ETSI GS MEC 002 V4.1.1 (2025-06)

Multi-access Edge Computing (MEC); Use Cases and Requirements

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
RGS/MEC-0002v411TechReq

Keywords
MEC, requirements, use case

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

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Multi-access Edge Computing (MEC).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 specifies the requirements for Multi-access Edge Computing with the aim of promoting interoperability and deployments. It contains normative and informative parts.

The present document also contains an annex describing example use cases and their technical benefits, for the purpose of deriving requirements.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 necessary for the application of the present document.

Not applicable.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GR MEC 001: "Multi-access Edge Computing (MEC); Terminology".

[i.2] "Mobile-Edge Computing - Introductory Technical White Paper", September 2014.

[i.3] IETF draft-flinck-mobile-throughput-guidance-03.txt: "Mobile Throughput Guidance Inband Signaling Protocol".

[i.4] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[i.5] Franck Le; Mudhakar Srivatsa; Arun K. Iyengar: "Byte Caching in Wireless Networks", IEEE™ 32nd International Conference on Distributed Computing Systems Macau, China, June 2012.

[i.6] Computer Science and Engineering: "A protocol-independent technique for eliminating redundant network traffic", 352350 University of Washington.

[i.7] IETF draft-sprecher-mobile-tg-exposure-req-arch-02.txt: "Requirements and reference architecture for Mobile Throughput Guidance Exposure".

[i.8] Small Cells Forum White Paper SCF081: "Enterprise unified communications services with small cells".

[i.9] IEEE 1588™: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[i.10] IETF draft-kanugovi-intarea-mams-protocol-05: "Multiple Access Management Services".

[i.11] IETF draft-zhu-intarea-mams-control-protocol-02: "Control Plane Protocols and Procedures for Multiple Access Management Services".

[i.12] IETF draft-zhu-intarea-mams-user-protocol-09: "User-Plane Protocols for Multiple Access Management Service".

[i.13] ETSI GS MEC 012: "Multi-access Edge Computing (MEC); Radio Network Information API".

[i.14] NGMN®: "5G security - Package 3: Mobile Edge Computing / Low Latency / Consistent User Experience".

[i.15] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.16] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".

[i.17] ETSI TR 126 957: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Study on Server And Network-assisted Dynamic Adaptive Streaming over HTTP (DASH) (SAND) for 3GPP multimedia services (3GPP TR 26.957)".

[i.18] ETSI TS 126 247: "Universal Mobile Telecommunications System (UMTS); LTE; Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH) (3GPP TS 26.247)".

[i.19] ISO/IEC 23009-5: "Information technology - Dynamic adaptive streaming over HTTP (DASH) - Part 5: Server and network assisted DASH (SAND)".

[i.20] H. Kagermann, W. Wahlster, and J. Helbig: "Recommendations for implementing the strategic initiative INDUSTRIE 4.0", Final report of the Industrie 4.0 working group, acatech, National Academy of Science and Engineering, Munich, April 2013.

[i.21] UK NIC (National Infrastructure Committee): "5G Infrastructure Requirements in the UK", final report.

[i.22] ETSI TS 123 501: "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501)".

[i.23] ETSI TS 123 502: "5G; Procedures for the 5G System (5GS) (3GPP TS 23.502)".

[i.24] ETSI GR MEC 022: "Multi-access Edge Computing (MEC); Study on MEC Support for V2X Use Cases".

[i.25] ETSI GR MEC 035: "Multi-access Edge Computing (MEC); Study on Inter-MEC systems and MEC-Cloud systems coordination".

[i.26] ABI Research: "Smart Home and Service Integration", 3Q 2018 (PT-1907).

[i.27] CableLabs®: "The Near Future. Bring it on".

[i.28] CableLabs®: "Behind the tech with Phil McKinney: The Near Future".

[i.29] CableLabs®: "The Near Future. Ready for Anything".

[i.30] CableLabs®: "The Near Future. Ready for Anything. Behind the Technology".

[i.31] ETSI GR MEC 041: "Multi-access Edge Computing (MEC); Study on MEC Security".

[i.32] ETSI GS NFV-SEC 024: "Network Functions Virtualisation (NFV) Security; Security Management Specification".

[i.33] ETSI GS MEC 003: "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[i.34] ETSI GS MEC 010-2: "Multi-access Edge Computing (MEC); MEC Management; Part 2: Application lifecycle, rules and requirements management".

[i.35] NIST SP800-53v5: "Security and Privacy Controls for Information Systems and Organizations".

[i.36] IETF RFC 9232: "Network Telemetry Data".

[i.37] NIST Computer Security Resource Center Glossary.

[i.38] IETF RFC 9334: "Remote Attestation Procedures".

[i.39] ETSI TS 133 535: "5G; Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS) (3GPP TS 33.535)".

[i.40] ETSI GR MEC 044: "Multi-access Edge Computing (MEC); Study on MEC Application Slices".

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.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR MEC 001 [i.1] and the following apply:

AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AR	Augmented Reality
BYO	Bring Your Own
CCM	Client Connection Manager
CFS	Customer Facing Service
CI/CD	Continuous Integration/Continuous Delivery
C-MADP	Client Multiple Access Data Proxy
CP	Control Plane
CPE	Customer Premises Equipment
DANE	DASH-Aware Network Element
DASH	Dynamic Adaptive Streaming over HTTP
DN	Domain Name
DSL	Digital Subscriber Line
DSRC	Digital Short-Range Communications
EAB	Edge Accelerated Browser
ECU	Engine Control Unit
EPC	Evolved Packet Core
EPG	Electronic Programme Guide
FQDN	Fully Qualified Domain Name
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HW	HardWare
IGMP	Internet Group Multicast Protocol
IM	Instant Messaging
IPTV	Internet Protocol TeleVision
ISP	Internet Service Provider
IT	Information Technology

LI	Lawful Interception
LOS	Line Of Sight
MAMS	Multiple Access Management Services
ME	Mobile Equipment
MIMO	Multiple Input Multiple Output
ML	Machine Learning
MPEG	Moving Pictures Experts Group
NCM	Network Connection Manager
NEF	Network Exposure Function
N-MADP	Network Multiple Access Data Proxy
NTP	Network Time Protocol
OBU	On Board Unit
OPEX	OPerating EXpenditure
OTT	Over-The-Top
PBX	Private Branch eXchange
PCC	Policy Control and Charging
PCF	Policy Control Function
PER	Packet Error Rate
PIM	Protocol-Independent Multicast
PSS	Packet-switched Streaming Service
PTP	Precision Time Protocol
RAT	Radio Access Technology
RD	Retained Data
RNC	Radio Network Controller
SAND	Server And Network assisted DASH
SLA	Service Level Agreement
SMF	Session Management Function
SMS	Short Message Service
SPID	Subscriber Profile ID
SRS	Sounding Reference Signal
STB	Set Top Box
TEID	Tunnel Endpoint ID
TEO	Third-party Edge Owner
TV	TeleVision
UX	User eXperience
VOD	Video On Demand
VR	Virtual Reality

4 Generic principles

4.1 Introduction

The following principles are important to understand in the context of Multi-access Edge Computing.

4.2 NFV alignment

Multi-access Edge Computing uses a virtualisation platform for running applications at the mobile network edge. Network Functions Virtualisation (NFV) provides a virtualisation platform to network functions. The infrastructure that hosts their respective applications or network functions is quite similar.

In order to allow operators to benefit as much as possible from their investment, it would be beneficial to reuse the infrastructure and infrastructure management of NFV to the largest extent possible, by hosting both Virtual Network Functions (VNFs) and MEC applications on the same or similar infrastructure. Subject to gap analysis, this might require a number of enhancements (e.g. regarding the sharing of resources with NFV Management and Orchestration, etc.).

4.3 Mobility support

Mobility is an essential functionality of 3GPP networks. Most devices connected to a 3GPP network are moving around within the mobile network. Even fixed devices can "move", especially when located at cell edge, but also when changing RATs, etc., or during exceptional events (e.g. power cut from a base station, etc.).

Some MEC applications are state-independent and do not need to keep state information related to the UEs they are serving. For example, an application in the category "network performance and QoE improvements" will only improve the performance of the UE traffic when the traffic goes through that MEC host. When the UE moves to a different location covered by another MEC host, it will be the application hosted on that MEC host that will take care of the UE after a brief transition period. Past interaction is not useful for the application.

Other MEC applications, notably in the category "consumer-oriented services", are specifically related to the user activity. Either the whole application is specific to the user, or at least it needs to maintain some application-specific user-related information that needs to be provided to the instance of that application running on another MEC host.

As a consequence of UE mobility, the MEC system needs to support the following:

- continuity of the service;
- mobility of application (VM); and
- mobility of application-specific user-related information.

4.4 Deployment independence

For reasons of performance, costs, scalability, operator preferred deployments, etc., different deployment scenarios need to be supported:

- deployment at the radio node;
- deployment at an aggregation point;
- deployment at the edge of the Core Network (e.g. in a distributed data centre, at a gateway);
- etc.

In order to fulfil all these deployment options, the framework of the MEC architecture needs to allow all these scenarios and the requirements need to be able to address all these deployment options. Requirements that cannot be fulfilled for all deployment options cannot be made mandatory, but might be conditional or optional.

When a MEC platform is deployed on a host located in a cell aggregation site, MEC services running on that platform might need to retrieve information from the radio node(s), for instance, to readout the traffic load and resource block usage of a specific cell.

In order to prevent the illegal access from dishonest terminals and MEC application developers, authentication and secure tunnel communication are necessary between the radio node(s) and the MEC service.

NOTE: The interface between the radio node(s) and the MEC service is not specified in Multi-access Edge Computing Group Specifications.

4.5 Simple and controllable APIs

In order to enable the development of a strong ecosystem for Multi-access Edge Computing, it is very important to develop APIs that are as simple as possible and are directly answering the needs of applications. To the extent this is possible, Multi-access Edge Computing specifications need to reuse existing APIs that fulfil the requirements.

In particular circumstances, operators might need to be able to control dynamically the access to certain APIs by a MEC application. Examples include the mitigation of high load of a radio node or MEC host, or when the information of a specific radio node or cell cannot be provided.

4.6 Smart application location

MEC applications have a number of requirements, in terms of computing, storage and network resources. More importantly, some applications might have requirements in terms of latency (including latency fairness), etc.

For a certain number of MEC applications, the conditions might evolve over time and require the MEC system to change the location of the application, e.g. as the UEs are moving from cell to cell.

Also, different locations may have different "costs" (in terms of resource availability, energy consumption, etc.), and it might not be always the best choice to run a MEC application at the "best" location (to the detriment of other applications).

For these reasons, MEC applications need to run "at the right place" at the right moment, and might have to move when the conditions evolve. In order to support this, the MEC system needs to provide a system-wide lifecycle management of applications.

4.7 Application mobility to/from an external system

In order to support service continuity when the user context and/or application instance is relocated, the system needs to be able to relocate a MEC - application running in an external cloud environment to a MEC host fulfilling the requirements of the MEC application and relocate a MEC application from a MEC host to an external cloud environment outside the MEC system.

NOTE: The scenario of application relocation from a MEC host to an external cloud environment outside the MEC system is for further study.

Two different aspects of application mobility need to be supported to enable user context and/or application instance relocation from an external cloud environment to a MEC host. Firstly, how to transfer files running in the external cloud to the target MEC host, and secondly how to relocate an application instance and the user context to the target MEC host.

For the file transfer there is a possible scenario: For OTT vendors that already have operations in the cloud, files running in the cloud can be uploaded to a functional unit at the MEC host via a portal, such as a customer facing service portal, where the cloud file template can be converted to an image file that can be instantiated in the MEC hosts.

Relocation of an application instance from the external cloud to the target MEC host can follow the application relocation approach between MEC hosts. When MEC is deployed in conjunction with a 5G network, the target UPF of 5G is selected based on UE location and DN connecting to the MEC host which the applications are running on. When the UE moves to the target MEC host serving area the 5G network may provide the information of the target UPF to the MEC system to identify the target MEC host for application relocation. Therefore, the external cloud can transfer both the user context (by client, MEC system assists or other assists) and/or application instance to the target MEC host based on the information reported by the MEC system.

4.8 Representation of features

The present document describes requirements towards the framework and architecture of Multi-access Edge Computing.

In addition to the definition of requirements applicable to all deployments, the present document introduces the concept of features in order to cater for the different needs of different deployments. A feature is defined as a group of related requirements and is assigned a unique name.

Support for a feature can be mandatory, optional or conditional. Where feature level support is optional or conditional, all other requirements (mandatory or optional) related to that feature are themselves dependent upon support for the feature itself.

The following example illustrates an optional feature with a conditional mandatory and a conditional optional requirement.

EXAMPLE: [Req-1] The MEC system may support a feature called *XYZ*.
[Req-2] When the MEC system supports the feature *XYZ*, the system shall…
[Req-3] When the MEC system supports the feature *XYZ*, the system may…

The architectural framework needs to support mechanisms to identify whether a specific feature is supported. Such information might need to be considered when executing certain tasks, such as the instantiation of an application.

4.9 Inter-MEC system communication

To enable the coordination between multiple MEC systems belonging to the same or different MEC providers (e.g. support of cooperation between devices that are connected to different MNOs) inter-MEC system communication is critical, which impacts MNO deployments.

Nowadays, it is very common for application/service providers to deploy applications or services on different MEC systems of the same, or different, MNOs. Inter-MEC communication may be used when a subscriber of one MNO is roaming on another MNO's network, so that services deployed on MEC systems can be delivered to a subscriber even whilst they are away from their home network. Inter-MEC communication may also be used to share edge capabilities between operators. MEC app-to-app communication and MEC service remote consumption are further important aspects that motivate the need for inter-MEC system communication, for which the following functionalities should be enabled:

- MEC system discovery including security (e.g. authentication, authorization, system topology hiding, encryption), charging, identity management and monitoring aspects.
- MEC platform discovery, by means of the MEC systems exchanging information about their MEC platforms, i.e. their identities, a list of their shared services, as well as authorization and access policies.
- Information exchange at MEC platform level, for MEC service consumption or for MEC app-to-app communication.

5 Generic requirements

5.1 Requirements on the framework

[Framework-01] The design of the MEC system should attempt to reuse the NFV virtualisation infrastructure and its management functionality, as described in the NFV architecture framework in ETSI GS NFV 002 [i.4], possibly with some enhancements. Concepts that have been developed or studied in NFV Group Specifications and that are needed for Multi-access Edge Computing should be reused whenever possible. This might require some enhancements specific to Multi-access Edge Computing.

[Framework-02] It shall be possible to enable the deployment of MEC applications on the same infrastructure as ETSI NFV-based VNFs.

[Framework-03] It shall be possible to deploy the MEC platform on MEC hosts in various locations of the fixed, mobile and wireless networks, including radio nodes, aggregation points, gateways, and in a distributed data centre at the edge of the Mobile Core Network.

[Framework-04] It shall be possible to deploy the MEC platform, applications and services in a more centralized location in the operator's or service provider's data centre.

[Framework-05] It shall be possible to deploy the MEC host in various stationary or moving nodes.

NOTE 1: A moving node could be e.g. an access point type device with wireless backhaul or a passenger vehicle.

NOTE 2: Some requirements might not be fulfilled by certain deployment options.

[Framework-06] The MEC system should provide capability to interact with the 5G core network on behalf of applications to influence on the traffic routing and policy control of UPF (re)selection and allow the corresponding user traffic to be routed to the applications running on MEC host.

5.2 Application lifecycle

[Lifecycle-01] The MEC host shall be available for the hosting of MEC applications.

[Lifecycle-02] The MEC management shall support the instantiation of an application on a MEC host within the MEC system.

[Lifecycle-03] The MEC management shall support the instantiation of an application on a MEC host when required by the operator. This may be in response to a request by an authorized third-party.

[Lifecycle-04] The MEC management shall support the termination of a running application when required by the operator. This may be in response to a request by an authorized third-party.

[Lifecycle-05] The MEC management shall be able to identify which features and MEC services a MEC application requires to run, and which additional features and MEC services it can use if available.

NOTE 1: This allows the MEC system to decide whether and on which MEC host to instantiate the application.

[Lifecycle-06] The MEC management shall be able to identify which features and MEC services are available on a particular MEC host.

NOTE 2: This allows the MEC management to decide whether a particular application can be instantiated on that host.

[Lifecycle-07] The MEC management shall support timely on-boarding of an application on a MEC host in response to a request from an authorized third-party.

[Lifecycle-08] The MEC management shall support the on-boarding of an application associated with information of the operational area or location(s) of the application service.

[Lifecycle-09] The MEC management shall support the instantiation of a MEC application in response to a request by an authorized third-party.

[Lifecycle-10] The MEC management shall support the termination of a MEC application in response to a request by an authorized third-party.

5.3 Applications environment

The applications environment describes the security, packaging and run-time environment models for hosting MEC applications on the MEC host.

[AppEnvironment-01] It shall be possible to deploy MEC applications on different MEC hosts in a seamless manner, without a specific adaptation to the application.

[AppEnvironment-02] The MEC management shall be able to verify the authenticity of a MEC application.

[AppEnvironment-03] The MEC management shall be able to verify the integrity of a MEC application (integrity protection).

[AppEnvironment-04] The MEC system shall support distributed edge cloud deployments and in doing so horizontally and vertically distributed applications, where horizontal implies peer to peer connectivity of the application components and vertical implies hierarchical connectivity between different application components.

[AppEnvironment-05] It should be possible to host a MEC platform in cloud resources owned, operated and orchestrated by third party edge owners.

NOTE: Application components may reside outside of the distributed edge cloud, for example in the device or central cloud.

5.4 Support of mobility

[Mobility-01] The MEC system shall be able to maintain connectivity between a UE and an application instance when the UE performs a handover to another cell associated with the same MEC host.

[Mobility-02] The MEC system shall be able to maintain connectivity between a UE and an application instance when the UE performs a handover to another cell not associated with the same MEC host.

[Mobility-03] The MEC platform may use available radio network information to optimize the mobility procedures required to support service continuity.

[Mobility-04] The MEC platform may use available core network information to optimize the mobility procedures required to support service continuity.

EXAMPLE: Using UE mobility information to optimize the handling of mobility events by the application (see clause 6.2.2, Connectivity) and of application mobility (see clause 6.3.2, Feature *SmartRelocation*).

6 Services requirements

6.1 General

The MEC platform on a MEC host provides a framework for delivering MEC services and platform essential functionality to MEC applications running on the MEC host.

A MEC service is provided and consumed. Both the MEC platform itself and authorized MEC applications can provide services. Similarly, both the MEC platform itself and authorized MEC applications can consume services.

In some cases, and especially in a multi-vendor environment, the service can be provided concurrently by multiple sources. This allows the platform or the applications consuming the service to receive all information required for executing their tasks.

Many of the applications require accurate time information synchronized to the time domain of the operator or application provider. Such applications require exact time of specific events occurrence for analytics information collection and pre-processing, time tagging of the location information, synchronized time intervals for the SLA throughput reports, platform performance monitoring for latency and response times and many others.

Since the platform is located in the synchronized environment required for the mobile network operation, accurate time of day information can be delivered to the platform by the same means as it is provided to the mobile Base Stations. Known techniques include usage of GNSS receivers, running IEEE 1588™ [i.9] PTP protocol, NTP protocol or a combination of the above.

The MEC platform will have a means to acquire accurate Time of Day information and make this information available to the hosted applications.

6.2 Platform essential functionality

6.2.1 MEC services

[Services-01] The MEC platform shall have the capability to provide MEC services that can be consumed by authorized MEC applications.

[Services-02] The MEC platform shall allow authorized MEC applications to provide services that can be consumed by the platform or by authorized MEC applications running on the MEC host.

NOTE 1: Providing a service by an application to the MEC platform includes that the platform can receive information from that application. This information can be used by the MEC platform to provide other services.

[Services-03] The MEC platform shall provide functionality to allow authorized MEC applications to communicate with MEC services provided by the platform.

[Services-04] The MEC platform shall allow authentication and authorization of providers and consumers of MEC services.

[Services-05] When necessary, the MEC system shall allow operators to dynamically control the access of running MEC applications to certain services.

[Services-06] The MEC platform shall provide a secure environment for providing and consuming MEC services when necessary.

NOTE 2: Specific services can require end-to-end mechanisms for security.

NOTE 3: A service can be provided concurrently by multiple sources. It depends on the actual service whether the multiple sources are visible to the service consumers or are consolidated and presented as a single source. This will be described as part of the service description.

[Services-07] The MEC platform shall allow MEC services to announce their availability. The platform shall allow the discovery of available MEC services.

[Services-08] The MEC platform shall provide functionality that presents the MEC service availability and the related interfaces to MEC applications.

[Services-09] The access to the information regarding MEC service availability and related interfaces shall only be allowed to authenticated and authorized MEC applications. Access to information about each MEC service shall be separately authorized. Separate authorization shall be possible for registering MEC services, and for obtaining information about registered MEC services.

