ETSI GR MEC 031 V2.1.1 (2020-10)

Multi-access Edge Computing (MEC)
MEC 5G Integration

Disclaimer

The present document has been produced and approved by the Multi-access Edge Computing (MEC) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/MEC-00315GIntegration

Keywords
5G, MEC

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Multi-access Edge Computing (MEC).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document describes the key issues, solution proposals and recommendations for MEC integration into 3GPP 5G system. The following aspects are addressed: MEC System interactions with the 5G System, including the correspondence of the current MEC procedures to procedures available in 3GPP 5G system specification, options for the functional split between MEC and 5G Common API framework, realization of MEC as 5G Application Function(s).

In addition the present document addresses the scope and the preferred way of proceeding with the identified future technical work, as well as the identification of any missing 5G system functionality for MEC integration.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 123 501: "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 Release 16)".

[i.2] ETSI TS 123 502: "5G; Procedures for the 5G System (5GS) (3GPP TS 23.502 Release 16)".

[i.3] ETSI TS 129 522: "5G; 5G System; Network Exposure Function Northbound APIs; Stage 3 (3GPP TS 29.522 Release 16)".

[i.4] ETSI TS 123 222: "LTE; 5G; Common API Framework for 3GPP Northbound APIs (3GPP TS 23.222 Release 16)".

[i.5] ETSI GS MEC 003: "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[i.6] ETSI White Paper No. 28: "MEC in 5G networks".

[i.7] ETSI GR MEC 018: "Mobile Edge Computing (MEC); End to End Mobility Aspects".

[i.8] ETSI GS MEC 012: "Multi-access Edge Computing (MEC); Radio Network Information API".

[i.9] ETSI TS 129 571: "5G; 5G System; Common Data Types for Service Based Interfaces; Stage 3 (3GPP TS 29.571 Release 16)".

[i.10] ETSI GS MEC 011: "Multi-access Edge Computing (MEC); Edge Platform Application Enablement".

[i.11] ETSI TS 129 222: "5G; LTE; Common API Framework for 3GPP Northbound APIs (3GPP TS 29.222 Release 16)".

[i.12] ETSI GS MEC 001: "Multi-access Edge Computing (MEC); Terminology".

[i.13] ETSI GS MEC 016: "Multi-access Edge Computing (MEC); Device application interface".

[i.14] ETSI GS MEC 021: "Multi-access Edge Computing (MEC); Application Mobility Service API".

[i.15] ETSI TS 129 501: "5G; 5G System; Principles and Guidelines for Services Definition; Stage 3 (3GPP TS 29.501 Release 16)".

[i.16] ETSI GS MEC 009: "Multi-access Edge Computing (MEC); General principles, patterns and common aspects of MEC Service APIs".

[i.17] RIC Measurement Campaign application.

NOTE: Available at https://docs.o-ran-sc.org/projects/o-ran-sc-ric-app-mc/en/latest/overview.html.

[i.18] RIC Application Architecture.

NOTE: Available at https://wiki.o-ran-sc.org/display/RICA/Architecture.

[i.19] ETSI TS 129 514: "5G; 5G System; Policy Authorization Service; Stage 3 (Release 16)"5G; 5G System; Policy Authorization Service; Stage 3 (3GPP TS 29.514 Release 16)".

[i.20] ETSI TS 129 500: "5G; 5G System; Technical Realization of Service Based Architecture; Stage 3 (3GPP TS 29.500 Release 16)".

[i.21] ETSI TS 129 523: "5G; 5G System; Policy Control Event Exposure Service; Stage 3 (3GPP TS 29.523 Release 16)".

[i.22] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

NOTE: Available at https://tools.ietf.org/html/rfc4122.

[i.23] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

NOTE: Available at https://tools.ietf.org/html/rfc3986.

[i.24] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

NOTE: Available at https://tools.ietf.org/html/rfc6749.

[i.25] ETSI GS MEC 002: "Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS MEC 001 [i.12] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS MEC 001 [i.12] and the following apply:

5GC	5G Core network
5GS	5G System
AF	Application Function
AMF	Access and Mobility management Function
AS	Application Server
BM-SC	Broadcast Multicast-Service Center

BSF	Binding Support Function
CAPIF	Common API Framework for 3GPP northbound APIs
CCF	CAPIF Core Function
CU	Central Unit
DN	Data Network
DNAI	Data Network Access Identifier
DNN	Data Network Name
GPSI	Generic Public Subscription Identifier
LADN	Local Area Data Network
LBO	Local Break Out
MBMS	Multimedia Broadcast Multicast Service
NEF	Network Exposure Function
NF	Network Function
NRF	Network Repository Function
NSSAI	Network Slice Selection Assistance Information
PCC	Policy and Charging Control
PCF	Policy Control Function
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
R-NIB	Radio-Network Information Base
RIC	RAN Intelligent Controller
RNIS	Radio Network Information Service
RRM	Radio Resource Management
RSRP	Reference Signal Receive Power
RT	Real Time
RU	Radio Unit
SCEF	Service Capability Exposure Function
SMF	Session Management Function
SRv6	Segment Routing over IPv6
UDR	Unified Data Repository
UE	User Equipment
UL	UpLink
UL CL	UpLink CLassifier
UPF	User Plane Function

4 Overview

4.1 Introduction

The present document describes the key study areas in the MEC 5G integration.

Clause 4 provides the description of each identified study area.

Clause 5 contains all identified key issues and their related solution proposals.

Clause 6 contains evaluation of proposed solutions. Based on identified gaps, recommendations for further work are provided.

4.2 MEC interactions with 5GS

3GPP 5G system supports the exposure of network information and capabilities to external consumers. MEC as an Application Function (AF) may interact with the 5G system for the following reasons as specified in ETSI TS 123 501 [i.1], clause 6.2.10:

- to influence the application traffic routing decisions, including User Plane Function (UPF) (re)selections;
- to access the Network Exposure Function (NEF) for network capabilities;
- to interact with the policy framework for policy control.

AFs that are not allowed by the operator to access directly the target Network Functions (NFs) use the NEF for their interactions. These AFs can be termed as an untrusted AF, outside the trust domain of a network operator, as compared to a trusted AF or trusted Network Functions (NFs) that is inside the trust domain, e.g. owned or operated by a network operator. An untrusted AF may be owned and operated by operator external entities such as a cloud or edge service provider, a gaming service provider, etc. It is out of scope of the present document to define which kind of information may be exposed to MEC, as an untrusted AF, to support better operation while maintaining security and privacy of operator's network. While the NEF is used for untrusted AFs, a trusted AF may interface with the 5GS via NEF or interface directly with 5GS functions, such as SMF, etc.

The NEF is the 5G NF in charge of securely exposing the network capabilities and events to AFs and other consumers as defined in ETSI TS 123 501 [i.1], clause 6.2.5. External exposure can be categorized as monitoring capability, provisioning capability, and policy/charging capability. The details of the external exposure of the capabilities are defined in ETSI TS 123 502 [i.2]. The Restful APIs for capability exposure are defined in ETSI TS 129 522 [i.3].

An AF can get services from multiple NEFs and an NEF can provide service to multiple AFs. Any instance of an NEF may support only a subset or all of the available NEF functionality.

An NEF may support Common API Framework (CAPIF) functionality, and more specifically the CAPIF API provider domain functions, for external exposure ETSI TS 123 222 [i.4].

4.3 MEC platform in 5G common API framework

4.3.1 Integrating MEC and CAPIF

In 3GPP, there are multiple northbound API-related specifications (e.g. APIs for SCEF, API for the interface between MBMS service provider and BM-SC, and also the current most important APIs for NEF). To avoid duplication and inconsistency of approach between different API specifications, 3GPP has considered the development of a common API framework for 3GPP northbound APIs (CAPIF) that includes common aspects applicable to any northbound service APIs.

The functional model for the common API framework (CAPIF) is organized into functional entities to describe a functional architecture which enables an API invoker to access and invoke service APIs and supports API exposing functions in publishing the API towards the API invokers. The CAPIF functional model can be adopted by any 3GPP functionality providing service APIs.

The relationship between the MEC API framework and the CAPIF is shown in figure 4.3.1-1.

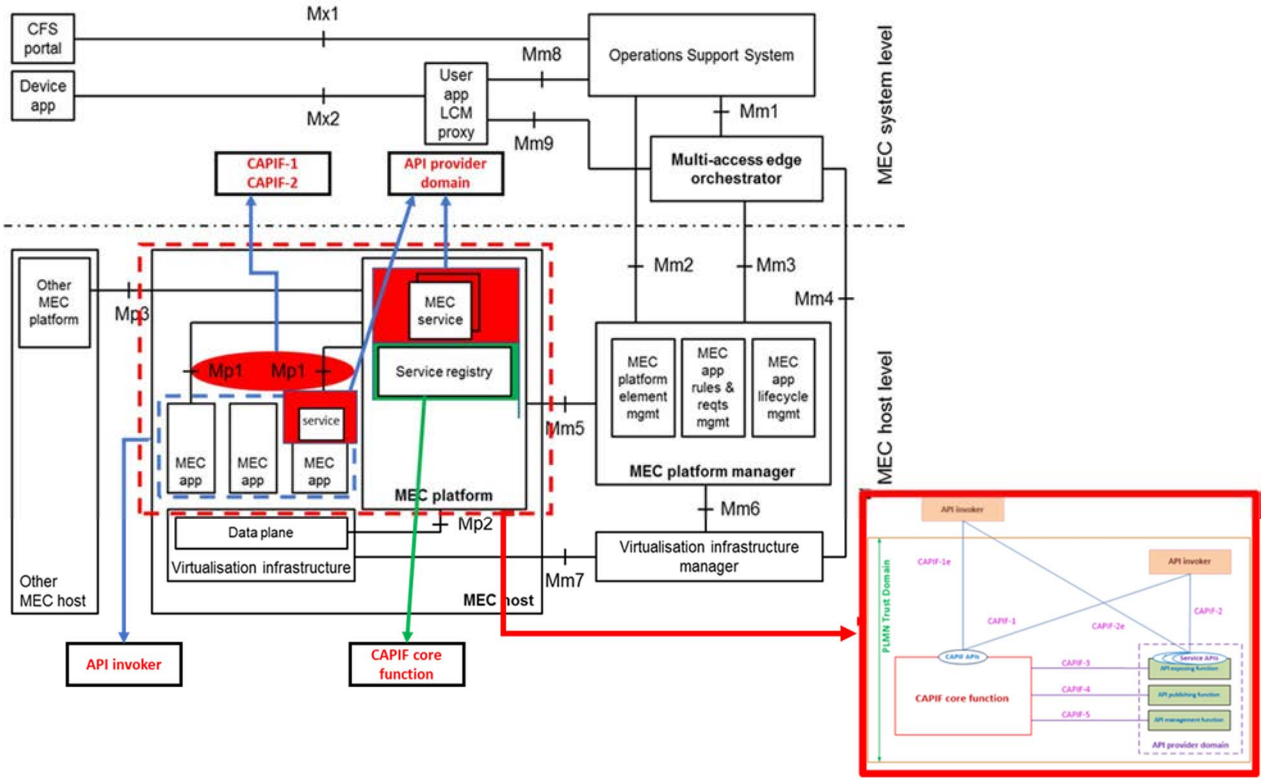

Figure 4.3.1-1: Relationship between MEC and 5G common API framework

MEC platform includes API-related platform functionality such as service registry. In addition the MEC platform can also expose MEC service APIs for consumption by MEC applications.

The API provider domain in CAPIF collectively represents the service APIs available for consumption in any 5G NF and any trusted 3rd party AF. A MEC service produced by a MEC application or the MEC platform can be mapped into the API provider domain in CAPIF.

A MEC application or MEC platform consuming a service is an API invoker in CAPIF.

The existing MEC platform functionality related to API enablement, can be mapped into the CAPIF core function.

The MEC platform also supports traffic rules control and DNS handling. These functionalities are outside the scope of CAPIF. Instead in 5GS the traffic rules control by an AF has been defined as a procedure between the AF and the SMF, possibly involving the NEF, as defined in ETSI TS 123 502 [i.2], clause 4.3.6.

4.3.2 Option #1: Providing access to MEC APIs via an external CAPIF instance

In this option, it is assumed that a MEC platform and a CAPIF deployment co-exist in the network, and that CAPIF API invokers want to access MEC services provided by the MEC platform or by MEC applications via the RESTful MEC service APIs.

In that case, the following applies:

- It needs to be possible to announce MEC APIs in CAPIF registry.
- It needs to be possible to use the CAPIF flavour of authorization when accessing MEC APIs. This might be realized via a gateway, or by updating the MEC API exposing functions to understand the CAPIF flavour of authorization.

This use case can be fulfilled by announcing the same service API redundantly in both the registry of the CAPIF core function in the network, and in the MP1 registries in the MEC platform(s).

NOTE 1: In MEC, location of the API producer matters. It has not been elaborated in the present document how to signal multiple instances of the same service available at different locations (e.g. different MEC platforms) when using CAPIF.

The following figure 4.3.2-1 illustrates the loosely coupled deployment.

The MEC reference point Mp1 supports publication of MEC services ("M-Publication"), discovery/announcement of MEC services ("M-Discovery") and further MEC application support ("Support") such as activation of traffic rules. The CAPIF core function supports publication ("C-Publication") and discovery ("C-Discovery") of CAPIF APIs.

The simplest integration possibility is to re-publish the MEC service APIs via CAPIF.

NOTE 2: Consumption/invocation of APIs is out of scope in this figure, but would need to be addressed separately.

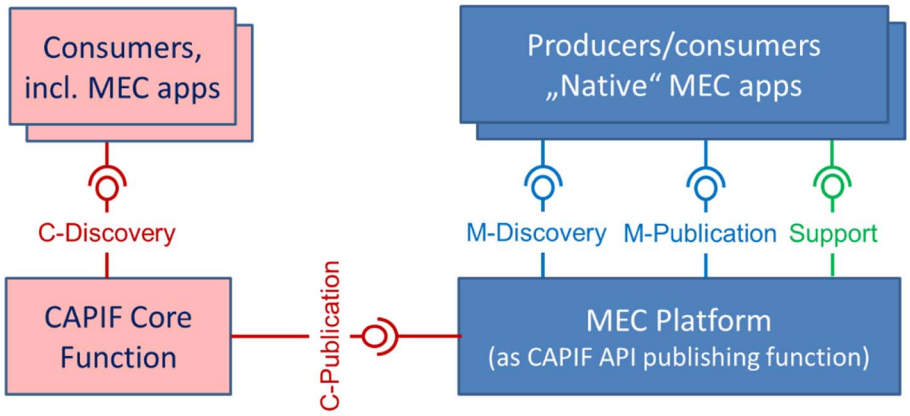

Figure 4.3.2-1: Loosely-coupled deployment of CAPIF and MEC

4.3.3 Option #2: CAPIF and MEC unified

In this option, it is assumed that a deployment exists that unifies MEC and CAPIF.

In such realization, CAPIF replaces those Mp1 parts that are overlapping with CAPIF (such as the MEC service registry of RESTful MEC services). The registry for the MEC services will be based on CAPIF; the same applies to authorization. The MEC platform can benefit from further CAPIF core function (CCF) support such as logging.

All invocations of RESTful APIs will be facilitated using CAPIF. This means that MEC applications would need to consume MEC APIs using CAPIF support and would need to support CAPIF's authorization. In addition, further MEC application support ("Support") is still provided. Figure 4.3.3-1 illustrates this option. The entity that exposes the interfaces is a deployment that combines capabilities defined for the MEC platform and capabilities defined for the CAPIF core function.

