ETSI GR MEC 038 V3.1.1 (2022-11)

Multi-access Edge Computing (MEC);
MEC in Park Enterprises deployment scenario

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-0038ParkEnterprises

Keywords

authentication, EDGE, location, MEC, UE identity

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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 needed to support MEC deployment in Park Enterprise scenario.

The following aspects are addressed: How 3GPP and MEC system cooperate for UEs to access MEC system based on location (e.g. based on ULCL insertion), including DN-AAA authentication and authorization, MEC application Slicing support, MEC efficient consumption of 5GC exposure capability and dynamic management according to user requirements, remote access of enterprise MEC applications.

In addition the present document considers the related work of other standard/industry bodies such as 3GPP and all related work done in ETSI. The outcome is to generate recommendations for future standard work, e.g. enhancements to current MEC system, interface enhancements, etc.

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 17)".

[i.2] ETSI TS 123 502: "5G; Procedures for the 5G System (5GS) (3GPP TS 23.502 Release 17)".

[i.3] ETSI GS MEC 003: "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[i.4] ETSI GR MEC 031: "Multi-access Edge Computing (MEC); MEC 5G Integration".

[i.5] ETSI GS MEC 011: "Multi-access Edge Computing (MEC); Edge Platform Application Enablement".

[i.6] ETSI GR MEC 001: "Multi-access Edge Computing (MEC); Terminology".

[i.7] ETSI GS MEC 014: "Multi-Access Edge Computing (MEC); UE Identity API".

[i.8] ETSI GS MEC 021: "Multi-access Edge Computing (MEC); Application Mobility Service API".

[i.9] ETSI GS MEC 002: "Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements".

[i.10] ETSI TS 133 501: "5G; Security architecture and procedures for 5G System (3GPP TS 33.501 Release 17)".

[i.11] ETSI GR MEC 024: "Multi-access Edge Computing (MEC); Support for network slicing".

[i.12] ETSI GS MEC 010-2: "Multi-access Edge Computing (MEC); MEC Management; Part 2: Application lifecycle, rules and requirements management".

[i.13] 3GPP TR 28.801: "Telecommunication management; Study on management and orchestration of network slicing for next generation network".

[i.14] 3GPP TR 23.748: "Study on enhancement of support for Edge Computing in 5G Core network (5GC)".

[i.15] ETSI TS 123 548: "5G; 5G System Enhancements for Edge Computing; Stage 2 (3GPP TS 23.548)".

[i.16] ETSI TS 129 518: "5G; 5G System; Access and Mobility Management Services; Stage 3 (3GPP TS 29.518)".

[i.17] ETSI GR MEC 044: "Multi-access Edge Computing (MEC); Study on MEC Application Slices".

[i.18] ETSI TS 123 558: "5G; Architecture for enabling Edge Applications (3GPP TS 23.558 Release 17)".

[i.19] ETSI TS 128 530: "5G; Management and orchestration; Concepts, use cases and requirements (3GPP TS 28.530 Release 17)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR MEC 001 [i.6] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR MEC 001 [i.6] and the following apply:

5GC	5G Core network
5GS	5G System
AF	Application Function
AMF	Access and Mobility management Function
CSMF	Communication Service Management Function
DN	Data Network
DNAI	Data Network Access Identifier
DNN	Data Network Name
FQDN	Fully Qualified Domain Name
GPSI	Generic Public Subscription Identifier
LADN	Local Area Data Network
LBO	Local Break Out
L-NEF	Local Network Exposure Function
NEF	Network Exposure Function
NF	Network Function
NRF	Network Repository Function
NSMF	Network Slice Management 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

PSA	PDU Session Anchor
SMF	Session Management Function
TA	Tracking Area
UDR	Unified Data Repository
UE	User Equipment
UL	UpLink
UL CL	UpLink Classifier
UPF	User Plane Function

4 Overview

The present document studies how MEC system can be used to provide MEC services for Park Enterprises' users based on ULCL insertion from 3GPP 5G network.

Clause 4 provides the description of each identified study area.

Clause 5 proposes 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.

5 Key issues and potential solutions

5.1 Key issue #1: ULCL PSA insertion based on Location

5.1.1 Description

At present, with the development of the Internet and the intensification of innovation, similar enterprises in parks have appeared all over the world. This type of company is small and relies on the unified communications services provided by the park. As 5G/MEC is convenient and fast, it becomes the first choice of communication services in the park.

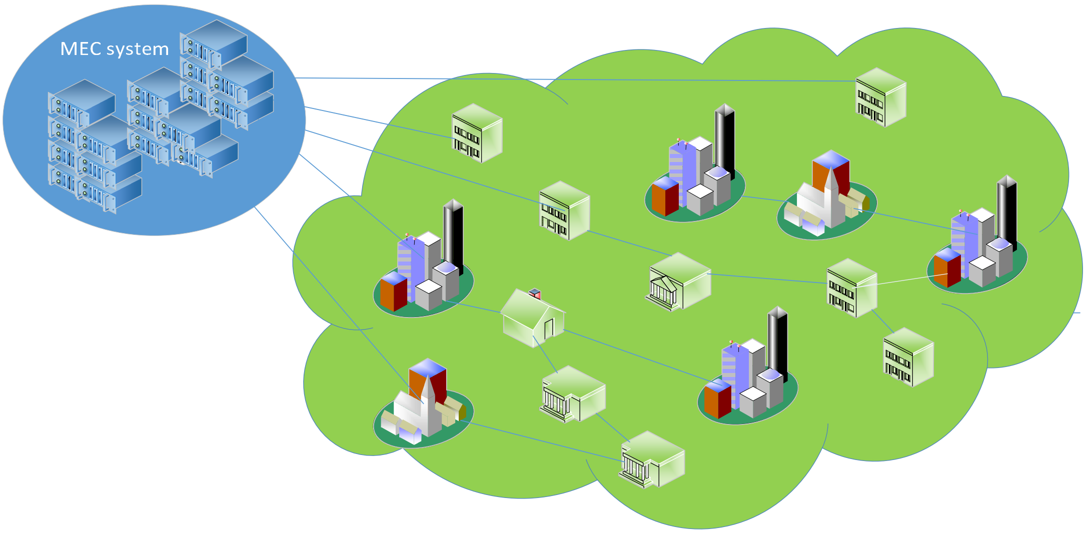


Figure 5.1.1-1: MEC in Park Enterprises

It is known that MEC is a nearby service for users who subscribe to MEC services and move to MEC's service area. 3GPP defines three ways to enable MEC services/local access to a DN, such as:

1) Uplink Classifier (UL CL).

2) IPv6 multi-homed PDU session.

3) Local Area Data Network (LADN).

For an industrial park, a location-based ULCL insertion is generally the preferred solution. The MEC service area of the park is mapped into a new Tracking Area (TA). When the user enters this new TA from other areas, SMF is triggered to insert ULCL PSA for the user. There are two types of operations:

1) If the user does not carry out the central business related to edge applications, SMF establishes edge UPF anchor points in advance for users entering the park, so that the anchor points can be directly placed on the edge DN when launching edge services.

2) If the user is engaged in services related to edge applications, the services will be transferred to the DN deployed on MEC to improve user experience.

The extended question here is whether the user has subscribed to edge MEC service. If the user subscribing to the MEC service has the permission to access to the MEC system, SMF will successfully insert ULCL. Therefore, this scenario is one of the main scenarios in which 5G interacts with MEC, that is, SMF directly enables traffic steering to the MEC system according to the users' location.

5.1.2 Solution proposal #1: AF detecting UE Location and report to PCF

5.1.2.1 Description

MEC system, as an Application Function (AF), can subscribe the location information of users served by MEC system through the NEF network element defined by 3GPP as stated in clause 5.6.7 of ETSI TS 123 501 [i.1]. When the user's location changes, the NEF will inform MEC system of the change.

More specifically, in the MEC system in Park Enterprise scenario, the process can be like the following: the end users initially register to 5G network and go through the central PSA/UPF by default, and there is a central AF deployed in the 5G network docking with all MEC systems at the edge to realize information exchange and enable system configuration and adjustment. When end users enter the park area, the central AF will receive notifications from AMF if the AF subscribes location event earlier. And then, the AF will enable the traffic guidance mode to instruct 3GPP network to add new PSA anchor points and transfer the users' business from the centre to the MEC system.

5.1.2.2 Backgrounds

5.1.2.2.1 NEF service operations information flow

The procedure is used by the AF to subscribe to notifications and to explicitly cancel a previous subscription. Cancelling is done by sending Nnef_EventExposure_Unsubscribe request identifying the subscription to cancel with Subscription Correlation ID. The notification steps 6 to 8 are not applicable in cancellation case.