6.2.2 Connectivity

[Connectivity-01] The MEC platform shall allow authorized MEC applications on the same MEC host to communicate with each other.

[Connectivity-02] The MEC system shall support two instances of a MEC application running on different MEC hosts to communicate with each other.

NOTE: This allows application-specific procedures to move information from one application instance to another, in order to maintain continuity of the service provided by the application as the UE moves around.

[Connectivity-03] The MEC platform shall be able to allow an authorized MEC application to communicate with another MEC application located on another MEC host.

[Connectivity-04] The MEC platform shall be able to allow an authorized MEC application to communicate with third-party servers located in external networks.

6.2.3 Storage

[Storage-01] The MEC platform shall be able to provide access to persistent storage space to an authorized MEC application.

6.2.4 Traffic routing

[Routing-01] The MEC platform shall provide functionality to allow authorized MEC applications to send user plane traffic to UEs.

[Routing-02] The MEC platform shall provide functionality to allow authorized MEC application to receive user plane traffic from UEs.

[Routing-03] The MEC platform shall provide functionality to route selected uplink and/or downlink user plane traffic from the network to authorized MEC applications.

[Routing-04] The MEC platform shall provide functionality to route selected uplink and/or downlink user plane traffic from authorized MEC applications to the network.

[Routing-05] The MEC platform shall provide functionality to allow authorized MEC applications to inspect selected uplink and/or downlink user plane traffic.

[Routing-06] The MEC platform shall provide functionality to allow authorized MEC applications to modify selected uplink and/or downlink user plane traffic.

[Routing-07] The MEC platform shall provide functionality to allow authorized MEC applications to shape selected uplink and/or downlink user plane traffic.

[Routing-08] The MEC platform shall provide functionality to route selected uplink and/or downlink user plane traffic from an authorized MEC application to another authorized MEC application.

[Routing-09] The MEC platform shall be able to select one or more applications to which the same traffic will be routed and assign priorities to them. The selection, prioritization and routing of traffic shall be based on traffic rules defined per MEC application.

NOTE 1: The prioritization is used to determine the routing order between the MEC applications.

[Routing-10] The MEC management shall allow the configuration of the traffic rules.

[Routing-11] The traffic rules shall allow setting packet filters based on network address and/or IP protocol.

[Routing-12] The traffic rules may allow setting packet filters based on the Tunnel Endpoint ID (TEID) and/or the Subscriber Profile ID (SPID) and/or the Quality Class Indicator (QCI) value(s).

[Routing-13] When the user plane traffic is encapsulated, then:

- the MEC host shall support the de-capsulation of the encapsulated (uplink) IP traffic and its routing to the authorized MEC applications;
- the MEC host shall support the encapsulation of (downlink) IP traffic received from authorized MEC applications before routing it to the network.

NOTE 2: IP traffic for example can be encapsulated with GTP header.

[Routing-14] The MEC host shall support routing user plane traffic to/from authorized MEC applications according to configurable parameters received from the MEC platform.

[Routing-15] The MEC system should support forwarding and processing of the IP packets for IP multicast group management.

[Routing-16] The MEC system should support forwarding the IP multicast packets based on application specific forwarding logic.

6.2.5 DNS support

[DNS-01] The MEC platform shall provide functionality that supports routing all DNS traffic received from any UE to a local DNS server/proxy.

[DNS-02] The MEC platform shall support configuring the local DNS server/proxy with the association of specific FQDN with IP addresses allocated to MEC application instances.

6.2.6 Timing

[Timing-01] The MEC platform shall provide a capability of supplying UTC time of day information to the authorized MEC applications. The information regarding time of day accuracy provided by the platform should be available to the applications.

[Timing-02] The MEC platform may provide authorized MEC applications with accurate time of specific user packets received or transmitted by the platform.

6.3 Features

6.3.1 Feature *UserApps*

[UserApps-01] The MEC system may support the feature called *UserApps*.

[UserApps-02] When the MEC system supports the feature *UserApps*, the MEC management shall support the instantiation of a MEC application on multiple MEC hosts following a single instantiation request.

[UserApps-03] When the MEC system supports the feature *UserApps*, the MEC management shall support the instantiation of a MEC application on a MEC host when required by the operator in response to a request by the user. The application instance needs to fulfil a number of potential constraints predefined for the application. Once instantiated, connectivity shall be established between the UE and the application instance.

NOTE 1: Potential constraints can include latency, location, compute resources, storage resources, network capability, security conditions.

[UserApps-04] When the MEC system supports the feature *UserApps*, the system shall, in response to a request by the user, support the establishment of connectivity between the UE and an instance of a specific MEC application fulfilling the requirements of the application regarding this UE. If no instance of the application fulfilling these requirements is currently running, the MEC system management shall create a new instance of the application on a MEC host that fulfils the requirements of the application. Once instantiated, connectivity shall be established between the UE and the new application instance.

NOTE 2: Requirements of the application can include latency, energy consumption, location, compute resources, storage resources, network capability, security conditions.

[UserApps-05] When the MEC system supports the feature *UserApps*, the system shall support the on-boarding of a MEC application during the execution of an instantiation request.

[UserApps-06] When the MEC system supports the feature *UserApps*, the system shall allow the establishment of connectivity between a UE and a specific instance of a MEC application.

[UserApps-07] When the MEC system supports the feature *UserApps*, the MEC management shall support the capability to terminate a MEC application instance when no UE is connected to it anymore.

[UserApps-08] When the MEC system supports the feature *UserApps*, the MEC management shall support the termination of a MEC application running on multiple MEC hosts following a single termination request.

6.3.2 Feature *SmartRelocation*

[SmartReloc-01] The MEC system may support the feature called *SmartRelocation*.

[SmartReloc-02] When the MEC system supports the feature *SmartRelocation*, the system shall support the feature *UserApps*.

[SmartReloc-03] When the MEC system supports the feature *SmartRelocation*, the MEC management shall support the relocation of a MEC application instance from one MEC host to a different host within the system.

[SmartReloc-04] When the MEC system supports the feature *SmartRelocation*, a MEC host may support the relocation of a MEC application instance from a different host (within the system) to this particular host, and from this particular host to a different host (within the system).

NOTE 1: Both hosts (source and target) need to support the feature *SmartRelocation* for relocation to be executed. If the ability to perform relocation is required for a MEC application, the MEC management will select a host that supports the feature *SmartRelocation* when instantiating the MEC application.

[SmartReloc-05] When the MEC system supports the feature *SmartRelocation*, the system shall be able to move MEC application instances between MEC hosts in order to continue to satisfy the requirements of the MEC application.

NOTE 2: Requirements of the application can include latency, energy consumption, compute resources, storage resources, etc.

[SmartReloc-06] When the MEC system supports the feature *SmartRelocation*, and based on a request from the UE, the system shall be able to relocate a MEC application running in a cloud environment to a MEC host fulfilling the requirements of the MEC application, and relocate a MEC application from a MEC host to a cloud environment outside the MEC system.

[SmartReloc-07] When the MEC system supports the feature *SmartRelocation*, the customer facing service portal may support the reception of application files from an external cloud system and may support conversion of such files to an application image that can be instantiated in the MEC system.

6.3.3 Feature *RadioNetworkInformation*

[RNI-01] The MEC system may support the feature called *RadioNetworkInformation*.

[RNI-02] When the MEC system supports the feature *RadioNetworkInformation*, there shall be a MEC service that exposes up-to-date radio network information regarding the current radio network conditions.

[RNI-03] When the MEC system supports the feature *RadioNetworkInformation*, there shall be a MEC service that provides appropriate up-to-date radio network information.

NOTE: The radio network information can be based on information received from external sources and/or generated locally.

[RNI-04] When the MEC system supports the feature *RadioNetworkInformation*, the radio network information shall be provided at the relevant granularity (e.g. per User Equipment (UE) or per cell, per period of time).

[RNI-05] When the MEC system supports the feature *RadioNetworkInformation*, the provided radio network information shall include measurement and statistics information related to the user plane. This information shall be based on information defined by 3GPP specifications.

[RNI-06] When the MEC system supports the feature *RadioNetworkInformation*, the provided radio network information shall include information related to UEs connected to the radio node(s) associated with the MEC host, their UE context and the related radio access bearers.

[RNI-07] When the MEC system supports the feature *RadioNetworkInformation*, the provided radio network information shall include information on changes related to UEs connected to the radio node(s) associated with the MEC host, their UE context and the related radio access bearers.

[RNI-08] When the MEC system supports the feature *RadioNetworkInformation*, the provided radio network information shall include QoS information on the specific connection.

[RNI-09] When the MEC system supports the feature *RadioNetworkInformation*, the provided radio network information shall include information on the actual throughput.

[RNI-10] When the MEC system supports the feature *RadioNetworkInformation*, the provided radio network information shall include a bitrate recommendation based on the actual real-time radio throughput available for a specific connection.

[RNI-11] When the MEC system supports the feature *RadioNetworkInformation*, the MEC system shall be able to convey radio and network status information to a DANE server located in the third party domain outside of the operator network.

6.3.4 Feature *LocationService*

[Location-01] The MEC system may support the feature called *LocationService*.

[Location-02] When the MEC system supports the feature *LocationService*, there shall be a MEC service that provides information about the location of specific UEs currently served by the radio node(s) associated with the MEC host.

[Location-03] When the MEC system supports the feature *LocationService*, there shall be a MEC service that provides information about the location of all UEs currently served by the radio node(s) associated with the MEC host.

[Location-04] When the MEC system supports the feature *LocationService*, there may be a MEC service that provides information about the location of a certain category of UEs currently served by the radio node(s) associated with the MEC host.

[Location-05] When the MEC system supports the feature *LocationService*, there shall be a MEC service that presents a list of UEs in a particular location.

NOTE: Location can be geolocation, Cell ID, etc.

[Location-06] When the MEC system supports the feature *LocationService*, there shall be a MEC service that provides information about the location of all radio nodes currently associated with the MEC host.

6.3.5 Feature *BandwidthManager*

[Bandwidth-01] The MEC system may support the feature called *BandwidthManager*.

[Bandwidth-02] When the MEC system supports the feature *BandwidthManager*, the MEC platform or a dedicated MEC application shall enable an authorized MEC application to register statically and/or dynamically its bandwidth requirements and/or priority.

[Bandwidth-03] When the MEC system supports the feature *BandwidthManager*, the MEC platform or a dedicated MEC application may allocate bandwidth and/or assign priority to any session or to any application.

[Bandwidth-04] When the MEC system supports the feature *BandwidthManager*, the MEC platform or a MEC application shall have means to allocate bandwidth and/or assign priority to a session, where the allocation request is associated with the auxiliary information on session duration, total size (e.g. in Mbytes), etc.

6.3.6 Feature *UEIdentity*

[UEIdentity-01] The MEC system may support a feature called *UEIdentity*.

[UEIdentity-02] When the MEC system supports the feature *UEIdentity*, the MEC platform shall provide functionality for a MEC application to register a tag (representing a UE) or a list of tags.

NOTE 1: Whether and how the mapping of IP addresses to tags is exposed to the application is described as part of the relevant API definition.

[UEIdentity-03] When the MEC system supports the feature *UEIdentity*, the MEC platform shall allow setting packet filters for routing traffic based on a tag representing the UE.

NOTE 2: The MEC application can obtain tags through mechanisms that are not defined within the system.

[UEIdentity-04] When the MEC system supports the feature *UEIdentity*, the MEC platform shall allow the routing of user-plane traffic of authorized UEs to a local network (e.g. enterprise network) connected to the MEC host without having to route the traffic via a MEC application.

[UEIdentity-05] When the MEC system supports the feature *UEIdentity*, the MEC host shall support the connectivity between authorized MEC applications and local networks (e.g. enterprise network) connected to the host.

[UEIdentity-06] When the MEC system supports the feature *UEIdentity*, the MEC platform shall provide functionality for a MEC application to obtain a tag (representing a UE) or a list of tags.

[UEIdentity-07] When the MEC system supports the feature *UEIdentity*, the MEC platform may act as an Authentication Proxy (as defined in ETSI TS 133 535 [i.39]).

6.3.7 Feature *WLANInformation*

[WLAN-01] The MEC system may support the feature called *WLANInformation*.

[WLAN-02] When the MEC system supports the feature *WLANInformation*, there shall be a MEC service that exposes up-to-date WLAN information regarding the current WLAN conditions.

[WLAN-03] When the MEC system supports the feature *WLANInformation*, there shall be a MEC service that provides appropriate up-to-date WLAN information.

NOTE: The WLAN information can be based on information received from external sources and/or generated locally.

6.3.8 Feature *V2XService*

NOTE: The following requirements are concluded from the study in ETSI GR MEC 022 [i.24].

[V2X-01] The MEC system may support the feature called *V2XService*.

[V2X-02] When the MEC system supports the feature *V2XService*, the MEC system shall support the capability to provide feedback information from the network to the vehicle in support of V2X functions, which helps with predicting whether a communication channel is currently reliable or not (e.g. in terms of fulfilling latency requirements and 100 % packet arrival).

[V2X-03] When the MEC system supports the feature *V2XService*, the MEC system shall support the capability to provide quality related information from the network to the vehicle about when the various connectivity parameters (like Latency, PER, signal-strength, etc.) are going to change.

[V2X-04] When the MEC system supports the feature *V2XService*, the MEC system shall be able to provide interoperability by supporting V2X information exchange among road users connected through different access technologies or networks or mobile operators.

[V2X-05] When the MEC system supports the feature *V2XService*, the MEC system shall enable multi-operator operation for V2X mobiles/users to provide service continuity across access network coverage nationwide and across borders of different operators' networks.

[V2X-06] When the MEC system supports the feature *V2XService*, the MEC system shall be able to provide interoperability in a multi-operator scenario, enabling MEC apps in different systems to communicate securely with each other, in order to enable synchronization in multi-operator systems also in absence of cellular coverage (outside of 3GPP domain).

[V2X-07] When the MEC system supports the feature *V2XService*, the MEC system shall be able to provide interoperability in a multi-operator scenario, enabling MEC apps to communicate securely with the V2X-related 3GPP core network logical functions (e.g. V2X control function) and gathering PC5 V2X relevant information (e.g. PC5 configuration parameters) from 3GPP network.

[V2X-08] When the MEC system supports the feature *V2XService*, the MEC system shall be able to provide information about available sensor data sources to the MEC applications.

[V2X-09] When the MEC system supports the feature *V2XService*, the MEC system shall be able to provide information on the endpoint of the external sensor data sources.

6.3.9 Feature *5GCoreConnect*

[5GCoreConnect-001] The MEC system may support the feature called *5GCoreConnect*.

[5GCoreConnect-002] When the MEC system supports the feature *5GCoreConnect*, and the MEC system requests to change the traffic routing and/or change the policy, the MEC system should send a request to the 5G Network Exposure Function on behalf of the MEC applications to request its required traffic routing and/or policy control.

[5GCoreConnect -003] When the MEC system supports the feature *5GCoreConnect*, the MEC system may receive information from the 5G Network Exposure Function or other 5G core network function. Based on this information the MEC system should support selection of a MEC host or MEC hosts and the instantiation of an application on the selected MEC host or hosts.

NOTE 1: The MEC orchestrator is responsible for selecting the most suitable MEC host to run the application and making the decision of the application instantiation.

[5GCoreConnect-004] When the MEC system supports the feature *5GCoreConnect*, the MEC system can subscribe relevant events and then receive notifications from the 5G Network Exposure Function or other 5G core network function. The MEC system may use the notification content to support relocation of the specific application instance to a particular MEC host, as part of the SmartRelocation feature.

NOTE 2: The MEC orchestrator is responsible for selecting the most suitable MEC host and deciding the application instance relocation when required.

6.3.10 Feature *MultiaccessTrafficSteering*

[MTS-01] The MEC system may support the feature called *MultiaccessTrafficSteering*.

[MTS-02] When the MEC system supports the feature *MultiaccessTrafficSteering*, the MEC platform or a dedicated MEC application shall enable an authorized MEC application to get informed of various multi-access traffic steering capabilities and multi-access network connection information.

[MTS-03] When the MEC system supports the feature *MultiaccessTrafficSteering*, the MEC platform or a dedicated MEC application shall enable an authorized MEC application to register, unregister, and update its multi-access traffic steering requirements.

6.3.11 Feature *CustomerPremiseEdge*

[CustomerPremiseEdge-01] The MEC system may support a feature called *CustomerPremiseEdge*.

[CustomerPremiseEdge-02] When the MEC system supports the feature *CustomerPremiseEdge*, the MEC platform shall enable MEC applications to offload tasks to or receive services from non-MEC computing resources available inside the home, enterprise or any other environment and in general proximity of the MEC host via MEC API framework.

[CustomerPremiseEdge-03] When the MEC system supports the feature *CustomerPremiseEdge*, the MEC platform shall enable connectivity and communication among different MEC and non-MEC resources available inside the home, enterprise or any other environment and in general proximity of the MEC host via MEC API framework.

[CustomerPremiseEdge-04] When the MEC system supports the feature *CustomerPremiseEdge*, the MEC system shall support Precise Indoor Positioning service to allow authorized edge applications, to obtain precise indoor position of a requested object inside home, enterprise or any other environment.

[CustomerPremiseEdge-05] When the MEC system supports the feature *CustomerPremiseEdge*, the MEC system shall support 3D object modelling service and mapping to allow authorized edge applications inside home, enterprise or any other environment to obtain a 3D Map of the facility.

6.3.12 Feature *MECFederation*

NOTE: The following requirements are concluded from the study in ETSI GR MEC 035 [i.25].

[Federation-01] The MEC system may support the feature called *MECFederation*.

[Federation-02] When the MEC system supports the feature *MECFederation*, the MEC system shall be able to select the appropriate external MEC system within the MEC federation that it is a part of based on essential prerequisites such as security (e.g. authentication, authorization, system topology hiding and encryption), charging, identity management and monitoring aspects.

[Federation-03] When the MEC system supports the feature *MECFederation*, the MEC platform shall be able to discover the appropriate MEC platform (e.g. based on a list of their shared services, authorization and access policies) that belongs to an external MEC system within the MEC federation to enable MEC app-to-app communication or remote consumption of MEC services.

[Federation-04] When the MEC system supports the feature *MECFederation*, the MEC system shall be able to exchange the necessary information (e.g. including that relating to security (authentication/authorization, system topology hiding/encryption), charging, identity management and monitoring aspects) with an external MEC system within the MEC federation for the needs of MEC service consumption or for MEC app-to-app communication.

[Federation-05] When the MEC system supports the feature *MECFederation*, the MEC platform shall be able to exchange the necessary information (e.g. shared services, authorization and access policies) with another MEC platform belonging to the same or a different MEC system within the MEC federation for the needs of MEC service consumption or for MEC app-to-app communication.

[Federation-06] When the MEC system supports the feature *MECFederation*, the MEC system should be able to handle direct or indirect communication with other MEC systems within a MEC federation.

[Federation-07] When the MEC system supports the feature *MECFederation*, a MEC application instance of this MEC system shall be able to discover other MEC application instances of the same application in the same or a different MEC system, considering performance requirement for application clients. In addition, an MNO's MEC system shall support a suitable rule for the efficient handling of the traffic between a MEC application instance hosted in this MEC system and another MNO's access network where the application client is connected.

[Federation-08] When the MEC system supports the feature *MECFederation*, the MEC system shall support the on-boarding and/or instantiation of a MEC application in response to a request by another MEC system containing the required key performance indicator value (e.g. latency).

[Federation-09] When the MEC system supports the feature *MECFederation*, the MEC system shall support information exchange for enabling communication between multiple MEC application instances hosted on MEC systems of different MNOs. Each MEC application instance serves users connected to an MNO equipped with its respective MEC system (option 1). Also, the MEC system shall support MEC application instance to serve all application clients, including those connected to different MNOs (option 2). Especially in the case where there are three or more application clients in the group, the MEC system shall support both options at the same time.

[Federation-10] When the MEC system supports the feature *MECFederation*, the MEC platform shall be able to discover the appropriate MEC service. MEC service discovery in a MEC federation can be performed when a MEC system of the MEC federation wants to obtain MEC service availability. This process could be triggered in the case where the service consumer (e.g. a MEC application or a MEC platform of a MEC system the service discovery query originates from) needs the specific MEC service that is not available at the collocated MEC platform.

6.3.13 Feature *HTCservice*

[HTC service-01] The MEC system may support the feature called *HTCservice*.

[HTC service-02] When the MEC system supports the feature *HTCservice*, the MEC system should be able to instantiate applications accounting for information available to it regarding the underlying transport network with the aim of negating transmission delay.

6.3.14 Feature *MASService*

NOTE: The following requirements are concluded from the study in ETSI GR MEC 044 [i.40].

[MAS service-01] The MEC system may support the feature called *MASService*.