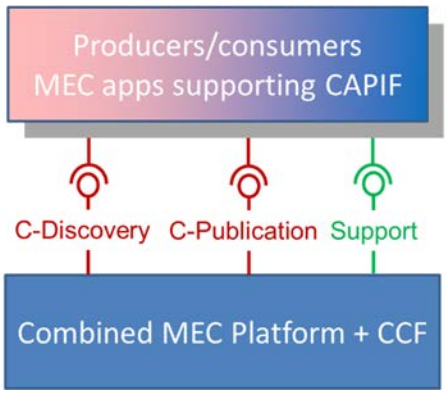

Figure 4.3.3-1: Fully-integrated hybrid deployment of CAPIF and MEC

Such a fully-integrated deployment would however not support the MEC concept of alternative transports; it would only apply to RESTful APIs. For additional support of alternative transports, a MEC service registry would still need to be supported. There is no need for redundancy, however, unlike in option #1 (clause 4.3.2), all RESTful service APIs are published and discovered via CAPIF; those services that are accessed via alternative transports are part of the MEC service registry.

Figure 4.3.3-2 illustrates a hybrid deployment.

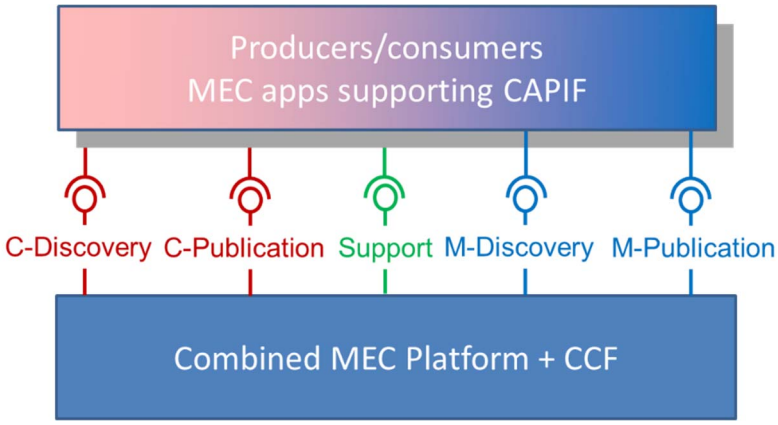

Figure 4.3.3-2: Hybrid deployment of CAPIF and MEC with support for MEC alternative transports

An alternative is the evolution of CAPIF by adding an extension mechanism, which would enable MEC to specify alternative transports as a MEC-specific CAPIF extension. Interaction with 3GPP is required for this.

4.4 MEC as Application Function(s) of 5G system

MEC system appears as an Application Function or Application Functions to a 5G system. This clause describes the study area for the MEC as an Application Function(s) of 5G system.

The MEC reference architecture is defined in ETSI GS MEC 003 [i.5]. MEC consists of functions at host level and system level. Host level functions include MEC Platform, MEC apps, and Virtualization Infrastructure. Host level management functions include MEC Platform Manager and Virtualization Infrastructure Manager. System level functions include MEC Orchestrator and OSS function. When MEC is integrated into the 5G system, the key definitions of MEC in ETSI GS MEC 003 [i.5] should be maintained.

The following examples illustrate the principle of MEC integration in the 5G system. An individual MEC application may appear as an AF to the 5G system. Similarly, a MEC platform that influences the traffic routing of the MEC application's traffic would appear as an AF to the 5G system. In yet another example the MEC orchestrator being notified of a UPF change would appear as an AF to the 5G system. These examples illustrate the principle of MEC as an AF; the 5G system exposes capabilities and information through a set of APIs to the AFs. Depending on the API in question the MEC AF may be represented by a different functional entities of the MEC system.

The MEC system has been defined and is deployed to enable application hosting in a secure, managed environment in the network. The impacts from the integration of MEC into a 5G system on MEC applications should be minimized. That is, the same functionality and APIs should be available for the application irrespective of the way how MEC has been deployed to avoid the need for deployment specific implementations of the same application.

Clause 5 of the present document contains the related key issues and proposed solutions.

4.5 Management of MEC applications in a 5G data network

The management of the MEC specific functionality of a particular MEC host and the applications running on it may be handled by the MEC management.

5 Key issues and potential solutions

5.1 Key issue #1: Traffic path update for mobility support

5.1.1 Description

5.1.1.1 Introduction

As described in the white paper "MEC in 5G networks" [i.6], in the extension from EPC to 5GC, 5GC has a new application function, i.e. the traffic influence service that realizes more flexible control of traffic paths as defined in ETSI TS 123 502 [i.2]. Since the function is exposed to the outside 5GC as described in ETSI TS 123 501 [i.1], MEC system becomes able to flexibly choose UPF(s) and the corresponding DN according to MEC operators' and/or MEC application providers' operation policy or unstable physical conditions. For instance, as for the mobility support, it enables to flexibly steer the u-plane traffic to keep connectivity between UE and application instance on source MEC host even in the case when the target MEC host is not able to host the application or the application instance in the source MEC host can still provide a satisfactory service. The present document considers two cases of mobility support, one is for the intra-operator case and the other one is for the inter-operator case.

5.1.1.2 Intra-operator MEC application mobility support

Regarding mobility support, in 5GC, UE mobility may cause gNB handover, then it may cause UPF changes. If required, the user context is transferred to the application instance in the target DN in accordance with UPF changes. In this case, traffic path would be updated accordingly as explained in ETSI GR MEC 018 (V1.1.1) [i.7], clauses 6.2.6.2, 6.2.6.3 and 6.2.6.4.

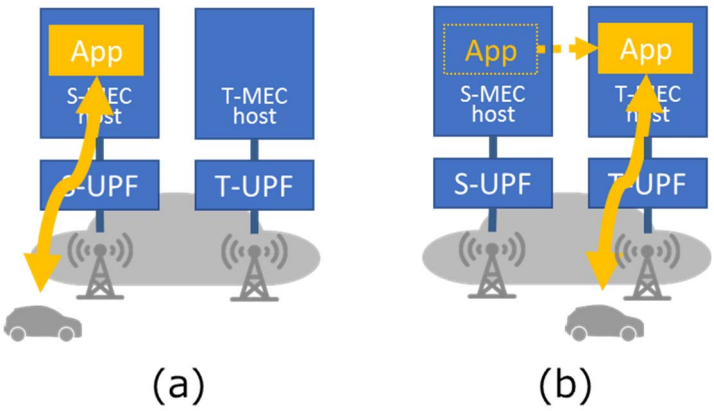

Figure 5.1.1.2-1: Mobility support

However, user context may not be transferred to the T-MEC for various reasons, e.g.:

1) in the case when the target MEC host (T-MEC host) is not able to host the application, e.g. the T-MEC host does not have sufficient resources;

2) the application instance in the source MEC host (S-MEC host) can provide a moving user with satisfactory service.

Even in these cases, the traffic path should be updated as it steers the application data to the S-MEC host via either of the T-MEC host (as depicted in figure 5.1.1.2-2 (b)) or the original UPF that associates with the S-MEC host (as depicted in figure 5.1.1.2-2 (c)). Note that figure 5.1.1.2-2 depicts only the case of user context transfer.

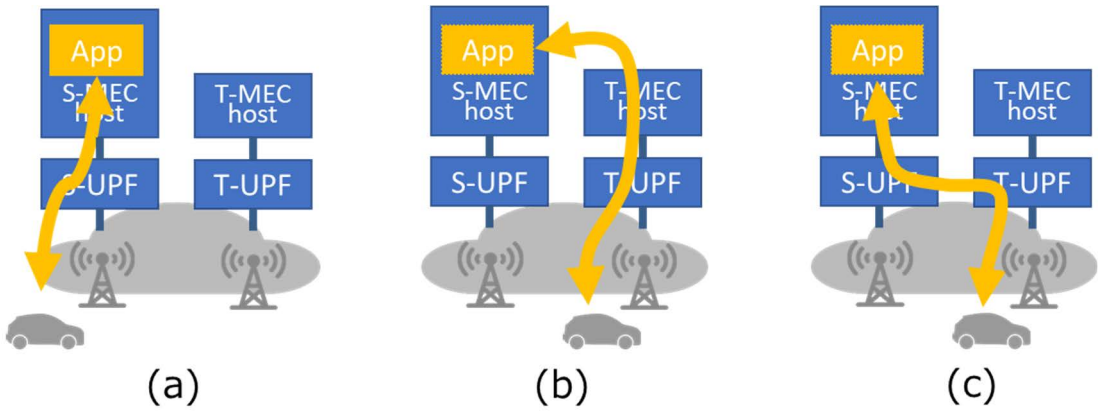

Figure 5.1.1.2-2: Mobility support, where the target MEC host cannot be used

Whichever application instance is successfully transferred to T-MEC host or not, the traffic path is supposed to be updated appropriately.

5.1.1.3 Inter-operator MEC application mobility support

As an extended use case from the previous one, MEC is also expected to support inter-operator MEC application mobility support that includes both inter-MEC operator case and inter-PLMN case. Similarly, in the intra-operator case, if required, the user context may be transferred to the application instance in the target DN. This is depicted in figures 5.1.1.3-1 and 5.1.1.3-2. Note that figures 5.1.1.3-1 and 5.1.1.3-2 depict only the case of user context transfer.

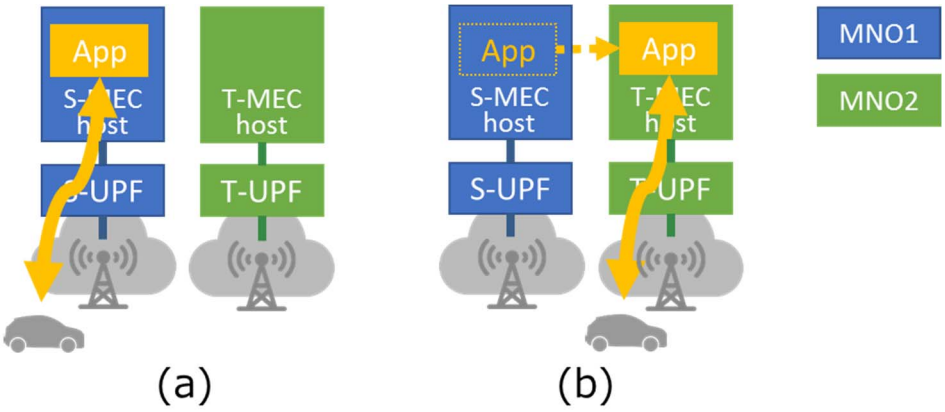

Figure 5.1.1.3-1: Inter-operator mobility support

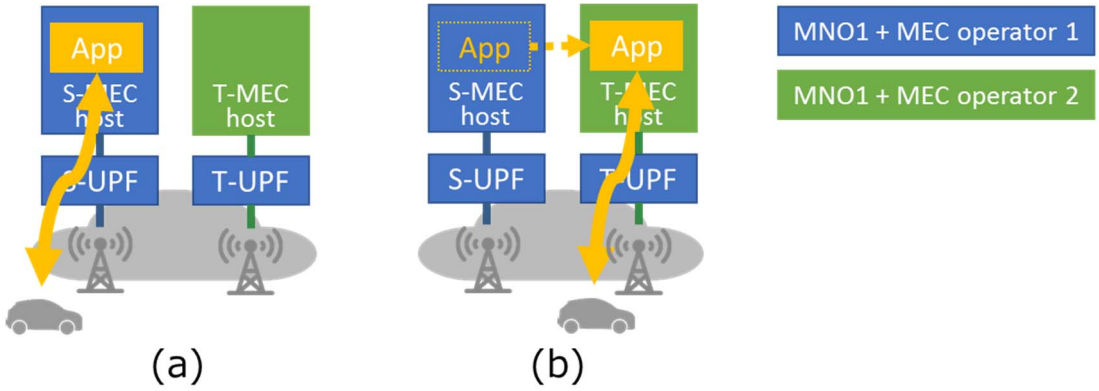

Figure 5.1.1.3-2: Inter-operator mobility support

In the case when the T-MEC host is not able to host the application, e.g. it does not have sufficient resources, or the application instance in the S-MEC still provides satisfactory service, the user context may not be transferred to the T-MEC host. Two options of the application's behaviour are possible.

- The application instance stays on the S-MEC host in the source operator side as depicted in figure 5.1.1.3-3 (b).
- The application instance is transferred to alternative MEC host (A-MEC host) in the target operator side as depicted in figure 5.1.1.3-3 (c).

In both options, the traffic path should be updated, which steers the application data from the target UPF to the source UPF in the same MNO's network as the source MEC host, or alternative UPF in the same MNO's network as the T-MEC host.

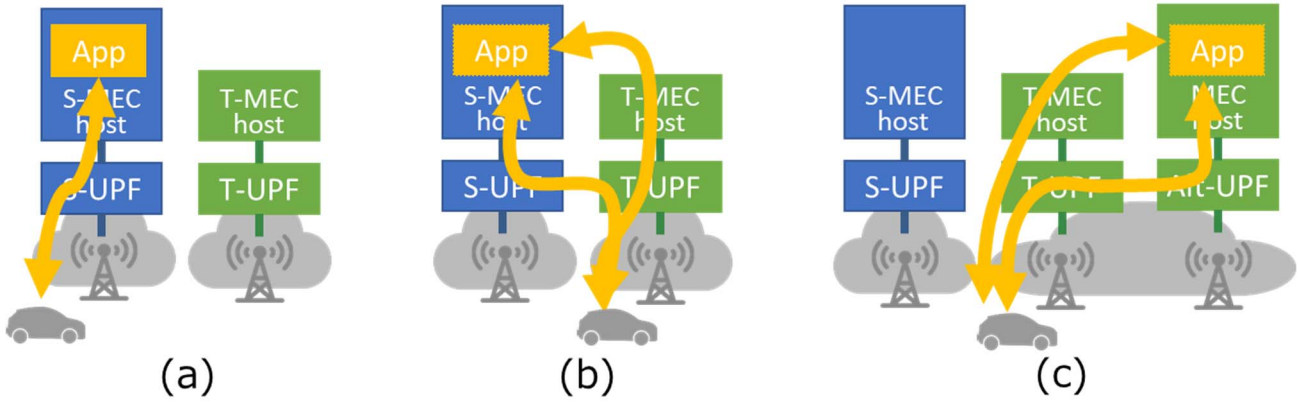

Figure 5.1.1.3-3: Inter-operator mobility support, where the T-MEC host cannot be used

Inter-PLMN coordination is out of scope for the present document.

5.1.2 Solution proposal #1: 5GC control plane solution

5.1.2.1 Obtaining the mandatory input parameters

For both cases, traffic path can be maintained or updated by using the Application Function influence on traffic routing procedures specified in ETSI TS 123 502 [i.2]. To use it, how to obtain the mandatory input parameters and how to call it in each case should be clarified.

When MEC system calls the Application Function influence on traffic routing procedure, it requires to know 4 mandatory input parameters:

- UE identifier;

- potential locations of applications;
- AF transaction identifier; and
- traffic description (see ETSI TS 123 501 [i.1]).

Each parameter can be obtained as follows:

- UE identifier:
  Referring to ETSI TS 123 501 [i.1], "UE identifier" could be individual UE identifier or UE group identifier. Regarding the individual UE identifier, it is not clearly specified either of IMSI, GUTI, or IP address. All of them are possible and practical since 5GS is supposed to be capable of resolving from one to the other. The MEC system can obtain one of them from MNO, UE or application.
- Potential locations of applications:
  Once MEC system can specify DNAI(s), 5GS can resolve the corresponding UPF, then, steer UP path to the target UPF. The MEC system is supposed to know the appropriate DNAI(s) in advance. The information might require to be provided by MNOs because DNAI is the pre-configured value that is generated by MNO.
- AF transaction identifier:
  According to ETSI TS 123 501 [i.1], AF transaction identifier is an internal ID that is generated by AF when AF receives a request from outside. Therefore, from the MEC's point of view, the MEC system does not need to take care of this ID.
- Traffic description:
  According to ETSI TS 123 501 [i.1], the information 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 application identifier can be obtained from MNOs since the identifier is preconfigured by them. If MEC system knows more detailed information, e.g. IP addresses, it provides detailed traffic description for fine-grained UP steering.