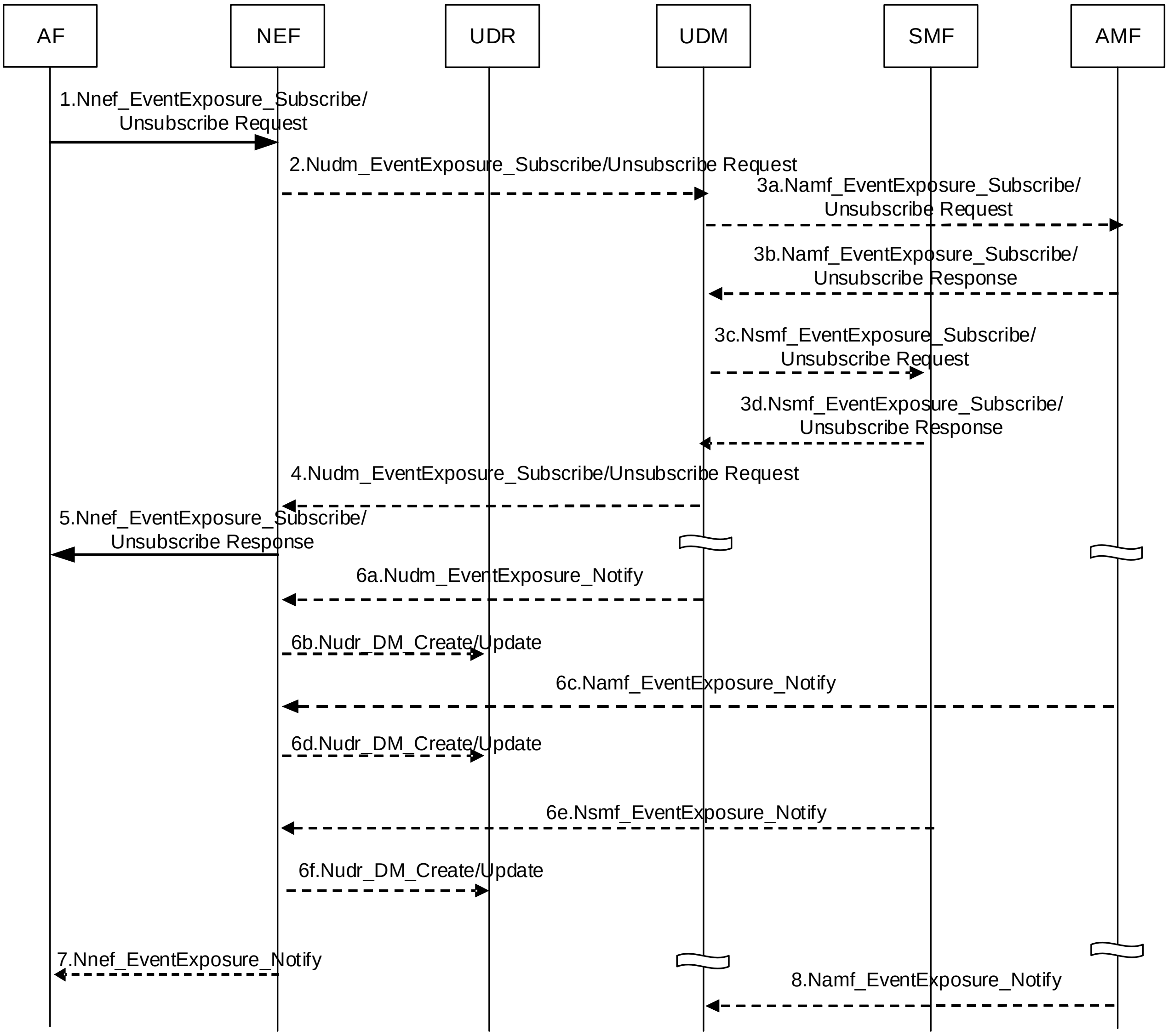

AF
NEF
UDR
UDM
SMF
AMF
1.Nnef_EventExposure_Subscribe/ Unsubscribe Request
2.Nudm_EventExposure_Subscribe/Unsubscribe Request
3a.Namf_EventExposure_Subscribe/ Unsubscribe Request
3b.Namf_EventExposure_Subscribe/ Unsubscribe Response
3c.Nsmf_EventExposure_Subscribe/ Unsubscribe Request
3d.Nsmf_EventExposure_Subscribe/ Unsubscribe Response
4.Nudm_EventExposure_Subscribe/Unsubscribe Request
5.Nnef_EventExposure_Subscribe/ Unsubscribe Response
6a.Nudm_EventExposure_Notify
6b.Nudr_DM_Create/Update
6c.Namf_EventExposure_Notify
6d.Nudr_DM_Create/Update
6e.Nsmf_EventExposure_Notify
6f.Nudr_DM_Create/Update
7.Nnef_EventExposure_Notify
8.Namf_EventExposure_Notify

Figure 5.1.2.2.1-1: Nnef_EventExposure_Subscribe, Unsubscribe and Notify operations

NOTE 1: The procedure is referenced from ETSI TS 123 502 [i.2], with the details described specifically for this solution.

1. The AF subscribes to Location Reporting (identified by Event ID) and provides the associated notification endpoint of the AF (IP address) by sending Nnef_EventExposure_Subscribe request.

   Event Reporting Information defines the type of reporting requested (e.g. one-time reporting, periodic reporting or event based reporting, for Monitoring Events). For this solution, Location Reporting is using event based reporting.

   AF is authenticated and authorized by the NEF if requested. The NEF records the association of the event trigger and the requester identity. The subscription may also include maximum number of reports and/or maximum duration of reporting IE.

2. [Conditional - depending on authorization in step 1] The NEF subscribes to received Event(s) (identified by Event ID) and provides the associated notification endpoint of the NEF to UDM by sending Nudm_EventExposure_Subscribe request. The NEF maps the AF-Identifier into DNN and S-NSSAI combination based on local configuration, and include DNN, S-NSSAI in the request.

   If the reporting event subscription is authorized by the UDM, the UDM records the association of the event trigger and the requester identity. Otherwise, the UDM continues in step 4 indicating failure.

3a. [Conditional] If the requested event (e.g. Location Reporting, monitoring of Loss of Connectivity) requires AMF assistance, then the UDM sends the Namf_EventExposure_Subscribe to the AMF serving the requested user. The UDM sends the Namf_EventExposure_Subscribe request to all serving AMF(s) (if subscription applies to a UE or a group of UE(s)), or all the AMF(s) in the same PLMN as the UDM (if subscription applies to any UE).

As the UDM itself is not the Event Receiving NF, the UDM should additionally provide the notification endpoint of itself besides the notification endpoint of NEF. Each notification endpoint is associated with the related (set of) Event ID(s). This is to assure the UDM can receive the notification of subscription change related event.

If the subscription applies to a group of UE(s), the UDM should include the same notification endpoint of itself, i.e. Notification Target Address (+ Notification Correlation Id), in the subscriptions to all UE's serving AMF(s).

NOTE 2: Using the same notification endpoint of UDM is to help the AMF identify whether the subscription for the requested group event is the same or not when a new group member UE is registered.

3b. [Conditional] AMF acknowledges the execution of Namf_EventExposure_Subscribe.

3c. [Conditional] If the requested event (e.g. PDU Session Status) requires SMF assistance, then the UDM sends the Nsmf_EventExposure_Subscribe request message to each SMF where at least one UE identified in step 2 has a PDU session established. The NEF notification endpoint received in step 2 is included in the message.

NOTE 3: In the home routed case, the UDM sends the subscription to the V-SMF via the H-SMF.

3d. [Conditional] The SMF acknowledges the execution of Nsmf_EventExposure_Subscribe.

3c-3d are not needed for this solution.

4. [Conditional] UDM acknowledges the execution of Nudm_EventExposure_Subscribe.

If the subscription is applicable to a group of UE(s) and the maximum number of reports is included in the Event Report information in step 1, the number of UEs is included in the acknowledgement.

5. NEF acknowledges the execution of Nnef_EventExposure_Subscribe to the requester that initiated the request.

6a - 6b. [Conditional - depending on the Event] The UDM (depending on the Event) detects the event occurs and sends the event report, by means of Nudm_EventExposure_Notify message to the associated notification endpoint of the NEF along with the time stamp. NEF may store the information in the UDR along with the time stamp using either Nudr_DM_Create or Nudr_DM_Update service operation as appropriate.

6a - 6b are not needed for this solution.

6c - 6d. [Conditional - depending on the Event] The AMF detects that the event occurs and sends the event report, by means of Namf_EventExposure_Notify message to associated notification endpoint of the NEF along with the time stamp. NEF may store the information in the UDR along with the time stamp using either Nudr_DM_Create or Nudr_DM_Update service operation as appropriate.

If the AMF has a maximum number of reports stored for the UE or the individual member UE, the AMF should decrease its value by one for the reported event.

For both step 6a and step 6b, when the maximum number of reports is reached and if the subscription is applied to a UE, The NEF unsubscribes the monitoring event(s) to the UDM and the UDM unsubscribes the monitoring event(s) to AMF serving for that UE.

For both step 6a and step 6b, when the maximum number of reports is reached for an individual group member UE, the NEF uses the number of UEs received in step 4 to determine if reporting for the group is complete. If the NEF determines that reporting for the group is complete, the NEF unsubscribes the monitoring event(s) to the UDM and the UDM unsubscribes the monitoring event(s) to all AMF(s) serving the UEs belonging to that group.

When the maximum duration of reporting expires in the NEF, the UDM and the AMF, then each of these nodes should locally unsubscribe the monitoring event.

6e - 6f. [Conditional - depending on the Event] When the SMF detects a subscribed event, the SMF sends the event report, by means of Nsmf_EventExposure_Notify message, to the associated notification endpoint of the NEF provided in step 3c. NEF may store the information in the UDR along with the time stamp using either Nudr_DM_Create or Nudr_DM_Update service operation as appropriate.

6e - 6f. are not needed for this solution.

7. [Conditional - depending on the Event in steps 6a-6f] The NEF forwards to the AF the reporting event received by either Nudm_EventExposure_Notify and/or Namf_EventExposure_Notify. In the case of the PDU Session Status event, the NEF maps it to a PDN Connectivity Status notification when reporting to the AF.

8. [Conditional - depending on the Event] The AMF detects the subscription change related event occurs, e.g. Subscription Correlation ID change due to AMF reallocation or addition of new Subscription Correlation ID due to a new group UE registered, it sends the event report, by means of Namf_EventExposure_Notify message to the associated notification endpoint of the UDM.

5.1.2.2.2 The relationship between AF and MEC system

As described in clause 4.4 of ETSI GR MEC 031 [i.4], the MEC system appears as an Application Function or Application Functions to a 5G system. Here, the relationship between AF and the MEC system are explained more in detail.

In this solution, it is actually the control function unit of the MEC system that appears as the AF. It is centrally deployed and the quantity is small. While other parts of the MEC system are distributed and edge oriented deployed, and the quantity is very large.

The function of the AF is to serve the MEC system and 3GPP interaction, which includes subscribe information from 3GPP, realize traffic guidance, allocate optimal edge nodes for users according to user location, and load balancing, etc.

