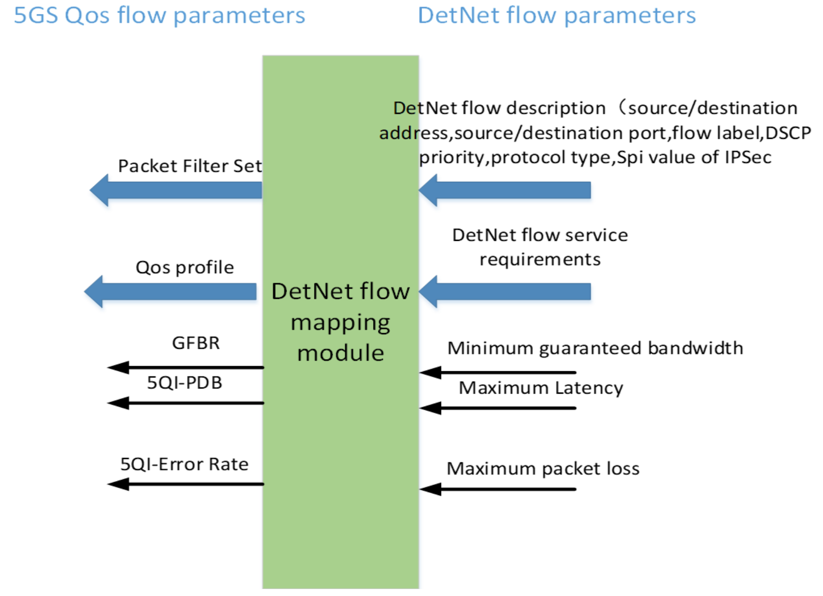


Figure: 5GS QoS Management Framework mapping with DetNet flow using the TSCTSF (Time Sensitive Communication and Time Synchronization Function)

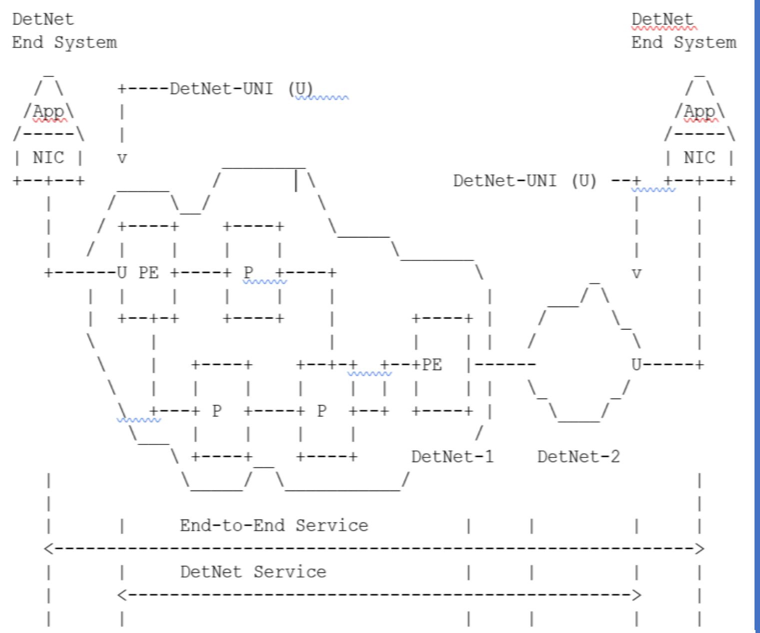


Figure: DetNet Architecture Multidomain Service Reference Model

5G System as a DetNet Node: 5G System interworking (integrated) with Deterministic Networking (DetNet) Architecture specification
An enhanced Architecture supporting the reporting of Mobile Network information to DetNet Control Layer is designed. 5G System report corresponding information to the DetNet Control Plane (CP) to assist the DetNet CP. **The Architecture enhances the Network Functions (NFs) of NEF, SMF, & UPF respectively, so as to support the Information Collection, Subscription & Reporting of DetNet Capability.**

Provisioning DetNet (Deterministic Networking) Configuration from the DetNet Controller to 5GS(System) - see Clause on mapping the End to End (E2E) Requirement to per Node requirement.

- Max-Latency to Required Delay.
- Min-Bandwidth to GFBR (Guaranteed Flow Bit Rate).
- Max-loss to Required PER (Packet Error Rate) (new in Rel-18).
- Max-Consecutive-Loss-Tolerance to Survival Time - when such mapping is possible, such as when there is only a Single Packet per Interval. Interval to Periodicity in TSC (Time-Sensitive Communication) info.
- Max-pkts-per-Interval * (Max-payload-Size + Protocol Header Size) to Max Burst Size.
- Max-pkts-per-Interval * (Max-payload-Size + Protocol Header Size)/ Interval to MFBR (Maximum Flow Bit Rate).
- DetNet Flow specification to 3GPP Flow description (also incl. the DSCP value & optionally IPv6 Flow label & IPsec SPI.

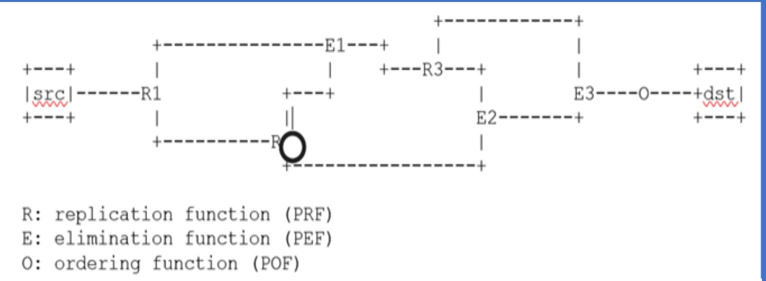


Figure: DetNet PREOF (Packet Replication, Elimination & Ordering Function) in a DetNet Network

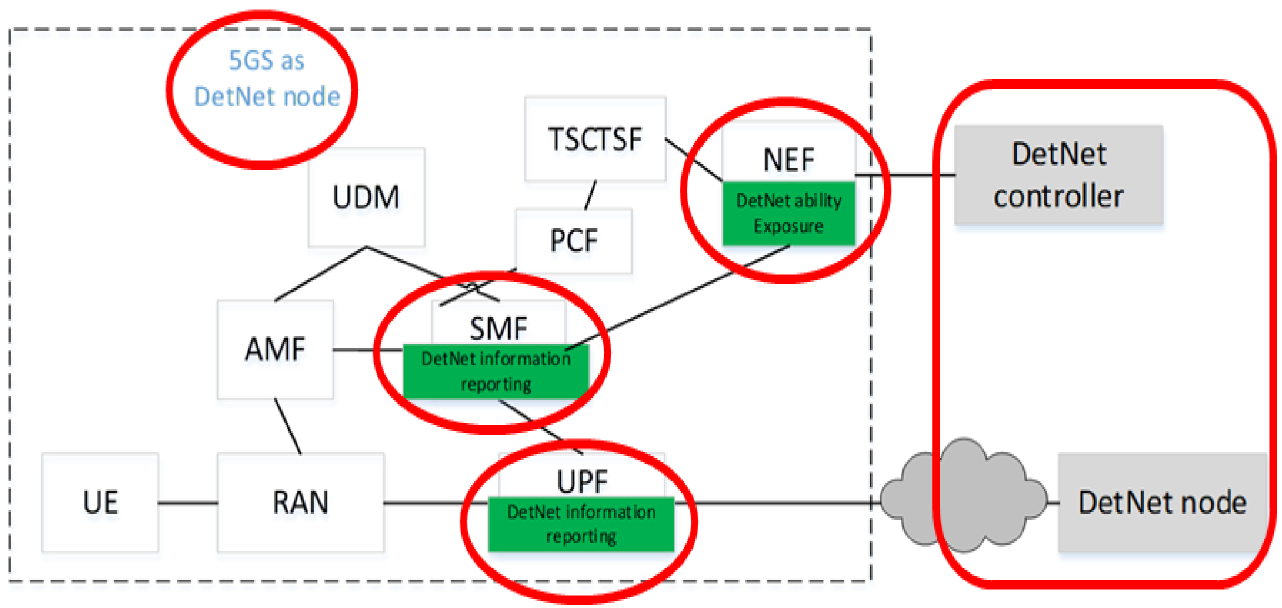


Figure: 5G System (as DetNet Node) Enhanced Architecture and Network Function (NF) to support 5GS DetNet Node reporting