5.1.2.2 High level message flow to influence traffic path for intra-operator case

Figure 5.1.2.2-1 depicts the detailed function blocks in intra-operator case. Interactions between these blocks make it possible to resolve the required traffic path update. The MEO acts as AF to interact with NEF as an example.

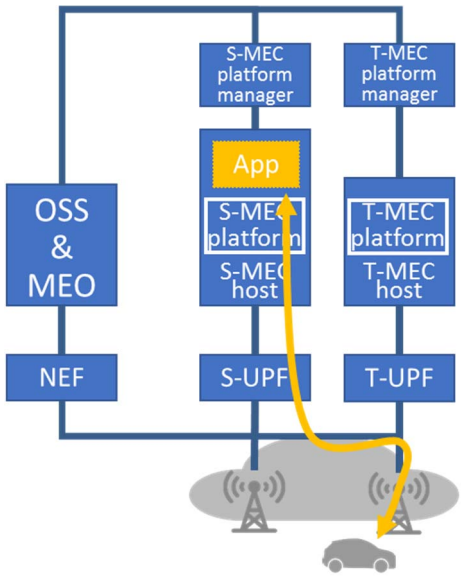

Figure 5.1.2.2-1: Function blocks in intra-operator case

Figure 5.1.2.2-2 depicts the option 1 of high-level information flow to influence the traffic flow, the MEO acts as AF to interact with NEF as an example.

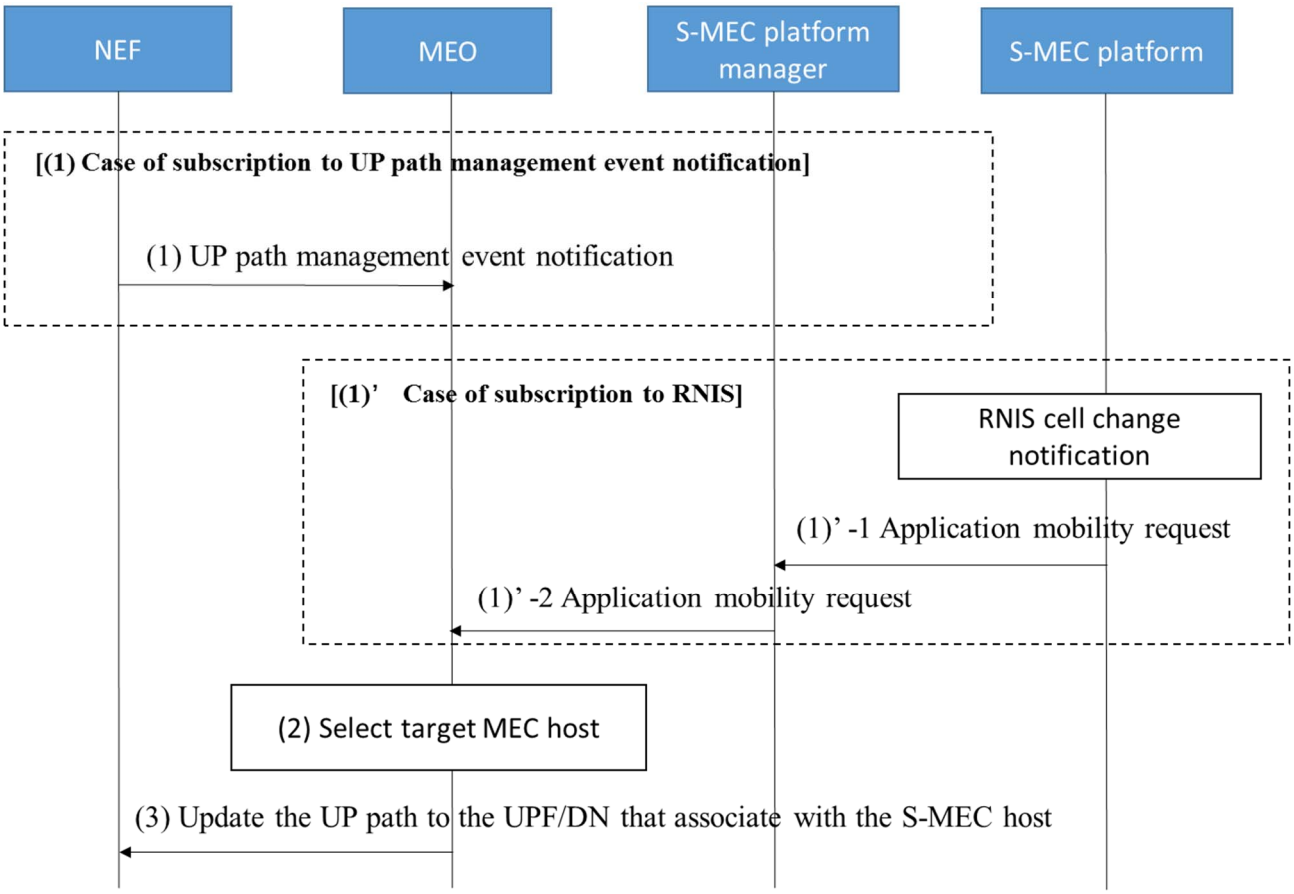

Figure 5.1.2.2-2: Option 1 of high-level information flow to influence the traffic flow in intra-operator case

The high level information flow to influence the traffic flow consists of the following steps:

(1) In the case where the MEC Orchestrator (MEO) subscribes the UP path management event notifications, MEC orchestrator receives the notification from SMF(s) directly or via NEF, which means UP and corresponding DN have changed according to the UE mobility.

(1') In the case of RNIS, the source MEC platform (S-MEC platform), on behalf of application instances, subscribes the cell change notification associated with a UE. After S-MEC platform receives the notification, it determines whether the UE has moved out of the coverage. If this is the case, S-MEC platform sends an application mobility request to MEO.

(2) MEO selects the target MEC host.

(3) In the case where the target MEC host is not available due to any reason, e.g. target MEC host does not have sufficient resources, the application instance should continue on the source MEC host and UP path should be redirected to the UPF associated with the S-MEC host.

(4) MEO sends Nnef_trafficinfluence update request with appropriate input parameters according to the notification from S-MEC platform manager and reply from T-MEC platform manager.

These steps provide the continuity of the connection between UE and MEC application that is located on the S-MEC host.

Figure 5.1.2.2-3 depicts the option 2 of high-level information flow to influence the traffic flow.

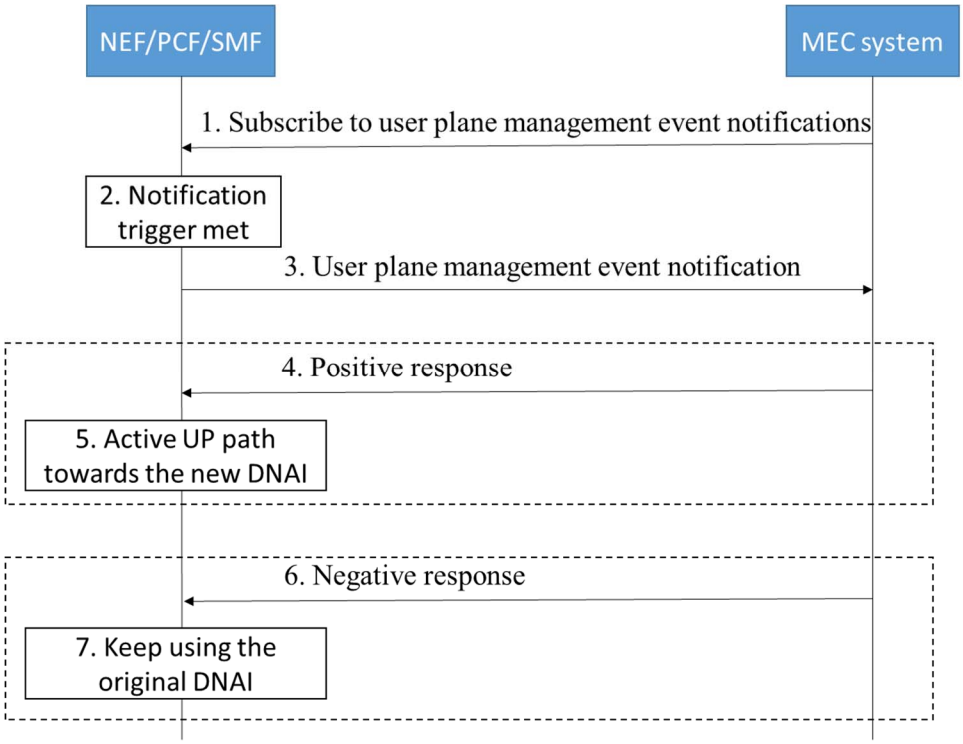

Figure 5.1.2.2-3: Option 2 of high-level information flow to influence the traffic flow in intra-operator case

NOTE: MEC system in this option can be MEO, MEC platform or MEPM.

The high level information flow to influence the traffic flow consists of the following steps:

1. Precondition: The MEC system has already informed the 5GC control plane the potential positions of the application instances. The MEC system requests to be subscribed to notifications about UP path management events. The "AF acknowledgment to be expected" indication is included. This request is sent to the PCF directly or via the NEF.

2. A condition for an AF notification has been met, for example the DNAI is going to be changed.

3. The SMF sends the notification to the MEC system directly or via the NEF. The notification type may be early notification or late notification. The source and destination DNAI are included if the DNAI will be changed. The SMF will wait for the acknowledgement from the MEC system.

4. The MEC system sends the positive response after application relocation is completed. The MEC system may also send the positive response immediately if it expects the UP path change but does not need application relocation.

5. The SMF activates the UP path towards the new DNAI.

6. The MEC system rejects the DNAI change by sending a negative response to the SMF directly or via NEF, in cases of the application relocation cannot be completed on time or the current application instance can satisfy the service requirement.

7. The SMF keeps using the original DNAI and may cancel related PSA relocation or addition. The SMF may perform DNAI reselection afterwards if needed.

5.1.2.3 High level message flow to update the traffic path for inter-operator case

Figure 5.1.2.3-1 depicts the detailed function blocks in inter-operator case. Interactions between these blocks make it possible to continue MEC application and to resolve the required traffic path update. Figure 5.1.2.3-2 depicts the high level information flow to update the traffic flow in inter-operator case.

NOTE 1: The presented flow is just one of the possible alternatives. Other possibilities are left for future specifications.

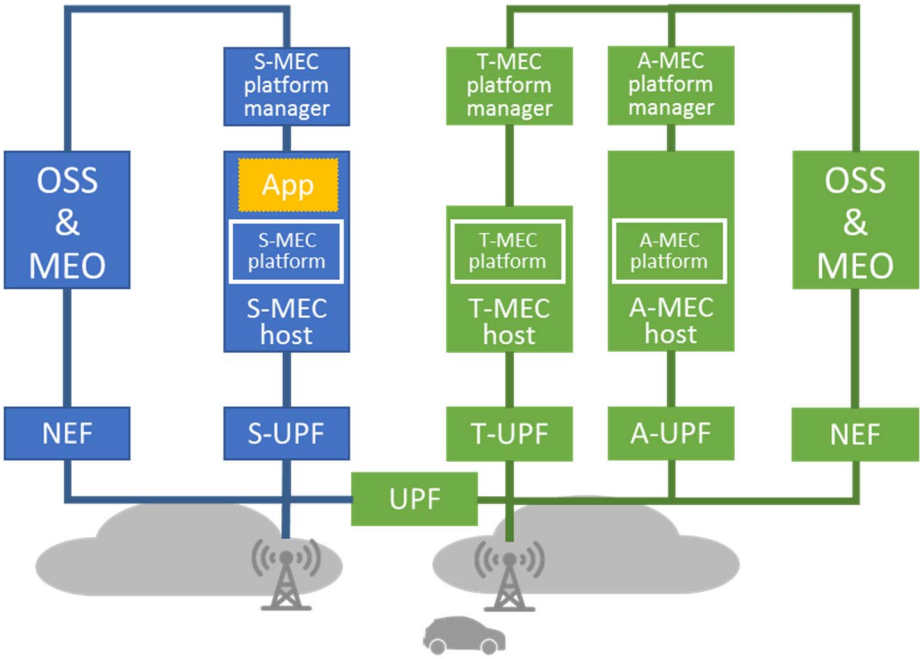

Figure 5.1.2.3-1: Function blocks in inter-operator case

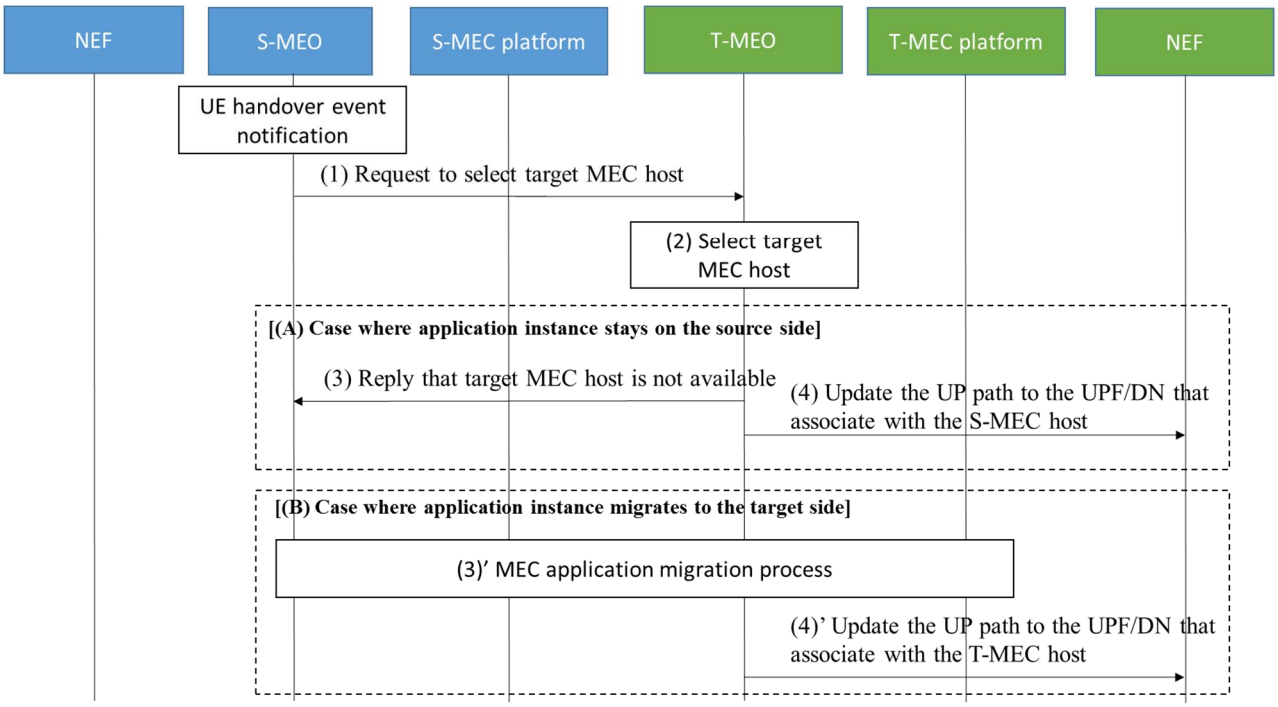

Figure 5.1.2.3-2: High level information flow to update the traffic flow in inter-operator case

The high-level information flow to update the traffic flow in inter-operator case consists of following steps:

(1) When the source MEC orchestrator receives the notification that indicates UE handover to another PLMN, the source MEC orchestrator (S-MEO) sends a request to the target MEC orchestrator (T-MEO) to select the target MEC host (T-MEC host). Note that the notification could be delivered by either NEF that associates with S-MEO, NEF that associates with target MEC orchestrator, or source MEC platform (S-MEC platform).