[MAS service-02] When the MEC system supports the feature *MASService*, the MEC system should allow the operator to create, modify, and delete a MEC Application Slice.

[MAS service -03] When the MEC system supports the feature *MASService*, the MEC system should allow the operator to define and update the set of services and capabilities supported in a MEC Application Slice.

[MAS service-04] When the MEC system supports the feature *MASService*, the MEC system should allow the operator to allocate the one or multiple appropriate MEC Application Slices to a tenant when required by the operator in response to a request by the enterprise customer.

[MAS service-05] When the MEC system supports the feature *MASService*, the MEC system should allow the operator to associate the appropriate MEC Application Slice(s) with a 5G network slice based on operator's policy.

[MAS service-06] When the MEC system supports the feature *MASService*, the MEC system should allow the operator to associate different instances of the same application to different MEC Application Slices.

[MAS service-07] When the MEC system supports the feature *MASService*, the MEC system should allow the operator to allocate the appropriate MEC Application Slice to a tenant based on the location of the related MEC hosts.

6.3.15 Feature *SMM*

NOTE: The following requirements are drawn from ETSI GR MEC 041 [i.31].

[SMM-01] The MEC system may support a feature called *SMM*.

[SMM-02] When the MEC system supports the feature *SMM*, the MEC system shall provide the necessary support to an SMM system.

[SMM-03] When the MEC system supports the feature *SMM*, the MEC system shall support the use of security profiles which describe the information MEC system entities can provide to an SMM system.

[SMM-04] When the MEC system supports the feature *SMM*, the MEC system shall support the use of security directives which describe what actions MEC system entities may take in response to an alert by an SMM system.

[SMM-05] When the MEC system supports the feature *SMM*, the MEC system shall have the capability to establish and maintain/manage security policies related to the configuration of its security profiles and security directives for an SMM system.

[SMM-06] When the MEC system supports the feature *SMM*, the MEC system shall provide functionality to allow secure collection, distribution, and storage of security monitoring related information.

[SMM-07] When the MEC system supports the feature *SMM*, the MEC system shall be able to respond to security directives it receives from the SMM system in response to an SMM alert.

6.3.16 Feature *CryptoAttestation*

NOTE: The following proposed requirements are drawn from ETSI GR MEC 041 [i.31].

[ATT-01] The MEC system may support a feature called *CryptoAttestation*.

[ATT-02] When the MEC system supports the feature *CryptoAttestation*, the MEC system shall support the functionality of a root of trust.

[ATT-03] When the MEC system supports the feature *CryptoAttestation*, the MEC system shall support the assessment of trustworthiness of MEC applications via cryptographic attestation.

6.3.17 Feature *APP-GW*

[AGW-01] The MEC system may support a feature called *APP-GW*.

[AGW-02] When the MEC system supports the feature *APP-GW*, the functionality shall be supported to control access from client applications to MEC applications hosted by the MEC system.

[AGW-03] When the MEC system supports the feature *APP-GW*, the functionality shall be supported to authenticate and authorize any external entity (client applications, network server) seeking access to MEC applications.

[AGW-04] When the MEC system supports the feature *APP-GW*, the capability shall be supported to, at any point, revoke access to MEC applications upon certain conditions.

[AGW-05] When the MEC system supports the feature *APP-GW*, MEC management may manage the APP-GW functionality.

7 Operation and management requirements

[OAM-01] It shall be possible to control the access of a MEC application to MEC services.

[OAM-02] The MEC platform management shall be able to collect and expose performance data regarding the virtualisation environment of the MEC host related to a specific MEC application.

[OAM-03] The MEC platform management shall be able to collect and expose performance data regarding the application performance related to a specific MEC application instance.

[OAM-04] The MEC system management shall be able to expose up to date performance data of the application to the authorized 3rd parties such as application developers and application providers.

[OAM-05] The MEC system management should support management of MEC host(s), including suspend, resume, configure, add and remove, by an authorized 3rd party.

8 Security, regulation and charging requirements

8.1 Security

[Security-01] The MEC system shall provide a secure environment for running services for the following actors: the user, the network operator, the third-party application provider, the application developer, the content provider, and the platform vendor.

[Security-02] The MEC platform shall only provide a MEC application with the information for which the application is authorized.

[Security-03] The MEC system shall be able to provide access control and rights management, e.g. based on roles.

8.2 Regulation

In order to meet Lawful Interception (LI) and Retained Data (RD) requirements, the following shall be satisfied, as identified by the NGMN MEC Security report [i.14]:

- Compliance with ETSI TS 101 331 [i.15] and ETSI TS 102 656 [i.16].
- Isolation of functions - see clause 1.2 in NGMN MEC Security report [i.14].
- Assurance checks on installation and update - see clause 1.4 in NGMN MEC Security report [i.14].
- Prevention of user plane attacks - see clause 1.5 in NGMN MEC Security report [i.14].
- For RD, assurance of data similar to that required for billing purposes - see clause 1.1 in NGMN MEC Security report [i.14].
- Storage and exchange of sensitive assets - see clauses 1.6 and 1.7 in NGMN MEC Security report [i.14].
- Specifically, there is a requirement to ensure target information is protected appropriately, potentially with a hardware root of trust, or utilizing a dynamic triggering model that minimizes the sensitive information available on the MEC element.

It is also important to meet requirements for the availability of data and identifiers, respecting national regulations. The following items shall be taken into account:

- It is a requirement that LI can take place for inbound roamers in the visited network without relying on the cooperation of the home network. Moreover, the identities of LI targets shall not be visible outside the country in which LI is taking place (so in the roaming case, they shall not be visible to the home network). These requirements need to be satisfied by any authentication solution - see clause 2.2 in NGMN MEC Security report [i.14].
- It is a requirement that unauthorized parties - including network employees not directly engaged in the application of LI in any network, and the interception targets themselves - cannot readily detect whether an individual is an interception target, e.g. because connections are visibly routed differently or have noticeably longer latency.
- There is a requirement that content is available in clear without operator-applied encryption, which is relevant to user data plane security - see clause 3.3 in NGMN MEC Security report [i.14].

[Lawful-01] The MEC system shall comply with regulatory requirements for lawful interception and retained data. These are referenced in ETSI TS 101 331 [i.15] and ETSI TS 102 656 [i.16].

8.3 Charging

[Charging-01] The MEC system shall allow the collection of charging-related information, log it in a secure way and make it available for further processing.

NOTE: Charging-related information can include traffic usage, application instantiation, access, usage duration, resource usage, etc.

Annex A (informative): Use cases

A.0 Labelling of related requirements

Related requirements in the following use cases are labelled in one of two ways to indicate their status within the present document and for the detailed specifications which are developed from it in ETSI ISG MEC.

The two categories are:

1) **Related requirements labelled with the suffix -xx**: these are only found in this informative annex and are not normative. They are included for information only. They have not been agreed for consideration in further specification work.

EXAMPLE 1: [Lifecycle-xx] It should be possible to support the instantiation of an application on multiple MEC systems across different networks.

2) **Related requirements labelled without the suffix -xx**: these have been agreed to be moved into the normative requirements clauses of the present document (clauses 5 to 8) and the label can be used to cross reference the use case which gave rise to the normative requirement. The full text of the requirement can be found in the relevant normative requirement clause higher up the present document.

EXAMPLE 2: [Lifecycle-01], [Services-03], [Connectivity-01], [Routing-01], [RNI-01].

A.1 Use case categorization

The presence of Multi-access Edge Computing at the edge of operators' networks enables a large number of new features to be developed in the mobile industry.

In order to develop the proper architecture and APIs for Multi-access Edge Computing, a number of use cases are described in order to derive a consistent set of requirements, listing the capabilities that the MEC system needs to support to enable the features mentioned above.

Three main categories have been identified for use cases. Requirements on the architecture are generally quite similar for use cases within a category, and quite different between the categories. However, all these categories need to be supported to allow Multi-access Edge Computing to enable a new era of services within the operators' networks.

The three categories are:

- **Consumer-oriented services:** these are innovative services that generally benefit directly the end-user, i.e. the user using the UE. This can include:
  - gaming;
  - remote desktop applications;
  - augmented and assisted reality;
  - cognitive assistance;
  - etc.
- **Operator and third party services:** these are innovative services that take advantage of computing and storage facilities close to the edge of the operator's network. These services are usually not directly benefiting the end-user, but can be operated in conjunction with third-party service companies:
  - active device location tracking;
  - big data;

- security, safety;
- enterprise services;
- etc.

- **Network performance and QoE improvements:** these services are generally aimed at improving performance of the network, either via application-specific or generic improvements. The user experience is generally improved, but these are not new services provided to the end-user:
  - content/DNS caching;
  - performance optimization;
  - video optimization;
  - etc.

The purpose of describing these use cases is to derive useful requirements. However, some requirements are defined by design constraints and do not originate from use cases.

A.2 Mobile video delivery optimization using throughput guidance for TCP and other transport protocols

A.2.1 Description

Category: Network performance and QoE improvements

Media delivery is nowadays usually done via HTTP streaming which in turn is based on the Transmission Control Protocol (TCP). The behaviour of TCP, which assumes that network congestion is the primary cause for packet loss and high delay, can lead to the inefficient use of a cellular network's resources and degrade application performance and user experience. The root cause for this inefficiency lies in the fact that TCP has difficulty adapting to rapidly varying network conditions. In cellular networks, the bandwidth available for a TCP flow can vary by an order of magnitude within a few seconds due to changes in the underlying radio channel conditions, caused by the movement of devices, as well as changes in system load when other devices enter and leave the network.

In this use case, a radio analytics MEC application, which uses services of Multi-access Edge Computing, provides a suitably equipped backend video server with a near real-time indication on the throughput estimated to be available at the radio downlink interface in the next time instant. The video server can use this information to assist TCP congestion control decisions. With this additional information, TCP does not need to overload the network when probing for available resources, nor does it need to rely on heuristics to reduce its sending rate after a congestion episode.

The throughput guidance is an application-specific figure which gives the video server a hint about the bitrate that can be expected to be available for its use during the upcoming time interval. Sprecher N et al. [i.7] and Flinck H. et al. [i.3] describe the concept and its integration with TCP in more detail. Note that [i.7] and [i.3] are individual submissions which are not endorsed by IETF. It is not foreseen to standardize or support standardization of throughput guidance as part of ETSI ISG MEC.

The above procedures on throughput guidance use up to date information about the radio conditions and current load. The procedures can be further optimized with additional IP flow specific information from the base station. Obtaining information about the currently available buffer size can be useful in order to adapt the TCP window size. This optimization can be used for a great variety of different TCP based services including web browsing and file downloading.

A.2.2 Use of MEC

A.2.2.1 Throughput Guidance radio analytics application

The Throughput Guidance radio analytics application computes throughput guidance based on the required radio network information it obtains from a MEC service running on the MEC host, and uses functionality of the platform to communicate this information to the video server.

When the Throughput Guidance radio analytics application has been started, it uses a service registry functionality to find the services that provide radio network information. Based on the relevant radio network information, the application computes throughput guidance values, using an application-specific algorithm.

These throughput guidance values are then transmitted in-band to the video server, by embedding the information into the uplink data packets that are sent to the video server by the video client on the user's device. These data packets are routed through the Throughput Guidance radio analytics application based on the traffic rules related to the application.

A.2.2.2 Transport layer congestion control assisted by MEC services

MEC is designed so that the software that runs on a MEC host can access information on the radio link and the user through well-defined, standardized interfaces to MEC services such as the RNI, the Location and the Bandwidth Management service. The TCP runtime support of an instantiated MEC application, which runs on the MEC host itself, can therefore access that information too. This information can be used to throttle the TCP traffic, by acting on its congestion control, in a finer and more refined way, so as to maximize the user experience, avoid congestion, and achieve a higher throughput.

For instance, including MEC service-originating information in TCP congestion control could allow:

1) discriminating losses due to congestion events from those due to transient conditions (e.g. temporary loss of line-of-sight, deep fading events);

2) anticipating the worsening of the radio conditions for a user, or handovers by consuming MEC services which expose radio network information together with location, bandwidth etc. information previously provided by other users under radio coverage;

3) adding a proactive approach to congestion mitigation on the radio link.

Transport Protocol Runtime (TPR) is defined as a generic term to indicate specifically TCPs, but also potentially other transport protocols. The use case consists in allowing TPRs at the server side (i.e. running on MEC hosts), to query MEC services, either:

i) periodically (e.g. by subscribing to RNI event notifications, especially if the application-related traffic is intensive); or

ii) triggered by specific events (e.g. a message timeout, a duplicated ACK, etc.);

in order to gain a better understanding of the capacity available to their connection, adapting their behaviour accordingly.

The use of MEC is clarified in Figure A.2.1.

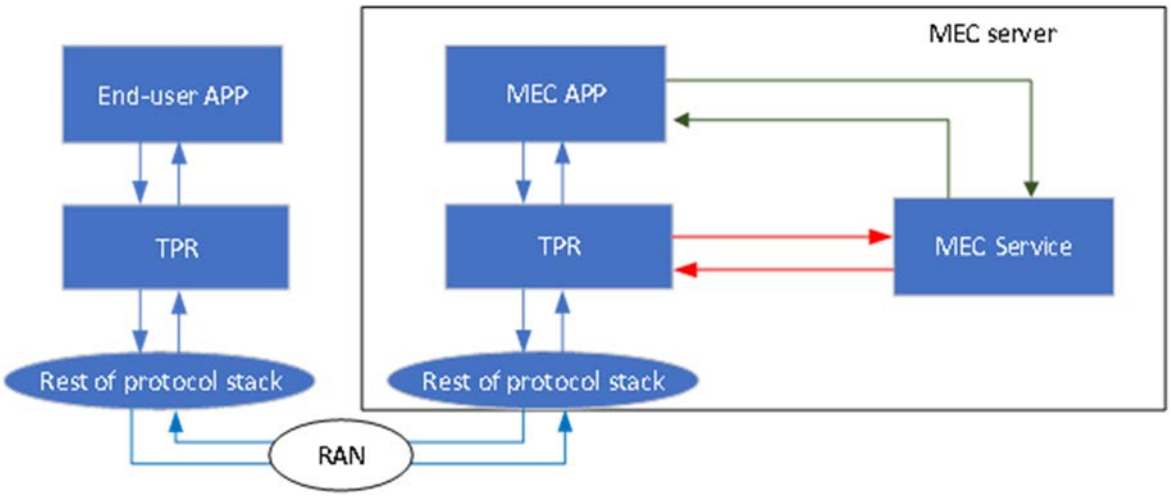


Figure A.2.1: Interactions between a server side TPR and a MEC service (red arrows), standard MEC interactions (black arrows), and data-path within the protocol stack (blue arrows)

The interaction between the (server/MEC host side) TPR and the MEC service can occur either following a request/response pattern (e.g. when triggered by specific events) or following a publish/subscribe pattern (e.g. for periodic updates). The choice of the interaction pattern may depend on the performance requirements posed by the end user app, e.g. regarding service reliability, end-to-end latency and, possibly, other metrics, together with the traffic rate (activity profile), as some end-user applications may require that output is provided at a frequent rate (e.g. high-resolution video segments), while others may only require scarce output rates (e.g. IoT/machine type communication devices).

For the sake of clarity, an example is provided with reference to a MEC application using TCP, sending data to a UE application in mobility in a cellular network.

With reference to Figure A.2.2, assume the UE enjoys a high Channel Quality Indicator (CQI), hence has a high throughput, and the TCP has a large Congestion Window (CW) accordingly. The downlink of the radio access is not congested. Suddenly, the UE enters an area with poor reception (e.g. a tunnel), where it will stay for some seconds. CQIs (in both the downlink and the uplink) drop down, hence traffic (including ACKs) is stalled for some seconds. Some TCP segments time out. Standard TCP would react by assuming congestion in the network. This has several consequences. First of all, the dropped segment(s) are retransmitted, using an exponentially increasing backoff window (vertical arrows in Figure A.2.2). This implies that, when the radio conditions allow the traffic to flow again, the TCP sender may still wait a non-negligible delay (in the order of seconds, or tens thereof, marked by "EB" in the figure) just because it is waiting for the backoff timer to expire before the next retransmission attempt. Moreover, when the UE exits the tunnel, and traffic transmission resumes, the connection will be in Slow Start (marked by "SS" in the figure), the CW will increase until half its former value, and then switch to Congestion Avoidance (CA). All things considered, a remarkable amount of time will elapse until the former throughput level is achieved again, without any compelling network reason (there is in fact no congestion).

A TCP runtime may instead exploit the consumption of instantiated MEC services to be (regularly) informed of:

a) the amount of occupied resources;

b) the user CQI;

c) possibly, UE location information (i.e. position and speed), which can be proved useful, e.g. when added to a geo-location/map service consumed by the UE (e.g. a vehicle), so as to identify low-signal location(s) and the expected visited time(s) by the UE.

The goal of the above MEC service consumption by the TPR entity is to infer that the problem is not due to congestion, but to temporarily poor channel quality. This way, when the mobile exits an area of low signal quality, the protocol (e.g. TCP) can react faster. First of all, it can detect that the radio conditions for the UE are good again, and therefore dispense with unnecessary waiting times due to the exponential backoff window. Moreover, it may assist in reverting the CW to its maximum (see the green line in Figure A.2.2) in a timely manner. This allows the end user to reach its target throughput sooner.

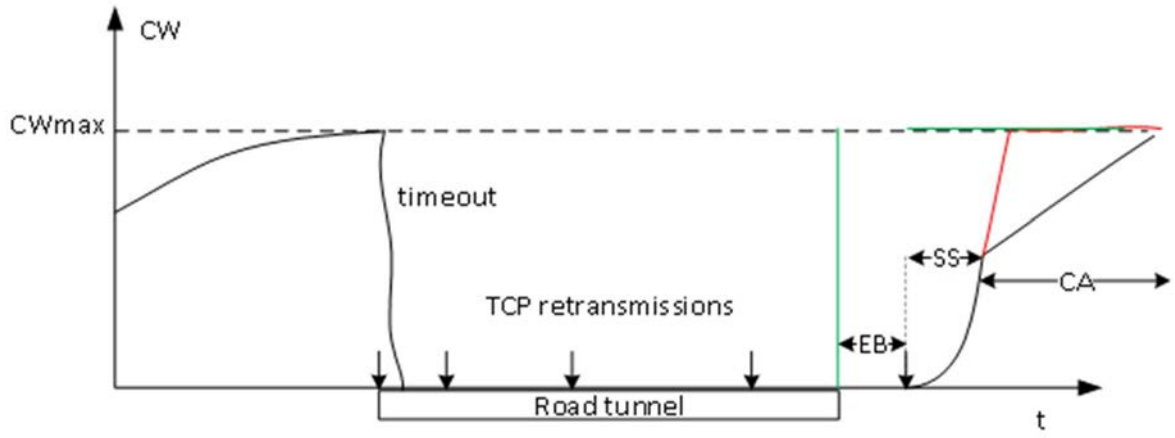


Figure A.2.2: CW scenario (qualitative)

For instance, when the timeout occurs, the TCP runtime can use information via consuming the following MEC services:

i) UE measurement report notifications from the RNI Service. This allows it to understand if the channel quality of the UE has dropped (e.g. if the CQI of the UE has dropped with respect to the previous measurements);

ii) the amount of allocated resource blocks in the serving cell from the Bandwidth Management Service. This allows it to understand the level of congestion of the radio frame (or, equivalently, the number of UEs competing for the same resource);

iii) possibly, the positioning information of the UE from the Location Service, to be compared against a layout of the area.

From (a subset of) the above information, the TCP runtime can clearly tell that there is no need to activate TCP congestion avoidance (e.g. reducing the CW, retransmitting the lost segment at intervals with increasing backoff, etc.). Rather, the sensible thing to do would be to halt the transmissions until the channel gets better (which can again be inferred using UE measurement reports from the RNI service) and then resume the transmissions at the same pace they had before (unless the radio frame has congested in the meantime).

A.2.3 Related requirements

- [Lifecycle-01]
- [Services-03], [Services-06], [Services-07], [Services-08]
- [Connectivity-01]
- [Routing-01], [Routing-02], [Routing-03], [Routing-04], [Routing-05], [Routing-06], [Routing-07], [Routing-08], [Routing-09], [Routing-10], [Routing-11]
- [RNI-01], [RNI-02], [RNI-03], [RNI-04], [RNI-05], [RNI-06], [RNI-07]

A.3 Local content caching at the mobile edge

A.3.1 Description

The fast paced development of smart phones, tablets and other handheld devices along with the success of global web based services has resulted in a significant increase in the use of mobile broadband services. The display and graphic processing technologies have evolved dramatically and high resolution video can be played on the go with handheld devices. Also, wide adoption of social media enables quick and efficient sharing of the topics, which start spreading in viral fashion.

Because of viral spreading, the content is many times consumed at about the same time in the same geographical area. This creates increased pressure to ensure sufficient bandwidth, and usually the capacity in the mobile broadband network becomes a bottleneck.