For this solution, AF and the MEC system can be considered as one entity, though they are responsible for different functionalities, and deployed in different locations.

Therefore, in the following procedure AF and the MEC system will appear together as one entity (AF/MEC system).

5.1.2.3 AF requests to influence traffic routing for Sessions based on location detection

Below is the solution procedure.

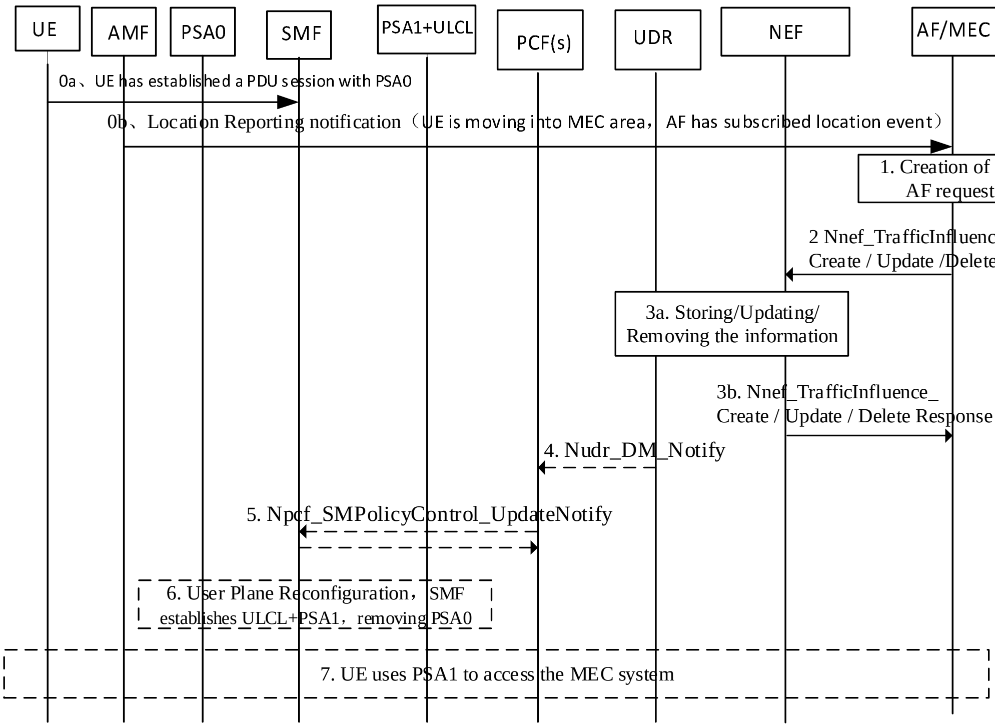

UE
AMF
PSA0
SMF
PSA1+ULCL
PCF(s)
UDR
NEF
AF/MEC
0a、UE has established a PDU session with PSA0
0b、Location Reporting notification（UE is moving into MEC area，AF has subscribed location event）
1. Creation of the AF request
2 Nnef_TrafficInfluence_ Create / Update /Delete
3a. Storing/Updating/ Removing the information
3b. Nnef_TrafficInfluence_ Create / Update / Delete Response
4. Nudr_DM_Notify
5. Npcf_SMPolicyControl_UpdateNotify
6. User Plane Reconfiguration，SMF establishes ULCL+PSA1，removing PSA0
7. UE uses PSA1 to access the MEC system

Figure 5.1.2-3-1: AF requests to influence traffic routing for Sessions based on location detection

UE has established a PDU session with PSA0, when UE moves to MEC area (PSA1 serves this area as an Edge PSA), AF/MEC system detects it and report to NEF, as described in clause 4.3.6.2 "Processing AF requests to influence traffic routing for Sessions not identified by an UE address" and clause 4.3.5.7 "Simultaneous change of Branching Point or ULCL and additional PSA for a PDU Session" of ETSI TS 123 502 [i.2].

The detailed description of the procedure is as follow:

0a. UE has established a PDU session with PSA0 (it is a central default UPF).

0b. AMF reports the UE location change to AF. UE is moving into MEC area (a new area), and AF/MEC system has subscribed the location event before.

1. AF/MEC system receives UE location change notification and decides to apply traffic routing and create a new request. The AF invokes a Nnef_TrafficInfluence_Create service operation. The content of this service operation (AF request) is defined in clause 5.2.6.7 of ETSI TS 123 501 [i.1]. The request also contains an AF Transaction Id.

2. The AF sends its request to the NEF. If the request is sent directly from the AF to the PCF, the AF reaches the PCF selected for the existing PDU Session by configuration or by invoking Nbsf_management_Discovery service.

   The NEF ensures the necessary authorization control, including throttling of AF requests and mapping from the information provided by the AF into information needed by the 5GC.

3. (in the case of Nnef_TrafficInfluence_Create or Update): The NEF stores the AF request information in the UDR (Data Set = Application Data; Data Subset = AF traffic influence request information, Data Key = AF Transaction Internal ID, S-NSSAI and DNN and/or Internal Group Identifier or SUPI.)

   (in the case of Nnef_TrafficInfluence_Delete): The NEF deletes the AF requirements in the UDR (Data Set = Application Data; Data Subset = AF traffic influence request information, Data Key = AF Transaction Internal ID.)

   The NEF responds to the AF.

4. The PCF(s) that have subscribed to modifications of AF requests (Data Set = Application Data; Data Subset = AF traffic influence request information, Data Key = S-NSSAI and DNN and/or Internal Group Identifier or SUPI) receive(s) a Nudr_DM_Notify notification of data change from the UDR.

5. The PCF determines if existing PDU Sessions are potentially impacted by the AF request. For each of these PDU Sessions, the PCF updates the SMF with corresponding new PCC rule(s) by invoking Npcf_SMPolicyControl_UpdateNotify service operation.

   The AF request includes a notification reporting request for UP path change, the PCF includes in the PCC rule(s) the information required for reporting the event, including the Notification Target Address pointing to the NEF or AF and the Notification Correlation ID containing the AF Transaction Internal ID.

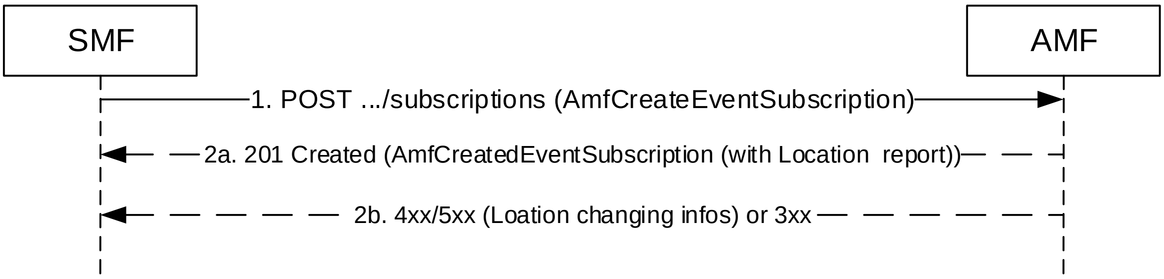
6. When the PCC rule is received from the PCF to request for UP path change, the SMF takes appropriate actions to reconfigure the User plane of the PDU Session as follows:

   - Adding PSA1 as ULCL point as serving UPF.
   - Removing PSA0 in the data path.
   - Allocating a new Prefix to the UE (when IPv6 multi-Homing applies).
   - Updating the UPF in the target DNAI with new traffic steering rules.

7. UE uses the PSA1 as the serving UPF to access to MEC system.

5.1.3 Solution proposal #2: SMF detecting UE Location changing

The SMF is the execution NF of ULCL insertion, based on instruction from PCF, but also based on information it obtains from AMF directly. 5G is a service-based architecture, and SMF can subscribe location-Report event of UEs from AMF. As stated in ETSI TS 129 518 [i.16], clause 6.1.3 "A NF subscribes to this event to receive the Last Known Location or the Current Location of a UE or a group of UEs or any UE, and Updated Location of any of these UEs when AMF becomes aware of a location change of any of these UEs with the granularity as requested."


SMF
AMF
1. POST .../subscriptions (AmfCreateEventSubscription)
2a. 201 Created (AmfCreatedEventSubscription (with Location report))
2b. 4xx/5xx (Loation changing infos) or 3xx

NOTE: In this solution there is no impact expected in MEC system.

Figure 5.1.3-1: SMF Subscribe for Location Report from AMF

5.1.4 Evaluation

The proposed solution is technically feasible. The end user has subscribed to multiple services and the terminal will be connected to the network via default UPF at the beginning. In this way, the MEC platform needs to subscribe to the UE location notification through NEF. When UE moves to MEC's service area, additional UPF anchor points would be added in time according to the user profile / subscription information to provide MEC services for UE.

5.2 Key issue #2: Unified AAA management of MEC system

5.2.1 Description

The unified AAA management of the park MEC system means that the MEC system serves as the entrance of enterprises in the park, and all accesses need to be authenticated.

When a user wants to access the MEC system to use its services, the MEC system will authenticate the user and confirm the user's access permissions according to the application information deployed on the MEC platform, so as to ensure that the user has subscribed the corresponding MEC service. After the authentication is completed, the user's service request will be transferred to the corresponding MEC application.