NOTE 2: How to receive the notification across different PLMNs is out of scope for the present document.

(2) T-MEO selects the target MEC host.

(3) In the case where T-MEC host is not available due to any reason, e.g. T-MEC host does not have sufficient resources, T-MEO decides to make the application stay on the source MEC host, T-MEO replies to S-MEO to notify the application instance continue on the source MEC host (S-MEC host).

(4) In the meantime, T-MEO sends Nnef_trafficinfluence update request with the appropriate input parameters to update the UP traffic path to source UPF that associates with S-MEC host.

NOTE 3: How to call Nnef_trafficinfluence across different PLMN is out of scope for the present document.

(3)' In the case where T-MEO selected the target MEC host, the MEC application instance or user context migration procedure will be executed.

NOTE 4: The detailed migration process is not specified yet.

(4)' After the migration process, T-MEO sends Nnef_trafficinfluence update request with the appropriate input parameters to update the UP traffic path to alternative UPF that associates with alternative MEC host.

These steps provide the continuity of the connection between UE and MEC application that is located either on the S-MEC host or A-MEC host.

5.1.3 Solution proposal #2: D-Plane overlay and AF use for N6 traffic steering policy alignment and enforcement

5.1.3.1 General design objectives and deployment aspects

Whereas the UPF selection and configuration is under control of the 5G System's (5GS) Session Management Function (SMF's N4 reference point to UPF), control of traffic treatment between a UPF and an Application Service (AS), which is denoted as N6 reference point, can be deployment specific.

A MEC System represents a DN for the 5GS, hence the SMF can select a suitable UPF according to the MEC System, which holds the AS being relevant to the mobile client. Preferably, a set of UPF instances are available for load balancing in the same location as the MEC hosts, which provide the ASs.

The solution proposal takes the following objectives into account:

- alignment of 5GS decision and events (UPF selection, UPF re-selection and change, UPF upstream policies) and MEC system internal traffic treatment policies on the N6 reference point;
- mitigate impact and dependency on the 5GS standardization;
- optimize MEC System local operations without involving 5GS for MEC System reconfiguration (i.e. change in Multi-access Edge Computing Platform-MEP and associated connectivity of a client).

5.1.3.2 Proposed Functional Architecture

The following are key aspects of the functional architecture:

- 5GS Application Function (AF) is leveraged as binding element between MEC System and 5G System.
- AF subscribes to 5GS:
  - to request policies associated with a client's connection, e.g. selected UPF, QoS attributes, etc.;
  - to receive notifications about changes in the configuration, e.g. UPF change.
- An AF is associated with a MEC Platform Manager (MEPM).
- MEPM can enforce traffic treatment rules on the MEP via Mm5 reference point, which apply to the MEC Host data plane:
  - For downlink traffic treatment, e.g. policy route/traffic steering, QoS, etc.;

- For extended functions, e.g. metering, uplink tunnel termination or label popping, etc.

- In order to avoid providing N6 upstream policies to the UPF, which involves always the 5GS, a loosely coupled data plane node (D-Plane) is assumed with one or multiple UPFs.
- MEPM can enforce traffic treatment policies on the D-Plane, which is loosely coupled with the client's UPF, indirectly via Mp2 interface.
- Leaving full control of traffic treatment policies on N6 to the MEC System speeding up local re-configuration and mitigates associated interworking and signalling with the 5GS.
- Relevant PEPs for N6 traffic treatment are the loosely coupled D-Plane and the MEC Host data plane.

Figure 5.1.3.2-1 shows the policy enforcement architecture.

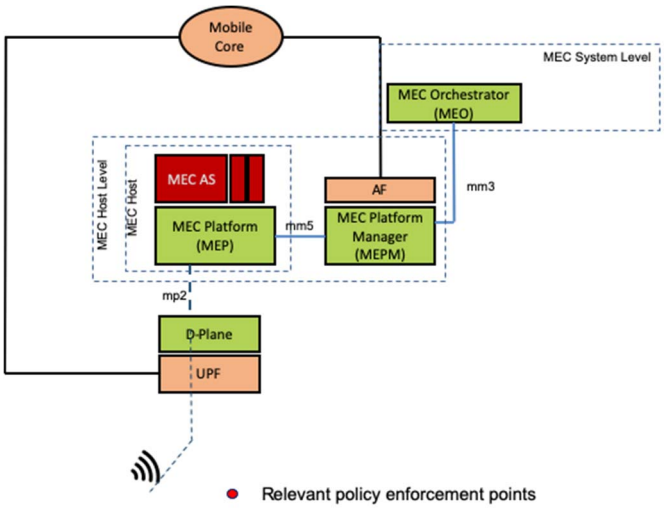

Figure 5.1.3.2-1: Policy enforcement architecture

5.1.3.3 Operational aspects - Traffic steering for intra-MEC Application Mobility

According to the above architecture, local re-configuration and changes in the MEC Host, which holds the AS serving a client, can be handled locally.

The MEC Orchestrator (MEO) enforces application mobility between two MEC Hosts and the associated MEP, see ETSI GS MEC 021 [i.14]. To re-configure the client's connection, the MEO instructs the MEPM to setup (on the target MEP) and update (on the loosely coupled D-Plane at client's UPF and on the source MEP) the traffic treatment policies, which include policies for steering uplink/downlink traffic between the UPF and the MEC AS on the target MEP.

The following figure 5.1.3.3-1 illustrates updating the traffic steering between the UPF and the MEC AS.

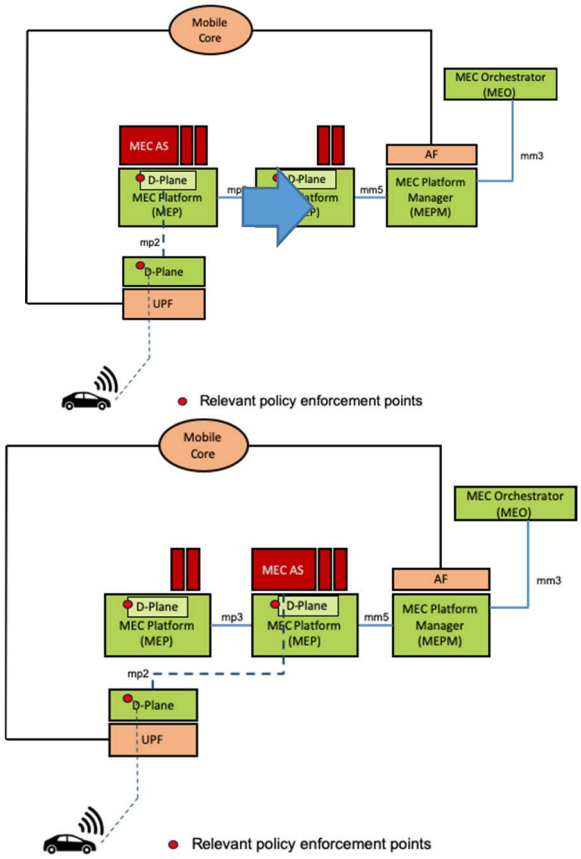

Figure 5.1.3.3-1: Traffic steering between UPF and MEC AS

5.1.3.4 Operational aspects - Traffic steering for inter-MEC Application Mobility

According to the proposed architecture, treatment of traffic during MEC application mobility between MEC Hosts in different DNs can be handled to a large extent on the MEC Host - and MEC System level. The 5GS is involved in the selection and configuration of a UPF in the target MEC system. Handling the traffic steering, the transient forwarding from the source MEC system to the target MEC system, as well as treatment of non-routable traffic in the target MEC using the D-Plane overlay avoids involvement of the 5GS, i.e. to temporarily setup UPFs in the source and target network as UpLink CLassifier (UL CL) according to the 3GPP procedure for AS mobility between DNs.

Transient forwarding of data plane packets between the source MEC system and the target MEC system can be accomplished for e.g. by means of segment routes (e.g. SRv6), tunnels, or locator re-write (e.g. Identifier-locator addressing for IPv6).

Dependent on the setup and administrative instances behind the source and the target MEC, MEC System level functions, such as the MEO, are involved in the coordination of policies for enforcement in the D-Plane overlay of the source- and target MEC.

Figure 5.1.3.4-1 illustrates AS mobility between DNs.

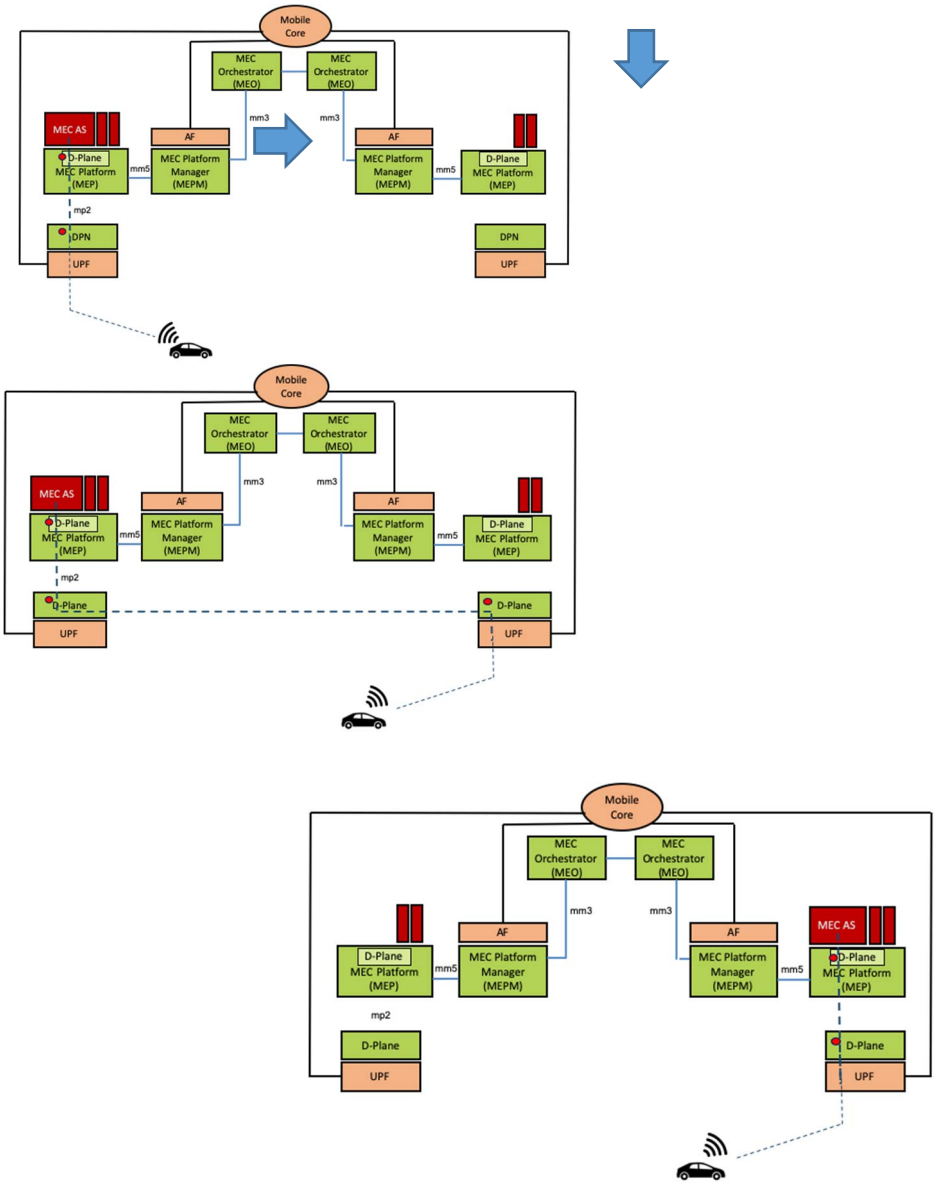

Figure 5.1.3.4-1: AS mobility between DNs

5.1.4 Evaluation

The solution proposal #1 is technically feasible in case of intra-operator case under the following conditions:

- MEO is capable of interacting with NEF, e.g. MEO acts as AF.

The solution proposal #1 is technically not feasible in case of inter-operator case due to the following premises:

- MEC systems need to appropriately handle Nnef_trafficinfluence requests across different PLMNs since AF is not allowed to request to influence traffic routing to PDU sessions established in Home Routed mode [i.1].
- The source and target MEC systems are capable of coordinating with each other. Inter MEC system coordination is recommended to be further studied and specified.

The solution proposal #2 is technically feasible under the following conditions:

- MEC platform manager acts as AF and is capable of interworking with NEF.
- MEC platform manager/AF is able to retrieve UE/flow identifiers for subscription to events at 5G System.

The solution proposal #2 is technically feasible for inter-operator case if the following condition is met:

- MEC systems need to connect to each other and utilize appropriate semantics to mutually exchange information on the source/target MEC, about UE/flow identifiers and the source/target UPF/D-Plane. Inter MEC system coordination is recommended to be further studied and specified.

5.2 Key issue #2: Ping-pong handover mitigation

5.2.1 Description

As described in ETSI GR MEC 018 [i.7], clause 6.2.9, in the scenario where the UE moving repeatedly across the ME host serving area's boundary, ME application relocation may also be performed repeatedly between the T-MEC host and S-MEC host as depicted in figure 5.2.1-1, which may cause significant waste of resources and bad user experiences.

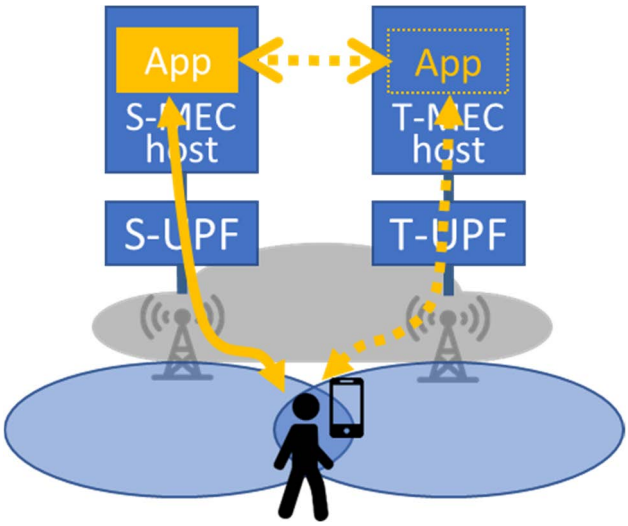

Figure 5.2.1-1: Frequent migration event caused by ping-pong handovers

Possible solutions may take place in either 3GPP system and/or MEC system.

5.2.2 Solution proposal #1: Make use of Nnef_trafficinfluence update.

The key idea of this possible solution is to mitigate the number of migration event that is controlled by MEO. High level information is depicted in figure 5.2.2-1.