This problem can be alleviated with caching the content locally, which can provide savings both in the backhaul and in the transport and at the same time improve the QoE of the consumer. Content caching has the potential to reduce the backhaul capacity requirements up to 35 % [i.2].

A MEC application can store locally the most popular content that is consumed in the geographical area and once requested then provide the content from the local cache. In that case there is no need to transfer the content over core network and therefore significant savings in the backhaul capacity can be achieved. In addition to capacity savings, the download times to receive the content can be greatly reduced.

A.3.2 Use of MEC

Local content caching at the MEC host can be realized with an authorized application. The content cache application can store the content that has been identified frequently used or otherwise beneficial from the service point of view. As any application, the content cache application needs to be authorized by the platform. Content cache application can use information obtained from other applications to identify the content that could be cached. Also, other criteria to decide the content to be cached can be used.

Once the content cache application receives a request for content that is stored in its local cache, the application starts directing the requested content to the user equipment, which requested the content. This results in savings in the backhaul capacity as well as improvement in QoE as content can be transferred without the additional delays caused by the core network and public internet.

A.3.3 Related requirements

- [Lifecycle-01]
- [Services-03], [Services-06], [Services-07], [Services-08]
- [Routing-01], [Routing-02], [Routing-05], [Routing-06], [Routing-07], [Routing-09], [Routing-10], [Routing-11]
- [RNI-03]
- [Lawful-01]

A.4 Security, safety, data analytics

A.4.1 Description

Category: operator and third-party services

This use case groups a number of innovative services for the operator or third-party vendors based on the gathering of huge amounts of data (video, sensor information, etc.) from devices analysed through a certain amount of processing to extract meaningful information before being sent towards central servers.

Applications might run in a single location (i.e. on a single host), or be spread over a given area (e.g. campus coverage) or even in the whole network. In order to support the constraints of the operator or the third party requesting the service, the applications might have to be run on all requested locations (MEC hosts).

This use case describes an application running on a MEC host close to the radio network, that receives a very large amount of information from devices and sensors connected to the radio node(s)) associated with the MEC host. The application then processes the information and extracts the valuable metadata, which it sends to a central server. A subset of the data might be stored locally for a certain period for later cross-check verification.

A number of service scenarios can be enabled via this use case:

- Security, safety: monitoring of an area for specific events, such as abandoned luggage, authorized access (e.g. with face recognition), car park car monitoring, etc.
- Big data: massive sensor data pre-processing, smart city, etc.

Information can be completed for example with device location tracking (see use case "Active device location tracking" in clause A.7).

A.4.2 Use of MEC

A MEC application can either be running permanently on the MEC host, or based on demand from the operator, possibly in response to a request by a third-party. The application can be instantiated on a number of different hosts.

Once running, the application connects to a number of specific UEs (devices, sensors) connected to the radio node(s) associated with the MEC host. It then interacts with the UEs for collecting information.

The application might need to store a large amount of data locally. The data might need to survive the application instance termination.

The application performs the required (application-specific) analysis and provides the analysis results to an external entity. In order to do this, the application needs to be able to connect to external applications.

The application might need to get location information regarding UEs.

A.4.3 Related requirements

- [Lifecycle-03], [Lifecycle-04]
- [Connectivity-04]
- [Storage-01]
- [UserApps-01], [UserApps-02]
- [Location-01], [Location-02], [Location-03], [Location-04]

A.5 Augmented reality, assisted reality, virtual reality, cognitive assistance

A.5.1 Description

Category: consumer-oriented services

Augmented reality allows users to have additional information from their environment by performing an analysis of their surroundings, deriving the semantics of the scene, augment it with additional knowledge provided by databases, and feed it back to the user within a very short time. The device can be for example a smartphone or any wearable device with a camera and other sensors.

Assisted reality is similar to augmented reality, but its purpose is to actively inform the user of matter of interest to her/him (danger warning, ongoing conversations, etc.). This might be used for example to support people with disabilities (blind, deaf, of old age, etc.) to improve their interactions with their surroundings.

Virtual reality is similar to augmented reality, but its purpose is to render the entire field of view with a virtual environment either generated or based on recorded/transmitted environments. This might be used for example to support gaming implementations or remote viewing while using the most natural input device available.

Cognitive assistance takes the concept of augmented reality one step further, by providing personalized feedback to the user on activities the user might be performing (e.g. cooking, recreational activities, furniture assembling, etc.). The analysis of the scene and the advice to the user need to be provided within a very short time.

Low latency applications, such as games, AR, or VR applications, can choose to implement the rendering pipeline either in a MEC application on the MEC host or directly on the client device (such as UE).

These applications can choose to offload part of the device computational load to a MEC application running on a MEC host. This can include for example simulation of physics, artificial intelligence and other components.

For all these cases, the interaction between the user and the application needs to be personalized, and the continuity of the service needs to be maintained as the user moves around.

Innovative applications are developed at a rapid pace and will evolve and be replaced in a very dynamic environment. In order to support and stimulate rapid innovation, it is necessary that new applications and new versions of applications can be provisioned dynamically, up to the point where the user requests the application to be run. If a specific application has not yet been on-boarded and the MEC system is able to fetch the application in a defined location, it needs to be able to do so.

Users are not necessarily going to be permanently using the mobile network environment for running their augmented reality, assisted reality and cognitive assistance applications. In some cases (e.g. in their home or at work), they might access their applications located in a cloud environment over other radio accesses, such as local Wi-Fi®. However, when moving away from their static environment or going back to it, they might want to continue using the application over the mobile network environment. Applications would then need to be relocated between the external cloud environment and the MEC system dynamically.

A.5.2 Use of MEC

In response to a request from the user, the UE needs to be connected to an instance of a specific application, running on an appropriate MEC host fulfilling the latency requirements of the application. A new instance of the application needs to be started if it is not yet running.

The application might have a set of requirements (e.g. latency, compute resources, storage resources, etc.) that needs to be fulfilled by the host. The MEC system needs to select a MEC host that fulfils all the requirements.

When the UE moves to an area which is not associated with the host on which the application is running, in order to fulfil the application requirements and depending on the application, either:

- the instance of the application might need to move to another appropriate host; or
- the application instance might need to transfer state information regarding the UE to another instance of the same application running on an appropriate host. To support this, the MEC system has to provide connectivity between these instances.

When all the users connected to a specific instance of an application have disconnected, the application instance can be terminated.

When a UE requests the MEC system to instantiate an application that is not already on-boarded in the system and when this is possible, the system needs to on-board the application dynamically.

The MEC system needs to be able to relocate applications from an external cloud environment to a MEC host fulfilling the requirements of the applications, and from a host to an external cloud environment, based on a request from the UE.

To support application-based distributed computation on UEs, an application can identify devices capable of supporting computation assistance and their connectivity capabilities. The application is able to determine, based on these devices' location and additional connectivity specific information, their ability to support distributed computation requests. Upon change of conditions, the application will be able to recover the connection.

A.5.3 Related requirements

- [Mobility-01], [Mobility-02], [Mobility-03]
- [Connectivity-02]

- [UserApps-01], [UserApps-03], [UserApps-04], [UserApps-05], [UserApps-06], [UserApps-07]
- [SmartReloc-01], [SmartReloc-05], [SmartReloc-06]

A.6 Gaming and low latency cloud applications

A.6.1 Description

Category: Consumer-oriented services

Games are very popular application on computers, tablets and smartphones. However, many games played on computers connected via LAN and/or broadband Internet connection require low latency values typically not available today for UEs, as the servers are usually reachable via the Internet, located beyond the RAN and Core Network.

By locating game server applications closer to the radio, a new kind of low latency-based games will become available to UE users. Of course, the use is not restricted to games, and can benefit any kind of applications requiring low latency, for example, using a "remote desktop" protocol to access cloud virtual machines, e.g. in the case the compute capacity is too high to be run efficiently on a tablet. In this case, for the user experience to be satisfactory, the latency between an action done by the user to the feedback received by the device needs to be very short.

Both general applications and games might be for either single or multiple users (e.g. equivalent to LAN gaming or shared whiteboard).

The user would start an application locally on the device that requests the connection to an application (remote desktop application, game server, etc.). For multi-user applications, the other users, via their local application, will request to access to the same instance of the game or application server. Latency constraints and other applications requirements (e.g. computing capacity, storage, etc.) will be defined for the applications. Latency constraints might include for example maximum acceptable latency, or maximum latency difference between users (e.g. in games, all users need to have a relatively similar latency to avoid unfair behaviour).

While the application/game is running, one or more users might move around, and be connected to a different radio node (handover). As this is happening, the service still needs to be provided (the connectivity between the UE and the application needs to be maintained).

As the user moves away from the original location, the latency between the UE and the application is likely to lengthen. In order to maintain the latency requirements (e.g. maximum value, fairness), the application might have to be relocated to another server.

Low latency applications, such as games or interactive applications, can choose to implement the rendering pipeline either in a MEC application running on the MEC host or directly on the client device (such as UE).

These applications can choose to offload part of the device computational load to a MEC application running on a MEC host. This can include for example simulation of physics, artificial intelligence and other components.

When all the users disconnect from the application, the application might be terminated or frozen.

Innovative applications are developed at a rapid pace and will evolve and be replaced in a very dynamic environment. In order to support and stimulate rapid innovation, it is necessary that new applications and new versions of applications can be provisioned dynamically, up to the point where the user requests the application to be run. If a specific application has not yet been on-boarded and the MEC system is able to fetch the application in a defined location, it needs to be able to do so.

Users are not necessarily going to be permanently using the mobile network environment for running their gaming or low latency cloud applications. In some cases (e.g. in their home or at work), they might access their applications located in a cloud environment over other radio accesses, such as local Wi-Fi®. However, when moving away from their static environment or going back to it, they might want to continue using the application over the mobile network environment. Applications would then need to be relocated between the external cloud environment and the MEC system dynamically.

A.6.2 Use of MEC

In response to a request from the user, a new instance of a specific application needs to be started on an appropriate MEC host fulfilling the latency and resources requirements of the application.

In response to requests from other users, connectivity needs to be established between their UEs and a specific instance of an already running application.

The application might have a set of requirements (e.g. latency, compute resources, storage resources, etc.) that needs to be fulfilled by the MEC host. The MEC system needs to select a MEC host that fulfils all the requirements.

When a UE moves to another radio node associated with the same host, connectivity needs to be maintained between the UE and the application.

When a UE is connected to a radio node not associated with the same MEC host where the application is running (e.g. after a UE moves between radio nodes), connectivity needs to be maintained between the UE and the application. In order to maintain the latency requirements, the MEC management might need to relocate the application to another host, while connectivity between the application and the UE(s) is maintained.

NOTE: This functionality is required for applications such as the ones described by this use case. This functionality is not required for some of the use cases.

When all the users connected to a specific instance of an application have disconnected, the application instance can be terminated.

When a UE requests the MEC system to instantiate an application that is not already on-boarded in the system and when this is possible, the system needs to on-board the application dynamically.

The MEC system needs to be able to relocate applications from an external cloud environment to a MEC host fulfilling the requirements of the applications, and from a host to an external cloud environment, based on a request from the UE.

To support application-based distributed computation on UEs, an application can identify devices capable of supporting computation assistance and their connectivity capabilities. The application is able to determine, based on these devices' location and additional connectivity specific information, their ability to support distributed computation requests. Upon change of conditions, the application will be able to recover the connection.

A.6.3 Related requirements

- [Mobility-01], [Mobility-02], [Mobility-03]
- [UserApps-01], [UserApps-03], [UserApps-05], [UserApps-06], [UserApps-07]
- [SmartReloc-01], [SmartReloc-05], [SmartReloc-06]

A.7 Active device location tracking

A.7.1 Description

Category: operator and third-party services

This use case enables real-time, network measurement based tracking of active (GPS independent and network determined) terminal equipment using 'best-in-class' geo-location algorithms.

This provides an efficient and scalable solution with local measurement processing and event based triggers. It enables location based services for enterprises and consumers (e.g. on opt-in basis), for example in venues, retail locations and traditional coverage areas where GPS coverage is not available.

Services can include mobile advertising, 'Smart City', footfall analysis, campus management, crowd management, personnel management, etc.

A.7.2 Use of MEC

The application can either be running permanently on the MEC host, or based on demand from the operator, possibly in response to a request from a third-party.

Once running, the application collects location-related information from the UEs connected to the radio node(s) which the MEC host is associated with. Depending on the application, specific UEs, specific categories of UEs, or all UEs need to be tracked, possibly anonymously (based on authorization).

The application performs the required (application-specific) analysis and provides the analysis results to an external entity. In order to do this, the MEC application needs to be able to connect to external applications.

A.7.3 Related requirements

- [Lifecycle-03], [Lifecycle-04]
- [Connectivity-04]
- [UserApps-01], [UserApps-02]
- [Location-01], [Location-02], [Location-03], [Location-04]

A.8 Application portability

A.8.1 Description

An application provider develops an application. This application can be instantiated on MEC hosts from different vendors without any modification.

A.8.2 Use of MEC

One of the main targets of ETSI ISG MEC is to ensure the portability of MEC applications across MEC systems from different vendors. Portability in this context means that the application needs no platform specific modifications, and can be installed on every platform.

In addition to this, the MEC system has to verify the authenticity and integrity of the application.

The MEC system needs to be able to control the access of applications to MEC services.

A.8.3 Related requirements

- [AppEnvironment-01], [AppEnvironment-02], [AppEnvironment-03]
- [OAM-01]

A.9 SLA management

A.9.1 Description

An application provider develops a MEC application. This application is instantiated on a MEC host. The application has certain performance requirements regarding the virtualisation environment of the host and the allocated virtual resources. These requirements are typically agreed and specified in Service Level Agreements (SLAs).

In order to verify how well the SLAs are met, performance data regarding the virtualisation environment of the MEC host has to be collected and made available for further processing.

An authorized application developer and application provider should have means to monitor on-line the performance of the specific MEC application in the MEC system. The specific parameters exposed for monitoring are agreed and specified between the MEC system owner and the application developer/provider in the SLA. The specific application performance data to be collected could be a topic for future standardization.

A.9.2 Related requirements

- [OAM-02], [OAM-03], [OAM-04]

A.10 MEC edge video orchestration

A.10.1 Description

Multi-access Edge Computing is expected to provide excellent performance and quality while at the same time providing savings in the backhaul capacity by being able to provide content as close to end user as possible. The biggest gains can be likely achieved in a scenario with a dense population of consumers in small geographical area.

The most popular content over mobile broadband is video, which already generates over 55 % of the total traffic volume. This is greatly due to fast paced enhancements on processing and graphics capabilities of handheld devices together with the top notch services offered by the service and content providers.

Proposed use case of edge video orchestration suggests a scenario where visual content can be produced and consumed at the same location close to consumers in a densely populated and clearly limited area. Such a case could be a sports event or concert where a remarkable number of consumers are using their handheld devices to access user select tailored content. The overall video experience is combined from multiple sources including locally produced video and additional information as well as master video from central production server. The user is given an opportunity to select tailored views from set of local video sources.

The MEC system is ideally suited for proposed edge video orchestration due to specific characteristics of the use case. The service production and consumption take both place and strictly limited area, which also gives the best chances to control the service quality and performance.

A.10.2 Use of MEC

The edge video orchestration application runs on top of a MEC host and uses the MEC services. The platform needs to provide mechanisms to connect the UEs used for local production devices (e.g. video cameras and sensors) to the video orchestration MEC application as well as the UEs of the consumers that use the video orchestration service.

The MEC platform needs to provide mechanisms to route the data traffic from the local video cameras and sensors to the video orchestration application. When UEs used for local data sources (e.g. cameras and sensors) send their data, the platform provides its services to route the data to the edge video orchestration application.

Requests from UEs to receive video are directed to the edge video orchestration application.

When a consumer selects the video stream, the edge video orchestration application sends the selected content to the user. The MEC platform is responsible of routing the data to the UE of the user, according to configurable rules.

A.10.3 Related requirements

- [Routing-01], [Routing-02], [Routing-03], [Routing-04], [Routing-05], [Routing-06], [Routing-10], [Routing-11]

A.11 Mobile backhaul optimization

A.11.1 Description

Category: Network performance and QoE improvements

Today there is no real coordination between the radio network and the backhaul network. When there is capacity degradation in the backhaul, the radio network is not informed about it, and vice versa, when radio network needs less capacity the backhaul is not aware of it too.

It is intended in this use case to combine information from the radio network together with information from the backhaul network to optimize the resources in the backhaul (in the future optimizing resources in the radio network can also be considered).

The analytic application uses services of Multi-access Edge Computing (like traffic monitoring, performance monitoring) to provide real time information about the traffic requirements of the radio network (taking into account the radio access scheduling, the application and backhaul condition).

The analytics application gets real time information from a monitoring application within the backhaul, and sends the traffic requirement to an optimization application within the backhaul network.

The optimization application can optimize the backhaul is several ways:

- shape the traffic per application at a remote aggregation point;
- reroute some of the traffic;
- increase/reduce power of microwave link based on actual capacity need.

A.11.2 Use of MEC

The traffic analytics application computes throughput based on the required radio network information it obtains from MEC service available via the MEC platform and the backhaul information it obtains from the monitoring application. The traffic analytics can use the traffic monitoring service to get the user plane traffic and identify the applications that the user uses. The traffic analytics application communicates this information to the optimization application within the backhaul using an interface which is out of scope of ETSI ISG MEC.

A.11.3 Related requirements

- [Connectivity-04]
- [Routing-05]
- [RNI-04], [RNI-05], [RNI-06], [RNI-07], [RNI-10], [RNI-11]

A.12 Direct interaction with MEC application

A.12.1 Description

MEC applications might require a flow/session that is originally intended to run between the UE and some application running on the Internet to be actually setup directly between the UE and that same application now running on the MEC host. This requires routing traffic between the UEs to/from each of these applications in the MEC host.

Traffic routing as described above requires two distinct functionalities:

- At application startup: IP connection setup (i.e. IP socket setup) with the MEC application instead of the application server in the cloud.

- While the IP session is active: termination and decapsulation of the GTP tunnel layer providing the application with "standard" IP traffic.

In practice, satisfying the above two requirements means that at least the following functionality needs to be supported:

- DNS re-direction: for many common applications, DNS is the method by which the application server IP address is discovered and therefore DNS re-direction is the way to satisfy the required re-direction at application startup.
- GTP tunnel termination: since GTP is the protocol used by 3GPP to encapsulate bearers, satisfying the required operation while the IP session is active requires the support of GTP tunnel termination, including encapsulation and decapsulation of traffic to/from the UE.

This can include:

- A DNS cache + server functionality which can be preconfigured with DNS resolutions including the IP addresses of applications that are running on the MEC host.
- A monitoring capability to analyse GTP tunnelled packets and identify the destination IP address inside the IP packets.
- Capability to strip the GTP layer from the IP packets, and route these packets as IP packets to the requested application.
- Capability to receive IP packets from other applications, re-encapsulation these IP packets into the GTP tunnel and send them out towards the UE.

A.12.2 Use of MEC

The UE application wants to interact with an application running on a MEC host (the UE application itself might be unaware that it is interacting with an application running in a Multi-access Edge Computing environment).

In order to do this, it first sends a DNS request for an FQDN to get the IP address of the application.

As part of the traffic handling functionality, the MEC host retrieves the IP packet from the user plane traffic, possibly after decapsulating the GTP bearer if necessary. The DNS traffic (i.e. port 53) is routed to the DNS server/proxy running on the host.

If the DNS server/proxy can resolve the FQDN locally, either because the FQDN was preconfigured or because it is cached from a previous request and is still valid, then it replies to the request. Otherwise, it might receive the response from the core network to which it could have forwarded the query. It then sends back the DNS response it receives from its own request or from the DNS server in the network.

The traffic handling functionality then sends the IP packet containing the answer back to the UE, possibly after encapsulating it in the GTP bearer if necessary.

The UE then interacts with the MEC application running on the MEC host using the IP address provided by the DNS server/proxy.

The traffic handling functionality retrieves IP packets with the destination IP address of the MEC application, possibly after decapsulating the GTP bearers if necessary.

The traffic from the application is then sent back to the UE, possibly after encapsulating it in the GTP bearer if necessary.

A.12.3 Related requirements

- [DNS-01], [DNS-02]
- [Routing-13], [Routing-14]

A.13 Traffic deduplication

A.13.1 Description

Category: Network performance and QoE improvements

The traffic in the network today contains a lot of content that arises from content providers like video content providers, etc. Studies show that a lot of the traffic repeats itself since many users consume same traffic, for example many users are upgrading apps on their smart phone, or looking at the same video clip.