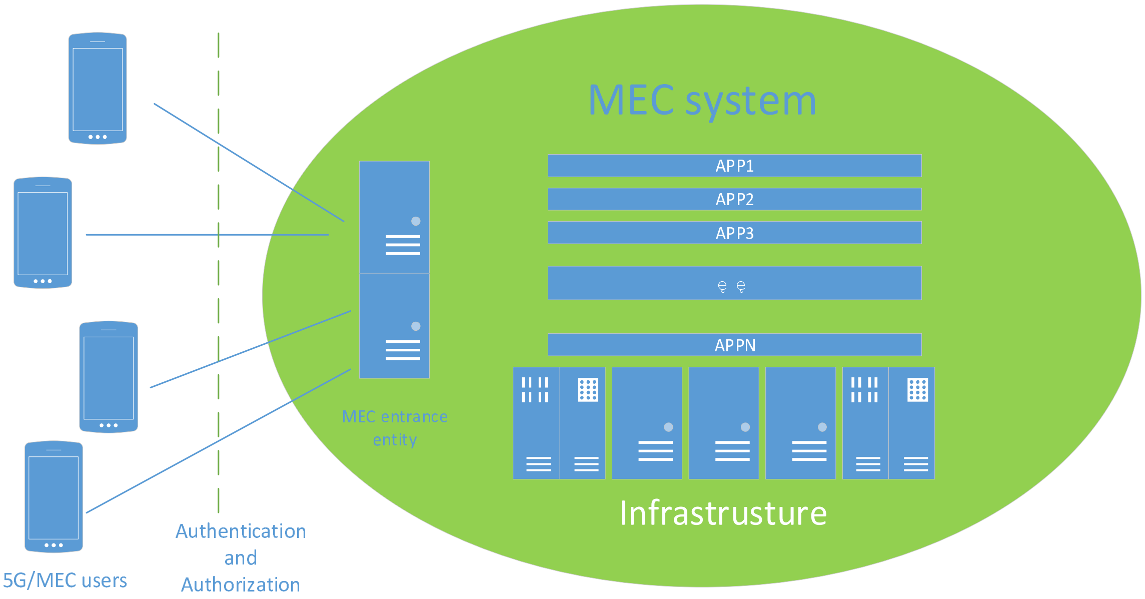


Figure 5.2.1-1: Unified AAA management of MEC system

5.2.2 Solution proposal #1: Using UE Identity API

As stated in ETSI GS MEC 014 [i.7], clause 5.1, when the MEC system supports the UE Identity feature, the MEC platform provides the functionality for a MEC application to register a tag (representing a UE) or a list of tags. Each tag has been mapped into a specific UE in the mobile network operator's system. And the purpose of the UE Identity feature is to allow UE specific traffic rules in the MEC system.

However, a MEC application does not always have this UE ID. For example, in the location-based ULCL insertion scenario, the access information at this time does not take GPSI, but other relevant information, such as IP address. For security, the MEC system may need to authenticate the new access, but only in the case of IP address, a MEC application cannot initiate secondary Re-authentication to SMF. Therefore, it may be necessary to obtain UE ID, such as a UE's GPSI.

In ETSI TS 123 558 [i.18], clause 8.6.5, there is a procedure whereby an Edge Enabler Server (EES) is able to expose a UE Identifier API to an Edge Application Server (EAS) to provide it with an identifier uniquely identifying a UE if the EAS does not have it. Therefore, it is proposed to re-use this procedure within MEC, thereby enabling the MEC platform to expose an UE Identity API to MEC APP instances in order to provide them with an identity uniquely identifying a UE for subsequent procedures over Mp1.

Figure 5.2.2-1 describes the UE Identity API Request/Response interactions between the MEC application and MEC platform to enable it to obtain a UE Identity.

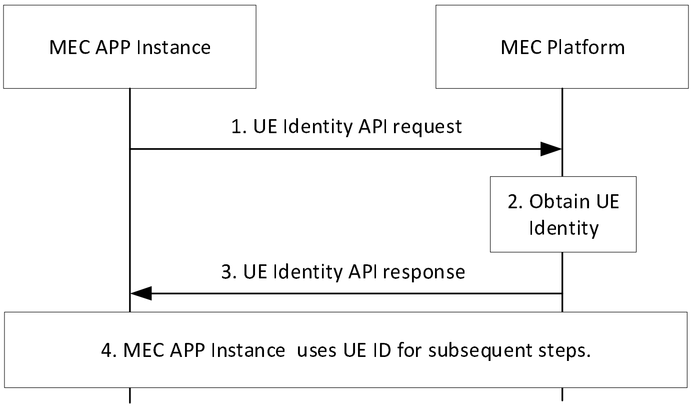

MEC APP Instance
MEC Platform
1. UE Identity API request
2. Obtain UE Identity
3. UE Identity API response
4. MEC APP Instance uses UE ID for subsequent steps.

Figure 5.2.2-1: UE Identity API Request/Response

1. The MEC APP Instance invokes the UE Identity API exposed by the MEP.
2. The MEP uses the received user information in the step 1 (e.g. IP address) and obtains the UE identity.

NOTE: It is outside of this study how the MEP determines the UE ID.

3. The MEP provides the obtained UE identity as UE ID to the MEC APP Instance. The UE ID is specific to the given MEC APP Instance and may be assigned by the 3GPP Network.
4. The MEC APP Instance uses the UE ID received in step 3 to perform the subsequent next steps.

5.2.3 Solution proposal #2: DN-AAA triggers Secondary authentication/authorization when ULCL inserting

The present document is aimed at the ULCL insertion scenario, that is, UE has completed the authentication with the centre AAA, when UE wants to access the MEC system, according to the local policy (based on security considerations, etc.), it still needs to carry out secondary re-authentication and authorization.

In other words, any new access to a MEC system needs to be authenticated by DN-AAA which resides in the MEC system.

As the description from clause 5.6.6 of ETSI TS 123 501 [i.1]: at any time, a DN-AAA server or SMF may trigger Secondary authentication procedure for a PDU Session established with Secondary Authentication as specified in clause 11.1.3 of ETSI TS 133 501 [i.10].

Combined with this scenario, the related procedure of this solution is given in figure 5.2.3-1.

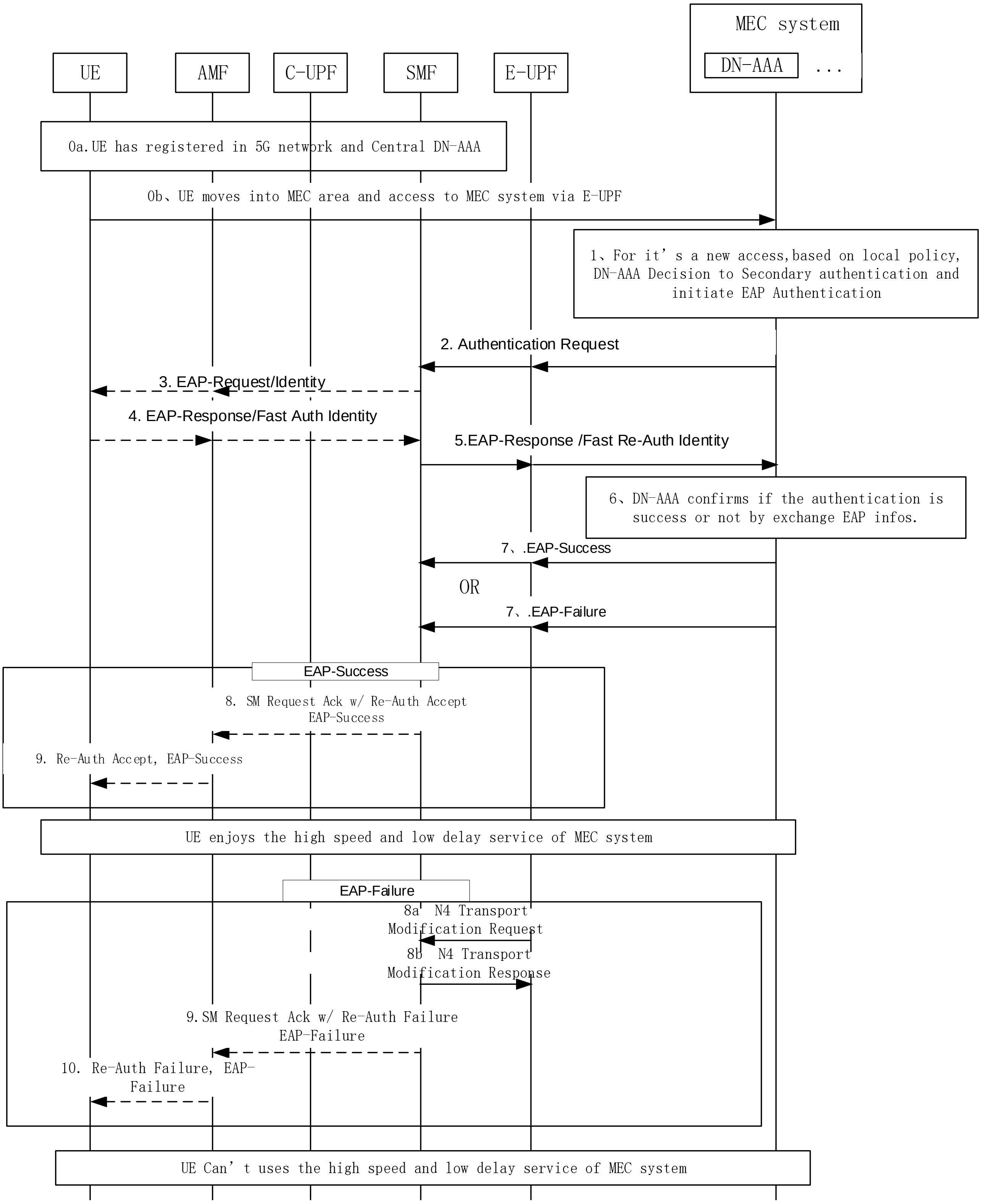

MEC system
DN-AAA
...
UE
AMF
C-UPF
SMF
E-UPF
0a.UE has registered in 5G network and Central DN-AAA
0b、UE moves into MEC area and access to MEC system via E-UPF
1、For it’ s a new access,based on local policy, DN-AAA Decision to Secondary authentication and initiate EAP Authentication
2. Authentication Request
3. EAP-Request/Identity
4. EAP-Response/Fast Auth Identity
5.EAP-Response /Fast Re-Auth Identity
6、DN-AAA confirms if the authentication is success or not by exchange EAP infos.
7、.EAP-Success
OR
7、.EAP-Failure
EAP-Success
8. SM Request Ack w/ Re-Auth Accept EAP-Success
9. Re-Auth Accept, EAP-Success
UE enjoys the high speed and low delay service of MEC system
EAP-Failure
8a N4 Transport Modification Request
8b N4 Transport Modification Response
9.SM Request Ack w/ Re-Auth Failure EAP-Failure
10. Re-Auth Failure, EAP-Failure
UE Can’ t uses the high speed and low delay service of MEC system

Figure 5.2.3-1: EAPAuthentication with 3GPP and MEC system

This procedure concerns only non-roaming scenario for MEC in Park. In the non-roaming and LBO roaming cases, only one SMF is involved.