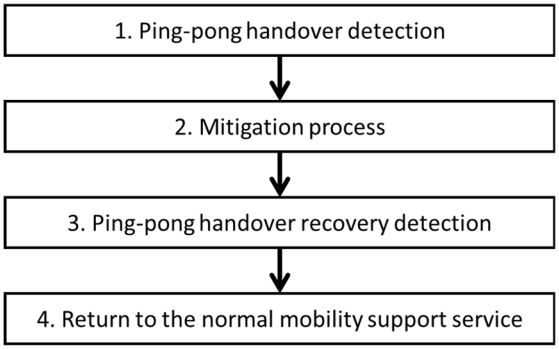

Figure 5.2.2-1: High level information flow to mitigate ping-pong handover effects

1. MEO is notified with the event of ping-pong handover that cause the frequent migration of MEC applications. That event could be detected by the frequency of the notification of UPF or UE bearer changes according to operation policy. That could be possibly triggered by or via SMF, NEF or RNIS.

2. MEO executes the ping-pong handover mitigation process using Nnef_trafficinfluence, which changes UPF/DN to connect the MEC application on S-MEH independently from the bearer condition as depicted in figure 5.2.2-2. The mechanism would reduce the number of migrations between S-MEH and T-MEH even in the case when UE is moving repeatedly across MEC host serving area. Regardless of changes of serving base station, UE continuously communicate with the application instance on S-MEC host via S-UPF.

3. MEO notices the ping-pong handover recovery event. The recovery event could be also detected by the frequency of the notification of UE bearer changes according to operation policy.

4. After the recovery event, MEO restores the ping-pong handover mitigation to normal state.

Figure 5.2.2-2 shows an example of the resulted steering traffic.

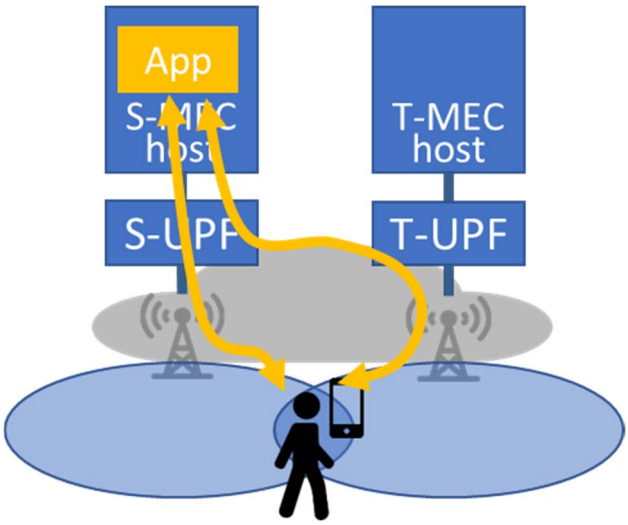

Figure 5.2.2-2: The example of resulted steered traffic

5.2.3 Evaluation

The solution #1 is technically feasible under the following conditions:

- MEO is capable of obtaining the handover events information and storing the information for sufficient time duration in order to handle the status for ping-pong handover mitigation.
- MEO is capable of communicating with NEF to call Nnef_trafficinfluence, e.g. MEO acts as AF.

5.3 Key issue #3: Enablers for local access to a DN in a 5GS

5.3.1 Description

A key issue on traffic routing and its enablers refers to clause 5.13 of ETSI TS 123 501 [i.1] (support for Edge Computing). More specifically, there are three ways to enable local access to a DN:

- Uplink Classifier (UL CL);
- IPv6 multi-homed PDU session; and
- Local Area Data Network (LADN).

In further detail:

- As per clause 5.6.4.2 of ETSI TS 123 501 [i.1]: *"the UL CL is a functionality supported by a UPF that aims at diverting (locally) some traffic matching traffic filters provided by the SMF. The insertion and removal of an UL CL is decided by the SMF and controlled by the SMF using generic N4 and UPF capabilities. The UE is unaware of the traffic diversion by the UL CL, and does not involve in both the insertion and the removal of UL CL"*.

- As per clause 5.6.4.3 of ETSI TS 123 501 [i.1]: *"a PDU Session may be associated with multiple IPv6 prefixes. This is referred to as multi-homed PDU Session. The multi-homed PDU Session provides access to the Data Network via more than one PDU Session Anchor. When the UE requests a PDU Session of type "IPv4v6" or "IPv6" the UE also provides an indication to the network whether it supports a Multi-homed IPv6 PDU Session"*.

- As per clause 5.6.5 of ETSI TS 123 501 [i.1]: *"the access to a DN via a PDU Session for a LADN is only available in a specific LADN service area. A LADN service area is a set of Tracking Areas. LADN is a service provided by the serving PLMN. The UE is configured to know whether a DNN is a LADN DNN and an association between application and LADN DNN"*.

From the above, it is evident that, in contrast to traffic redirection using a UL CL, IPv6 multi-homed PDU session and LADN require some level of interaction with the UE to support traffic redirection to the local DN. As a result of such interaction, both these ways of traffic redirection may impact the UE (the former may crucially impact the UE and is only applicable to IPv6 traffic, whereas the latter may impact the UE less significantly). On top of that, LADN imposes geographical constraints, which would introduce performance challenges in high mobility environment (e.g. automotive use cases), because the UE would have to frequently establish and release the PDU Session to the LADN, thus causing significant signaling traffic. Hence, the issue lies in supporting access to a local DN in a 5GS, in a way that minimally impacts the UE and best addresses the use case, while minimizing signaling load in the system.

5.3.2 Solution proposal #1: UE capability and use case-aware traffic redirection

With regards to routing complexity, the UL CL relies on traffic enforcement (e.g. tunnelling) between the "offloading point" at the UL CL and the destination in the local DN.

NOTE: As per ETSI TS 123 501 [i.1], the mechanisms for packet forwarding on the N6 reference point between the PDU Session Anchor providing local access and the DN highly rely on UE capability, so it is up to the operator to determine whether the UL CL is the best approach in all possible deployments.

It is up to operators to determine based on UE capability which approach (or combination of approaches) of traffic routing within the 5GC network for edge computing is best applicable to the use case and best addresses the trade-off between UE signalling overhead and routing complexity. For instance, in a scenario where the local access is strongly correlated with the geographic location, LADN may be preferable, as compared to UL CL, because it relies on plain IP routing on the N6 reference point.

However, at the initial stage of 5G commercialization, operators are more likely to adopt UL CL, then LADN for geographic location service, when terminals supporting multiple DNNs. But for IPv6 multi-homed PDU session, it will be introduced late, and it is not sure, whether there are requirements on terminals, networks and services.

5.3.3 Evaluation

The proposed solution is technically feasible, on condition of the network being aware of UE capabilities and traffic routing operation requirements for the considered use cases.

5.4 Key issue #4: Support for the Radio Network Information Service

5.4.1 Description

One of the key standardized services that may be offered by the Multi-access Edge Computing Platform (MEP) is the Radio Network Information Service (RNIS) as specified in ETSI GS MEC 012 [i.8]. From the description of the service, it is stated that the information provided may include:

- up-to-date radio network information regarding radio network conditions;
- measurement information related to the user plane based on 3GPP specifications;
- information about UEs connected to the radio node(s) associated with the MEC host, their UE context and the related radio access bearers;
- changes on information related to UEs connected to the radio node(s) associated with the MEC host, their UE context and the related radio access bearers.

The service is provided northbound, i.e. from the MEP to service consuming applications. The southbound interface from the MEP to the entity providing information, such as 3GPP UE connection specific Radio Resource Control (RRC) measurement information, is not currently in scope of the RNIS specification, or the overall MEC system specifications. Therefore, the key issue to be raised in this clause is by which means might the RNIS source the information it exposes in relation to the 5GS. A linked key issue is whether RNIS itself requires further enhancement to expose further 5G Radio Access Network (RAN) specific radio network information, particularly lower layer information in support of centralized coordinated beam management approaches for instance. Of note is that version 2 of the RNIS specification already includes 5G New Radio (NR) RRC measurement related information reporting, but currently not lower layer information.

In the 5GS, specifically the 5GC, the Network Functions (NFs) and the services they produce are registered in Network Resource Function (NRF). Clause 7.2 of ETSI TS 123 501 [i.1] details the available Network Function Services. Relevant to RNIS, the Access and Mobility Management Function (AMF) NF does enable other NF consumers to subscribe or get notified of (UE) mobility related events and statistics. MEC acting as an AF could be such a subscriber, through the Network Exposure Function (NEF) if necessary. However, capabilities to expose more detailed RAN information (e.g. RRC measurement information) to NF consumers are not currently specified.

5.4.2 Solution proposal #1: O-RAN RIC

In addition to ETSI ISG MEC, there are other (non-SDO) groups such as the O-RAN Alliance (https://www.o-ran.org/) interested in capturing 3GPP RAN related information. The O-RAN reference architecture, depicted in figure 5.4.2-1, includes familiar 3GPP entities such as the Central Unit (CU), Distributed Unit and Radio Unit (RU). It also includes O-RAN specific entities such as the Radio Network Information Base (R-NIB) within the RAN Intelligent Controller (RIC) near-Real Time (RT). The R-NIB captures the near-RT state of the underlying radio network via the E2 interface and receives commands from the RIC non-RT via the A1 interface. Both are O-RAN defined interfaces and it is the former that is most relevant to MEC and provision of a RNIS service. This is because it is through the E2 interface that data is fed into the RIC near-RT (specifically the R-NIB), where the data includes various RAN measurements. In the context of the near-RT RIC, such RAN information is expected to be used to facilitate "next generation" radio resource management (RRM). This is to be based on real-time analytics, which are targeted at driving embedded machine learning systems and artificial intelligence backend modules. Such systems and modules will be aimed at empowering network intelligence that is expected to, for instance, enhance decisions and predictions relating to user mobility and traffic load. One possible solution for this is for example utilizing an E2 supported RNIS to achieve similar goals and provide input to the near-RT RIC. In this scenario the exposed radio network information would remain within operator's trust domain. Even so, at a more general level, what is of primary interest is the use and availability of the O-RAN defined E2 interface to provide a source of information to facilitate the RNIS and in doing so provide a solution to the key issue describe in clause 5.4.1. The open issue is that there is no 3GPP defined entity that currently supports the E2 interface for radio network information exposure. This proposed solution would be bound by the requirement to only securely expose information to authenticated and authorized AF. Depending on the operator deployment and as described in clause 5.2.5 of [i.1], this exposure could either be directly to the AF or through the external exposure framework via the NEF.

A diagram illustrating the architecture as described above can be found at https://www.o-ran.org/.

5.4.3 Evaluation

It was highlighted in clause 5.4.1 that the 5GS does not currently specify capabilities to expose lower layer detailed RAN information (e.g. RRC measurement information) to NF consumers, which would be required in order to provide all components of the MEC RNIS. However, it has been identified that there are alternative means to obtain such information. One such example is provided in the solution described in clause 5.4.2. This clause highlights that 3GPP radio network deployments based on the O-RAN reference architecture may support the capability to expose such RAN information if the O-RAN specified E2 interface is supported. The practicality of extracting such information has also been demonstrated through the O-RAN Software Community initiative, specifically the RIC Measurement Campaign application [i.17]. This is an RIC hosted application (termed xApp [i.18]) that supports calculation of a number of metrics and KPIs based on information extracted from 3GPP specified X2 (inter-eNB interface) messages, exposed to the xApp over E2. These messages include those relating to UE measured signal power, e.g. Reference Signal Receive Power (RSRP), which is typical of the RAN information exposed by RNIS.

Therefore the evaluation to Key Issue #4 is that not all deployments will have the capability to provide all components of the MEC RNIS. However, there are deployment options available if that is a critical requirement for the MEC service provider in combination with the PLMN provider, where such deployment options are not covered by a standard or dependent on a standard.

5.5 Key Issue #5: AF Influence on traffic routing

5.5.1 Description

This key issue about MEC as AF influence traffic routing refers to clause 5.6.7 of ETSI TS 123 501 [i.1].

The MEC system may send requests to influence SMF routing decisions for User Plane traffic of PDU Sessions. MEC requests may influence UPF (re)selection and allow routing of user traffic to a local access (identified by a DNAI) to a data network. The AF may also provide in its request subscriptions to SMF events.

But all this applies to non-roaming and to LBO deployment, not home routed deployments.

The MEC system may send request to PCF directly or use the NEF to interact with the 5GC, depending on operators' strategy.

If the MEC system interacts with PCF via the NEF, the NEF performs the mappings where needed, described in ETSI TS 123 502 [i.2], clause 4.3.6.

MEC requests refer to an individual UE by its UE address. Of course such requests target an on-going PDU Session. These requests are routed (by the AF or by the NEF) to an individual PCF. If necessary, the UE's PCF is determined using the BSF.

MEC requests described in clause 5.6.7 of ETSI TS 123 501 [i.1] targeting a group of UE(s), or any UE accessing a combination of DNN and S-NSSAI, or targeting individual UE by a GPSI as described in table 5.6.7-1 may also affect UE(s) with an established PDU session. For such requests the AF contacts the NEF and the NEF stores the AF request information in the UDR. PCF(s) receive a corresponding notification if they had subscribed to the creation/modification/deletion of the AF request information corresponding to UDR data keys/data sub-keys. Such requests can target on-going or future PDU sessions.

5.5.2 Solution Proposal #1: AF request targeting an individual UE

Figure 5.5.2-1 copied from ETSI TS 123 502 [i.2], figure 4.3.6.4-1, introduces the flow for processing AF requests to influence traffic routing for sessions identified by an individual UE address.

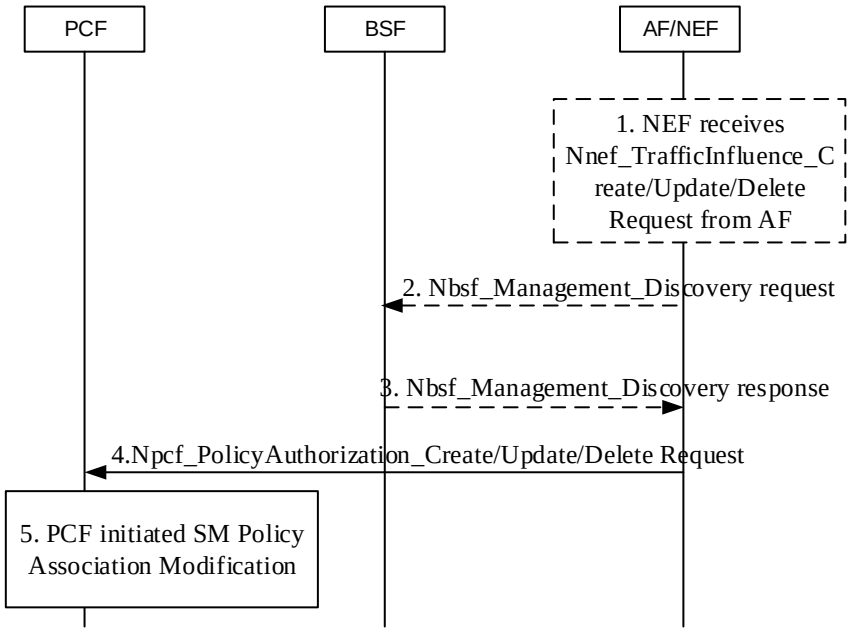

Figure 5.5.2-1: Handling an AF request targeting an individual UE address to the relevant PCF (ETSI TS 123 502 [i.2])

Depending on the AF deployment (see ETSI TS 123 501 [i.1], clause 6.2.10), the AF may send the AF request to PCF directly, in which case step 1 is skipped, or via the NEF. In addition. Step 1 is referred to ETSI TS 129 514 [i.19].

If AF/NEF does not know the PCF in which the UE is located, it is necessary to inquire at BSF first and find the corresponding PCF through BSF (refer to steps 2 and 3). Of course AF/NEF finds the BSF based on local configuration or using the NRF, by providing at least the UE address.