Traffic deduplication is a technique made of two functions, compressor and decompressor [i.5]. The compressor and decompressor identify repeating patterns in the traffic, which are stored close to the user at the decompressor. The compressor identify the pattern as well and instead of sending them, it sends just indexes that identify the specific pattern stored at the decompressor [i.6]. This technique reduces significantly the amount of traffic sent for a repeating pattern, and overall studies show reduction of more than 30 % of the overall traffic in the segment between the compressor and decompressor. In this use case the decompressor application uses services of Multi-access Edge Computing like traffic routing to perform in real time the detection of the repeating pattern, storing them and reconstruct the original content. It is important to note that if there are other applications on the platform that use the same traffic flows, this application needs to be performed first to allow the other applications to see the original traffic (and not the indexes).

A.13.2 Use of MEC

When De-Compressor application starts, it interacts with the MEC platform to enable traffic routing.

The De-Compressor application starts a communication channel with the Compressor application and coordinates with it the detection of repeated pattern and their storage.

The compression application is responsible for detecting repeated patterns and sends just indexes of those pattern to the de-compressor. The De-Compressor application is responsible to regenerate the original traffic from the received indexes.

A.13.3 Related requirements

- [Connectivity-04]
- [Routing-03], [Routing-04], [Routing-09]

A.14 Vehicle-to-infrastructure communication

A.14.1 Description

Category: Operator and third party services

Communication of vehicles and roadside-sensors is intended to increase the safety, efficiency, and convenience of the transportation system, by the exchange of critical safety and operational data.

The roadside application incorporates algorithms that use data received from vehicles and roadside sensors to recognize high-risk situations in advance, and sends alerts and warnings to the vehicles in the area. The drivers of the vehicles can immediately react, for example by avoiding the lane hazard, slowing down or changing the route.

3GPP technologies (e.g. 4G and 5G) can significantly accelerate the deployment of car-to-roadside communications. 3GPP radio technologies (e.g. LTE, NR) can provide "beyond the horizon" visibility in the critical 2 km range. Cars can leverage their increasingly inbuilt 3GPPconnectivity.

Vehicle-to-Infrastructure communication has tight latency requirements, below 10 ms in some use cases. Messages, such as hazard warnings (e.g. accident, danger on lane, etc.), could be distributed in real time over 3GPP technologies, eliminating the need to build a countrywide, Digital Short-Range Communications (DSRC) network. In deployments where DSRC exists, the 3GPP technologies would be able to complement it.

Multi-access Edge Computing can be used to extend the connected car cloud into the highly distributed mobile network environment. Applications can be deployed on MEC hosts to provide the roadside functionality. The roadside applications can receive local messages directly from the applications in the vehicles and the roadside sensors, analyse them and then propagate (with extremely low latency) hazard warnings and other latency-sensitive messages to other cars in the area. This enables a nearby car to receive data in a matter of milliseconds, allowing the driver to immediately switch lanes, slow down or change his route.

The roadside application can inform other applicable MEC applications running on other MEC hosts about the event(s), and in so doing, enable the propagation of hazard warnings to cars that are close to the affected area.

The roadside application can send local information to the applications at the connected car cloud for further processing.

A.14.2 Use of MEC

The roadside MEC application uses functionality of the MEC platform to receive data from client applications in the vehicles or the roadside sensor that can be used to recognize high-risk situations in advance. It uses the computing resources to analyse the data and then utilizes the functionality of the platform to propagate (with extremely low latency) hazard warnings and other latency-sensitive messages to other cars. As an example, a roadside MEC application monitors a road segment for identifying jaywalking pedestrians. The roadside MEC application can exploit data from roadside sensors (e.g. cameras and/or LiDARs) to identify pedestrians and to trigger an alert to be sent to the vehicles in the area.

When the roadside MEC application starts, it uses the MEC platform to enable traffic routing. Based on the data received from the vehicles, the roadside application uses application-specific algorithms to recognize high-risk situations in advance. The application generates warnings messages and sends them to nearby cars with extremely low latency.

The roadside MEC application performs the required (application-specific) analysis and provides the analysis results to an external entity (either on an adjacent MEC host or at a connected car cloud). In order to do this, the application needs to be able to connect to external applications.

A.14.3 Related requirements

- [Services-03], [Services-06], [Services-07], [Services-08]
- [Connectivity-03], [Connectivty-04]
- [Routing-01], [Routing-02], [Routing-03], [Routing-04], [Routing-05], [Routing-06], [Routing-10], [Routing-11], [Routing-13]
- [Lawful-01]
- [V2X-08], [V2X-09]

A.15 Location-based service recommendation

A.15.1 Description

Category: User-oriented services

Users' activities usually largely depend on where users are. For instance, users at shopping mall probably buy some goods and users at a museum would be interested in a specific art work. In that sense, if some user services related to users' context are to be recommended, users' location can be of great significance. Location information exactly tells that users are in certain place at certain moment.

Location based service recommendation allows a variety of services which are tightly coupled with a specific place such as shopping mall, museum, etc. to be recommended to users at the right time. In order to improve QoE with respect to usefulness of recommended user services, users' behaviour log and preference can be collected in users' mobile terminal, and then be delivered to the location based service recommendation application, and also data from sensors around users can be delivered to service recommendation application.

Location can be detected as users are connected to a specific cell. Attachment information of user terminals to a specific radio node can be used to get location information of users especially when users are connected to an indoor small cell. In that sense, location information would represent the proximity to a certain place.

The user service recommendation application can make use of machine learning and/or inference engine to determine proper services for users at the moment. The service recommendation can be done in cooperation with big data analysis which is fulfilled by backend server in internet. Services can be represented in a variety of form. For instance, at a department store, coupons can be recommended or some of goods can be recommended. On the other hand, at the museum, video clips can be recommended for a specific art piece.

A.15.2 Use of MEC

The application can run on an appropriate MEC host and use some of the MEC services provided via the MEC platform that fulfils the requirements of the application in order to respond the user's request. These can include requirements on latency, computing resources, response time. The MEC system needs to select a host fulfilling all the requirements. A new instance of the application might be created by the first request of the user, or can be created prior to any request from users.

The user's request can be routed to an appropriate MEC application, and also the MEC application might be able to send request to a specific user through the MEC host. The application might be connected to the external servers through the MEC host.

A.15.3 Related requirements

- [Location-05]

A.16 Bandwidth allocation manager for applications

A.16.1 Description

Different MEC applications running in parallel on the same MEC host might require specific static/dynamic up/down bandwidth resources. In some cases, different sessions running in parallel in the same application can each have specific bandwidth requirements. As all these applications and application sessions are competing over the same shared bandwidth resources, it is suggested that a central bandwidth resource allocator exists on the MEC host, preferably on the MEC platform. The proposed function can include the following:

- an API enabling all registered applications to statically and/or dynamically register for specific bandwidth allocation;

- an interface with the radio network information service to receive network conditions and available bandwidth;
- the capability to calculate optimal bandwidth allocation per session/application according to available and required bandwidths;
- the capability to manage the allocated bandwidth to each of the sessions/applications according to the calculations.

A.16.2 Use of MEC

The MEC host can support applications running in parallel. These applications will be running over the same hardware and network resources, with each having its own requirements.

In order to assure that all the applications/sessions are receiving the bandwidth resources they require in an optimal way, the MEC platform can include functionality that will collect required bandwidth resources and available bandwidth resources and allocate bandwidth to each session/application according to static/dynamic requirements.

A.16.3 Related requirements

- [Bandwidth-01], [Bandwidth-02], [Bandwidth-03]

A.17 MEC platform consuming information from operator trusted MEC application

A.17.1 Description

Category: operator and third-party services

This use case allows an application to target a specific subscriber or a group of subscribers. For example:

- allowing an anonymous group of flat rate billing subscribers access content locally from the MEC host;
- targeted advertising for a certain group of users within the mobile network;
- providing content to a specific group of users that might be in the same club, association, public service group, etc.;
- providing enterprise services to company employees.

The ability to target a particular subscriber or a group of subscribers from the MEC platform can add significant value to the Multi-access Edge Computing offering. In order to do this within the network, the MEC host needs to be capable of routing traffic to the MEC application based on UE IP address rather than destination IP address. The mapping of UE IP address to subscriber is not available on the MEC platform. This information needs to be provided by an external source (e.g. in the core network). In this use case an operator trusted MEC application (see annex B) receives this information from an external source and provides this information to the platform.

Figure A.17.1 illustrates an example use case for this concept.

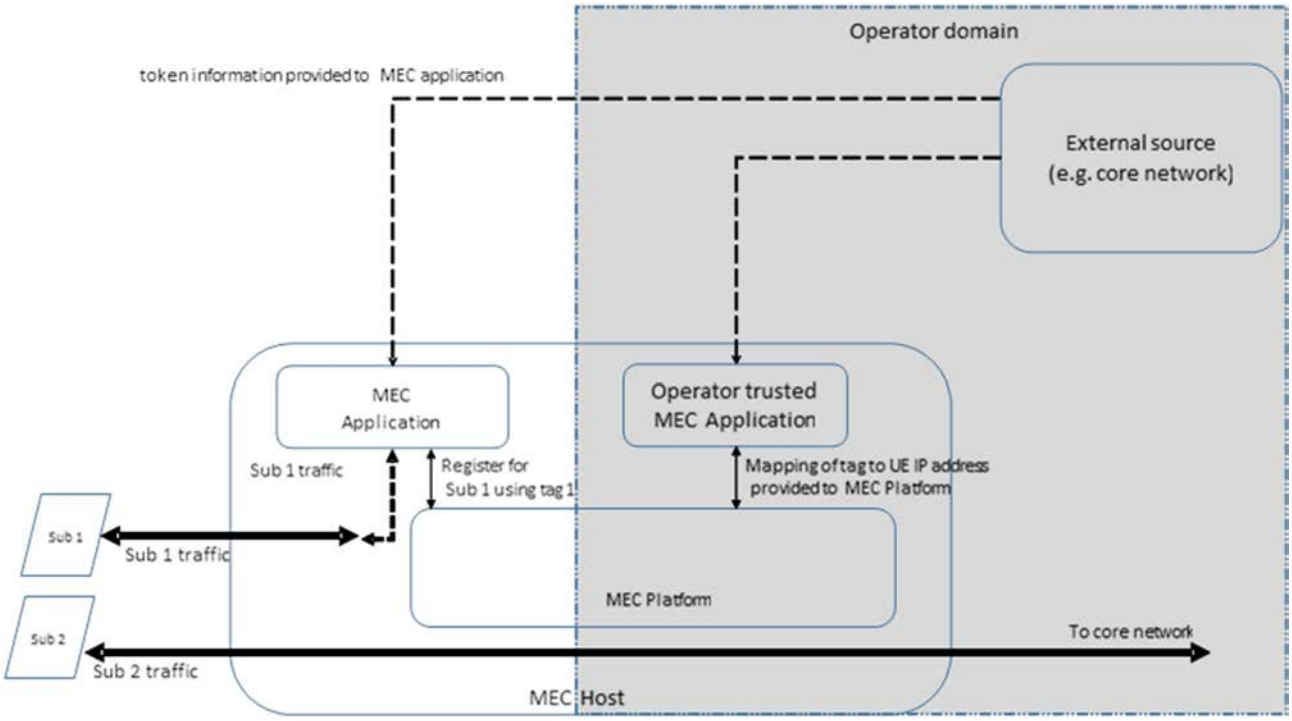


Figure A.17.1: Subscriber based routing

After being provided the subscriber tag information, the application registers to receive traffic associated with a subscriber, in this example Subscriber 1. The MEC platform registers this information. On receiving information associated with Subscriber 1, the platform triggers the routing of all application traffic to the application as illustrated above. The traffic reference (UE IP address) can change periodically, which will be updated via the operator trusted application, but the reference provided to the application will remain the same.

A.17.2 Use of MEC

The MEC platform will support receiving information from an authorized application and using this information to provide a service to other applications.

A.17.3 Related requirements

- [Services-02]

A.18 Video caching, compression and analytics service chaining

A.18.1 Description

Consider the use case where traffic which is sent from the content caching application to a UE is steered first through the video compression application and then through the video analytics application.

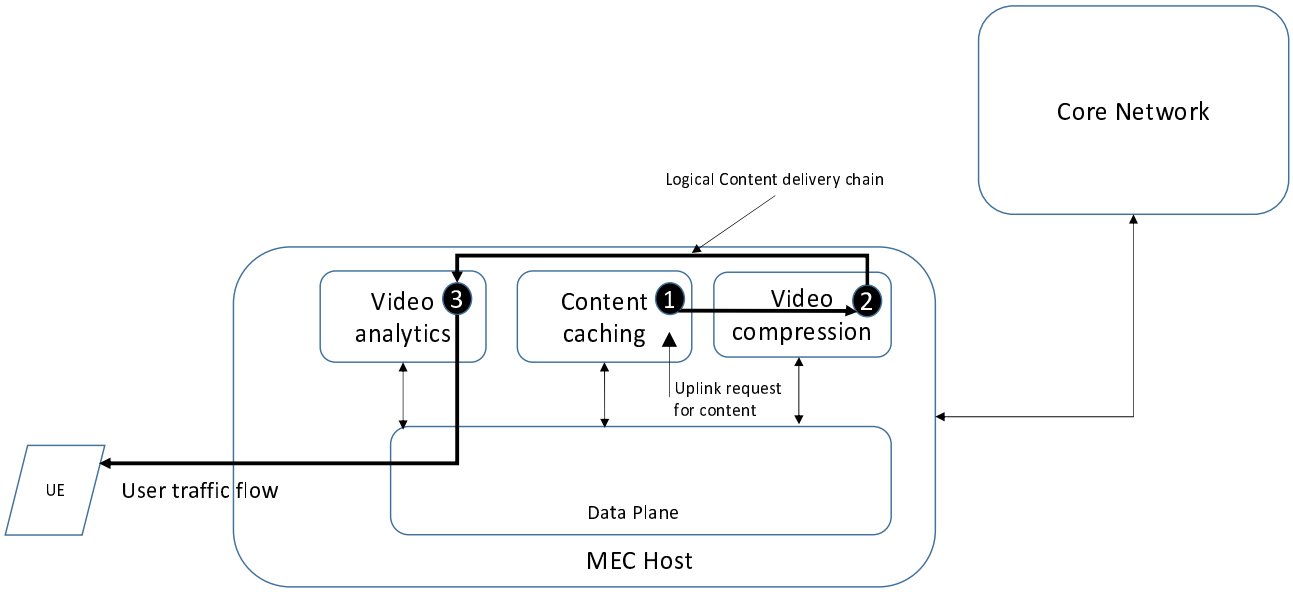


Figure A.18.1: Video content delivery

When the uplink request arrives at the MEC platform, the content request is routed to the Content caching application in order to retrieve the content.

Once the content is identified, the user traffic needs to be passed to the Video compression and Video analytics application before it be delivered to the end user.

The platform needs to support this scenario, whereby it will classify the traffic and then steer the traffic through multiple applications.

A.18.2 Use of MEC

The MEC host is capable of hosting multiple applications.

Based on policy, classified traffic needs to be steered through multiple applications in a particular sequence.

A.18.3 Related requirements

- [Routing-09]

A.19 Radio access bearer monitoring

A.19.1 Description

Category: Network performance improvements

A UE can have multiple dedicated bearers in addition to the default bearer. A dedicated bearer is used to tunnel one or more specific traffic types (e.g. VoLTE, video, etc.). One of the dedicated bearers can be used for example to tunnel traffic that requires low latency and is assigned with a QCI value of 1. Another bearer can be used for high throughput traffic and is assigned with a QCI value of 9. The QCI value is used within the radio access network to control packet forwarding treatment.

Having the ability to route traffic based on bearers' information allows monitoring services on a particular bearer.

An application running on a MEC host can perform monitoring of traffic on specific bearers or bearers with specific QCI values.

A.19.2 Use of MEC

User plane traffic which is tunnelled through a specific bearer and which can also be assigned with a particular QCI value is routed to a MEC application for monitoring services.

NOTE: This refers to the application level traffic rather than the transport level traffic.

A.19.3 Related requirements

- [Routing-12]

A.20 MEC host deployment in dense-network environment

A.20.1 Description

Category: Network Performance and QoE improvements

This use case considers how to maintain the low latency requirement for gaming and new user experience under deployments intended to mitigate wireless network congestion.

Due to the nature of the wireless access network, the capacity of radio fluctuates based on numbers of users and types of applications. Multi-access Edge Computing can participate to the definition of solutions for wireless network capacity issues. Inter-UE communication such as 'Device to Device Communication' can be used by applications deployed on UEs to help resolve specific situations of network congestion by limiting network traffic in addition to fulfilling low-latency requirement.

Another deployment alternative is the use of Relay Nodes. In that case, the MEC host can be deployed on Relay Nodes. The MEC system can manage these hosts on Relay Nodes similarly to other MEC hosts, allowing the system to have further options to fulfil the set of application requirements (e.g. latency, compute resources, storage resources, throughput, etc.).

A.20.2 Use of MEC

In order to identify wireless network congestion, a MEC service available via the MEC platform provides radio network information to a dedicated application. When network congestion is identified, the MEC application can communicate with counterpart applications running on devices, to request them to activate direct device-to-device communication network capabilities through application-specific means.

If radio nodes such as Relay Nodes are deployed, a MEC application can collect radio network information including radio node location information and perform certain application-specific tasks to distribute optimally the processing of applications at the different locations.

Once the MEC application receives radio network information indicating that network congestion has been mitigated, it can deactivate application-specific support through direct device-to-device communication. Interaction resumes between UE applications and the corresponding MEC applications running on MEC hosts associated with their respective radio nodes.

The radio network information enables the selection of appropriate MEC hosts in order to fulfil a set of requirements (e.g. latency, compute resources, storage resources, throughput, etc.) of MEC applications.

A.20.3 Related requirements

- [Location-06]

A.21 Radio network information generation in aggregation point

A.21.1 Description

As different MEC applications might require radio network information to enable them to run in a more optimal way, a radio network information service is defined. In the scenario in which the MEC host is located at the radio node site it is understandable this information can be received by the MEC service from the radio node. When placing the MEC host in an aggregation point (and RNC) or in a Core Network gateway in which the radio network information is not available locally, it is more complicated to extract the required information.

This use case proposes to enable the generation of the required information independently also in MEC hosts located in other deployments such as an aggregation point or gateway.

In order to achieve the most accurate measurement for the radio network information, the MEC platform or a dedicated MEC application that provides the service can take into the calculation several parameters extracted from the traffic going over the network. The service can also involve a self-learning method to adapt the end results to changing conditions at each location and different radio nodes, which can be used by applications that register for this information and are authorized to receive it.

A.21.2 Use of MEC

A number of applications running on a MEC host might require radio network information to optimize their performance. A MEC service could provide such information to such authorized applications, even in deployments where radio network information might not be available to the MEC service, by generating this information autonomously.

A.21.3 Related requirements

- [RNI-03]

A.22 Unified enterprise communications

A.22.1 Description

This description is based on SCF081 [i.8]. Mobile devices are gradually replacing fixed communications hardware, laptop software, and office services in the enterprise market by leveraging native desktop interfaces as well as additional value-added apps. This is a replication of trends in the consumer market. Since about 2010, the consumer market has seen many devices and physical world technologies replaced by smartphone and tablet hardware and software and internet cloud platforms.

Once robust coverage and capacity are available indoors, the enterprise can start to move towards a truly mobile office where the business tools are migrated into the mobile devices and there is ubiquitous access to cloud-based business tools. The presence of a MEC deployment of Small Cells on enterprise premises makes it a natural candidate for support of enterprise applications in the mobile edge.

Figure A.22.1 describes a Multi-access Edge Computing-based breakout to an enterprise network, enabling employees using smartphones and tablet PCs to enjoy a fast broadband connection directly to the enterprise LAN.