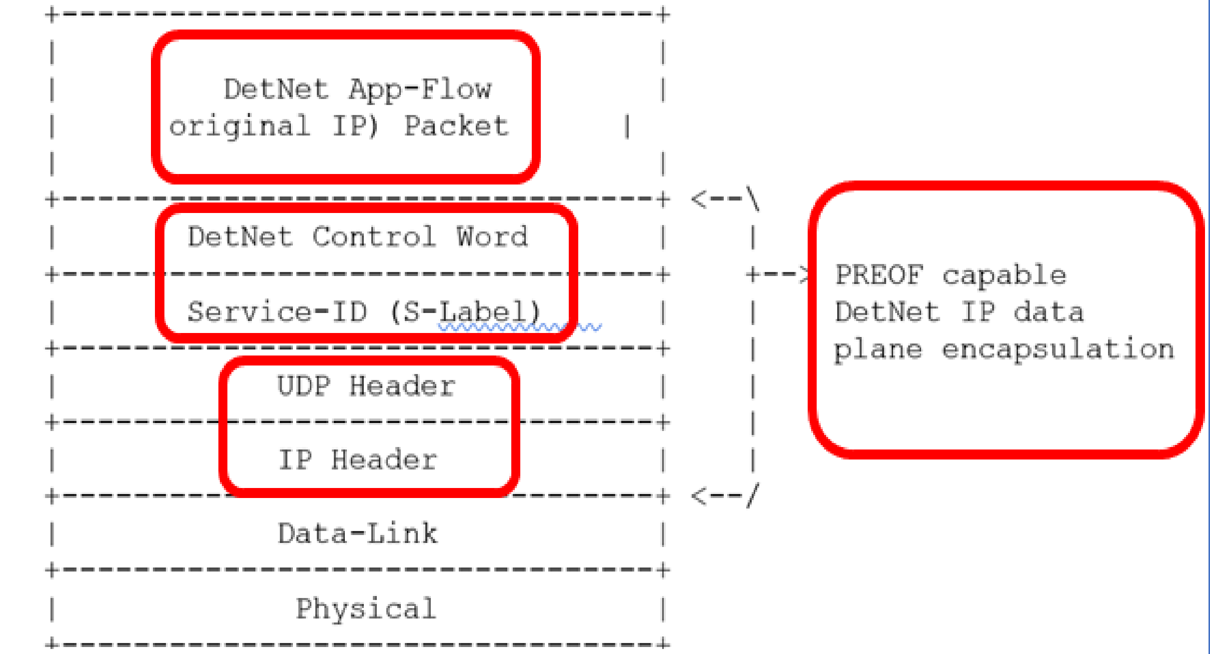
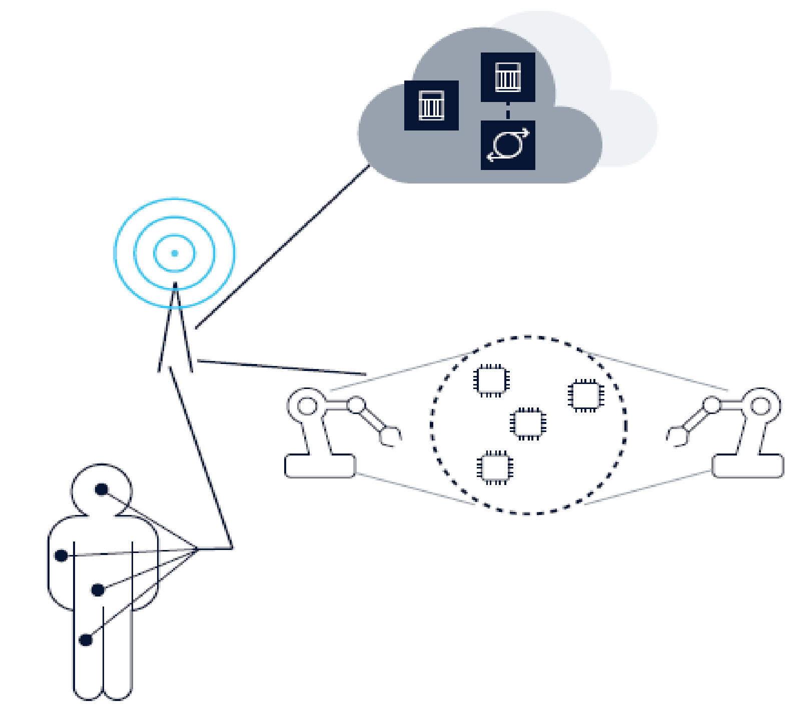


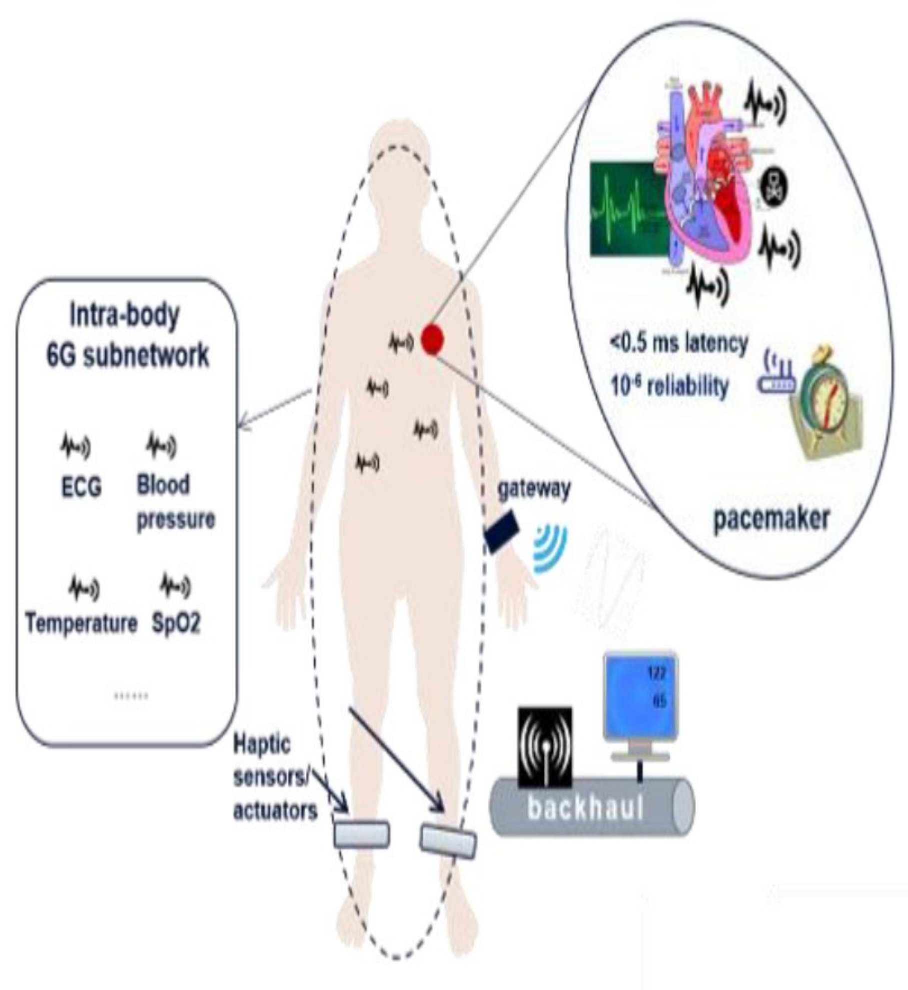
Figure: DetNet PREOF capable DetNet IP encapsulation

Sensing Networks, EHAW, BANs, PIoT/PINs

1



End point is a network



ericsson.com Products and solutions Discover Transforming enterprises Future technologies

Welcome to the internet of senses

Ref. Ericsson, 10 Hot Consumer Trends 2030, Dec 2019

10 Hot Consumer Trends 2030

Welcome to the internet of the senses.

01. Your brain is the user interface

Fifty-nine percent of consumers believe that we will be able to see map routes on VR glasses by simply thinking of a destination.

02. Sounds like me

Using a microphone, 67 percent believe they will be able to take on anyone's voice realistically enough to fool even family members.

03. Any flavor you want

Forty-five percent predict a device for your mouth that digitally enhances anything you eat, so that any food can taste like your favorite treat.

04. Digital aroma

Around 6 in 10 expect to be able to digitally visit forests or the countryside, including experiencing all the natural smells of those places.

05. Total touch

More than 6 in 10 expect smartphones with screens that convey the shape and texture of the digital icons and buttons they're pressing.

06. Merged reality

VR game worlds are predicted by 7 in 10 to be indistinguishable from physical reality by 2030.

07. Verified as real

"Fake news" could be finished – half of respondents say news reporting services that feature extensive fact checks will be popular by 2030.

08. Post-privacy consumers

Half of respondents are "post-privacy consumers" – they expect privacy issues to be fully resolved so they can safely reap the benefits of a data-driven world.

09. Connected sustainability

Internet of senses-based services will make society more environmentally sustainable, according to 6 in 10.

10. Sensational services

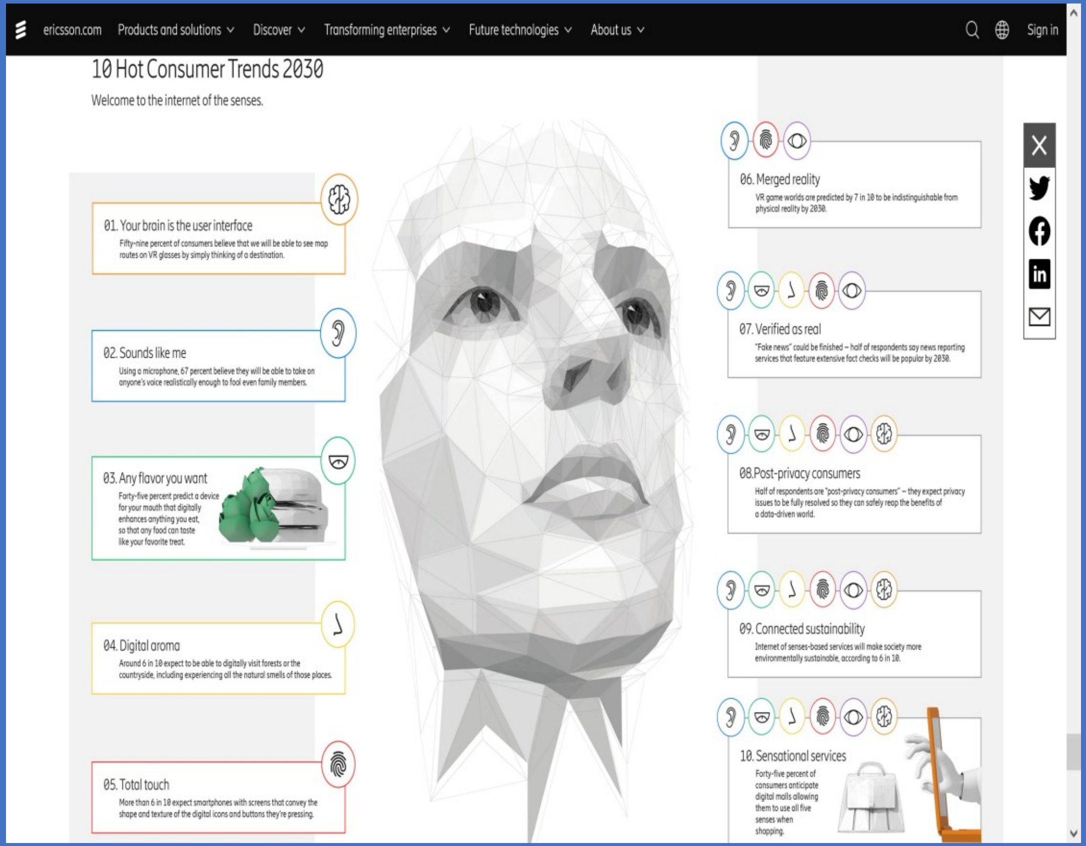
Forty-five percent of consumers anticipate digital malls allowing them to use all five senses when shopping.