Preconditions:

0a. UE has registered in 5G network and Central DN-AAA.

0b. UE moves into MEC area and access to MEC system via E-UPF.

1. Because it is a new access, based on local policy (any new access to the MEC system needs to be authenticated by DN-AAA), DN-AAA decides to Secondary Re-authenticate and initiate EAP Re-Authentication.

2. The DN-AAA should send a Secondary Authentication request to UPF and the UPF forwards to SMF. The Secondary authentication request contains the GPSI, if available, and the IP/MAC address of the UE allocated to the PDU Session and the MAC address if the PDU session is of Ethernet PDU type.

3. The SMF should send an EAP Request/Identity message to the UE.

4. The UE should respond with an EAP Response/Identity message (with Fast-Auth Identity).

5. The SMF forwards the EAP Response/Identity to UPF, selected during initial authentication, over N4 interface. This establishes an end-to-end connection between the SMF and the external DN-AAA server for EAP exchange.

   The UPF should forward the EAP Response/Identity message to the DN-AAA Server.

   The DN-AAA server and the UE should exchange EAP messages as required by the EAP method.

6. DN-AAA confirms if the authentication is successful or not, by exchanging EAP info.

7. After the completion of the authentication procedure, DN-AAA server either sends EAP Success or EAP Failure message to the SMF. This completes the Re-authentication procedure at the SMF.

8-9. If the authorization is successful, EAP-Success should be sent to UE.

UE enjoys the high speed and low delay service of MEC system now.

8-10. If the authorization is not successful, the SMF notifies failure to UPF. Upon completion of a N4 Session Modification procedure with the selected UPF, SMF sends EAP-Fail to UE via AMF.

UE cannot use the high speed and low delay service of MEC system.

Secondary Authentication and Authorization Revocation: At any time, a DN-AAA server may revoke the authentication and authorization for a PDU Session according to the request from the DN-AAA server.

Therefore, from the perspective of MEC security and unified authentication management, it is recommended that every new access should be authenticated, no matter the access is through an authenticated PDU session from the perspective of 3GPP or not.

5.2.4 Evaluation

The unified AAA management of the MEC system referred to here is for the ULCL insert scenario, where ULCL inserts from 3GPP taking IP address instead of UE ID, such as GPSI. For security, MEC application wants to initiate the authentication/authorization to make sure the access is secure.

Solution proposal#1 is to obtain UE ID, such as GPSI.

Solution Proposal#2 triggers the secondary Re-authentication with the GPSI sending in step2 obtained in Solution1. So both solutions together make a complete Unified AAA management of MEC system.

5.3 Key issue #3: Dynamic management according to user requirements

5.3.1 Description

As stated in ETSI GS MEC 002 [i.9], the MEC host supports routing user plane traffic to/from authorized MEC applications according to configurable parameters received from the MEC platform. This "configurable parameter" to reflect the parameters will include all the customers' requirements.

The dynamic management function obtains user access permission rules (such as access period, access frequency) from the system through UE public identifier, as specified in ETSI TS 123 501 [i.1], clause 5.6.7.

The dynamic management function can record and present the traffic status on the platform, including real-time, non-real-time, user based, service based and other different perspectives.

The dynamic management function can flexibly handle the access and use of the terminal on the platform according to the traffic usage of the terminal, such as graded charging, slow down processing, limited access time, etc.

5.3.2 Solution proposal #1: Defining the traffic gateway function of MEP

As mentioned in the description, the MEC platform has to face a variety of services, and its data processing requirements are far greater than those of network elements, such as UPF. In order to make up for the business requirements that Traffic Rule Control + UPF cannot meet, a new entity need to be introduced, as a supplement to the traffic rules control + 3GPP UPF.

As shown in figure 5.3.2-1, the Traffic Gateway (TG) can be set in two places. The first one is set on MEP. As a basic function of MEP, it does not affect Mp2 interface. The second one is set on Data plane. So Mp2 needs to be changed according to specific requirements.

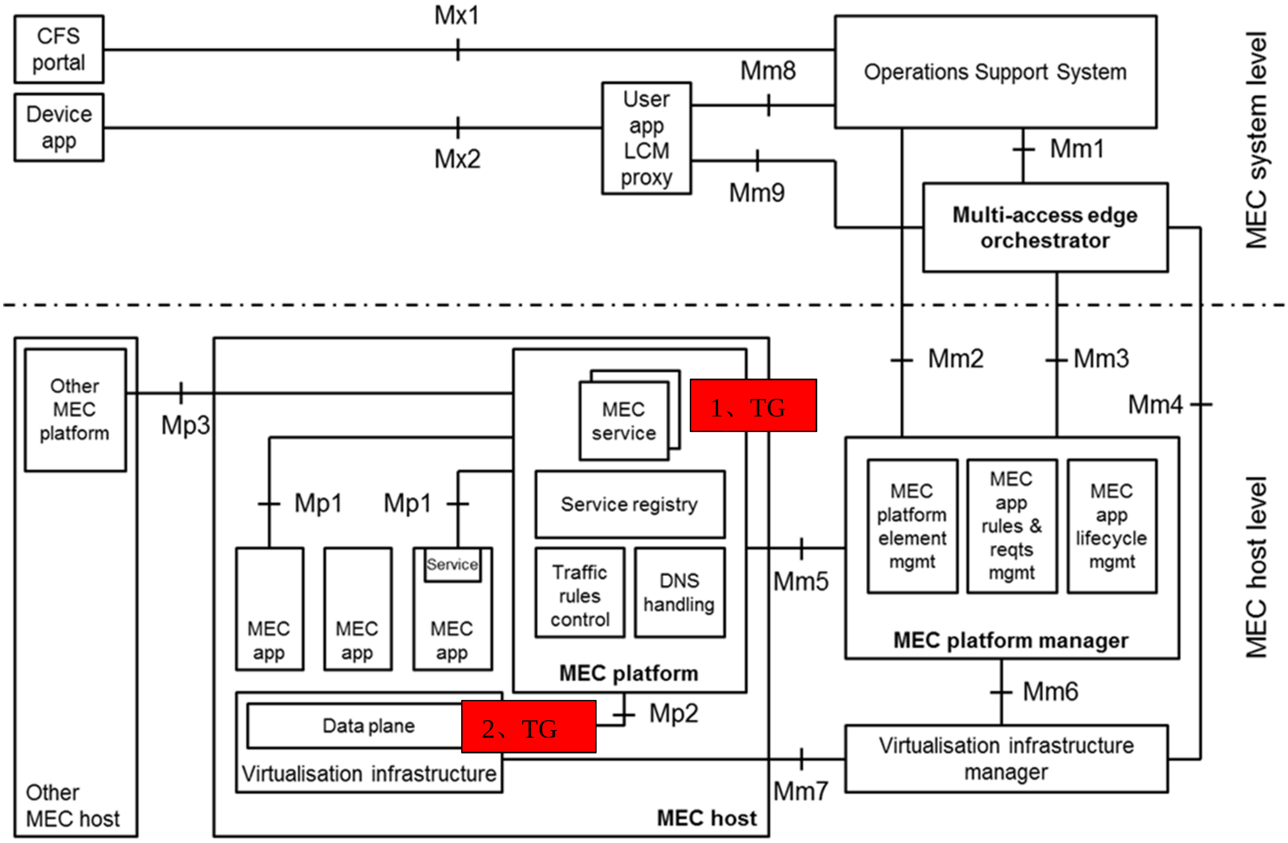


Figure 5.3.2-1:Traffic gateway function of MEP

At the same time, TG (traffic gateway) can get information from OSS/MEAO from the standard Mm5.

5.3.3 Solution proposal #2: Add a time dimension to business attributes

After a detailed analysis of service requirements of the MEC platform, it is confirmed that there is still a lack of time period control. 3GPP SMF/UPF cannot complete the work of this service side, and the MEC platform does not have such attribute definition. Therefore, it is suggested to add the time dimension aspects to the MEC service information. The time dimension related attributes are used to allow different services to have different serving time, enabling MEC platforms to better optimize resources and achieve the best revenue ratio. For example, by providing none-busy time service, busy time service time, to carry out different charges.

5.3.4 Solution proposal #3: Add UE Identity tags list to MEC platform

After a detailed analysis of user access control rules of the MEC platform, it is confirmed that there is still a lack of user access control rules. Therefore, it is suggested to add UE Identity tags list to the MEC platform. The UE Identity tags list include the allowed UE Identity tags list and/or the rejected UE Identity tags list, enabling MEC platforms to identify users and provide differentiated services more accurately. For example, when the terminals initially access application and the allowed UE Identity tags list is enabled, only terminals who are in the allowed UE Identity tags list are allowed to access the application. Similarly, if the rejected UE Identity tags list is enabled, then the terminals belonging to that list will be rejected when trying to access the applications.

5.3.5 Evaluation

The dynamic management function is very important for enterprises deployed in the park and can significantly improve the efficiency of enterprises.

In solution #1, a Traffic Gateway is introduced to be as a supplement to the traffic rules control + 3GPP UPF.

In solution #2, it is proposed to add a time dimension to business attributes to realize the management and control of time dimension.

In solution #3, it is proposed to add UE Identity tags list to the MEC platform to implement admission control based on UE Identity tags. This is currently not yet supported by MEC.