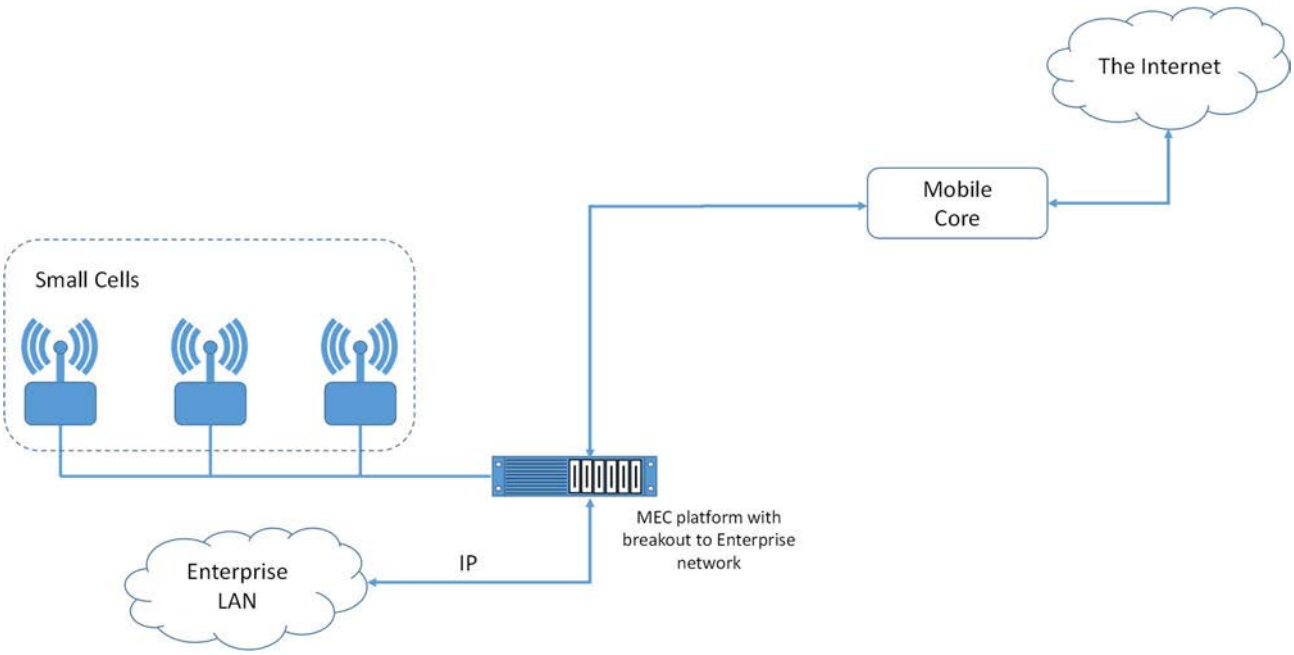


Figure A.22.1: Multi-access Edge Computing-based breakout to an enterprise network

An example of such a unified service which is in direct market demand today is that of unified communications with the enterprise PBX, allowing the enterprise user's BYO Device's to be used for enterprise communications.

Based on the discussion in SCF081 [i.8], an example (and very incomplete) set of features required for the unification of Multi-access Edge Computing with PBX is as follows:

- **internal call re-routing:** support of routing and processing of IP-PBX (internal extension call) traffic for enterprise employees;
- **identity1:** association of the user's enterprise identity with the mobile network traffic to support traffic rules based in the enterprise users identity;
- **identity2:** the association between the user's enterprise identity and the mobile network identity (e.g. GPSI) to support authentication based on the enterprise user identity;
- **time of day routing:** the capability to set rules/policies so that UE traffic can be handled in different ways based on the time of day;
- **enterprise messaging:** support selective re-routing of mobile messaging application traffic based on enterprise user's identity for the purposes of integration of enterprise IM and SMS, for example, to implement enterprise paging features.

A.22.2 Use of MEC

The MEC platform provides functionality which facilitates the association of IP traffic flows with a particular UE to which an external network identifier (e.g. via active directory) is associated using an externally defined tag. This association is performed using industry-standard techniques that preserve user privacy and the secrecy of the identity information at both the mobile network and the enterprise.

EXAMPLE: The service could involve facilitation of the use of a trusted 3rd party identity management service (e.g. an OpenID provider) with which the operator and the external network (e.g. enterprise) have the necessary trust relationships in place.

The MEC platform provides the capability to route user plane traffic of enterprise users between the operator network and the enterprise network without having to pass through the application. The application is responsible for managing issues associated with access control, integrity, etc. of the user content.

A.22.3 Related requirements

- [UEIdentity-01], [UEIdentity-02], [UEIdentity-03], [UEIdentity-04], [UEIdentity-05], [UEIdentity-06]

A.23 Application computation off-loading

A.23.1 Description

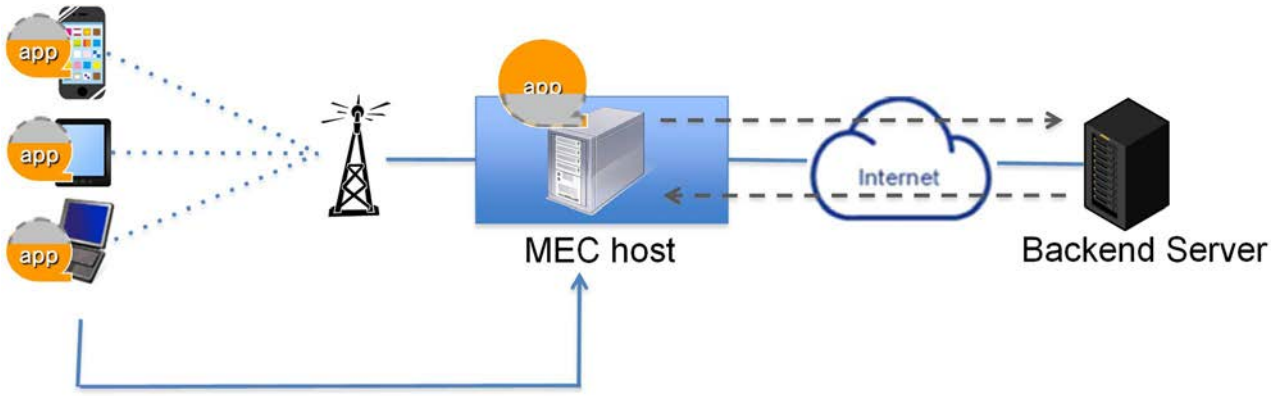


Figure A.23.1: Application computation off-loading using MEC

In the application computation off-loading use-case, the MEC host executes compute-intensive functionalities with high performance instead of mobile devices as shown in Figure A.23.1. By providing rich computation resources on a MEC host, application computation can be off-loaded to the MEC host to be accelerated even if a user uses relatively low performance devices, and user experience can be satisfied regardless of the type of UE.

This use-case is effectively used for especially computation-hungry applications such as graphical rendering (high-speed browser, artificial reality, 3D game, etc.), intermediate data-processing (sensor data cleansing, video analysing, etc.), and value-added services (translation, log analytics, etc.). One example of application computation offloading is the Edge Accelerated Browser (EAB). Most parts of the browsing functions, such as Web contents evaluation, rendering and optimized transmission, are off-loaded to the MEC application, while the UE just renders reconstituted browser graphics on its display. This can transfer a compute-intensive process from a UE to a MEC host to accelerate an application and make rich applications available on various types of mobile devices.

A.23.2 Value proposition

Application computation off-loading provides the following values to both service provider and end users:

- service providers:
  - deliver high-performance applications regardless of end device capability;
  - off-load computation resource required by an application by using rich compute resource in MEC host;
  - process application data collected from end devices (M2M, video, etc.) on MEC host to mitigate both end device and centre server load;
  - provide value added services by adding extra value to application data on MEC host;
- end users:
  - improve user experience through an off-loaded application on their mobile devices;
  - get low cost end devices by off-loading compute capacity to MEC host;

- get new types of service offerings like auto-translation and recommendation based on log analytics by application linkage on MEC host.

A.23.3 Use of MEC

In response to a request from the user, a new instance of a specific application (or part of application function) needs to be started on an appropriate MEC host fulfilling the latency and resources requirements of the application.

In response to requests from other users, connectivity needs to be established between their UEs and a specific instance of an already running application.

The application might have a set of requirements (e.g. latency, compute resources, storage resources, location, network capability, security condition, etc.) that needs to be fulfilled by the MEC host. The MEC system needs to select a host fulfilling all the requirements.

When all the users connected to a specific instance of an application have disconnected, the application instance might be terminated.

A.23.4 Related requirements

- [Connectivity-04]
- [UserApps-02], [UserApps-03], [UserApps-04], [UserApps-07], [UserApps-08]

A.24 Optimizing QoE and resource utilization in multi-access network

A.24.1 Description

Multi-access Edge Computing, as its name implies, enables the hosting of applications close to end users in a communications network that consists of multiple different access technologies. From the end user device's point of view, this results in multi-connectivity scenarios where the devices can be simultaneously connected to applications and services of a distributed cloud over different access technologies such as Wi-Fi®, LTE, MuLTEfire™ and DSL.

In such an environment, the overall QoE perceived by the end users as well as utilization of the resources can be optimized with smart selection and combination of the paths used for the user plane. In an advanced solution, the network paths can be dynamically selected based on knowledge of current conditions in the relevant access networks. The present document of MEC already contains the RNI API that can be used to obtain up to date information from the 3GPP LTE networks. Similarly, information from other accesses such as Wi-Fi® and Fixed networks can be provided in Phase 2 of MEC. Offering information from all access technologies is a useful enabler for multi-access scenarios, but it is not yet sufficient. Also, a solution to manage and control the user plane path selections is needed.

IETF has ongoing work on Multiple Access Management Services (MAMS) that offers a full framework and reference architecture for smart selection and flexible combination of access and core network paths based on defined policies [i.10], [i.11] and [i.12]. By use of up to date information from available access networks the best possible network efficiency and end user QoE perception based on application needs can be guaranteed.

With MAMS framework, the optimal network paths can be selected on user plane level without any impact on the control plane signalling of the underlying access networks. As an example, in the case of a multi-access network with LTE and Wi-Fi® options available the standard procedures to set up the connections are used in both LTE and Wi-Fi®.

A.24.2 Use of MEC

Multiple Access Management Services (MAMS) can be used to manage smart and flexible user plane path selections in multi-access networks. MAMS consists of the following functions:

- Client Connection Manager (CCM) that negotiates the network path usage with NCM based on clients' needs and capabilities.
- Network Connection Manager (NCM) uses information obtained from the access network and based on policy, current conditions and the information exchanged with client, configures the user plane paths for the multi-connectivity device.
- Client Multiple Access Data Proxy (C-MADP) handles the user plane selection procedures at the client.
- Network Multiple Access Data Proxy (N-MADP) handles the user plane selection procedures at the network.

The functions that are located in the network side i.e. NCM and N-MADP can be hosted either at a centralized location or at the Edge Cloud. They can be deployed either as MEC application or co-located with other functions (e.g. the MEC platform).

NCM as the function responsible for intelligent network path selection needs up to date information from the access networks. This information can be exposed over APIs by the MEC platform the same way as it exposes Radio Network Information over RNI API.

For new accesses in the Multi-access Edge Computing framework, solutions to receive information about the conditions need to be defined. ETSI GS MEC 012 [i.13] RNI API focuses on exposure of 3GPP Mobile network information. Similar levels of information should be defined for Wi-Fi®, MuLTEfire and DSL either by amending the existing RNI API or by defining new APIs specific for the new access technologies.

A.24.3 Related requirements

- [Multi-access-01] The MEC system may support the feature called *AccessNetworkInformation*.
- [Multi-access-02] When the MEC system supports the feature *AccessNetworkInformation*, there should be a MEC service that exposes up-to-date information regarding specific access network technology.
- [Multi-access-03] When the MEC system supports the feature *AccessNetworkInformation*, the provided Network information should include access technology type, for example WLAN, MuLTEfire, xDSL, Ethernet, etc.
- [Multi-access-04] When the MEC system supports the feature *AccessNetworkInformation*, the provided Network information may include bi-directional bandwidth information that is delivered to/from the specific user.
- [Multi-access-05] When the MEC system supports the feature *AccessNetworkInformation*, the provided Network information may include granular bi-directional bandwidth information that is delivered to/from the specific user on the level of specific application, class of service, etc.
- [Multi-access-06] When the MEC system supports the feature *AccessNetworkInformation*, the provided Network information may include latency information. This information may indicate measured, expected or estimated unidirectional, bi-directional or round trip delay and/or delay variation for the data delivered through the access network. The latency information may be provided per specific UE or in more granular form such as per specific application level or class of service.
- [Multi-access-07] When the MEC system supports the feature *AccessNetworkInformation*, the provided Network information may include access technology specific information such as network identifiers, physical link conditions, radio link conditions, etc. and network conditions such as congestion, overload, etc.

A.25 Camera as a service

A.25.1 Description

A typical use case for camera surveillance is to monitor an area for events that may then trigger further actions. The basic mode of operation may be surveillance for detecting events or objects, and then commence tracking of the detected objects or events and trigger possible further actions. An object can be a bar code, license plate, a human face, etc., while an event can be e.g. an object in an area where there should not be any objects, a moving object with abnormal direction or speed, or detection of a wanted criminal.

A video surveillance system consists of a multitude of cameras connected to the rest of the infrastructure either wirelessly or via a wired access. When cameras are active they are constantly searching for pre-defined objects or events. To avoid the need to stream the video constantly in real time to the customer's facilities (e.g. central cloud), the descriptions of pre-defined objects or events, i.e. triggers, are stored lower in the system hierarchy at the edge, or in the camera devices themselves. Such arrangement minimizes the consumed system resources on actions of no value. For any events, the system attempts to do some preliminary processing to determine the need for further actions. This preliminary processing requires near zero latency and may take place in the camera device itself, requiring the camera device to support some computing capabilities, e.g. to receive and instantiate customer specific algorithms or instructions. The device side computing functions represent the device component of the application.

Based on the preliminary processing, further action may be necessary on the selected objects, e.g. further analysis of the object's track, detailed identification of the object, etc. Such processing may be tasked for the edge cloud component of the application. A further action may also consist of instructing the video stream to be routed into the customer's central facility, possibly requiring on-demand bandwidth and QoS reservations for the end-to-end connection, including also the link between the device and the access network. Also the tracking of the individual object may commence, involving information exchange within the network of connected camera devices, possibly controlled or orchestrated by the main cloud or edge cloud components of the surveillance application. Such information exchange may include, e.g. activating camera devices along the predicted route of the object, passing on accurate descriptor vector of the object from the source area to target area and camera devices there.

The camera as a service use case as described above expects the following system entities and capabilities to be present:

- Surveillance application with central cloud component (public or private cloud facility), edge cloud components and device cloud components.
- The application components in the distributed edge infrastructure allowed and enabled to communicate with each other, with the device cloud component and with the central cloud component, i.e. the customer's cloud facilities.
- Distributed edge computing infrastructure, i.e. MEC hosts, available for the edge cloud component of the camera application, supporting the on-demand on-boarding and on-demand instantiation of the application component by the customer.
- Onboarding of the application component in the distributed edge supporting the associated (deployment) information that specifies the geographical area where the camera-as-a-service needs to operate.
- Network of connected camera devices that may support the on-demand reception and instantiation of the device cloud components of the camera application, e.g. algorithms, instructions or trigger definitions.

Figure A.25.1: Camera as a service system architecture

A.25.2 Use of MEC

Void.

A.25.3 Related requirements

- [AppEnvironment-04]
- [Lifecycle-07], [Lifecycle-08], [Lifecycle-09], [Lifecycle-10]
- [Bandwidth-04]

A.26 Video production and delivery in a stadium environment

A.26.1 Description

The use case of edge video processing suggests a scenario where visual content is produced, composed, processed and consumed locally. Such a case can be events such as sport, concerts, public meetings, conferences, etc. Consumers can select tailored content using their hand-held device. This may include a specific viewing angle, multi-viewing angles, slow motion replay, analytics and statistics, side by side comparison between players, etc. Users may request a viewing angle or a shot from a location which is not available from the user's physical seat or section. This is especially relevant for events distributed over a wide area (such as ski, bicycle or Formula 1 car race).

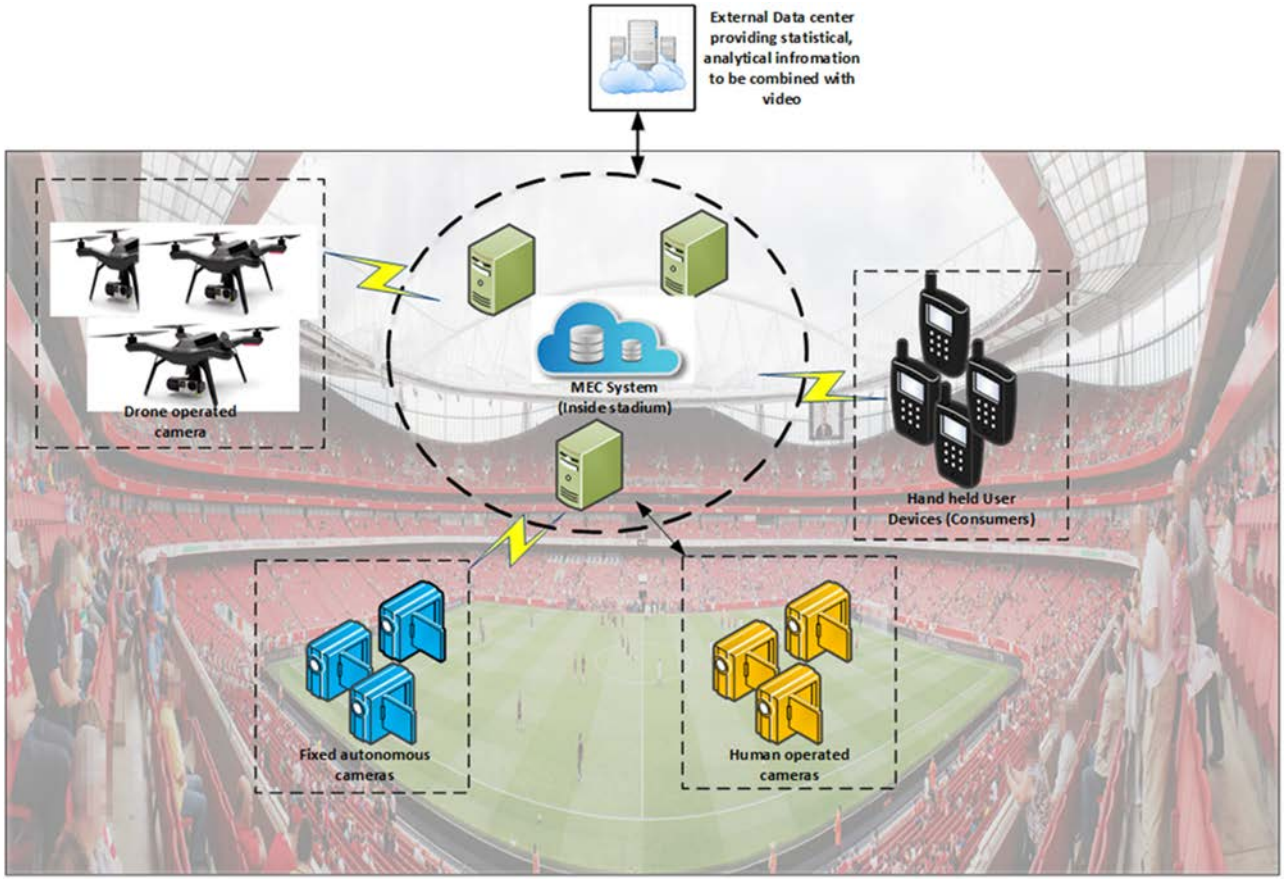


Figure A.26.1: Video production and delivery system in a stadium environment

The "MEC system", which is deployed inside the venue, is ideally suited for proposed video production use case. "Edge Video Applications", which are responsible for video editing, composition, are running on the MEC system. Running the video applications at the edge, allows easy control of service quality and improvement in performance of video delivery and consumption.

The video production service may be provided by Third party service providers or by Traditional Network Operators. In this use case, it is assumed that Network operator owns cloud resources. Third party service providers supply MEC applications and corresponding requirements to Network operators. If Network operators provide the video production service, then the MEC applications are owned by Network operator.

The video is captured from multiple sources. There may be multiple stationary cameras mounted throughout the stadium, drones flying around the stadium (both inside and potentially outside) capturing video and humans ("venue personal" and end-users) with video cameras moving around the stadium. The various video capturing devices (cameras, drones, users) may be uploading their captured content over a wired or wireless connection (cellular or Wi-Fi®). The video capture devices may first connect to a pre-filtering edge application, which filters video based on pre-set quality threshold, running on the MEC system inside the stadium. After preliminary filtering, second level processing takes place.

The next level of processing of the captured video streams is performed by one or more video applications running on different hosts in the MEC system within the stadium. These video processing applications allow editing and composing of videos from multiple sources. They may also fetch statistical and analytical data about a player, actor, etc. from a cloud server across the Internet. Multi-angle, multi-location videos combined with statistical data is then published for end user consumption. The MEC system may also convert the composed video in multiple video formats to support the wide range of media players present in end user devices.

The preliminary processing of the captured video, such as pre-filtering, may be done at the location of camera itself. This is a resource constrained environment, where technologies like "Container" may be suitable. The computation intensive applications such as editing, formatting is done in the facility where more computation resources are available. In this environment, technologies such as Virtual Machine (VM) may be used.

The edge video applications may be scaled up or scaled down dynamically, based on demand. As number of users increases, multiple instances of the application may be created and direct users to the most appropriate instance (based on location, server load balancing, etc.).

End users are provided with an interface/portal to connect to the local video servers running on the edge. End users may be connected over radio access networks (Wi-Fi® or Cellular), potentially from different service providers. Their request for local content is directed to the MEC system, running video applications, in the stadium.