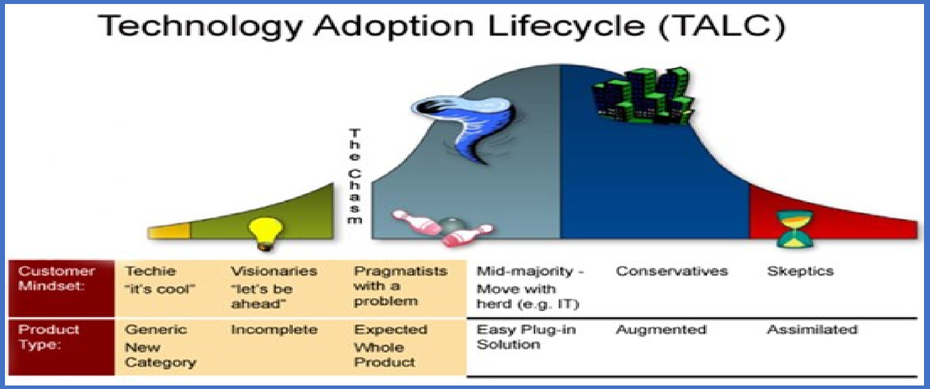
Methodology

The Quantitative Results referred to in the Report are based on an **Online Survey of Residents** in Bangkok, Delhi, Jakarta, Johannesburg, London, Mexico City, Moscow, New York, San Francisco, São Paulo, Shanghai, Singapore, Stockholm, Sydney and Tokyo, carried out in October 2019.

The **Sample** consists of at least **500 Respondents from each city (12,590 respondents were contacted in total, out of whom 7,608 qualified), aged 15–69, who currently are either regular users of augmented reality (AR), virtual reality (VR) or virtual assistants, or who intend to use these technologies in the future.**

Correspondingly, **they represent only 46 million citizens out of 248 million living in the metropolitan areas surveyed, and this, in turn, is just a small fraction of consumers globally**. However, we believe their early adopter profile makes them important when exploring expectations on technology for the next decade.

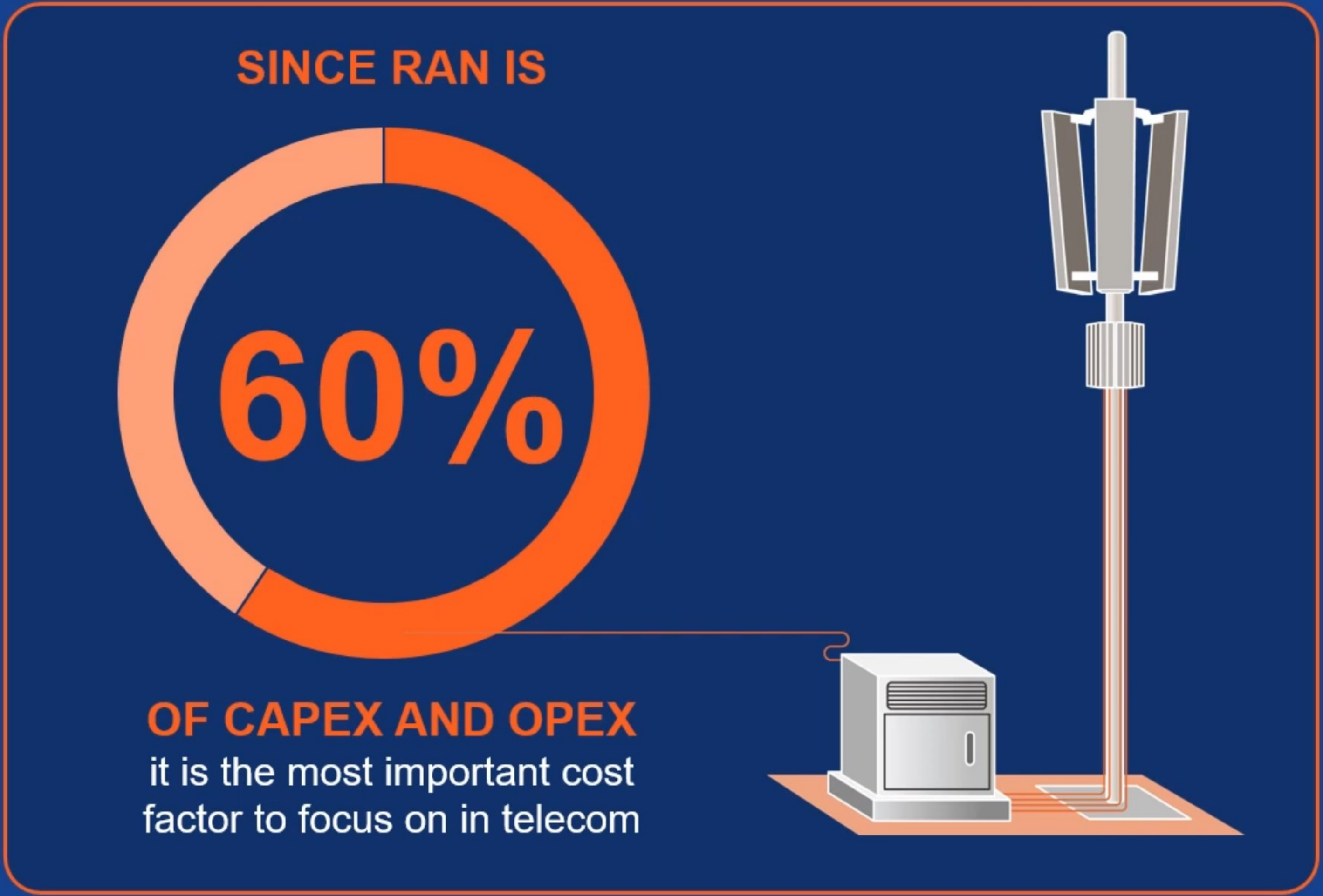




Ref. Ericsson, 10 Hot Consumer Trends 2030, Dec 2019

WHY OPENRAN?

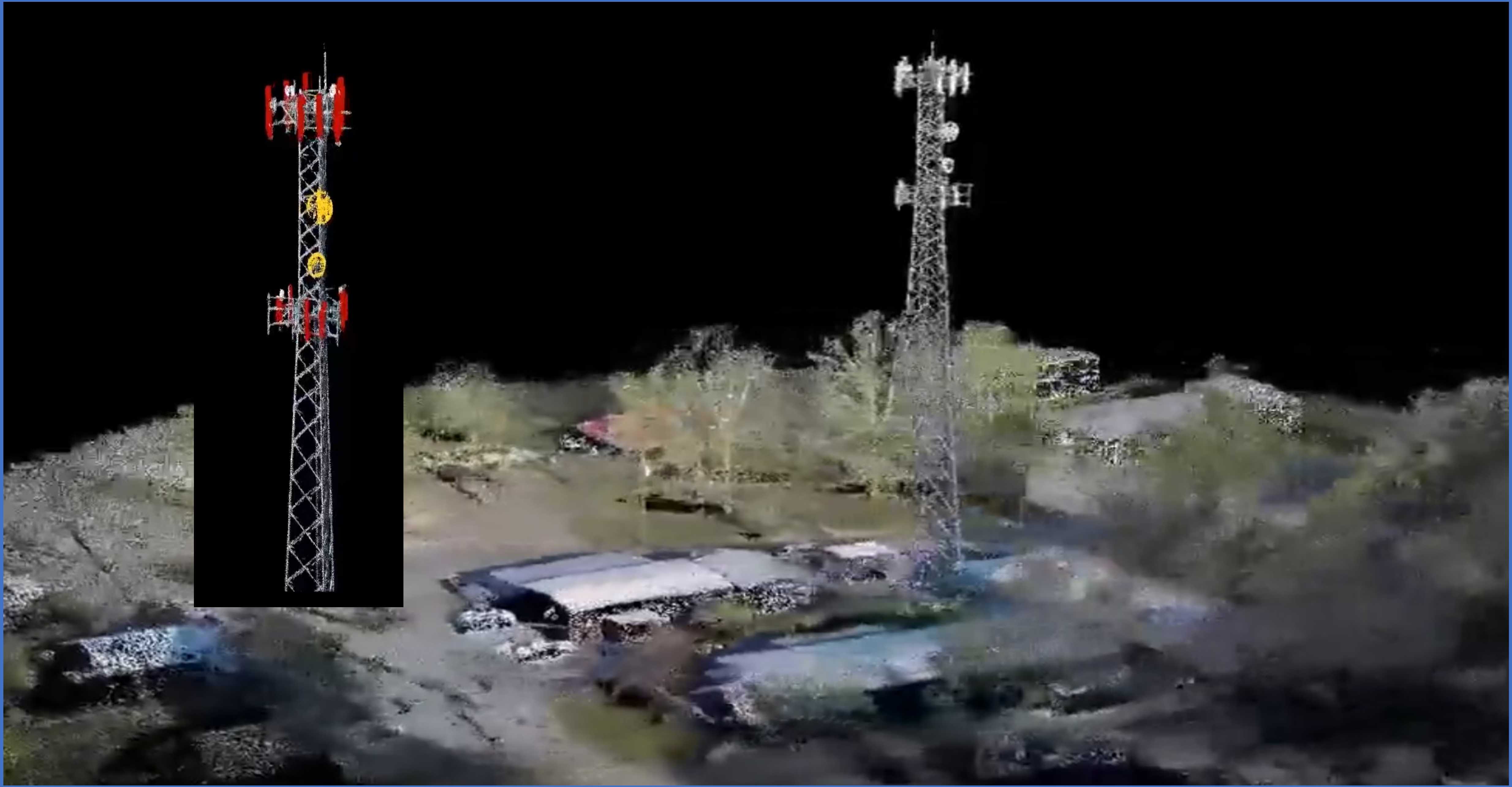
The Facebook TIP Open Compute Initiative started the movement towards OpenRAN–