Therefore, based on this evaluation, 3 solutions realize dynamic management from different angles.

5.4 Key issue #4: Remote access of enterprise MEC applications

5.4.1 Description

When an employee is working in the enterprise park, he/she could access the MEC applications of the enterprise, e.g. group messaging/chat tools, video conference tools, business management tools, e-learning applications, etc. Also, it is a common case that when the employee is travelling, for example, going abroad to attend a global event, or meeting the customers for solving problems, he/she may still need to access the same enterprise applications as he/she is in the park, for discussion, report or retrieving information purposes.

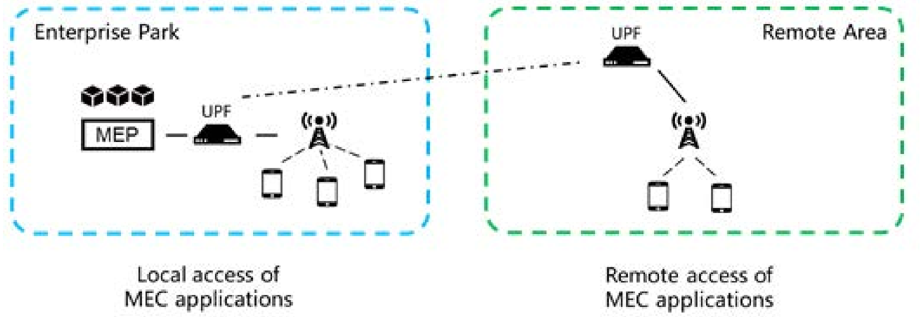

Enterprise Park
UPF
Remote Area
MEP
UPF
Local access of MEC applications
Remote access of MEC applications

Figure 5.4.1-1: Remote access of enterprise MEC applications

In such scenarios, the employee would access the enterprise MEC applications remotely, and the service requests need to be routed back to the edge applications deployed in the enterprise park.

5.4.2 Solution proposal #1: Remote access through Internet

One of the solution for this scenario is to route the remote service requests to the MEC applications which are deployed in the enterprise park through the Internet.

This requires the MEC applications that provide the services to have public IP addresses exposed, or a VPN is set up between the employee's device and the enterprise's private network. In either case, the MEP needs to authorize the employee's identity and rights, and configure the Data Plane to route the traffic to the appropriate MEC service if the client is authorized.

5.4.3 Solution proposal #2: Remote access through mobile backbone network

Another solution for this key issue is to route the remote service requests to the MEC applications in the enterprise park through the mobile backbone network, i.e. through the N9 reference point between the remote UPF and the local UPF in the park.

Similar to solution #1, the employee's device can access the MEC applications through backbone network routing, enterprise's private VPN or VPN set up by the mobile network. The MEP needs to authorize the client before routing the service request to the appropriate MEC applications.

5.4.4 Evaluation

Enterprises have a strong demand on data security and service quality, therefore a highly secured and quality assured transport would be preferable when an employee tries to access the enterprise MEC applications remotely.

In solution #1, a VPN could be set up to provide some security support for the transport, however, this would either rely on a solution provided by the park's internet service provider and/or the mobile operator, or the enterprise's private VPN solution. In the former case, setting up the VPN could be troublesome as the park's ISP may not be the same as the mobile operator, while in the latter case, it would require the employee to install certain software on his/her device. Besides, there is no guarantee of the network service quality on the Internet, so the remote access may be affected by jitter and lag.

In solution #2, the mobile network operator could provide a controlled IP network connection between the remote UPF and the local UPF, thus providing an isolated and quality assured transport for the remote access. Unlike the Internet, the mobile backbone network is fully managed and controlled by the operator, and has additional guarantee on both security and service quality. Therefore, based on this evaluation, solution #2 may be more feasible for enterprises to use.

5.5 Key issue #5: MEC application Slicing support

5.5.1 Description

Network slicing is an on-demand networking scheme that allows operators to cut out multiple virtual end-to-end networks on a unified infrastructure. This makes network slicing a good solution to support multiple enterprises being hosted in MEC in park environments and deploying various types of business applications. A network slice includes at least wireless sub-slice, bearer sub-slice and core network sub-slice. This is the definition and requirement of 3GPP for 5G slices as described in clause 4.1.3 of ETSI TS 128 530 [i.19].

The MEC system in the park faces different enterprises/applications with different requirements/priorities, such as different importance and security level, so there will also be a demand for slices of the MEC system.

ETSI GR MEC 024 [i.11] has studied how MEC can support network slicing in detail from use cases to instantiation of MEC applications, and provided solutions. The present concept complies with ETSI GR MEC 024 [i.11], but provides additional solutions allowing operators to better provide MEC services in MEC in park scenarios.

5.5.2 MEC application slice

"Network Slice" has been widely used. Specifically for 5G, "Network Slice" implies 5G slice, see clause 4.2 of ETSI GR MEC 024 [i.11]. MEC applications can exist as part of Network Slice as described in clause 5.3 of ETSI GR MEC 024 [i.11]. That clause describes the instantiation of a Network Slice integrating MEC applications and using 3GPP elements. It says: "Regarding MEC deployment, after the reception of the NSI(Network Slice Instance) creation request from the core NSSMF, the NFVO requests the deployment of the VNFs for the MEC application instances by either using an extended VNFD (which includes the AppD fields), or the AppD included in the NSD (extended to include AppD)". Details of this are described in clause 4 of ETSI GS MEC 010-2 [i.12].

From the perspective of network facilities of operators, there is no problem in instantiation MEC in this way. However, from the customer-oriented perspective, it seems that the network slice and application slice should be considered separately, because the network slice and application slice together make a user service slice.

Currently, MEC is deployed in the park to serve many enterprises. Many enterprises require not only network quality assurance, but also the guarantee of application layer isolation. Based on customers' perspective, operators should provide end-to-end slice based on user service requirement. End-to-end slice means a combination of network slice and application slice.

Therefore, it seems better to consider both, the 5G core network aspects and also the MEC application aspects. In the present document the term "MEC application slice" is used to indicate that besides the network slicing aspects covered in 3GPP, MEC applications layer is included in the end-to-end considerations, while those are not covered in the 3GPP specifications of clause 4.1.3 of ETSI TS 128 530 [i.19].

To be able to serve multiple enterprises in a MEC in park deployment, it is expected that MEC application slices which compose of MEC application instances would provide quality assurance and isolation between the consumers on both network and application level.

MEC application slice corresponds to multiple MEC application instances. An enterprise consumes network slices and MEC application slices from the operator.

5.5.3 Solution proposal #1: Introducing MEC Slice Management

From the users perspective, MEC Application slice is introduced. Then the corresponding management unit should be introduced, e.g. MEC Application Slice Management Function (MEC App-SMF).

MEC App-SMF is responsible for management and orchestration of MEC Slice Instance (MSI), deriving MEC Application Slice related requirements from Communication Service Management Function (CSMF).

MEC Application Slice can reuse CSMF of 5G Slice as described in clause 4.10 of 3GPP TR 28.801 [i.13].

CSCF is responsible for translating the communication service related requirement to network slice and communicate with MEC Slice Management Function (MEC App-SMF).

Figure 5.5.3-1 shows a MEC Application Slice and a corresponding to 5G network Slice.

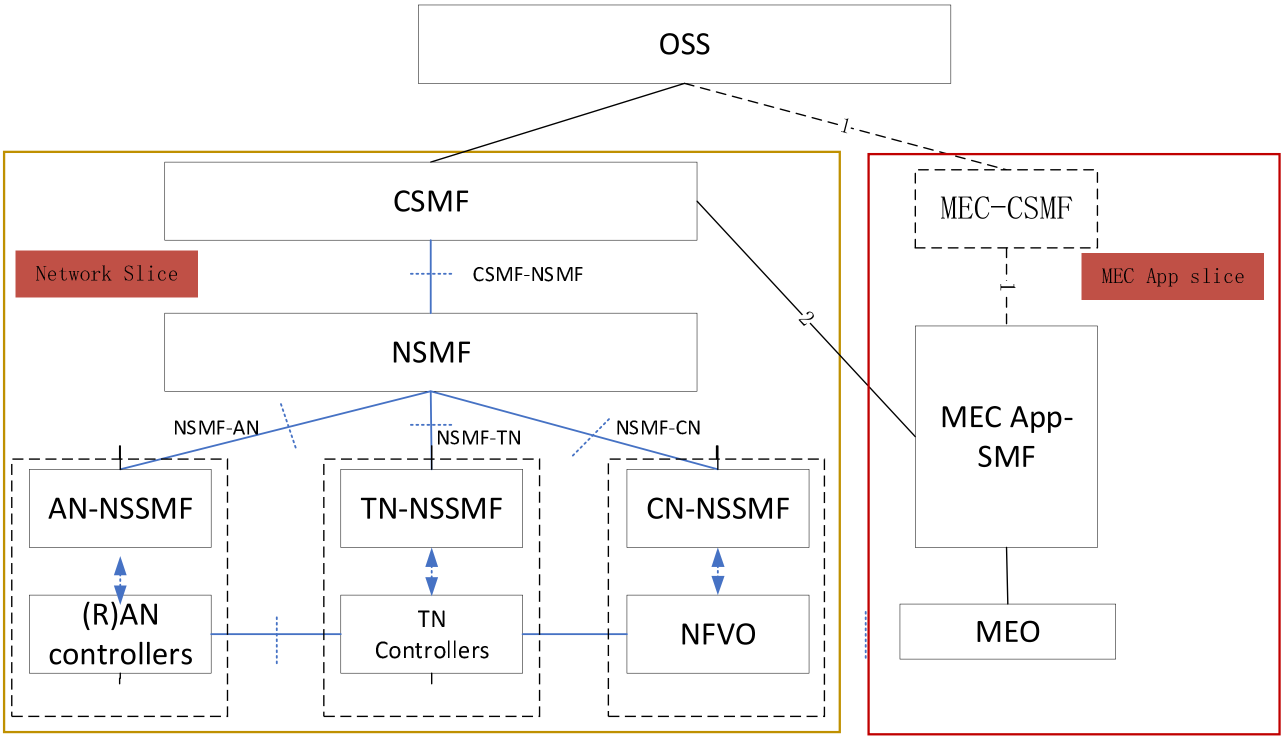


Figure 5.5.3-1: MEC Application Slice corresponding to network slice

MEC-CSMF:

The function is the same as CSMF of Network slice. So they are at the same architecture level, as shown in figure 5.5.3-1.