The video production use case expects the following system capabilities:

- Video service at the edge may consist of multiple application instances and may use services from other edge systems or the distant cloud.
- The deployed video application components may use different virtualisation technology such as VM, Containers, micro-services, etc.
- MEC system can deploy the application components considering application requirements, resource availability, networking capability, edger server load and performance, etc.
- MEC system provides connectivity among these application instance components or micro-services.
- Application instances may be replicated or decommissioned on demand as consumer and producer increases or decreases respectively.
- As application instances are replicated their connectivity may also be changed or redirected.
- Producer devices and consuming users need to be directed to the correct application instance as the MEC system is scaled up or down.

A.26.2 Use of MEC

Void.

A.26.3 Related requirements

- [Lifecycle-xx] The MEC system should support deploying a suite/collection of applications (or application components) across single or multiple hosts, which are part of the MEC system.
- [Lifecycle-xx] The MEC system should support deploying applications (or application components) which may use different technology, e.g. VM, Container, etc.
- [Lifecycle-xx] The MEC system should support scaling up or down applications (or application components) which are part of the application suite.
- [Routing-xx] The MEC system should support setting up of routes among edge applications, cloud services, and application client in UE.
- [Routing-xx] The MEC system should support fast redirection of routes among edge applications, cloud services and application client in UE as the system scales up or down.
- [Services-xx] The MEC system should support MEC applications or MEC platform to consume services provided by authorized applications running on a different network or in a distant cloud.

A.27 Media Delivery Optimizations at the Edge

A.27.1 Description

Category: Network performance and QoE improvements

The delivery of multimedia data has become a major application of the data transport services provided by mobile and fixed networks. Due to the continuous growth of traffic demand, several multimedia services are trying to improve the perceived Quality of Experience (QoE) by optimizing the traffic delivery. Server And Network assisted DASH (SAND) offers standardized interfaces for service providers, CDNs and operators to enhance streaming Quality of Experience (QoE). A SAND application can be a particular MEC application for the multimedia delivery optimization at the edge, In particular, SAND realizes the following:

- Streaming enhancements via intelligent caching, processing and delivery optimizations on the server and/or network side, based on feedback from clients on anticipated media segments, accepted alternative media content, client buffer level and requested bandwidth.
- Improved adaptation on the client side, based on network/server-side information such as cached Segments, alternative Segment availability, recommended media rate and network throughput/QoS.

As such, a SAND edge server can leverage network/link status related information from a MEC server toward determining the assistance messages to be sent to a streaming client.

A.27.2 Use of MEC

A particular MEC application for the use case described in the above is the SAND application, defined by 3GPP standard. SAND in 3GPP Rel-15 is part of their Packet-switched Streaming Service (PSS). SAND helps fulfil the 3GPP-adopted edge compute use cases on proxy caching, consistent QoE/QoS and network assistance to improve streaming applications. The detailed 3GPP SAND use cases can be found in ETSI TR 126 957 [i.17]. In particular:

- SAND can be deployed over the existing 4G legacy architecture (EPC) as well as over the newly defined 5G architecture.
- SAND fulfils the 3GPP-adopted edge compute use cases on proxy caching, consistent QoE/QoS and network assistance to improve streaming applications.
- Use of SAND can leverage availability of ETSI MEC APIs to further optimize streaming, i.e. via exposition of RAN-level network information in a SAND-based proxy/edge server (DANE) via ETSI MEC-based APIs.
- When SAND is deployed by an OTT service provider where the DANE is located in the third party domain outside of the operator network, ETSI MEC APIs may be used to convey radio and network status information to a DANE.
- By referring to ETSI TS 126 247 [i.18] (reference also to MPEG spec number ISO/IEC 23009-5 [i.19]) the relevant SAND messages in this context are QoS Information and Throughput messages.
- These messages are signalled from the edge server to the DASH client with a goal to improve the client adaptation logic.

From this perspective, the MEC system should provide information as a useful mapping with the previously mentioned QoS Information and Throughput messages in SAND. In particular, it should provide:

- explicit QCI characteristics, that could be helpful for external applications (e.g. SAND) in order to better exploit this information (e.g. to optimize the video streaming);
- actual video throughput information, e.g. in order to provide information in accordance with SAND messages, or again inform the SAND client about the bit rate allocated to it;
- a bitrate recommendation based on the actual real-time radio throughput available for a specific connection.

NOTE: It should be clarified that the above signalling of bitrate recommendation is aimed at informing the DANE so that the DANE provides the DASH streaming clients with the recommendation of the highest suitable media rate. The recommended bitrate is based on network estimations or predictions of available link bandwidth for the ensuing period of time. The recommended bitrate may not necessarily be enforced by the network, nor is the network required to make any commitment that the recommended rate will be honoured.

A.27.3 Related requirements

- [Connectivity-04]
- [Routing-05]
- [RNI-04], [RNI-05], [RNI-06], [RNI-07], [RNI-08], [RNI-09]

A.28 Factories of the Future

A.28.1 Description

The manufacturing industry is currently subject to a fundamental change, which is often referred to as the "4th Industrial Revolution" or simply "Industry 4.0" [i.20]. The main goals of Industry 4.0 are to improve flexibility, versatility, resource efficiency, cost efficiency, worker support, and quality of industrial production and logistics. These improvements are important for addressing the needs of increasingly volatile and globalized markets. A major enabler for all this are cyber-physical production systems based on a ubiquitous and powerful connectivity and computing infrastructure, which interconnects people, machines, products, and all kinds of other devices in a flexible, secure and consistent manner.

There are several application areas that can be briefly characterized as follows:

- Factory automation: Factory automation deals with the automated control, monitoring and optimization of processes and workflows within a factory. This includes aspects like closed-loop control applications (e.g. based on programmable logic or motion controllers), robotics, as well as aspects of computer-integrated manufacturing.
- Process automation: Process automation refers to the control of production and handling of substances like chemicals, food & beverage, etc. Sensors measuring process values, such as pressures or temperatures, are working in a closed loop via centralized and decentralized controllers with actuators, e.g. valves, pumps, heaters.
- HMIs and Production IT: Human-Machine Interfaces (HMIs) include all sorts of devices for the interaction between people and production facilities, such as panels attached to a machine or production line, but also standard IT devices, such as laptops, tablet PCs, smartphones, etc. In addition to that, also Augmented and Virtual Reality (AR/VR) applications are expected to play an increasingly important role in future, which may be enabled by special AR/VR glasses, but also by more standard devices, such as tablet PCs or the like.
- Logistics and warehousing: Logistics and warehousing refers to the organization and control of the flow and storage of materials and goods in the context of industrial production. In this respect, intra-logistics is dealing with logistics within a certain property (e.g. within a factory), for example by ensuring the uninterrupted supply of raw materials on the shop-floor level using Automated Guided Vehicles (AGVs), fork lifts, etc. This is to be seen in contrast to logistics between different sites, for example for the transport of goods from a supplier to a factory or from a factory to the end customer.
- Monitoring and maintenance: Monitoring and maintenance refers to the monitoring of certain processes and/or assets without an immediate impact on the processes themselves This particularly includes applications such as condition monitoring and predictive maintenance based on sensor data, but also big data analytics for optimizing future parameter sets of a certain process, for instance.

A.28.2 Use of MEC

Figure A.28.1 gives an overview of the different deployment scenarios in the industrial automation. A MEC host can be deployed at field level. One example is to support sensor networks in a factory. Sensor networks monitor the processes and the corresponding parameters in an industrial environment using various types of wired and wireless sensors such as microphones, CO_2 sensors, pressure sensors, humidity sensors, and thermometers. The monitored data from such a system is used to detect anomalies in the data, i.e. by leveraging Machine Learning (ML) algorithms. These algorithms usually require a training phase before a trained ML algorithm can later work on a subset of the available measured data. The training as well as the analysis of the data may be realized in a centralized or distributed manner. MEC could be used to host local monitoring function, which can provide additional external computational resources for the simple sensors. Such local approach is preferred over a more centralized approach in order to keep sensitive data in a fabrication site and keep the automated process independent of an Internet connection.

A MEC host can also be deployed at wide area network level, which is particularly beneficial for the application areas such as "HMIs and production IT" as well as "logistics and warehousing". Such application areas typically require mobile robots and mobile platforms (e.g. Automated Guided Vehicles (AGVs)) in industrial and intra-logistics environments. Mobile robots and AGVs are monitored and controlled from a guidance control system. MEC could be used to host such remote control system, which would support for example the processes for handling goods and materials, especially incoming and outgoing goods, in warehousing and commissioning, in transportation as well as transfer and provision of goods.

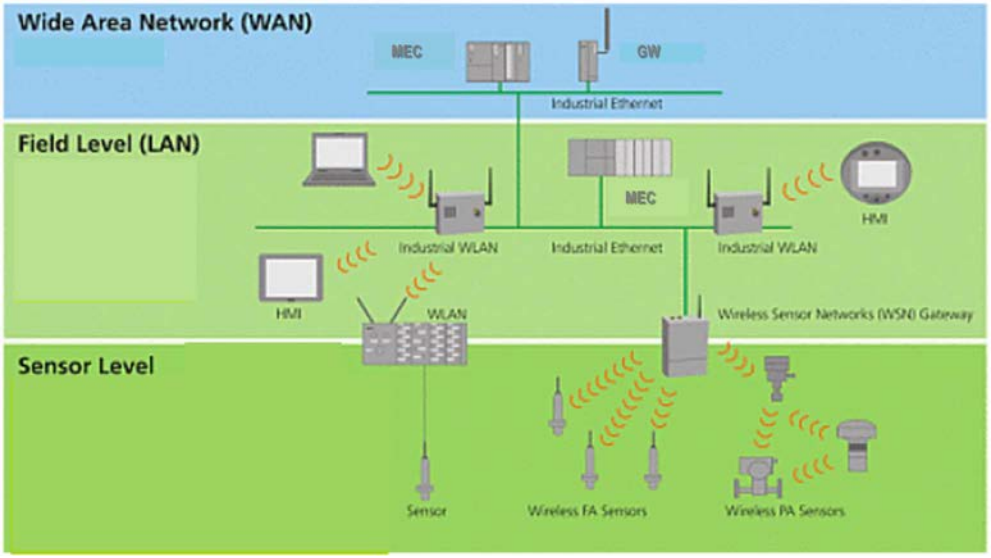


Figure A.28.1: Deployment scenarios in the industrial automation

A.29 Flexible development with Containers

A.29.1 Description

Alice is service crafting architect at new company called Determined Hippo. Together with her colleague Bob, who is head of UX, they create new mind-blowing experiences for their customers that are seeking to digitize their offering.

Determined Hippo has been on a market for 4 years and they are famous for their extremely high valuation among their targeted customer segments. Determined Hippo has continuously provided the fastest time to market for their apps, together with the performance and objective quality, that has clearly exceeded those offered by competition. There may be multiple reasons for their success, but one of those fundamentals is their operational model, which is agile and focused.

Part of their success comes from the fact that their primary customers are those that are in the forefront of digitization, pioneering the service creation concepts and changing the traditional industries. Those companies use the latest philosophies and design principles to minimize the waste and to accelerate the time to market. The end user perception and strong buy from the customers is ensured with the co-creation model, where the feedback from the real end users is integrated in the design loop.

The model used can be always argued, but it has been proven a success story both from Determined Hippo's and their customers' point of view.

There are many building blocks in the operational model, but one of those is containers. Determined Hippo is mainly focusing to develop services using container as technology of choice and their agile design processes have been fine-tuned based on those. When asked, they mainly see the benefits with the containers. According to their chief architect the most important benefits are in flexibility, foot print, comprehensive set of development tools. It fits well with their design flow and allows continuous development in flexible manner.

Whilst they mostly see only benefits, there are also some downsides suggested by their design folks. Their chief security & crypto expert Eve has continuously raised her concerns on security that is compromised with the cost of flexibility. But she also admits that containers are safe to use in most of the use cases, but that extra attention needs to be paid to design in area of security.

Determined Hippo has MEC technology in their radar and they are eager to provide their expertise in ME services and apps development. However, as their design model is optimized for containers, they rather wait for the industry to enable those in the MEC ecosystem rather than branch for the areas that are not their strongest footholds.

Amongst Determined Hippo's expectations regarding telco MEC technology which they could access in the future are:

- Availability of a container runtime environment at the MEC infrastructure site.
- Ability to develop applications for the cloud and then also to deploy those same applications in MEC service provider's infrastructure.
- Ability to deploy a complex application whereby a part runs on-premises in a private data centre, a part runs as an ME app in a container and a part runs on the end user device.
- Networking support such that the different application components can be networked together.
- A container management solution that provides the customer with insight into the state of the application incl. its container(s) for monitoring purposes.
- An ability to upgrade the application, including the ME app running in container(s) in a highly flexible way akin to CI/CD (continuous integration, continuous delivery).

A.29.2 Use of Multi-access Edge Computing

The MEC systems will support multiple virtualisation technologies including Virtual Machines and Containers. Depending on the case the application developers will decide which is the best applicable virtualisation technology and then design and package their application accordingly.

When 3rd party is providing their new application as a container or as a set of containers, the delivery can be made the same way as earlier with the VMs. In this case Determined Hippo uses the CFS portal offered by the carrier and makes the application package to available within MEC system. The MEC management system functions on both system and host level support the same needed procedures as with VM to onboard the application and to instantiate it in the desired targeted location. Also with the lifecycle management, all the needed functionalities are available for this container application.

In some cases, containers are the preferred solution for distributed application deployments where smaller footprint is one of the differentiating factors. The MEC management system also supports both system and lifecycle management procedures of distributed applications.

A.30 Third Party Cloud Provider

A.30.1 Description

This use case is related to an emerging business model, where computational resources for edge cloud service are provided by alternative facility providers that are non-traditional network operators. This is due to the situation for many specific localized use cases, where network operators may not have necessary real estate available. They may even not be willing to spend on CAPEX and OPEX for said point-of-presence, because there is no clear path for sustainable cost recovery [i.21].

The industry is witnessing the emergence of real estate owners such as building asset or management companies, cell tower owners, railway companies or other facility owners willing to deploy edge cloud resources. The facility provider, e.g. cell tower owner or building management company, deploys edge computing resources throughout their installation in the country. They have their own operation and management software, which is capable of resource deployment, scale up or scale down resources, deploy edge applications from third party service providers.

They are capable of offering service to more than one network operator at a specific location, thus acting as a "neutral host". The facility provider, which owns cloud resources and provides application services, is referred to as "Third party Edge Owner (TEO)".

NOTE: Although not strictly required, a growing proliferation of resource management and orchestration frameworks such as (ETSI) MANO NFV, exposing those resources through developing standards on templated orchestration as well as virtualisation above the HW level can be expected.

There is more than one stakeholder in this ecosystem, e.g. Network Service Provider, Real estate owner, Cloud capability (compute and storage resource) provider, Application/service provider. An entity can assume more than one role. From network operators point of view there may be "Cloud provider" or "Cloud service provider" depending on the roles assumed by external entity.

"Cloud Providers" provide cloud resources (compute and storage) to network operators. Network operators rent those resources and manage MEC host by themselves. Network operator can set up application traffic rules, so that traffic can be processed, by that host.

"Cloud Service Providers" not only make resources available to network operators or service providers, but also provides management and hosting service. They can host edge applications on behalf of application service providers and sets up user plane traffic to be steered towards the edge application.

This new business model allows real estate owners and other stake holders to derive additional revenue from their property, whereas network operators and service providers can focus on their core business. It allows them to temporarily expand their asset footprint, particularly in locations where such investments would not be sustainable in longer term timescales. It will therefore allow for faster deployment of Edge services due to the pooling of resources with facility owners that already have invested to deploy throughout the nation. Network Service Providers, such as MNOs, can extend their edge service offerings through such temporary leasing of resources without the long-term investment into own facilities.

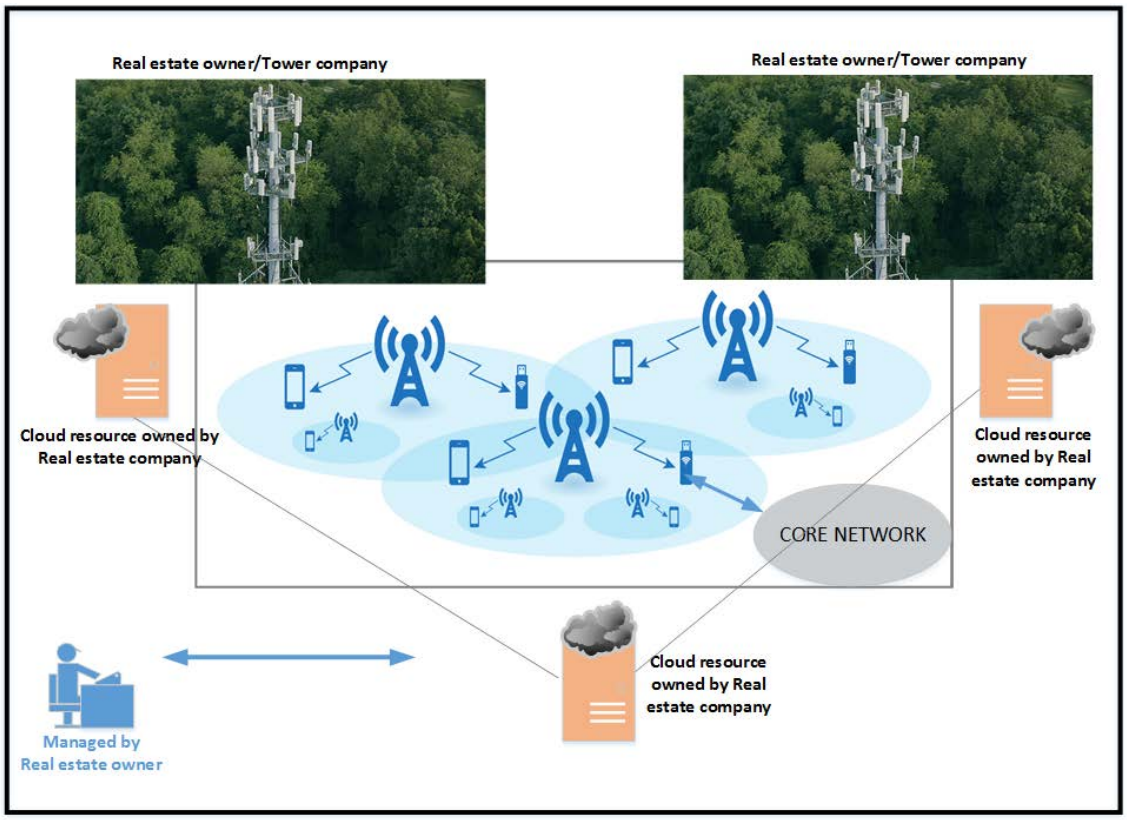


Figure A.30.1: Provision of third party owned cloud resources

Network Service Providers such as MNOs or ISP set up a business agreement with TEO, which allows them to steer traffic towards the edge computing applications running on the edge computing facility owned by the TEO.

MEC system and its functionality gets distributed across TEO and Network Service Provider. E.g. TEO may run hosting function and network operator may provide network information services, such as Radio Network Information Service, Location Service, etc., to TEO.

A.30.2 Use of MEC

MEC system allows distribution of functionality among multiple stake holders. Several owners, such as TEO, Network Service Provider and Service Provider may own parts of MEC system. It should allow TEO to provide simple resource renting facility to Network Service Provider. Network Operator can manage MEC host, Edge applications by themselves.

MEC system should also allow TEO to manage Cloud resources, run their own MEC host and Edge applications. TEO can set up traffic path, so that user traffic can be processed by edge applications hosted by them. MEC system should provide capabilities to TEO to set up traffic rules and policies to "steer traffic" between operator's network and Edge Cloud resources.

MEC system provides capabilities by which TEO can obtain network related information, such as Radio Network Information, Core Network Information etc. to better manage edge computing resources.

MEC System should be able to enforce privacy and security requirements on TEOs. MEC System should be able to generate billing data based on traffic measurements, e.g. traffic diverted towards external edge cloud.

A.30.3 Related requirements

- [AppEnvironment-05]
- [OAM-05]

- [Services-xx] A MEC platform running on third party cloud should be capable of obtaining network information, which is authorized for use by the network service provider.
- [Routing-xx] A functional entity of a MEC system running on third party cloud should be capable of informing the network service provider, such as MNO, of its preferred user plane configuration and routing.
- [Routing-xx] A MEC platform owned by a third party should be capable of steering user plane traffic to/from the network service provider's network, according to the network service provider's policies.

Acknowledgment:

This use case aligns with the work in the H2020 5G-PPP 5G-TRANSFORMER project.

A.31 Multi user, multi network applications

A.31.1 Description

Multi network applications, e.g. Online Gaming, involving multiple users across multiple networks are becoming very popular. Users play games inside their homes as well as when they are outside, travelling, waiting in a shopping mall or waiting for train or plane etc. They play on multiple devices and demand rich applications with very low latency. To provide such rich gaming applications with very low latency, game service providers are using edge computing service. The edge computing service may be provided by network operators or third party service providers.