Ericsson 6G Vision

Ref. 5G++ Summit in Drezden, Keynotes, May 2021

Ericsson 6G Vision - use of Digital Twins for RAN sites



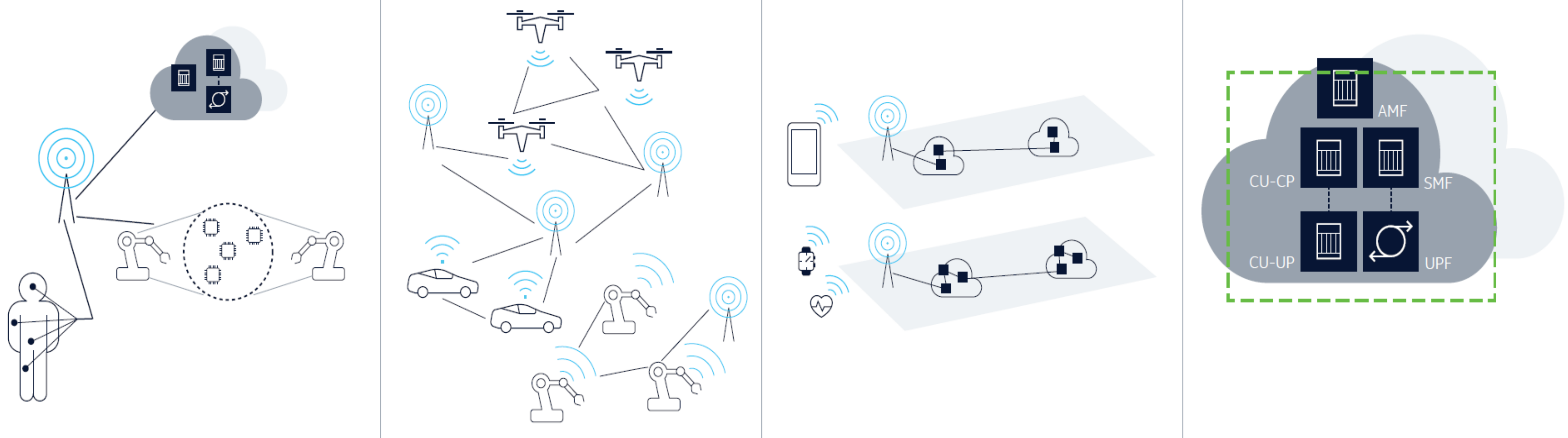
Ref. 5G++ Summit in Drezden, Keynotes, May 2021

1

3

2

6G Architecture Themes



End point is a network

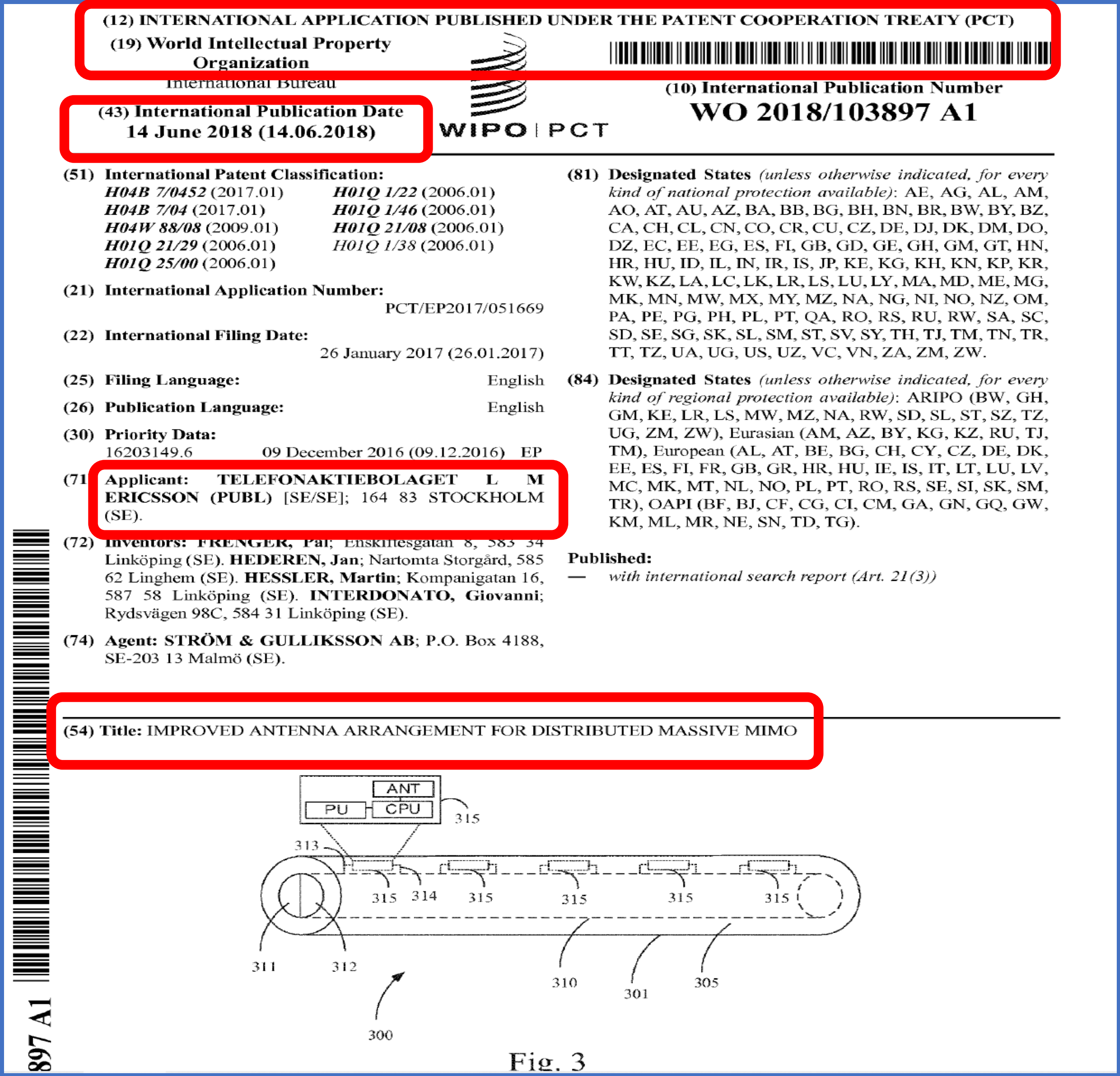
Cell free/mesh

Hyper-specialized slicing

RAN-Core convergence

Ref., Nokia, Communications in the 6G Era, WP, Aug., 2020:15

Cell-free Massive MIMO - Improved Antenna Arrangement for Distributed Massive MIMO - Cell - free Architecture with Radio es



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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2018 (14.06.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/103897 A1

(51) International Patent Classification:
H04B 7/0452 (2017.01) *H01Q 1/22* (2006.01)
H04B 7/04 (2017.01) *H01Q 1/46* (2006.01)
H04W 88/08 (2009.01) *H01Q 21/08* (2006.01)
H01Q 21/29 (2006.01) *H01Q 1/38* (2006.01)
H01Q 25/00 (2006.01)

(21) International Application Number: PCT/EP2017/051669

(22) International Filing Date: 26 January 2017 (26.01.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16203149.6 09 December 2016 (09.12.2016) EP

(71) Applicant: TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) [SE/SE]; 164 83 STOCKHOLM (SE).

(72) Inventors: FRENGER, Pål; Enskiftesgatan 8, 583 34 Linköping (SE). HEDEREN, Jan; Nartomta Storgård, 585 62 Linghem (SE). HESSLER, Martin; Kompanigatan 16, 587 58 Linköping (SE). INTERDONATO, Giovanni; Rydsvägen 98C, 584 31 Linköping (SE).