There are two scenarios for how to use this function:

1) As shown in the dotted line on the right, MEC-CSMF is independent and gets service requirements directly from the OSS.

2) As shown by the solid line in the figure above, MEC App-SMF directly interfaces with CSMF, so MEC-CSMF does not need to exist.

MEC App-SMF:

- The function is the fusion of NSMF and NSSMF. So the block diagram of MEC App-SMF corresponds to NSSF and NSSMF.
- MEC App-SMF functions can be summarized as is responsible for management and orchestration of MSI (MEC Slice Instance) and communicates with CSMF.
- For mapping, MEO corresponds to the fourth layer of Network slice, such as NFVO.

5.5.4 Evaluation

The basic concept of MEC Application Slice is introduced in the present document. Further details, e.g. MEC-CSMF (and whether it should be part of the MEO, of the OSS or as a separate function), are to be further studied in ETSI GR MEC 044 [i.17].

5.6 Key issue #6: MEC efficient consumption of 5GC exposure capability

5.6.1 Description

As described in ETSI TS 123 501 [i.1], clause 5.20, the Network Exposure Function (NEF) supports external exposure of capabilities of 5GC network functions. In many cases, the MEC applications would need to consume the 5GC exposed capabilities through the NEF. ETSI GR MEC 031 [i.4] has explored this issue, see clause 5.7 "Key Issue #7": "*MEC application consumes 5GC exposed capabilities. However, the current solution seems not ideal in commercial deployment and usages. This is mainly because the specification only focus on the basic issue on how NEF can be used to provide 5GC exposed capabilities to MEC, but not considering the efficiency of the solution, i.e. exposure through a centralized NEF may cause high latency, and may not be tolerable by the MEC applications*".

3GPP has noticed this problem and further studied it in Release 17 (see 3GPP TR 23.748 [i.14], clause 5.3). Several solutions are proposed to take low latency into consideration and provide optimized solution for 5GC capability exposure. Also, it is necessary to align the study in MEC to improve the work in ETSI GR MEC 031 [i.4].

5.6.2 Solution proposal #1: Local NEF Deployment for (local) network information exposure to MEC with Low Latency

This solution proposes to deploy Local NEF for MEC applications and expose real-time network information, e.g. network congestion condition or real-time user path latency, to the MEC system.

Referring to ETSI TS 123 548 [i.15], clause 6.4.2, Local NEF deployed at the edge can be used to support network exposure timely to local AF. The local NEF can support one or more of the functionalities described in ETSI TS 123 501 [i.1], clause 6.2.5.0, and can support a subset of the APIs specified for capability exposure based on local policy. The local NEF needs to support Nnef_AFSessionWithQoS service operation for the local AF. In summary, the Local NEF is almost equivalent to NEF in terms of functionality, the main difference is the deployment location.

The MEC system, as a local AF, can discover the Local NEF (L-NEF) to serve the applications deployed in MEC system to timely get the real-time information from 5GS:

- Option 1: If MEC is preconfigured of L-NEF IP address/FQDN, then MEC can initiate Nnef_AFSessionWithQoS_Creat_request to L-NEF directly.

- Option 2: If AF/MEC is not a trusted AF by the operator, and only knows the (central) NEF, it can initiate a service operation (e.g. a Nnef_AFSessionWithQoS_Creat_request) towards this NEF, the NEF could re-direct the request to a L-NEF if the NEF detects that it is not the most suitable NEF instance to serve AF/MEC request. If the NEF which receives request from the AF cannot find a suitable L-NEF for the AF/MEC, the NEF initiates Nnrf_NFDiscovery_Request to NRF, and forward the response to the AF/MEC. This procedure occurs often when UE moves. How to update to a suitable serving MEC is defined in ETSI GS MEC 021 [i.8]. Because the serving AF/MEC changes, the corresponding L-NEF will change accordingly.

- Option 3: If AF/MEC is a trusted AF by the operator, AF/MEC initiates Nnrf_NFDiscovery_Request to NRF directly to get the L-NEF IP address/FQDN. As specified in ETSI TS 123 501 [i.1], clause 6.2.5.0 and clause 6.13.4, the NRF may be used by the AF/MEC to discover the L-NEF.

Figure 5.6.2-1 illustrates the three options for AF/MEC initiates Nnef_AFSessionWithQoS_Creat_request procedure.

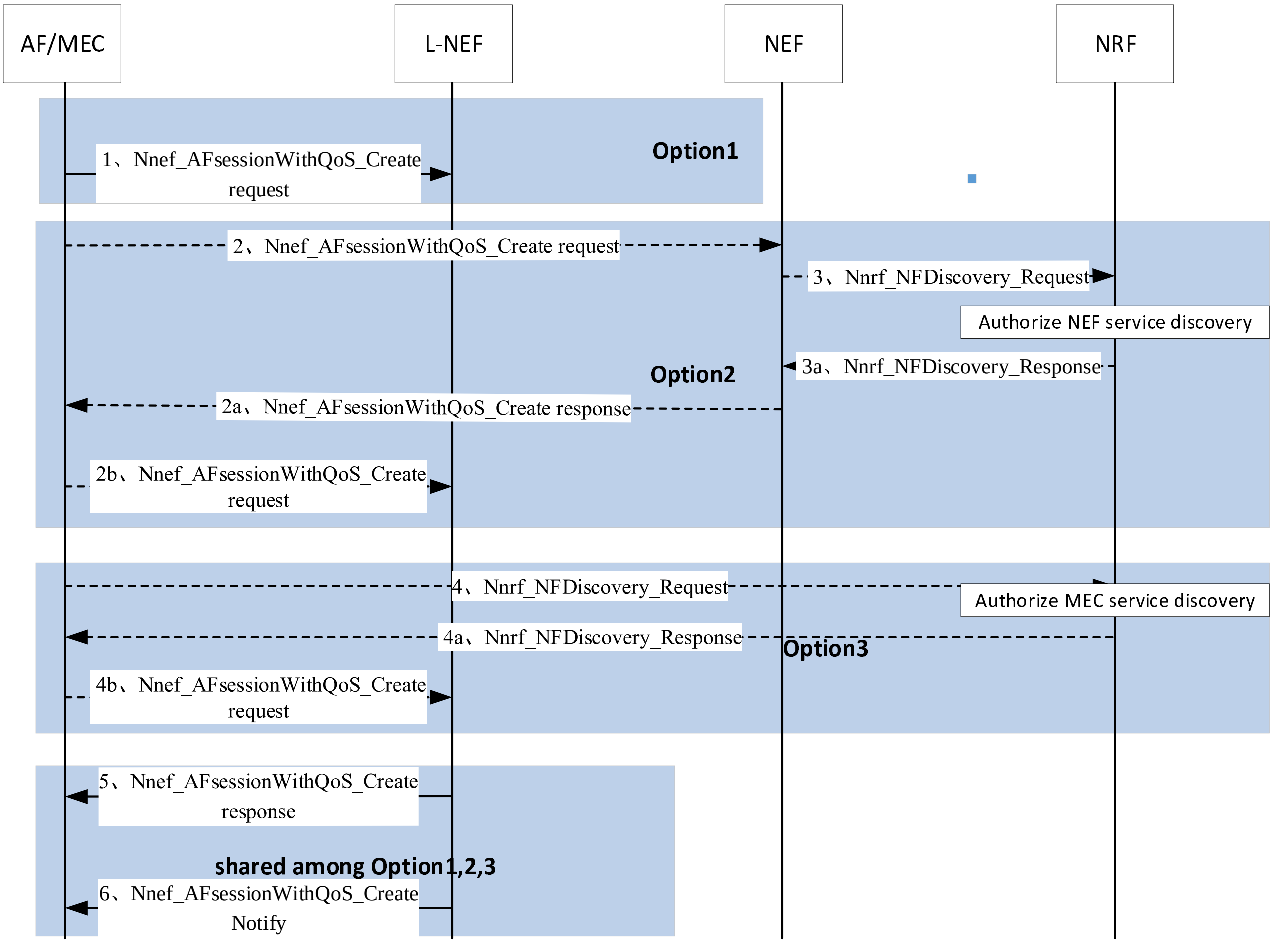

AF/MEC
L-NEF
NEF
NRF
Option1
1、Nnef_AFsessionWithQoS_Create request
2、Nnef_AFsessionWithQoS_Create request
3、Nnrf_NFDiscovery_Request
Authorize NEF service discovery
Option2
3a、Nnrf_NFDiscovery_Response
2a、Nnef_AFsessionWithQoS_Create response
2b、Nnef_AFsessionWithQoS_Create request
4、Nnrf_NFDiscovery_Request
Authorize MEC service discovery
4a、Nnrf_NFDiscovery_Response
Option3
4b、Nnef_AFsessionWithQoS_Create request
5、Nnef_AFsessionWithQoS_Create response
shared among Option1,2,3
6、Nnef_AFsessionWithQoS_Create Notify

Figure 5.6.2-1: AF/MEC initiates Nnef_AFSessionWithQoS_Create _request

Figure 5.6.2-1 mixes several procedures and operations, details are as follows:

1） Step 1, step 2, step 2a, step 2b, step 4b, step 5 and step 6 are referred to ETSI TS 123 502 [i.2], clause 4.15.6.6 and description are referred to ETSI TS 123 501 [i.1], clause 6.2.5.0. If changing the "Create" to "Update", that is AF session with required QoS update procedure, referred to ETSI TS 123 502 [i.2], clause 4.15.6.6a.