The PCF updates the SMF with corresponding new PCC rule(s) with PCF initiated SM Policy Association Modification procedure as described in ETSI TS 123 502 [i.2], clause 4.16.5.2. When a PCC rule is received from the PCF, the SMF may take appropriate actions, when applicable, to reconfigure the User plane of the PDU Session to realize the function of AF request targeting an individual UE.

5.5.3 Solution Proposal #2: AF request targeting a group of UEs

Figure 5.5.3-1 copied from ETSI TS 123 502 [i.2], figure 4.3.6.2-1,introduces the flow for processing AF requests to influence traffic routing for sessions not identified by a UE address, which means AF request targeting a group of UEs.

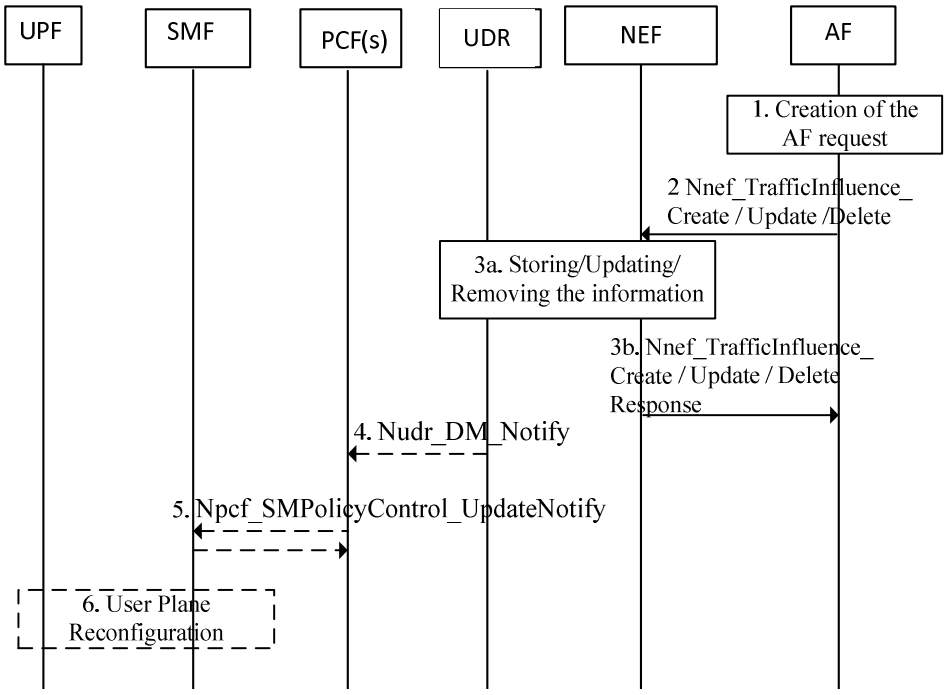

Figure 5.5.3-1: Processing AF requests to influence traffic routing for Sessions not identified by an UE address(ETSI TS 123 502 [i.2])

This is a complete signaling procedure, from the creation of the AF Request to the User Plane reconfiguration . AF sends the request to NEF, NEF stores/updates/removes the request information to UDR. PCF subscribes the UDR data updating in advance. So the UDR will therefore push data to PCF. PCF forms SM strategy to SMF, SMF reconfigures the User Plane according to SM strategy from PCF.

Also this procedure is targeting a group of UEs for the ongoing PDUs or future PDUs.

5.5.4 Evaluation

The proposed solution is technically feasible, in cases when the MEC as AF is trusted or not. Cases affecting a specific UE or a group of UEs are covered. It applies to non-roaming and to LBO deployment, but not to home routed deployments.

5.6 Key Issue #6: Mapping MEC API framework to CAPIF

5.6.1 Description

When replacing the Mp1 parts that are related to service registry, service discovery and service announcement by CAPIF, a mapping is necessary. Mapping includes resources mapping and information model mapping.

This key issue describes the current situation and explores ways towards achieving such mapping.

5.6.2 Solution proposal #1: Mapping of the APIs

5.6.2.1 Overview

The mapping between the MEC and CAPIF APIs needs to include:

- Mapping of the URI structures.
- Mapping of the service discovery query parameters.
- Mapping of the data models for the payload bodies of the RESTful protocols.

Clause 5.6.2.2 provides an initial mapping of the URI structures and clause 5.6.2.3 defines an initial mapping of the service discovery URI query parameters.

Clause 5.6.2.4 provides the relevant HTTP message body data types defined by CAPIF and MEC for API discovery, publication and announcement. Referenced named types are folded in to provide comprehensive information about the attribute sets that are available in each message body. This information can be used to define guidelines or provisions how MEC services can be published, discovered and announced using CAPIF replacing the service management part of ETSI GS MEC 011 [i.10]. The definition of these detailed guidelines or provisions is beyond the scope of the present document.

5.6.2.2 Mapping of the resource structures

The resource structure of the MEC service management API as defined in ETSI GS MEC 011 [i.10] can be mapped to the CAPIF resources as defined in ETSI TS 129 222 [i.11].

Table 5.6.2.2-1 shows the mapping of MEC resources to CAPIF resources. This mapping shows which CAPIF resources can be used to represent particular MEC resources, and also indicates the gaps.

Table 5.6.2.2-1: Mapping of MEC resources and CAPIF resources for service management and discovery

MEC resource name	MEC resource URI	CAPIF resource name	CAPIF resource URI
A list of meService	mec_service_mgmt/v1/service	All published service APIs	/service-apis/v1/allServiceApis
Individual meService	mec_service_mgmt/v1/services/{serviceId}	-	-
A list of meTransport	mec_service_mgmt/v1/transports	- (subset is part of service API information)	-
A list of meService of an application instance	mec_service_mgmt/v1/applications/{appInstanceId}/services	APF published APIs	/published-apis/v1/{apfId}/service-apis
Individual meService of an application instance	mec_service_mgmt/v1/applications/{appInstanceId}/services/{serviceId}	Individual APF published API	/published-apis/v1/{apfId}/service-apis/{serviceApiId}
Parent resource of all meMp1Subscription of a subscriber	mec_service_mgmt/v1/applications/{appInstanceId}/subscriptions	CAPIF Events Subscriptions	/capif-events/v1/{subscriberId}/subscriptions/
Individual meMp1Subscription	mec_service_mgmt/v1/applications/{appInstanceId}/subscriptions/{subscriptionId}	Individual CAPIF Events Subscription	/capif-events/v1/{subscriberId}/subscriptions/{subscriptionId}

5.6.2.3 Mapping of the service discovery queries

CAPIF has a large set of URI query parameters for the Service discovery query (GET request to/service-apis/v1/allServiceApis). MEC has a more compact list. Some CAPIF URI query parameters may be mapped to MEC payload body attributes. In general, there is a set of MEC parameters that cannot be mapped to CAPIF counterparts currently.

Table 5.6.2.3-1 shows the mapping of service discovery query parameters.

Table 5.6.2.3-1: Mapping of service discovery query parameters of MEC and CAPIF

CAPIF query parameter	MEC query parameter	Can map to other MEC attribute
api-invoker-id	-	{applicationId} of the requesting MEC app
api-name	ser_name	n/a
api-version	-	version string in MEC resource URI
comm-type	-	TransportTypes (partial)
protocol	-	TransportInfo/protocol
aef-id	-	{applicationId} of the service-producing MEC app
data-format	-	ServiceInfo/serializer
supported-features	-	-
-	ser_instance_id	
-	ser_category_id	
-	scope_of_locality	
-	consumed_local_only	
-	is_local	

5.6.2.4 Data models for service API discovery and publication

5.6.2.4.1 MEC: Data model for MEC services

Table 5.6.2.4.1-1 has been created by joining the following types into the "ServiceInfo" type:

- TransportInfo
- SerializerTypes
- LocalityTypes
- SecurityInfo
- CategoryRef
- EndPointInfo

The "ServiceInfo" type and the above-mentioned types that were joined into it are documented in ETSI GS MEC 011 [i.10].

Table 5.6.2.4.1-1: MEC type "ServiceInfo" with appropriate other types expanded inline (source: ETSI GS MEC 011 [i.10])

Attribute name	Data type	Cardinality	Description
serInstanceId	*String*	*0..1*	*Identifier of the service instance assigned by the MEPM/MEC platform. For the uniqueness of the identifier across the MEC system, UUID format [i.22] is recommended.* *Shall be absent in POST requests, and present otherwise.*
serName	*String*	*1*	*The name of the service. This is how the service producing MEC application identifies the service instance it produces.*
serCategory	*CategoryRef*	*0..1*	*A Category reference.* *(The category resource is used to group product offerings, service and resource candidates in logical containers. Categories may contain other categories and/or product offerings, resource or service candidates.) (see note 1)* *For the serCategory, the example values include:* • *"RNI"* • *"Location"* • *"Bandwidth Management".*
>href	*URI*	*1*	*Reference of the catalogue.*
>id	*String*	*1*	*Unique identifier of the category.*
>name	*String*	*1*	*Name of the category.*
>version	*String*	*1*	*Category version.*
version	*String*	*1*	*The version of the service.*

Attribute name	Data type	Cardinality	Description
state	*Enum (inlined)*	*1*	*Contains the service state: ACTIVE, INACTIVE.*
transportId	*String*	*0..1*	*Identifier of the platform-provided transport to be used by the service. Valid identifiers may be obtained using the "Transport information query" procedure. May be present in POST requests to signal the use of a platform-provided transport for the service, and shall be absent otherwise. See note 2.*
transportInfo	*TransportInfo*	*0..1*	*Information regarding the transport used by the service. May be present in POST requests to signal the use of an application-provided transport for the service, and shall be present otherwise. See note 2.*
>id	*String*	*1*	*The identifier of this transport.*
>name	*String*	*1*	*The name of this transport.*
>description	*String*	*0..1*	*Human-readable description of this transport.*
>type	*TransportTypes*	*1*	*Type of the transport.* • *REST_HTTP* • *MB_TOPIC_BASED* • *MB_ROUTING* • *MB_PUBSUB* • *RPC* • *RPC_STREAMING* • *WEBSOCKET*
>protocol	*String*	*1*	*The name of the protocol used. Shall be set to "HTTP" for a REST API.*
>version	*String*	*1*	*The version of the protocol used.*
>endpoint	*EndPointInfo*	*1*	*Information about the endpoint to access the transport.*
>>uris	*String*	*0..N*	*Entry point information of the service as string, formatted according to URI syntax (see IETF RFC 3986 [i.23]). Shall be used for REST APIs. See note 7.*
>>addresses	*Structure (inlined)*	*0..N*	*Entry point information of the service as one or more pairs of IP address and port. See note 7.*
>>>host	*String*	*1*	*Host portion of the address.*
>>>port	*Integer*	*1*	*Port portion of the address.*
>>alternative	*Not specified*	*0..1*	*Entry point information of the service in a format defined by an implementation, or in an external specification. See note 7.*
>security	*SecurityInfo*	*1*	*Information about the security used by the transport.*
>>oAuth2Info	*Structure (inlined)*	*0..1*	*Parameters related to use of OAuth 2.0. Shall be present in case OAuth 2.0 (see IETF RFC 6749 [i.24]) is supported to secure the provision of the service over the transport.*
>>>grantTypes	*Enum (inlined)*	*1..4*	*List of supported OAuth 2.0 grant types.* *Each entry shall be one of the following permitted values:* • *OAUTH2_AUTHORIZATION_CODE* *(Authorization code grant type)* • *OAUTH2_IMPLICIT_GRANT* • *(Implicit grant type)* • *OAUTH2_RESOURCE_OWNER* • *(Resource owner password credentials grant type)* • *OAUTH2_CLIENT_CREDENTIALS* • *(Client credentials grant type)* *Only the value "OAUTH2_CLIENT_CREDENTIALS" is supported in the present document.*
>>>tokenEndpoint	*URI*	*0..1*	*The token endpoint. Shall be present unless the grant type is OAUTH2_IMPLICIT_GRANT.*
>>(extensions)	*Not specified*	*0..N*	*Extensions for alternative transport mechanisms. These extensions depend on the actual transport, and are out of scope of the present document.* *For instance, such extensions may be used to signal the necessary parameters for the client to use TLS-based authorization defined for alternative transports (see ETSI GS MEC 009 [i.16] for more information).*

Attribute name	Data type	Cardinality	Description
>implSpecificInfo	*Not specified*	*0..1*	*Additional implementation specific details of the transport.*
serializer	*SerializerTypes*	*1*	*Indicate the supported serialization format of the service.* • *JSON* • *XML* • *PROTOBUF3*
scopeOfLocality	*LocalityTypes*	*0..1*	*The scope of locality as expressed by "consumedLocalOnly" and "isLocal".* *If absent, defaults to MEC_HOST. See notes 3, 5 and 6.* *Valid values:* • *MEC_SYSTEM* • *MEC_HOST* • *NFVI_POP* • *ZONE* • *ZONE_GROUP* • *NFVI_NODE*
consumedLocalOnly	*Boolean*	*0..1*	*Indicate whether the service can only be consumed by the MEC applications located in the same locality (as defined by scopeOfLocality) as this service instance (TRUE) or not (FALSE).* *Default to TRUE if absent.*
isLocal	*Boolean*	*0..1*	*Indicate whether the service is located in the same locality (as defined by scopeOfLocality) as the consuming MEC application (TRUE) or not (FALSE).* *Default to TRUE if absent. See note 4.*
NOTE 1: The service category may be included in the application descriptor. It may be allocated by the operator or by the application developer. *NOTE 2: Either transportId or transportInfo but not both shall be present in POST requests.* *NOTE 3: Values NFVI_POP, ZONE and NFVI_NODE are used when the service instance is deployed as a VNF.* *NOTE 4: The isLocal is used only in service availability query response and service availability subscription/notification messages.* *NOTE 5: Value ZONE_GROUP can be used when the service instance is deployed as a VNF.* *NOTE 6: Regarding the value MEC_SYSTEM, if the service is running on the same MEC system as the MEC app, then it will be local to it.* *NOTE 7: Exactly one of "uris", "addresses" or "alternative" shall be present.*			

5.6.2.4.2 CAPIF: Data model for service APIs

Table 5.6.2.4.2-1 has been created by joining the following types into the "ServiceAPIDescription" type:

- AefProfile
- Version
- Resource
- CustomOperation
- Protocol
- DataFormat
- CommunicationType
- Operation
- InterfaceDescription
- ShareableInformation
- PublishedApiPath

The "ServiceAPIDescription" type and the above-mentioned types that were folded in are documented in ETSI TS 129 222 [i.11].