(74) Agent: STRÖM & GULLIKSSON AB; P.O. Box 4188, SE-203 13 Malmö (SE).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

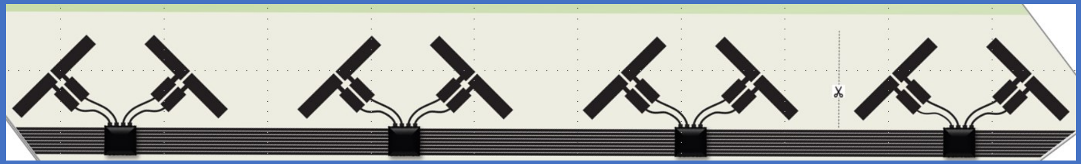
(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) Title: IMPROVED ANTENNA ARRANGEMENT FOR DISTRIBUTED MASSIVE MIMO

Fig. 3

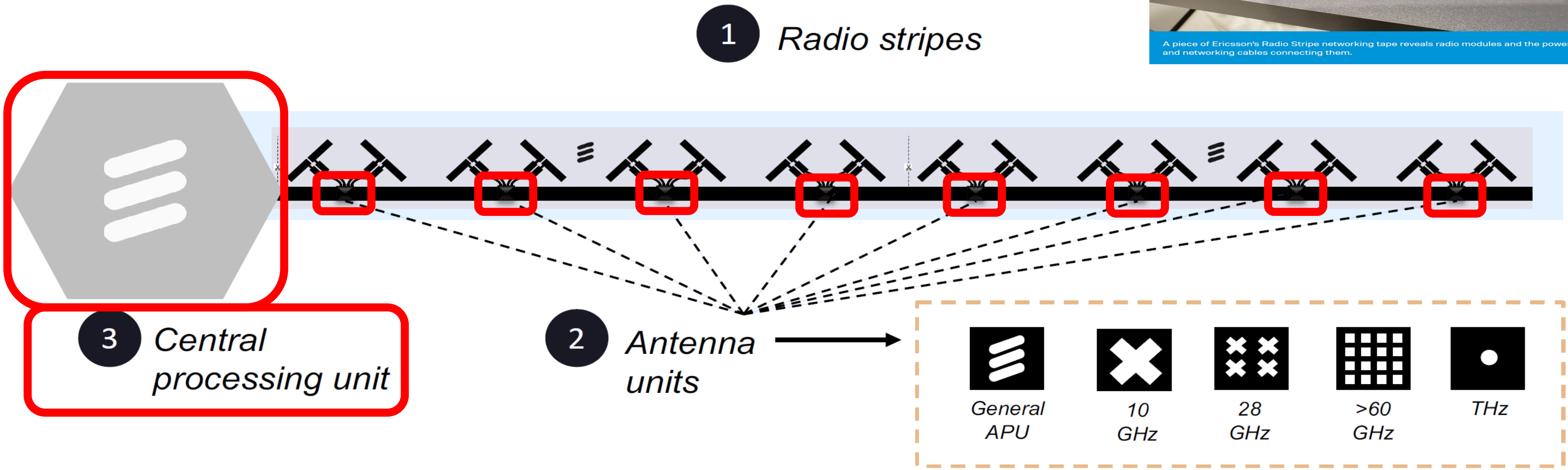
897 A1



A piece of Ericsson's Radio Stripe networking tape reveals radio modules and the power and networking cables connecting them.

Implementation Architecture: Radio Stripes


A piece of Ericsson's Radio Stripe networking tape reveals radio modules and the power and networking cables connecting them.

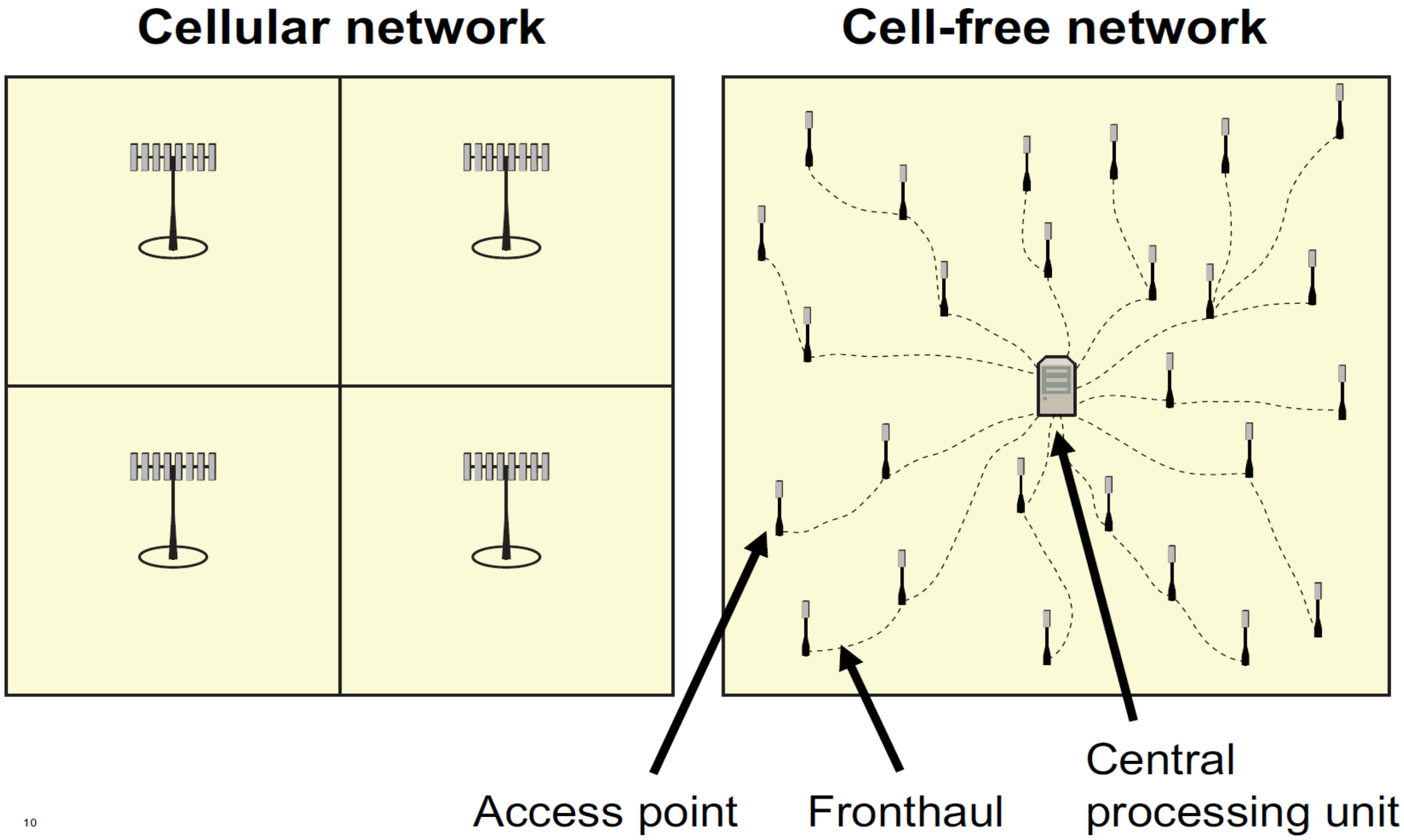


Can create as long stripes as we need

LINKÖPING UNIVERSITY

ERICSSON

Moving Beyond the Cellular Paradigm



Massive number of distributed antennas:

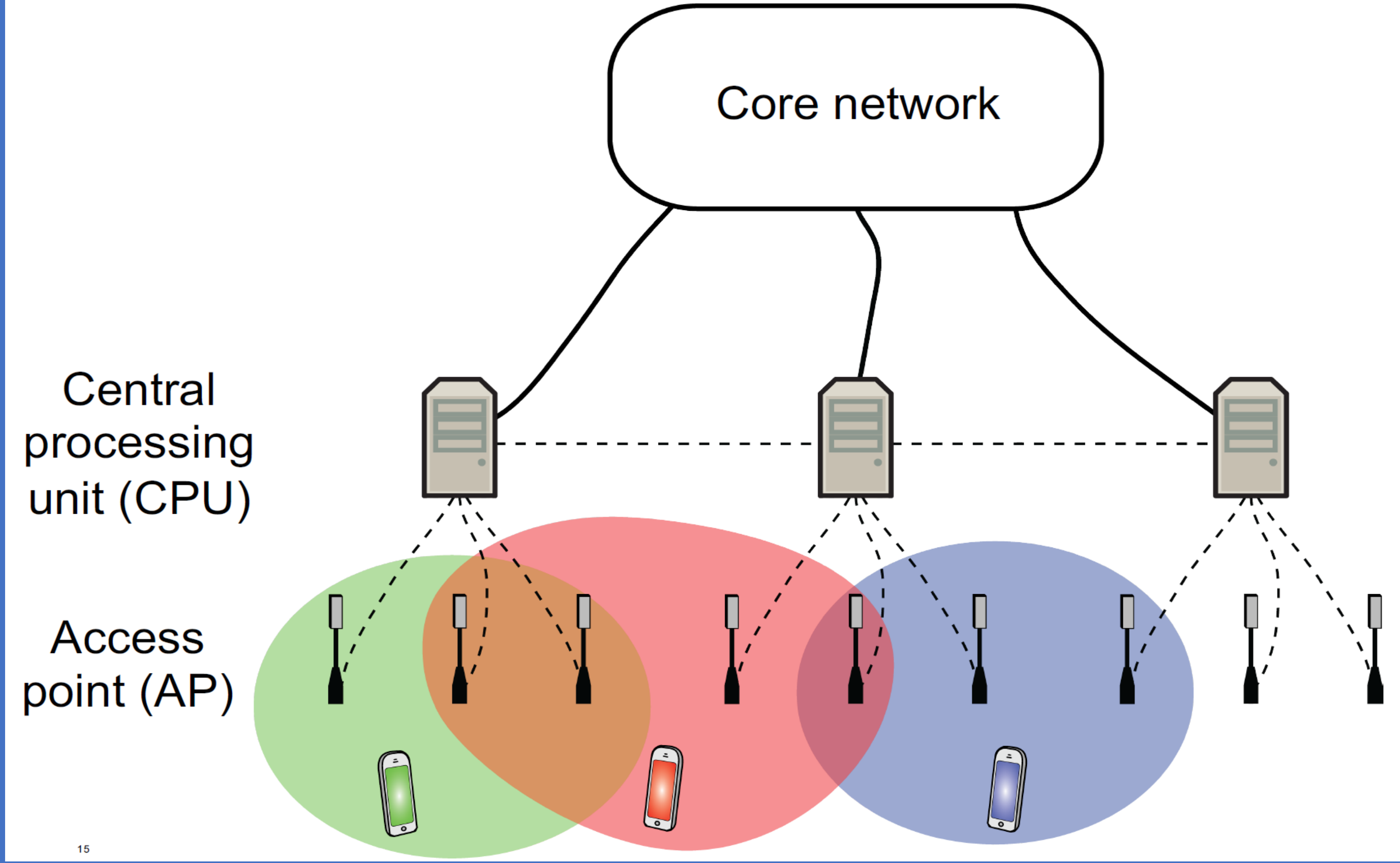
Short distance from user to some antennas