2) Step 3, step3 a, step 4 and step 4a are referred to ETSI TS 123 502 [i.2], clause 4.17.4 and clause 5.2.7.

Discovery and using of L-NEF is the key point for MEC to reduce latency and improve application experience.

5.6.3 Solution proposal #2: Usage of Nupf_EventExposure to Report QoS Monitoring

This solution proposes that UPF directly reports QoS monitoring to AF/MEC instead of the current ETSI R16 procedure UPF->SMF->PCF->NEF->AF/MEC, which is a long path.

Figure 5.6.3-1 mainly illustrates the UPF notification to AF/MEC or L-NEF (referred to ETSI TS 123 548 [i.15]).

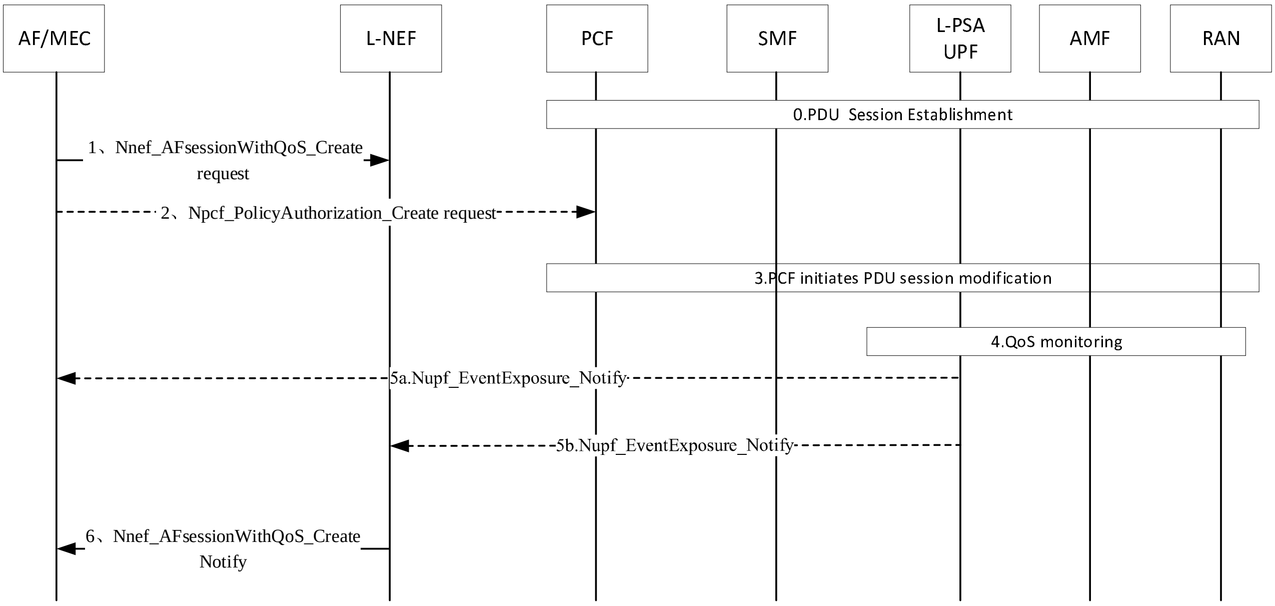

AF/MEC
L-NEF
PCF
SMF
L-PSA UPF
AMF
RAN
0.PDU Session Establishment
1、Nnef_AFsessionWithQoS_Create request
2、Npcf_PolicyAuthorization_Create request
3.PCF initiates PDU session modification
4.QoS monitoring
5a.Nupf_EventExposure_Notify
5b.Nupf_EventExposure_Notify
6、Nnef_AFsessionWithQoS_Create Notify

Figure 5.6.3-1: Network exposure through Nupf_EventExposure

The main process is as follows：

- AF/MEC initiates Nnef_AFSessionWithQoS_Creat_request to L-NEF（step 1). If AF/MEC is trusted by the operator, it can also initiate Npcf_Authorization_Subscribe service via PCF (step 2) directly. In this case, reporting is done directly from the UPF to the local AF.

- Based on the request of direct event notification and operator's policy, the PCF may include an indication of direct event notification (including target local NEF address or target AF/MEC address) within the PCC rule that it provides to the SMF (step 3).

- SMF sends the QoS monitoring request to the RAN and N4 rules to the L-PSA UPF. RAN and LPSA UPF starts QoS monitoring (step 4), this is as defined in ETSI TS 123 501 [i.1], clause 5.33.3.

- Finally L-PSA UPF notifies the QoS Monitoring event (when to notify is triggered based on N4 rules from SMF) information to the AF/MEC, step 5a (or via L-NEF, step 5b, then to AF/MEC, step 6).

- The L-PSA UPF could support Nupf_EventExposure_Notify service operation, as defined in ETSI TS 123 502 [i.2], clause 5.2.26. This avoids the long path defined in R16, and significantly shortens delay and improves efficiency.

5.6.4 Evaluation

Enterprises in the park have a strong demand for consumption of 5GC exposure capability and require fast, low latency and efficient notifications.

In solution #1, MEC acting as a AF can consume 5GC exposed capability through L-NEF, if UE moves, serving MEC changes and then L-NEF changes accordingly. There are three ways for MEC acting as a AF to find a L-NEF, as follows:

1) pre-configure L-NEF IP address/FQDN;

2) pre-configure NEF IP address/FQDN, sending corresponding request information such as location to NEF, NEF redirects the request to L-NEF;

3) utilize NRF to find L-NEF, in this scenario, MEC is a trusted AF of the operator.

MEC sends requests through L-NEF, and receives corresponding notification from L-NEF, this can significantly shorten the delay and improve the efficiency.

In solution #2, MEC acting as a AF can be notified by L-PSA UPF directly. This replaces the previous long path method by UPF->SMF->PCF->NEF. This solution also considers the UE moving scenario. When UE moves, serving MEC changes and then L-PSA UPF changes accordingly.

Therefore, based on this evaluation, two solutions together make MEC consumption of 5GC exposure capability more efficient. Overall, solution#2 is more important than solution#1.

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: ULCL PSA insertion based on Location	5.1	#1: AF detecting UE Location and report to PCF	No	3GPP based solution
		#2: SMF detecting UE Location changing	No	3GPP based solution
#2: Unified AAA management of MEC system	5.2	#2: Using UE Identity API	Yes, ETSI GS MEC 014 [i.7]	No
		#1: DN-AAA triggers Secondary authentication/authorization when ULCL inserting	Yes, ETSI GS MEC 002 [i.9]	3GPP based solution
#3: Dynamic management according to user	5.3	#1: Defining the traffic gateway function of MEP	Yes, ETSI GS MEC 003 [i.3]	No
		#2: Add a time dimension to business attributes	Yes, ETSI GS MEC 011 [i.5]	No
		#3: Add UE Identity tags list to MEC platform	Yes, ETSI GS MEC 011 [i.5]	Np
#4: Remote access of enterprise MEC applications	5.4	#1: Remote access through Internet	No	No
		#2: Remote access through mobile backbone network	No	No
#5: MEC application Slicing support	5.5	#1: Introducing MEC Slice Management	Yes, ETSI GR MEC 044 [i.17]	No
#6: MEC efficient consumption of 5GC exposure capability	5.6	#1: Local NEF Deployment for (local) network information exposure to MEC with Low Latency	No	3GPP network capability exposure C
		#2: Usage of Nupf_EventExposure to Report QoS Monitoring	No	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 follow-up work in ETSI ISG MEC:

- Requirements and possibly related use-cases need to be added to ETSI GS MEC 002 [i.9] related to the interworking between the MEC platform and the 5GC network for unified management AAA.
- A new procedure for UE Identity API Request/Response needs to be added to ETSI GS MEC 014 [i.7] related to the API usage scenario when the MEC APP Instance invokes the UE Identity API exposed by the MEP.
- ETSI GR MEC 044 [i.17] is dedicated to address KI#5.
- A description needs to be added, e.g. a time dimension to business attributes, UE Identity tags list to ETSI GS MEC 011 [i.5], on dynamic management of MEC.

Annex A:
Change History

Version	Date	Information about changes
	October 2020	TB adoption of WI, see contribution MEC(20)000365 in RC MEC(20)DEC124
V3.0.1	December 2020	Implements document MEC(20)000381r3
V3.0.2	January 2021	Implements document MEC(20)000402r1 and MEC(20)000403
V3.0.3	February 2021	Implements document MEC(21)000085r1 and MEC(21)000086r2
V3.0.4	April 2021	Implements documents MEC(21)000140r1,MEC(21)000141r1,MEC(21)000142r2
V3.0.5	June 2021	Implements document MEC(21)000202r2
V3.0.6	August 2021	Implements documents MEC(21)000286r1, MEC(21)000288r2 and MEC(21)000289r2
V3.0.7	October 2021	Implements documents MEC(21)000445r1, MEC(21)000446r1, MEC(21)000447 and MEC(21)000514r2
V3.0.8	December 2021	Implements documents MEC(21)000536r1 and MEC(21)000550
V3.0.9	January 2022	Implements documents MEC(21)000551r3, MEC(21)000584r1 and MEC(21)000588r2
V3.0.10	February 2022	Implements documents MEC(22)000016r3 and MEC(22)000011r1
V3.0.11	March 2022	Implements documents MEC(22)000093r1, MEC(22)000094r3,MEC(22)000149r1
V3.0.12	April 2022	Implements documents MEC(22)000174r1, MEC(22)000190r1, MEC(22)000191r1, MEC(22)000192r1, MEC(22)000193r1
V3.0.13	April 2022	Implements documents MEC(22)000191r1
V3.0.14	May 2022	Implements documents MEC(22)000213 and MEC(22)000233
V3.0.15	June 2022	Implements documents MEC(22)000241 and MEC(22)000248

History

Document history		
V3.1.1	November 2022	Publication