Table 5.6.2.4.2-1: CAPIF type "ServiceAPIDescription" with appropriate other types expanded inline (source: ETSI TS 129 222 [i.11])

Attribute name	Data type	P	Cardinality	Description	Applicability
apiName	*string*	*M*	*1*	*API name, it is set as {apiName} part of the URI structure as defined in clause 4.4 of ETSI TS 129 501 [i.15].*	
apiId	*string*	*O*	*0..1*	*API identifier assigned by the CAPIF core function to the published service API. Shall not be present in the HTTP POST request from the API publishing function to the CAPIF core function. Shall be present in the HTTP POST response from the CAPIF core function to the API publishing function and in the HTTP GET response from the CAPIF core function to the API invoker (discovery API).*	
aefProfiles	*array(AefProfile)*	*M*	*1..N*	*AEF profile information, which includes the exposed API details (e.g. protocol).*	
>aefId	*string*	*M*	*1*	*AEF identifier*	
>versions	*array(Version)*	*M*	*1..N*	*API version*	
>>apiVersion	*string*	*M*	*1*	*API major version in URI (e.g. v1)*	
>>expiry	*DateTime*	*O*	*0..1*	*Expiry date and time of the AEF service. This represents the planned retirement date as specified in clause 4.3.1.5 of ETSI TS 129 501 [i.15].*	
>>resources	*array(Resource)*	*O*	*1..N*	*Resources supported by the API. It may include the custom operations with resource association.*	
>>>resourceName	*string*	*M*	*1*	*Resource name*	
>>>commType	*CommunicationType*	*M*	*1*	*Communication type used by the API resource*	
>>>uri	*string*	*M*	*1*	*Relative URI of the API resource, it is set as {apiSpecificResourceUriPart} part of the URI structure as defined in clause 4.4 of ETSI TS 129 501 [i.15].*	
>>>custOpName	*string*	*O*	*0..1*	*it is set as {custOpName} part of the URI structure for a custom operation associated with a resource as defined in clause 4.4 of ETSI TS 129 501 [i.15].*	
>>>operations	*array(Operation)*	*C*	*1..N*	*Supported HTTP methods for the API resource. Only applicable when the protocol in AefProfile indicates HTTP.*	
>>>description	*string*	*O*	*0..1*	*Text description of the API resource.*	
>>custOperations	*array(CustomOperation)*	*O*	*1..N*	*Custom operations without resource association.*	
>>>commType	*CommunicationType*	*M*	*1*	*Communication type used by the API resource* *- REQUEST_RESPONSE* *- SUBSCRIBE_NOTIFY*	
>>>custOpName	*string*	*M*	*1*	*it is set as {custOpName} part of the URI structure for a custom operation without resource association as defined in clause 4.4 of ETSI TS 129 501 [i.15].*	

Attribute name	Data type	P	Cardinality	Description	Applicability
>>>operations	array(Operation)	C	1..N	Supported HTTP methods for the API resource. Only applicable when the protocol in AefProfile indicates HTTP. - GET - POST - PUT - PATCH - DELETE	
>>>description	string	O	0..1	Text description of the custom operation.	
>protocol	Protocol	O	0..1	Protocol used by the API. - HTTP_1_1 - HTTP2	
>dataFormat	DataFormat	O	0..1	Data format used by the API - JSON	
>securityMethods	array(SecurityMethods)	O	1..N	Security methods supported by the AEF for all interfaces. Certain interfaces may have different security methods supported in the attribute interfaceDescriptions. - PSK - PKI - OAUTH	
>domainName	string	O	0..1	Domain to which API belongs to (NOTE 1)	
>interfaceDescriptions	array(InterfaceDescription)	O	1..N	Interface details (NOTE 1)	
>>ipv4Addr	Ipv4Addr	O	0..1	String identifying an IPv4 address (NOTE 3)	
>>ipv6Addr	Ipv6Addr	O	0..1	String identifying an IPv6 address (NOTE 3)	
>>port	Port	O	0..1	Port	
>>securityMethods	array(SecurityMethods)	M	1..N	Security methods supported by the interface. It takes precedence over the security methods provided in AefProfile, for this specific interface - PSK - PKI - OAUTH	
description	string	O	0..1	Text description of the API	
supportedFeatures	SupportedFeatures	O	0..1	Used to negotiate the supported optional features of the API as described in ETSI TS 129 222 [i.11], clause 7.8. This attribute shall be provided in the HTTP POST request and in the response of successful resource creation.	
shareableInfo	ShareableInformation	O	0..1	Represents whether the service API and/or the service API category can be published to other CCFs.	
>isShareable	boolean	M	1	Set to "true" indicates that the service API and/or the service API category can be shared to the list of CCF provider domain information. Otherwise set to "false"	
>ccfProvderDomains	array(string)	O	1..N	List of CCF provider domains to which the service API information to be shared.	
serviceAPICategory	string	O	0..1	The service API category to which the service API belongs to.	
apiSuppFeats	SupportedFeatures	O	0..1	The features supported by the service API indicated by the apiId attribute. See ETSI TS 129 571 [i.9]	ApiSupportedFeaturePublishing
pubApiPath	PublishedApiPath	C	0..1	It contains the published API path within the same CAPIF provider domain. it shall be provided by the CCF when publishing the service API to other CCF via the CAPIF-6 reference point.	

Attribute name	Data type	P	Cardinality	Description	Applicability
>ccfIds	array(string)	O	1..N	A list of CCF identifiers where the service API is already published.	
NOTE 1: Only one of the attributes "domainName" or "interfaceDescriptions" shall be included. NOTE 2: Notification or callback type of resource is not included. NOTE 3: Only one of the attributes "ipv4Addr" or "ipv6Addr" shall be included.					

5.6.2.5 Data models for service API announcement/notification

5.6.2.5.1 MEC: Data model for service availability subscriptions and notifications

Table 5.6.2.5.1-1 reflects the "SerAvailabilityNotificationSubscription" type:

Table 5.6.2.5.1-1: MEC type "SerAvailabilityNotificationSubscription (source: ETSI GS MEC 011 [i.10])

Attribute name	Data type	Cardinality	Description
subscriptionType	String	1	Shall be set to "SerAvailabilityNotificationSubscription".
callbackReference	URI	1	URI selected by the MEC application instance to receive notifications on the subscribed MEC service availability information. This shall be included in both the request and the response.
_links	Structure (inlined)	0..1	List of hyperlinks related to the resource. This shall only be included in the HTTP responses.
>self	LinkType	1	Self-referring URI.
filteringCriteria	Structure (inlined)	0..1	Filtering criteria to match services for which events are requested to be reported. If absent, matches all services. All child attributes are combined with the logical "AND" operation.
>serInstanceIds	SerInstanceId	0..N	Identifiers of service instances about which to report events. See note.
>serNames	SerName	0..N	Names of services about which to report events. See note.
>serCategories	CategoryRef	0..N	Categories of services about which to report events. See note.
>states	ServiceState	0..N	States of the services about which to report events. If the event is a state change, this filter represents the state after the change.
>isLocal	Boolean	0..1	Restrict event reporting to whether the service is local to the MEC platform where the subscription is managed.
NOTE: The attributes "serInstanceIds", "serNames" and "serCategories" provide mutually-exclusive alternatives to define a set of services. Only one of them may be present.			

Table 5.6.2.5.1-2 reflects the "ServiceAvailabilityNotification" type.

Table 5.6.2.5.1-2: MEC type "ServiceAvailabilityNotification" (source: ETSI GS MEC 011 [i.10])

Attribute name	*Data type*	*Cardinality*	*Description*
notificationType	*String*	*1*	*Shall be set to "SerAvailabilityNotification".*
serviceReferences	*Structure (inlined)*	*1..N*	*List of links to services whose availability has changed.*
>link	*LinkType*	*0..1*	*Link to the resource representing the individual service. Shall be present unless "changeType"="REMOVED".*
>serName	*SerName*	*1*	*Name of the service*
>serInstanceId	*SerInstanceId*	*1*	*Identifier of the service*
>state	*ServiceState*	*1*	*State of the service after the modification.*
>changeType	*Enum (inlined)*	*1*	*Type of the change.* *Valid values:* • *ADDED: The service was newly added.* • *REMOVED: The service was removed.* • *STATE_CHANGED: Only the state of the service was changed.* • *ATTRIBUTES_CHANGED: At least one attribute of the service other than state was changed. The change may or may not include changing the state.*
_links	*Structure (inlined)*	*1*	*Object containing hyperlinks related to the resource.*
>subscription	*LinkType*	*1*	*A link to the related subscription.*

5.6.2.5.2 CAPIF: Event subscription and event notification

Table 5.6.2.5.2-1 has been created by joining the following types into the "EventSubscription" type:

- CAPIFEvent
- CAPIFEventFilter

The "EventSubscription" type and the above-mentioned types that were folded in are documented in ETSI TS 129 222 [i.11].

Table 5.6.2.5.2-1: CAPIF type "EventSubscription" with appropriate other types expanded inline (source: ETSI TS 129 222 [i.11])

Attribute name	Data type	P	Cardinality	Description	Applicability
events	*array(CAPIFEvent)*	*M*	*1..N*	*Subscribed events* *Valid values related to publish and discover:* - *SERVICE_API_AVAILABLE* - *SERVICE_API_UNAVAILABLE* - *SERVICE_API_UPDATE*	
eventFilters	*array(CAPIFEventFilter)*	*O*	*1..N*	*Subscribed event filters. The n^{th} entry in the "eventFilters" attribute shall correspond to the n^{th} entry in the "events" attribute. For event not having event filter, an empty event filter entry without any sub-attribute shall be provided.*	*Enhanced_event_report*
>apiIds	*array(string)*	*O*	*1..N*	*API identifiers that the event subscriber wants to know in the interested event.*	
>apiInvokerIds	*array(string)*	*O*	*1..N*	*API invokers that the event subscriber wants to know in the interested event.*	
>aefIds	*array(string)*	*O*	*1..N*	*String identifying the AEF.*	
eventReq	*ReportingInformation*	*O*	*0..1*	*Represents the reporting requirements of the event subscription.* *This is a policy defined in ETSI TS 129 523 [i.21].*	*Enhanced_event_report*
notificationDestination	*Uri*	*M*	*1*	*URI where the notification should be delivered to.*	
requestTestNotification	*boolean*	*O*	*0..1*	*Set to true by Subscriber to request the CAPIF core function to send a test notification as defined in ETSI TS 129 222 [i.11], clause 7.6. Set to false or omitted otherwise.*	*Notification_test_event*
websockNotifConfig	*WebsockNotifConfig*	*O*	*0..1*	*Configuration parameters to set up notification delivery over Websocket protocol as defined in ETSI TS 129 222 [i.11], clause 7.6. (data type imported from ETSI TS 129 222 [i.11])*	*Notification_websocket*
supportedFeatures	*SupportedFeatures*	*O*	*0..1*	*Used to negotiate the supported optional features of the API as described in ETSI TS 129 222 [i.11], clause 7.8. This attribute shall be provided in the HTTP POST request and in the response of successful resource creation. (data type imported from ETSITS 129 571 [i.9])*	

Table 5.6.2.5.2-1 reflects the "EventNotification" type with the "CAPIFEventDetail" data type folded in.

The "EventSubscription" type and the "CAPIFEventDetail" type that was folded in are documented in ETSI TS 129 222 [i.11].

Table 5.6.2.5.2-2: CAPIF type "EventNotification" with appropriate other types expanded inline (source: ETSI TS 129 222 [i.11])

Attribute name	Data type	P	Cardinality	Description	Applicability
subscriptionId	*string*	*M*	*1*	*Identifier of the subscription resource to which the notification is related - CAPIF resource identifier*	
events	*CAPIFEvent*	*M*	*1*	*Notifications of individual events*	
eventDetail	*CAPIFEventDetail*	*O*	*0..1*	*Detailed information for the event.*	*Enhanced_event_report*
>serviceAPIDescriptions	*array(ServiceAPIDescription)*	*O*	*1..N*	*Description of the service API as published by the APF.*	
>apiIds	*array(string)*	*O*	*1..N*	*API identifiers.*	
>apiInvokerIds	*array(string)*	*O*	*1..N*	*API invokers that are onboarded/offboarded.*	
>accCtrlPolList	*AccessControlPolicyListExt*	*O*	*0..1*	*Access control policy updated list.*	
>invocationLogs	*array(InvocationLog)*	*O*	*1..N*	*Invocation logs*	

5.6.3 Evaluation

It appears possible to use CAPIF to signal MEC services, as long as these MEC services expose a REST API but do not use alternative transports. In case of using CAPIF, authentication of access to the MEC services has to be performed according to CAPIF, not according to MEC.

The following gaps exist currently in CAPIF:

- Info model extensions storage would enable more MEC use cases (3GPP supports in the NRF registry the use of vendor-specific extensions as per ETSI TS 129 500 [i.20], clause 6.6.3, this could be ported to CAPIF).
- CAPIF does not support service deactivation (i.e. setting a service to inactive). This would mean that such service would need to be de-registered in CAPIF, or that functionality would need to be added to CAPIF to deactivate a service.

As part of possible follow-up work, it could be documented e.g. in an Annex of ETSI GS MEC 011 [i.10] how to publish, discover and announce a MEC service using CAPIF.

5.7 Key Issue #7: MEC application consumes 5GC exposed capabilities

5.7.1 Description

The 5G NF Network Exposure Function (NEF) supports external exposure of capabilities of network functions. External exposure which refers to clause 4.15.2 of ETSI TS 123 502 [i.2] can be categorized as Monitoring capability, Provisioning capability, Policy/Charging capability, network status reporting capability, and Analytics reporting capability. MEC applications should be able to be supported to consume these network capabilities.

5.7.2 Solution proposal #1: MEC application accesses NEF directly

Figure 5.7.2-1 shows the flow for a MEC application accessing the NEF directly.

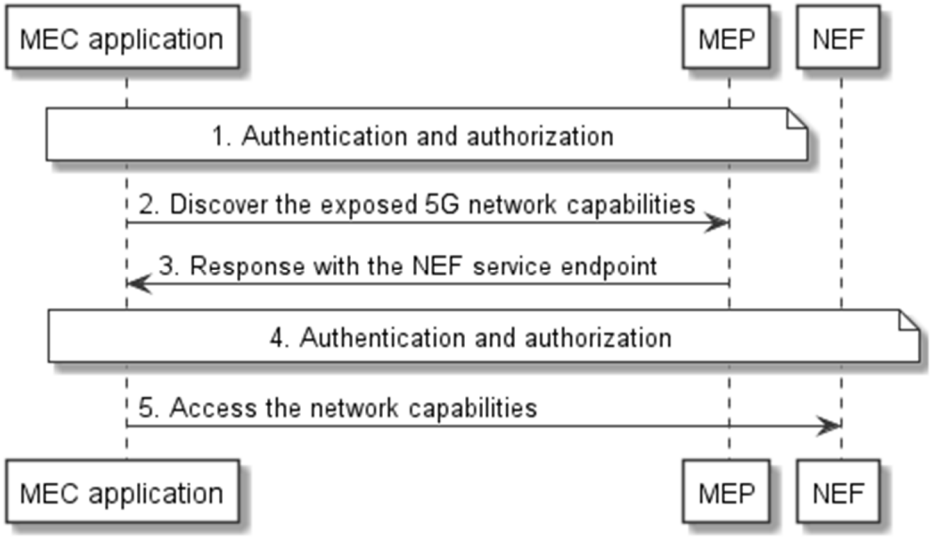

Figure 5.7.2-1: MEC application accesses NEF directly

1. MEP authenticates the MEC application and authorizes it to access the network capabilities.
2. MEC application discovers the exposed 5GC network capabilities via Mp1 through MEP.
3. MEP responses with the NEF service endpoint which provides the requested network capabilities.
4. NEF authenticates the MEC application and authorizes it to access the network capabilities.
5. MEC application sends request to NEF service endpoint to access the network capabilities, and may require notification in case of network functionality/status change.

5.7.3 Solution proposal #2: MEP proxies MEC application to access NEF

Figure 5.7.3-1 shows the flow for a MEC application accessing the NEF using MEP as proxy.