Connection to Massive MIMO:

$M \gg K$

M antennas, K users

Signal Processing: Centralized versus Distributed



Processing tasks
Channel estimation
Precoding/combining
Data en-/de-coding

Centralized version
Every done at a CPU

Distributed version
Most processing at AP, fusing of signals at a CPU

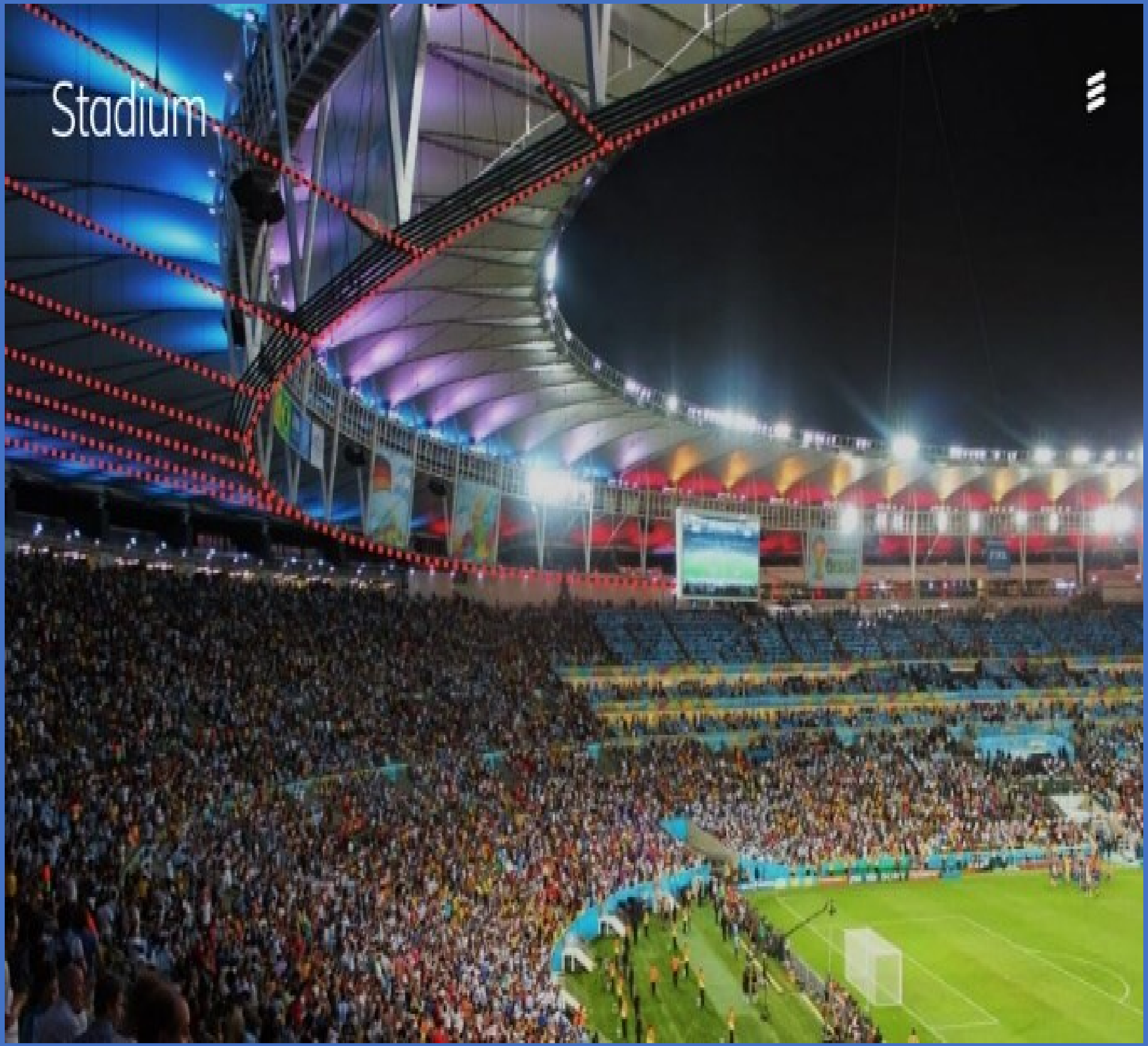
Ericsson Cell Free Radio Stripes

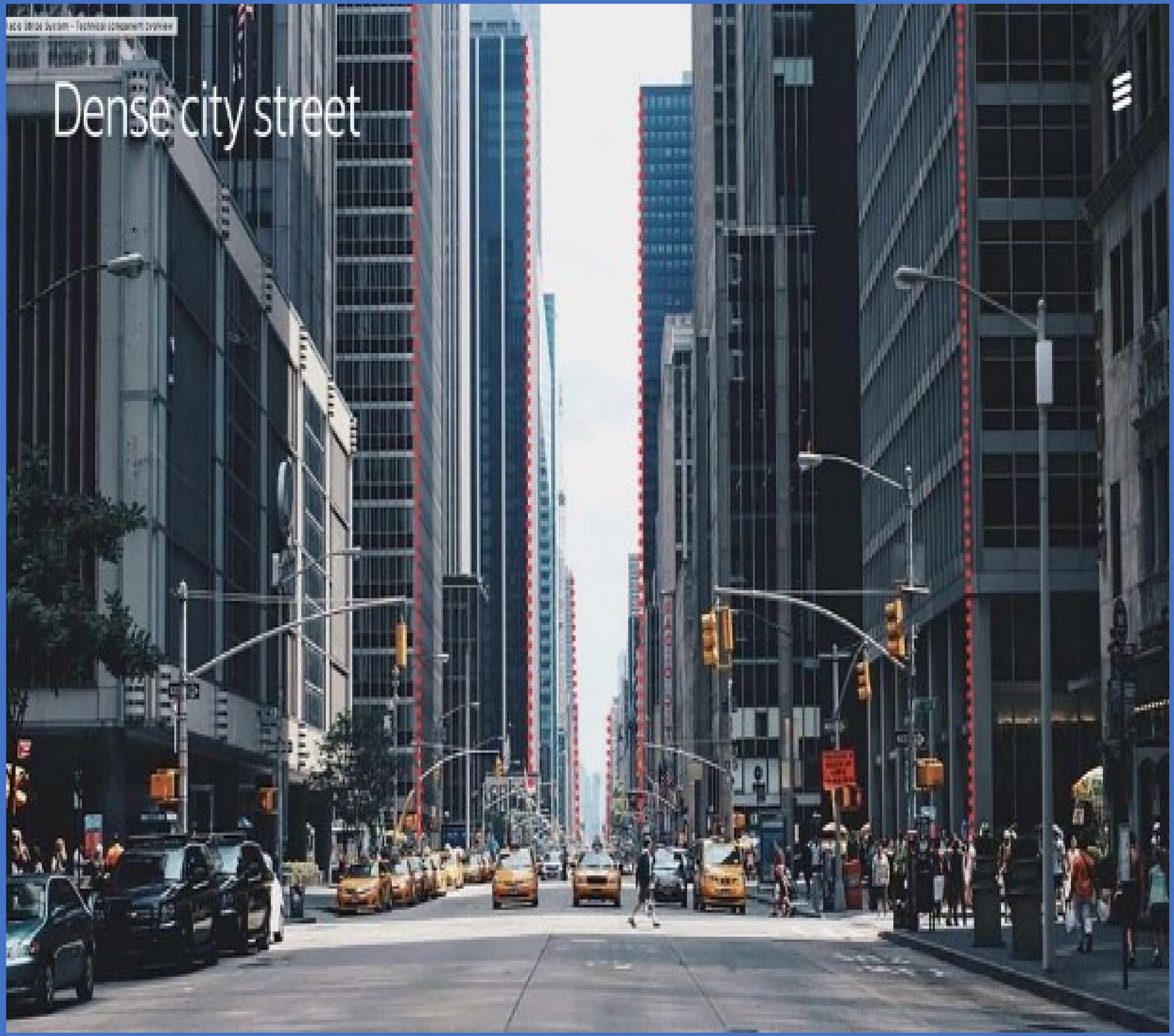
Pål Frenger, Radio Network Energy Performance Manager at Ericsson Research

A piece of Ericsson's Radio Stripe networking tape reveals radio modules and the power and networking cables connecting them.

Ref. Digital Trends, Ericsson 5G Radio Stripe Network MWC 2019&
Linköpings Universitet, Wireless communication by the metre, Dec. 2019

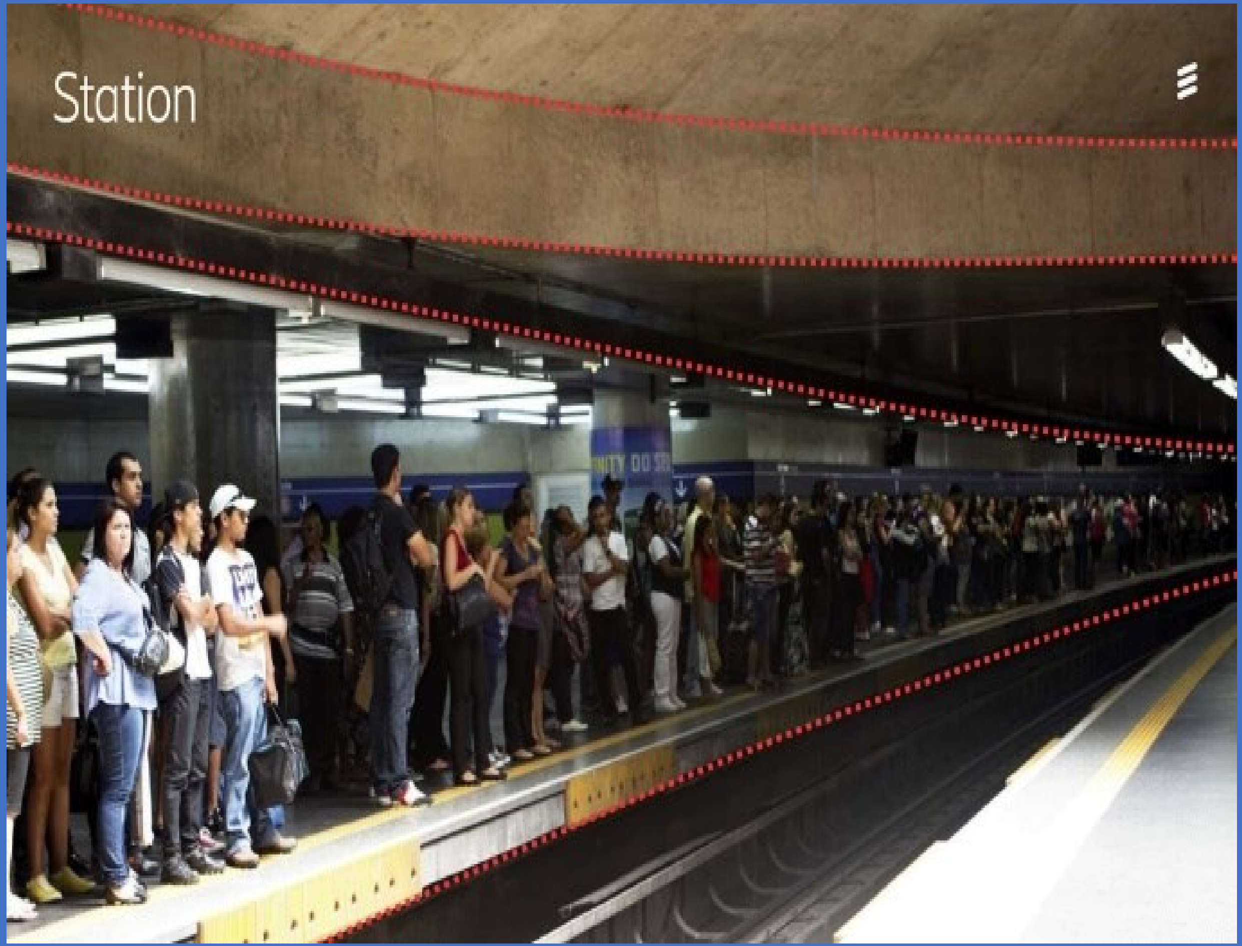
Ericsson Cell Free Radio Stripes Use Cases (UCs) - 1





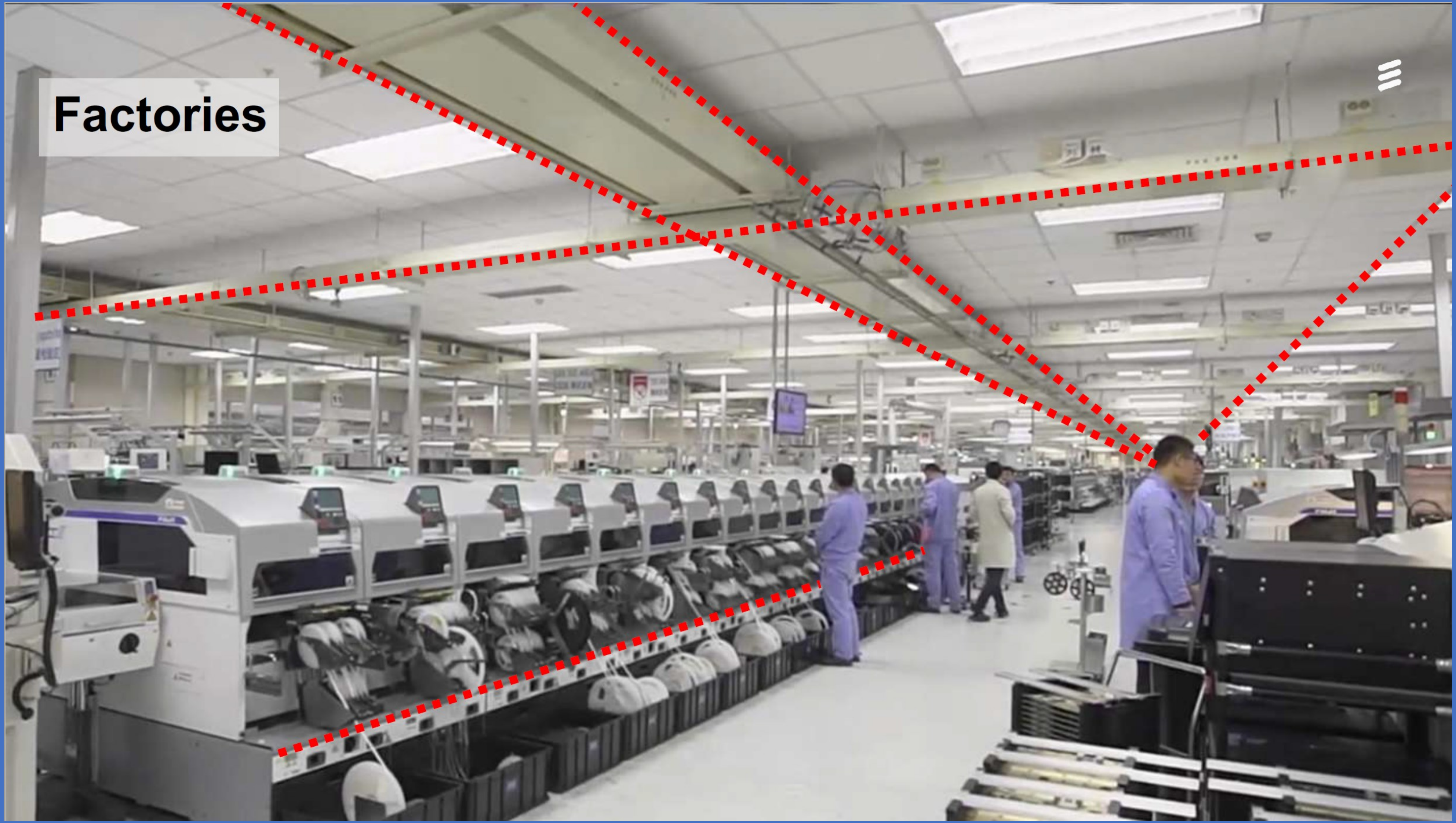
Ref. Ericsson, Radio Stripes: Re-Thinking Mobile Networks, Feb., 2019

Ericsson Cell Free Radio Stripes Use Cases (UCs) - 2



Ref. Ericsson, Radio Stripes: Re-Thinking Mobile Networks, Feb., 2019

Ericsson Cell Free Radio Stripes Use Cases (UCs) - 2



Ref. Assoc. Prof. Emil Björnson, Pres, Beyond the Cellular Paradigm: Cell-free Architectures with Radio Stripes April, 2020: 22

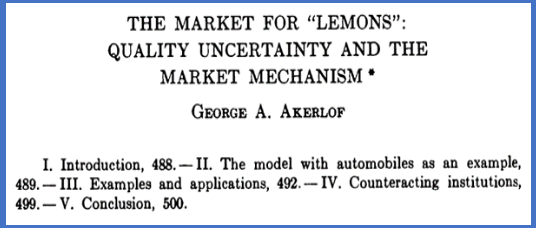
Ericsson Cell Free Radio Stripes

Pål Frenger, Radio Network Energy Performance Manager at Ericsson Research

A piece of Ericsson's Radio Stripe networking tape reveals radio modules and the power and networking cables connecting them.

Ref. Digital Trends, Ericsson 5G Radio Stripe Network MWC 2019&
Linköpings Universitet, Wireless communication by the metre, Dec. 2019

Annex 5: Business Aspects: The Big Shift - from "Caveat Emptor" to "Caveat Venditor" - When Information is Ubiquitous


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.