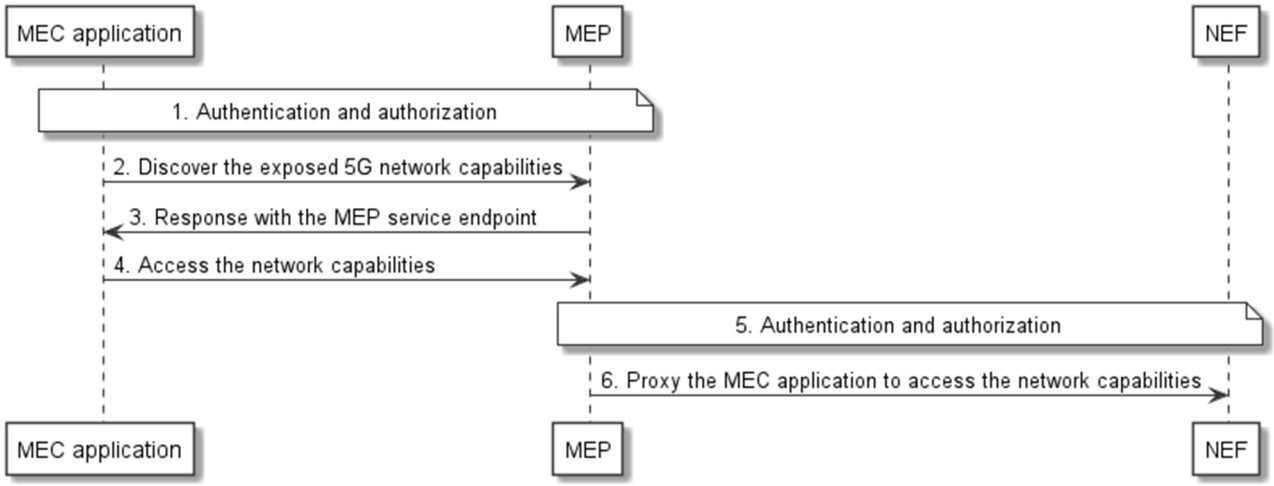

Figure 5.7.3-1: MEP proxies MEC application to access NEF

1. MEP authenticates the MEC application and authorizes it to access the network capabilities.
2. MEC application discovers the exposed 5GC network capabilities via Mp1 through MEP.
3. MEP responses with the service endpoint which points to the MEP itself.
4. MEC application sends request to the service endpoint to access the network capabilities, and may require notification in case of network functionality/status change.

5. NEF authenticates the MEP and authorizes it to access the network capabilities.

6. MEP proxies the MEC application to access the network capabilities from NEF.

5.7.4 Evaluation

Both solution proposals presented in clauses 5.7.2 and 5.7.3 are valid and should be considered as viable solutions for MEC applications to consume 5GC exposed capabilities.

The solutions require that the available 5GC exposed network capabilities can be discovered via Mp1 through MEP, which implies the capabilities are available from the MEC service registry as MEC Platform offered services. This could be achieved through local configuration. As an alternative, if CAPIF is used in the 5GC as the API framework, the MEC Platform may use the discovery capabilities of the CAPIF core function to determine the 5GC exposed network capabilities and populate its own service registry. Further MEC integration options with CAPIF are presented in clause 4.3.

5.8 Key issue #8: Information exposure for MEC Application Instances

5.8.1 Description

Deployment of MEC Hosts and MEC Applications may not be uniform throughout the network. In some locations, one host may serve more than one cell, on the other hand many hosts can be associated with a single cell. MEC Hosts may run more than one instances of the same MEC Application.

MEPM provides DNS/Traffic rules for the data plane. MEC Applications, while being brought up, may enable and select appropriate DNS/Traffic Rules. Service requests, originating from users, are handled by matching against the DNS/Traffic Rules. If there are multiple instances of same MEC Application in a local area, multiple entries are created in Traffic Rule Descriptor of the MEC host.

Recent work in 3GPP SA2 and SA6, related to Edge Computing, indicates that there may be a capability requirement to know about available application instances and make a choice of the instance based on certain criterion.

In case of multiple available MEC application instances, there is no mechanism to determine the best MEC application instance capable of serving user request.

Ongoing work on ETSI GS MEC 016 [i.13] proposes mechanisms to obtain instance address of user application instances by device applications over Mx2 reference point.

There is no mechanism available to obtain MEC application instance address by MEC applications, MEC services from MEC host.

The key issue, which needs to be addressed, is to identify how to expose MEC application instance address to MEC applications, MEC services and user devices.

5.8.2 Solution proposal #1: MEC Platform exposes the information of all running instances

MEC Platform may gather information about all running instances of a MEC Application in this MEC system, such as the IP addresses, CPU load, etc. Some of this information may be obtained from the MEPM and the MEO.

MEC Platform may obtain certain information from 5GS, such as Network Location, Information about user demand in an area, etc. This interaction may happen through NEF or directly in case of trusted AFs.

Application Instance Information gathered by MEP may include:

- **Name** - the FQDN associated with an edge application.
- **IP address** - an IP address associated with the FQDN.

- **Instances Specific Information** such as:
  - **IP address** - edge instance IP address.
  - **CPU/GPU load** - current processing usage, normalized measurement in terms of CPU units maybe used.
  - **Memory load** - current memory usage.
  - **Storage load** - current storage usage.
  - **Request Resolution Latency** - latency required to resolve a request, it is a common metric used in HTTP based services. Indicates the mean time that an application server takes to resolve a request.
  - **Geo-location** - may be used to enable geographical proximity use cases. It is Geo spatial co-ordinate identifying the "Service Area", which is served by an application instance.
  - **Network-location** - identified by the UPF/PSA, with which the local data network is attached.

MEC platform may use this information to assist the DNS handling function for application instance selection.

MEC Platform may also expose this information to the authorized MEC Applications.

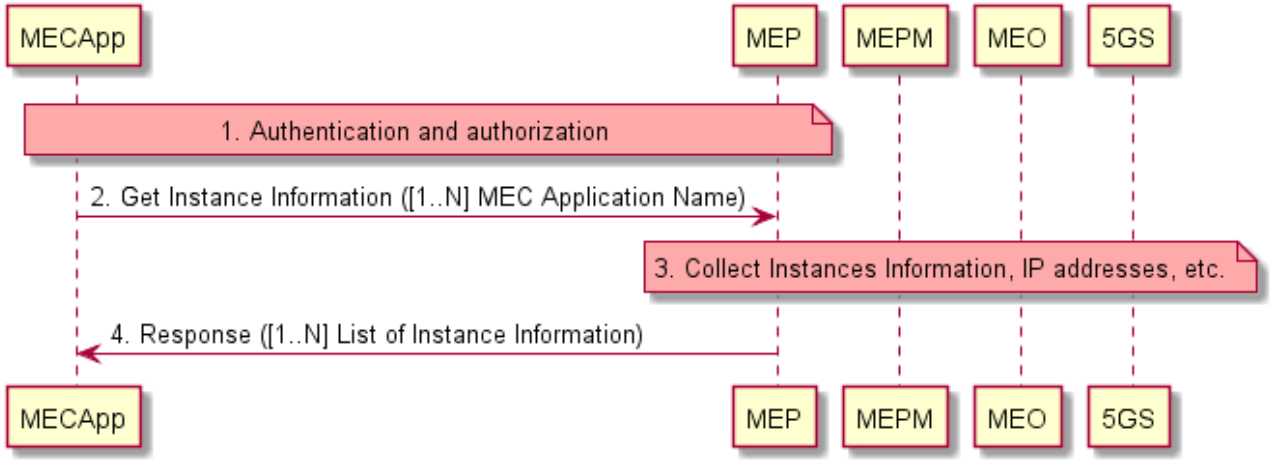

Figure5.8.2-1: Exposing MEC Application Instances Information through MEC Platform

1. MEC Application authenticates with MEP.
2. MEC Application requests for "instance information" of a different MEC App, referencing it by name. It could send a request for one or more "MEC Application Name", i.e. a list of names.
3. For each requested MEC Application Name, MEC system collects information for all instances of that MEC application, such as IP addresses, etc., including interacting with the 5GS.
4. MEP returns a List of Instance Information for each requested MEC Application name.

5.8.3 Evaluation

The proposed solution is technically feasible, subject to the following conditions:

i) the 5GC exposes network specific information; and

ii) that information may be consumed by MEC Applications through MEC Platform offered services.

6 Gap analysis and recommendations

The mapping of the key issues, identified in clause 5, to their associated solutions is provided in table 6-1. This includes highlighting any identified gaps and external dependencies.

Table 6-1: Key issue and solution evaluation

Key issues	Clause #	Solution	Gap	External dependency
#1: Traffic path update for mobility support	5.1	#1: 5GC control plane solution	Yes, ETSI GS MEC 002 [i.25]	3GPP based solution
		#2: D-Plane overlay and AF use for N6 traffic steering policy alignment and enforcement	Yes, ETSI GS MEC 002 [i.25]	3GPP based solution
#2: Ping-pong handover mitigation	5.2	#1: Make use of Nnef_trafficinfluence update	Yes, ETSI GS MEC 002 [i.25]	No
#3: Enablers for local access to a DN in a 5GS	5.3	#1: UE capability and use case-aware traffic redirection	No	3GPP based solution
#4: Support for the Radio Network Information Service	5.4	#1: O-RAN RIC	No	O-RANbased solution
#5: AF Influence on traffic routing	5.5	#1: AF request targeting an individual UE	No	3GPP network capability exposure
		#2: AF request targeting a group of UEs	No	3GPP network capability exposure
#6: Mapping MEC API framework to CAPIF	5.6	#1: Mapping of the APIs	Yes, ETSI GS MEC 011 [i.10]	3GPP CAPIF
#7: MEC application consumes 5GC exposed capabilities	5.7	#1: MEC application accesses NEF directly	Yes, ETSI GS MEC 003 [i.5]	3GPP network capability exposure and CAPIF, if used in the 5GC
		#2: MEP proxies MEC application to access NEF	Yes, ETSI GS MEC 003 [i.5]	3GPP network capability exposure and CAPIF, if used in the 5GC
#8: Information exposure for MEC Application Instances	5.8	#1: MEC Platform exposes the information of all running instances	Yes, ETSI GS MEC-011 [i.10]	3GPP network capability exposure

Taking into account the gap analysis provided in table 6-1, in order to address the identified gaps, extensions to the MEC requirements, architecture and certain reference points are required. It is therefore recommended the following topics need to be addressed in normative follow-up work in ETSI MEC:

- Requirements and possibly related use-cases need to be added to ETSI GS MEC-002 [i.25] related to the interworking between the MEC platform and the 5GC network.
- A new reference point needs to be specified in ETSI GS MEC 003 [i.5] between the MEC platform and the 5GC network. This reference point is used by the MEC platform acting as AF to access to 3GPP Core Network functions and APIs for retrieval of network capability information.
- A description needs to be added, e.g. in an annex of ETSI GS MEC 011 [i.10], on how to publish, discover and announce a MEC service using CAPIF.

A new service may be specified to expose information relating to running application instances.

Annex A:
Change History

Date	Version	Information about changes
2018-11	2.0.0	Initial version of the GR
2018-12	2.0.1	Implements documents MEC(18)000521r1, MEC(18)000522r1, MEC(18)000523r1, MEC(18)000524r1
2019-03	2.0.2	Implements document MEC(19)000055r1
2019-04	2.0.3	Implements documents MEC(19)000073r3, MEC(19)000074r1, MEC(19)000089r1, MEC(95)000095r2, MEC(19)000106r3, MEC(19)000107
2019-06	2.0.4	Implements documents MEC(19)121r1, MEC(19)000159, MEC(19)000160r1, MEC(19)000164r1, MEC(19)000171, MEC(19)000172, MEC(19)000173, MEC(19)000174r1, MEC(19)000175
2019-06	2.0.5	Implements document MEC(19)000163r3
2019-08	2.0.6	Implements document MEC(19)000232. In addition changing the 3GPP TSs to their corresponding ETSI TSs in the list of references.
2019-10	2.0.7	Implements documents MEC(19)000193r1, MEC(19)000304r1, MEC(19)000305r1
2019-10	2.0.8	Implements documents MEC(19)000406r1 and in addition adds the missing figure titles. Implements document MEC(19)000412r2 and in addition adds the missing reference [i.13] to ETSI GS MEC016 and makes editorial corrections in the included text. Implements document MEC(19)000413r1
2019-12	2.0.9	Implements document MEC(19)000391 MEC031 Use cases for MEC and CAPIF integration split from 305 and related editorial fixes Implements document MEC(19)000469 MEC031 fixing CAPIF clause Available Editorial fixes
2020-03	2.0.10	Editorial changes Implement MEC(19)000350r2 - Data plane policy management for MEC relocation Implement MEC(20)000072 MEC031 Move CAPIF to clause 4 Implement MEC(20)000076 MEC031 - Evaluation of Key Issue #3 on enablers for local access to a DN in a 5GS
2020-03	2.0.11	Fix implementation of MEC(20)000076 to use revision 1. MEC(20)000073r1 MEC031 Editors Notes and Editorials clause 3-4 MEC(20)000089 MEC031 Editorial Changes
2020-03	2.0.12	MEC(20)000096r1 MEC031 Addressing EN on available 5GC exposed services (app #157) MEC(20)000102 - MEC031 Editorial corrections round 2 MEC(20)000105 - MEP service registry exposure of 5GC network capabilities
2020-04	2.0.13	MEC(20)000103r1 MEC031 remove some Editor's Notes MEC(20)000120r1 MEC031_proposal_for_editors_note MEC(20)000121r1 MEC031_Soln_KI_Information_exposure_for_MEC_application_instance MEC(20)000123 MEC031 Editors note in clause 4.3.1
2020-04	2.0.14	MEC(20)000134 MEC031 remove incomplete key issue #4 MEC(20)000138r2 MEC0031_KI#9_input_for_editor_note_evaluation_section
2020-06	2.0.15	MEC(19)000150r2 MEC031 Evaluation of KI4 Support for the RNIS MEC(19)000160r1 MEC031 Revision of the solution of key issue 1 Delete double message flows in clause 5.1.2, figures 5.1.2-2 and 5.1.2-4 MEC(20)000180r1 MEC-031 - Descriptions to KI#5: AF Influence on traffic routing MEC(20)000181 MEC-031 - solutions of KI#5:AF Influence on traffic routing MEC(20)000182 MEC-031-Adding reference (Correct reference numbering) MEC(20)000183 MEC-031 - corrections to KI#3:Enablers for local access to a DN in a 5GS MEC(20)000185 MEC031_Correct the MEC host selection

Date	Version	Information about changes
2020-06	2.0.16	MEC(20)000161r2 MEC031 resolving ENs related to CAPIF MEC(20)000196r1 MEC-031 - mending to KI#7:MEC application consumes 5GC exposed capabilities MEC(20)000197 MEC-031 - Evaluation of KI#5: AF Influence on traffic routing
2020-06	2.0.17	Implements MEC(20)000213 MEC031 add missing abbreviations MEC(20)000214 MEC031 editorial corrections Declared stable draft
2020-07	2.0.18	Implements MEC(20)000230 MEC031 Proposal for gap analysis & recommendations clause MEC(20)000232 MEC031 - Evaluation for Key issue #2 MEC(20)000233r3 MEC031 - Evaluation for Key issue #1 MEC(20)000234 MEC031 more editorial fixes
2020-07	2.0.19	Implements MEC(20)000246r1 MEC031 resolving the shall in CAPIF clause MEC(20)000256r1 MEC031 Use 3GPP Release 16 references and some editorials
2020-07	2.0.20	Clean-up done by ***editHelp!***
2020-08	2.0.21	Editorial clean-up done
2020-09	2.0.22	MEC(20)000278r1 MEC031 Fix reference to O-RAN association MEC(20)000279r1 MEC031 Fix comment from RC #1 MEC(20)000280r1 MEC031 Fix comment from RC #2 MEC(20)000281r1 MEC031 Fix comment from RC #3
2020-10	2.0.23	MEC(20)000339 MEC031 Fix comments from second Remote Consensus

History

Document history		
V2.1.1	October 2020	Publication