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 and Agile Service Deployment.**

The Big Shift - from "Caveat Emptor" to "Caveat Venditor" - 3

To see what the Problem is before jumping in to Resolve it

Problem Solving Approach turns upside down Two (2) "Traditional Sales Skills:

A) From "Access Information" to "Curating Information":

- Sorting - out through massive amount of Data
- Presenting the most Relevant & Clarifying Aspects

B) From "Answering Questions" to "Asking Questions"
in order to

Possibilities
Uncover => Surfacing Latent Issues
Unexpected problems

C) Apply "Contrast Principle" (R. Cialdini) & move from "Upselling" to "Upserving"

Most Important Question:

"Compared to What"? => Value

Annex 6: 5G Architecture related Difference in Business Models between Telecom and DevOps

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

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

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

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

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

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

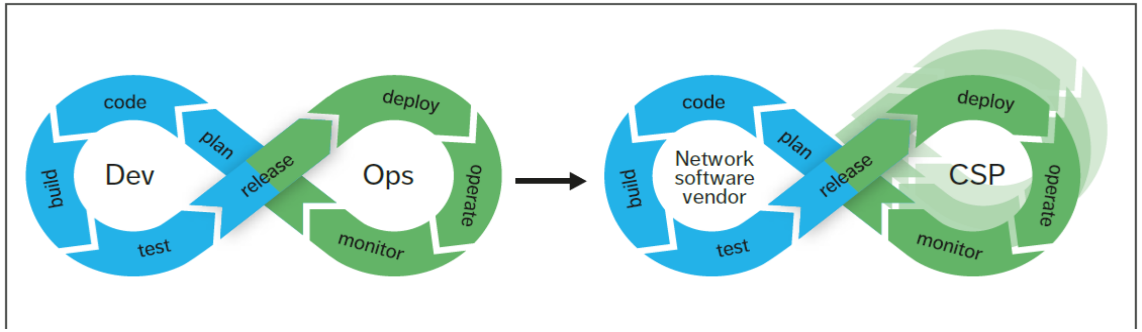


Figure 1: The DevOps and (Telecom) aaP Business Models

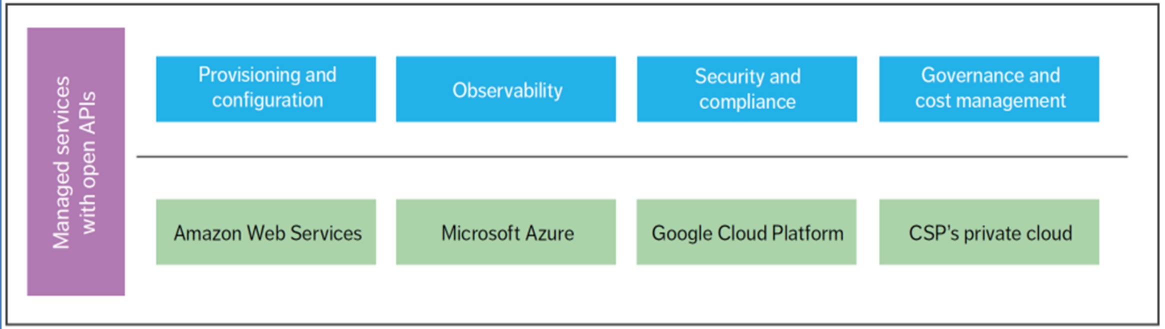


Figure 3: Key Enablers for a Multi-Cloud Native Application

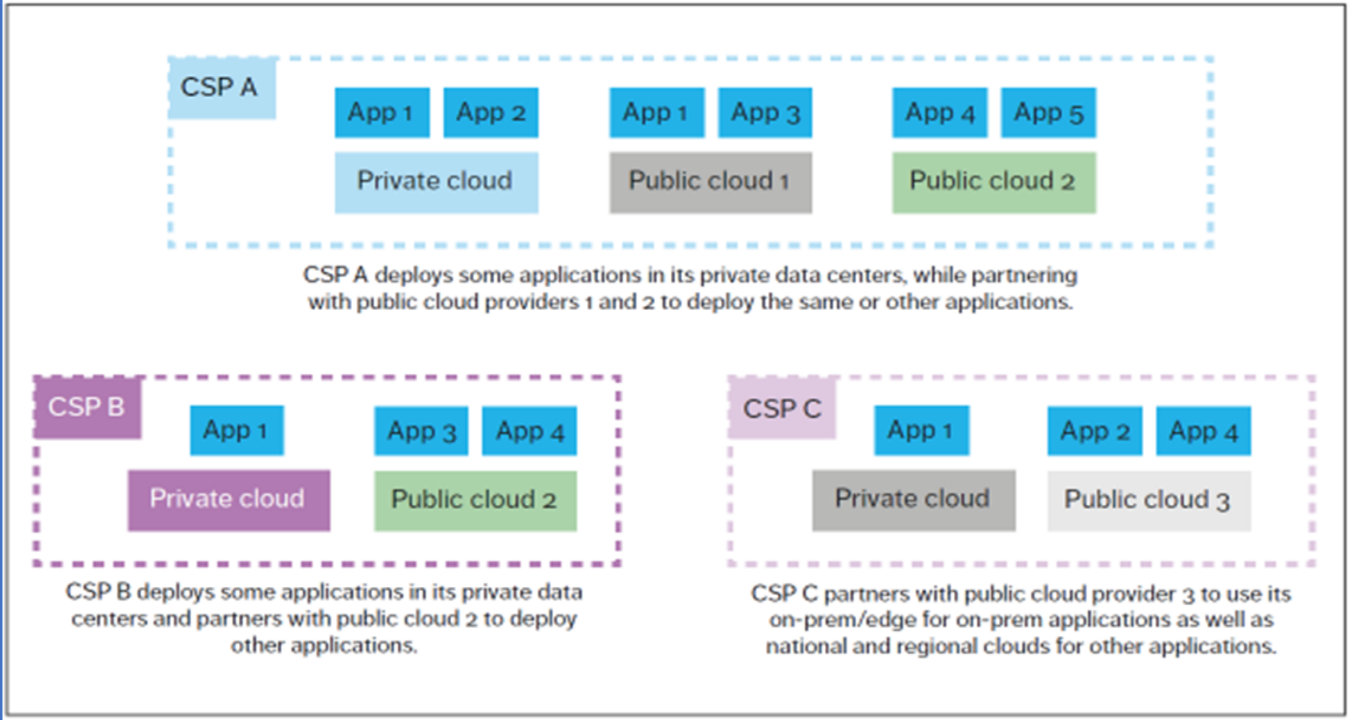


Figure 2: Examples of Hybrid and Multi-Cloud Deployment Scenarios that Applications must be able to support

Annex 7. Mobile Networks to evolve from:

a Design that offers "Best-effort Services

to

a Design that offers Performance and User Experience Guarantees

Capabilities related to e.g.:

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

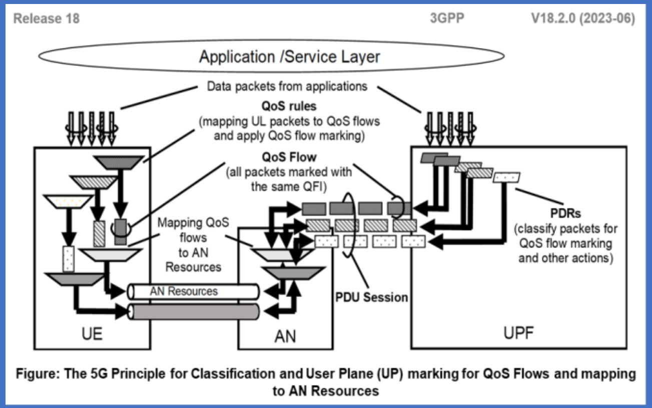


Figure: The 5G Principle for Classification and User Plane (UP) marking for QoS Flows and mapping to AN Resources

=>

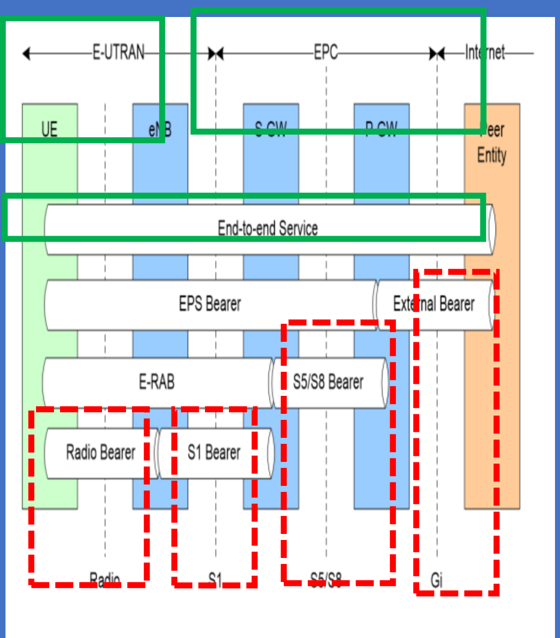


Figure : EPS Bearer Service Architecture

=>

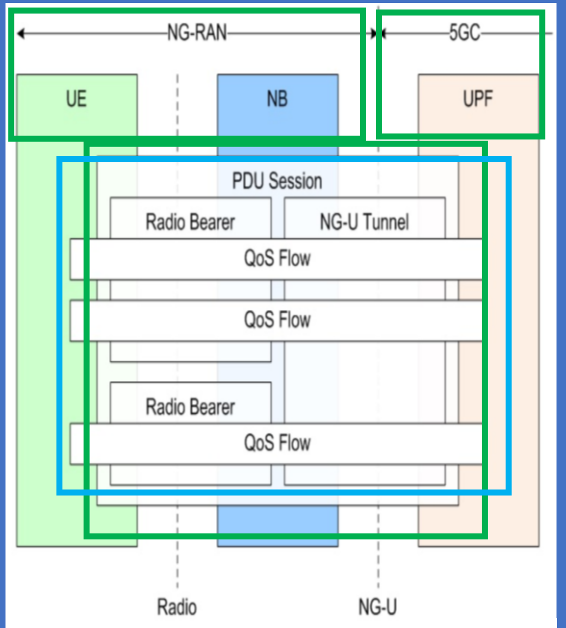


Figure: 5G CN NG-RAN Bearer Services QoS Architecture

Measurement Assistance Information shall include the addressing information of *a* ***Performance Measurement Function*** (**PMF**) **in the UPF, the UE can send PMF protocol messages** incl.:

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

Remarks & Questions?