Network operators own and operate more than one network such as 3GPP network and Wi-Fi® (managed) network. They may own and deploy cloud resources across networks. On the other hand, different networks may be owned by different operators. They may deploy and operate cloud resources within their network independently. For example the 3GPP network and Wi-Fi® network may be owned by different operators and each may own different MEC systems. It should be possible to deploy and manage applications across MEC systems.

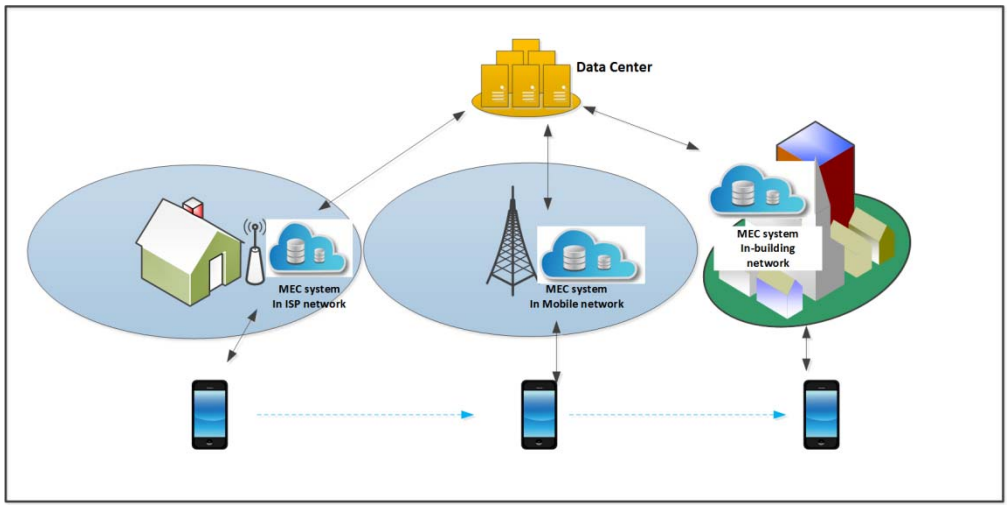


Figure A.31.1: Multi-user multi-network application

As the gaming industry evolves, it is becoming common to deploy applications in a tiered fashion. For example, a tiered application may consist of "frontend" applications (e.g. media asset provisioning, user interaction management, etc.) running at the edge of the network (3GPP, Wi-Fi®, Fixed Network) and distant cloud-based "backend" applications to run computation intensive applications (e.g. state synchronization, simulation of physics, artificial intelligence). MEC systems across networks manages and controls the deployment of gaming applications at the frontend across different networks. These applications can collaborate among themselves and also with applications running on the distant cloud. The same "frontend" application may be deployed across different network edges.

The user would start an application on a suitable device that requests the connection to the gaming application. For multi-user applications, other users, will request connection to the same gaming application. Different users may be connected to the gaming application over different access networks (e.g. 3GPP, Wi-Fi®, Fixed Network). MEC system allows the application instances to process user request and collaborate with application in distant cloud.

After initial connection, one or more users might move around or change devices, while they are playing the game. The users may get connected over different access networks. E.g. an user may start the game while in his home connected through his/her ISP. The user may be served by the gaming application running at the edge of the ISP network. The user continues playing the game and steps out of his house. The user gets connected over 3GPP network. MEC system allows the user to be served by the application at the edge of 3GPP network without any disruption.

A.31.2 Use of MEC

MEC systems owned by different owners can deploy same edge application across different networks. Service provider can use capabilities exposed by MEC system to deploy and manage applications across MEC systems. The edge application running on different MEC systems is capable of cooperating and synchronizing state among themselves. MEC system allows the application to consume services from other application running in different networks or distant cloud. As users move or network condition changes, MEC system can redirect and setup the communication quickly. It should be possible to maintain session continuity as user moves across different MEC systems.

A.31.3 Related requirements

- [Lifecycle-xx] It should be possible to support the instantiation of an application on multiple MEC systems across different networks.
- [Lifecycle-xx] It should be possible to support deployment of application using different technologies, such as VM and container, across different networks.
- [Application environment-xx] MEC system should expose details of its virtualisation environment to enable an authorized 3rd party service provider to deploy applications across different networks.
- [Mobility-xx] It should be possible to maintain the application session for a UE, when the serving MEC application for that UE is changed to another MEC systems.

A.32 Indoor Precise Positioning and Content Pushing

A.32.1 Description

Category: operator and third-party services

In some indoor scenarios, e.g. shopping mall, home, the GNSS coverage is limited and the indoor small cell deployment limits the use of massive MIMO antennas. Thus current wireless techniques cannot perform precise positioning; reach the expectation of 1 m accuracy in an indoor LOS and low moving environment, 3 - 5 m accuracy in horizontal and 3 m in vertical domains under other environments.

This use case enables regional, precise positioning of distributed indoor antennas and terminals, provides an efficient and low cost positioning solution with local processing and computing, which will benefit for some business scenarios with less mobility, for example museum guidance, smart home, and advertisement push in shopping mall.

A.32.2 Use of MEC

By deploying the MEC application on the ME host near the radio node or limited area, the radio network information related to positioning (e.g. such as SRS measurement, timing advance) will be collected and reported to the MEC applications or services. The MEC application or service will calculate the UE position based on the received radio network information and generate target content pushing policy. The policy would be used to guide distributing the advertisement to a UE or a group of UEs within certain areas based on computed position information. In order to achieve precise positioning, the UEs and/or network is required to provide more accurate positioning related information in a short time or real-time.

The indoor precise positioning information offered by the MEC system is applicable to multiple access technologies, for example radio network, WLAN, Ethernet, etc.

A.32.3 Related requirements

- [Lifecycle-01]
- [Services-01], [Services-03], [Services-06], [Services-07], [Services-08]
- [RNI-01], [RNI-02], [RNI-03], [RNI-04], [RNI-05]

A.33 Multi-RAT application computation offloading

A.33.1 Description

Category: Network performance and QoE improvements

The evolution of communication systems poses increasing challenges from an energy consumption perspective. The computational tasks performed by user equipment, may increase as the complexity of such communication systems increases and this may have a detrimental impact on energy consumption, i.e. the energy consumption is quite different when the UE is using different radio technologies. The divergence becomes bigger if the radio condition is quite different. It is also obvious that using multi-RAT aggregation also increases the power consumption comparing to only using one RAT. The situation becomes severe if the UE is suffering from low power. Additionally, the evolution of wireless applications, in its turn, also leads to increased application complexity, which may also cause computation needs to increase. However, user equipment battery technology has not been able to evolve at the same pace as application complexity. Figure A.33.1 shows some scenarios of task offloading within a multi-RAT environment. It should be noted that these are exemplary scenarios, as the use case also refers to cases where MEC resources are shared by different APs of the same RAT and/or by APs of different RATs.

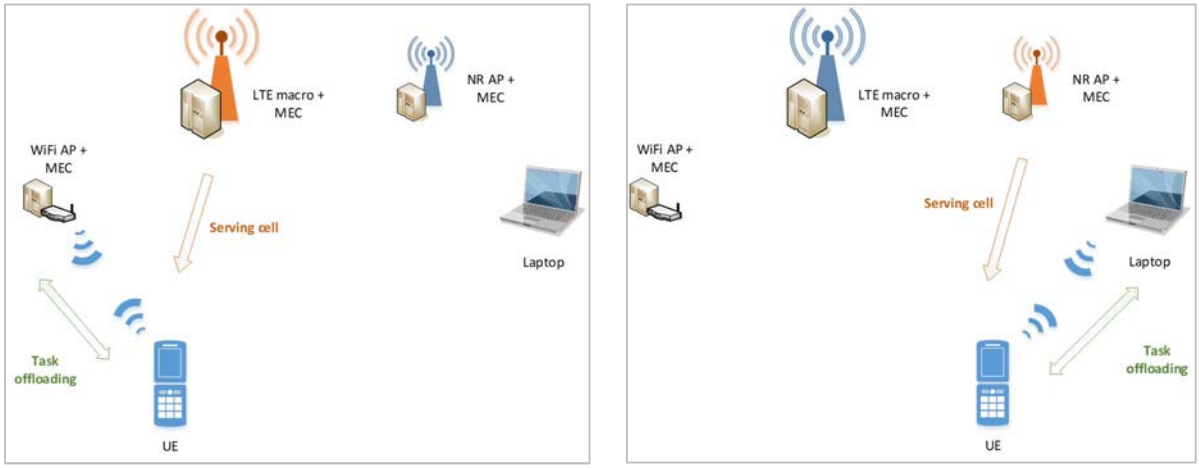


Figure A.33.1: Examples of task offloading within a multi-RAT environment

A.33.2 Use of MEC

MEC technology is designed to be implemented at different RATs, and may enable flexible and rapid deployment of new applications and services for subscribers. The MEC system could also help the application to select the most power efficient RAT for the UE to improve the user experience in the network with multi-RAT coverage, apart from considering other performance indicators (e.g. offloading latency).

A.33.3 Related requirements

- [Connectivity-04]
- [UserApps-02], [UserApps-03], [UserApps-04], [UserApps-07], [UserApps-08]

- [Framework-03], [Framework-05]
- [RNI-01], [RNI-02], [RNI-03]
- [SmartReloc-05], [SmartReloc-06]
- [WLAN-01], [WLAN-02], [WLAN-03]

A.34 IPTV over WTTx

A.34.1 Description

Wireless to the x (WTTx) provides wireless broadband services through wireless broadband access networks like LTE/E-UTRAN, taking full benefit of the well-known qualities of wireless wide area coverage and their ability to meet and exceed the performance of fixed access-based solutions. WTTx allows operators and content providers to shorten their infrastructure deployment cycles and save in network investment costs. IPTV over WTTx provides the operators with fast access to home entertainment markets over existing LTE networks.

IPTV system is usually deployed with a two-level topology. The first level is the IPTV central node which provides live TV service and acts as the source of Video On Demand (VOD) content. The second level is the IPTV edge node which provides Electronic Program Guide (EPG) and VOD services for consumers. The IPTV central node is usually deployed in densely populated areas, e.g. in a capital city or major metropolitan areas. The IPTV edge nodes are then distributed closer to the consumers to ensure the desired quality of experience.

Routing the IPTV traffic through the network operators core network (EPC) and from there to the IPTV edge nodes can significantly impact the core network GWs and the transmission network. Additional latency would also be introduced. On the other hand, the IPTV service providers prefer to use the existing IP multicast mechanism to support live TV service to save in bandwidth investments. However the transport network of EPC often may not enable IP multicast.

Considering the above mentioned aspects in IPTV service delivery, there is room for optimized solutions where the IPTV traffic is offloaded from the rest of the mobile broadband network infrastructure.

A.34.2 Use of MEC

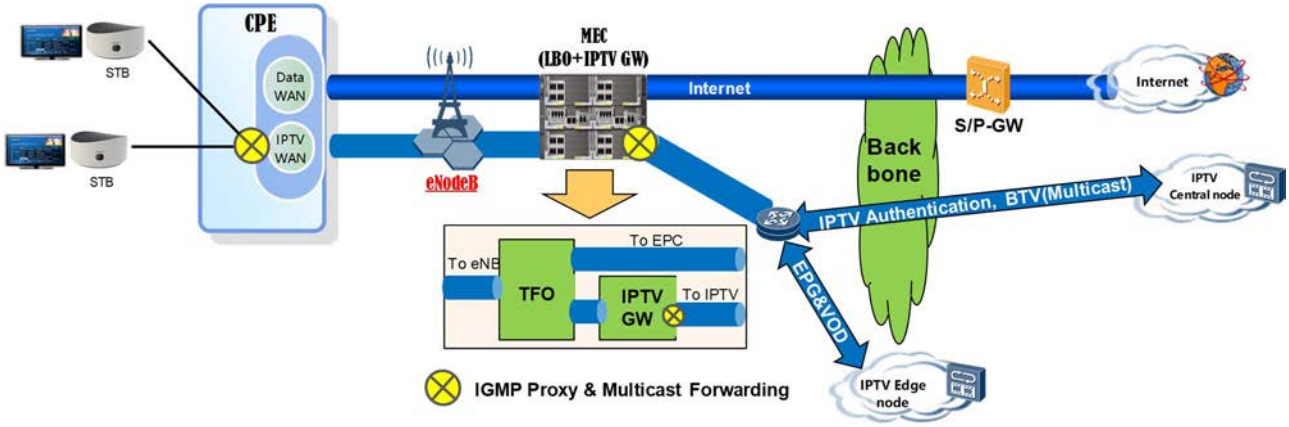


Figure A.34.1: Example MEC deployment for IPTV over WTTx

For Video On Demand (VOD) traffic in IPTV over WTTx, a MEC deployment can offload the traffic to IPTV edge nodes. This way the VOD traffic does not traverse through the EPC, saving both network and transmission resources there, while at the same time improving the Quality of Experience of the consumers.

For live TV, a MEC deployment hosts an IPTV Gateway function to do the multicast group management and to forward the multicast traffic. Customer Premises Equipment (CPE) receives IGMP messages from the Set-Top Box (STB) and proxies them to IPTV GW function hosted in MEC. The IPTV GW function connects with the multicast router to join the intended multicast group with multicast routing protocol such as Protocol-Independent Multicast (PIM). The IPTV central node sends multicast packets to the multicast router that routes these packets to the target IPTV GW functions. An IPTV GW function forwards the multicast packets based on the forwarding rules it has created for its CPEs and their multicast groups. Finally the CPE multicasts the packets to Set-Top Box (STB) for decoding and rendering them on TV.

A.34.3 Related requirements

- [Routing-15], [Routing-16]

A.35 MEC System deployment in 5G environment

A.35.1 Description

Category: Network Performance and QoE improvements

This use case considers how to interact 5G System architecture for supporting applications running on a MEC system deployed in 5G environment.

3GPP 5G System architecture defines the User Plane (UP) functions separated from the Control Plane (CP) functions to allow UP's independent scalability, evolution and flexible deployments. UPF of UP can be deployed at the edge of 5G network. When supporting application running on the edge computing, the 5G Core Network selects a UPF close to the UE and instructs it to steer the traffic to the local Data Network via a N6 interface. The 5G system uses the Network Exposure Function (NEF) in the Control Plane to expose the capabilities of network functions to external entities. The external entities may send requests on behalf of applications to 5G core network to influence on traffic routing and policy control. For example, an external entity may request NEF to deliver the policy/information for control of user data traffic routing. The NEF transfers the request of routing policy information to PCF which then forwards the routing policy information to SMF as part of PCC rules. PCC rules are used to control UPF to route specific traffic flows to the target edge data network as the external entities request.

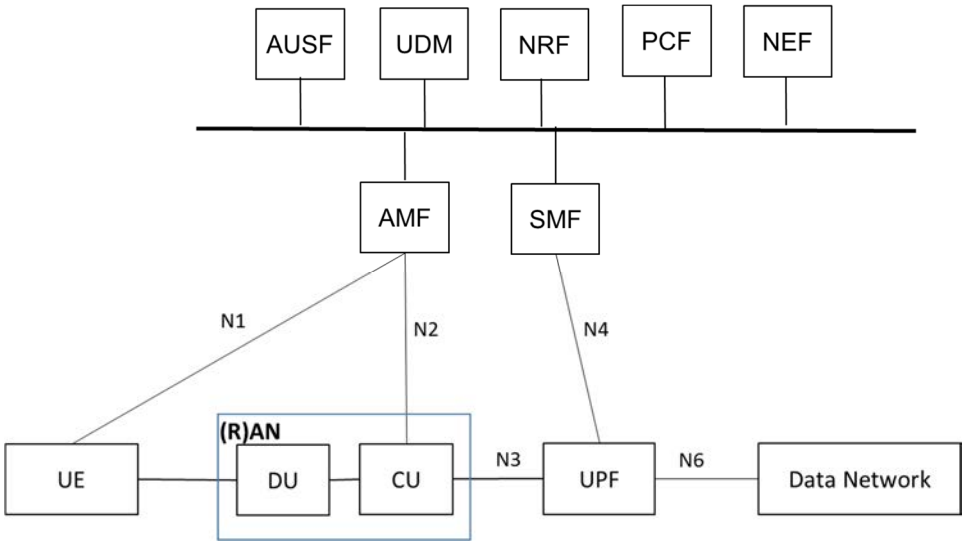


Figure A.35.1: 5G system architecture

The details of 5G network architecture are described in ETSI TS 123 501 [i.22] and ETSI TS 123 502 [i.23].

A.35.2 Use of Multi-access Edge Computing

The MEC system provides orchestration of infrastructure resource required by an application, instantiation of application, configuration of application rules based on the application description. When MEC system is deployed in 5G networks, it is essential for applications to expose to the 5G network the traffic steering control information. As applications are managed and orchestrated by MEC system, it is reasonable for MEC system to provide the support of interaction with 5G system on behalf of the applications. Right now, MEC system reference architecture is divided into MEC system level and MEC host level. The system level management components could be centralized and deployed for easily communicating with outside entities. For example, OSS receives requests from CFS portal. User application lifecycle management proxy receives requests from UE application. When being deployed in 5G, MEC needs to support providing 5G network of the traffic steering and policy control information of applications. Therefore it may need some enhancement in MEC system level management to communicate with the 5G NEF. By providing traffic steering information, MEC can influence the specific user traffic flow routed from the 5G network to applications running on specific MEC host.

A.35.3 Related requirements

- [Framework06]
- [5GCoreConnect-001], [5GCoreConnect-002], [5GCoreConnect-003], [5GCoreConnect-004]

A.36 In-vehicle MEC hosts supporting automotive workloads

A.36.1 Description

Today's passenger vehicles incorporate a diverse embedded computing environment, responsible for handling various functionalities of different nature. Such an environment is composed of processing units and processes, where, information is exchanged by means of specific industrial message buses, however it is rather complex, hardly reconfigurable and also highly specialized in order to cater to dissimilar functions. To remedy such issues, the proposed use case consists in the availability of in-vehicle MEC hosts supporting automotive workloads encountered in a passenger vehicle. Such workloads may be tailored to several similar or diverse functions (e.g. relevant to safety, telematics, high resolution maps for navigation, as well as video and other infotainment applications) impacting different On Board Units (OBUs), for instance, the Engine Control Unit (ECU) of a passenger vehicle. As an example, Figure A.36.1 illustrates a system scenario, according to which, two passenger vehicles running different applications, are connected to a given radio node (cellular connectivity). Each application is running on a MEC host embedded within the corresponding passenger vehicle.

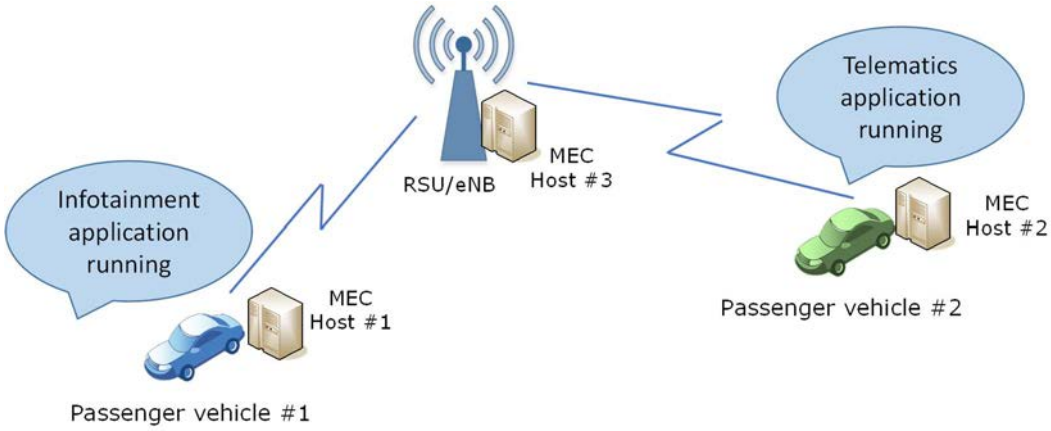


Figure A.36.1: Exemplary case of passenger vehicles each of which embeds a MEC host; the two passenger vehicles are running different applications

A.36.2 Use of MEC

As a recent trend in automotive industry is to develop the software architecture utilizing less processing units and encompassing more open operating systems, MEC technology can add constructively to such a trend as it offers an open, standardized environment for efficiently integrating applications running on a passenger vehicle. Additionally, MEC architecture, materialized by means of MEC hosts deployed on-board passenger vehicles, can offer content storage and memory capabilities and can enhance contextual awareness via exploiting radio network, location, and/or any other information relevant to the changing environment during journey time. It is noteworthy that the fluctuating connectivity conditions an in-vehicle MEC host may experience, together with its possibly limited processing, memory and storage capabilities and vehicle ownership aspects may impact its efficient management.

Among the functionalities for in-car MEC hosts, are the following:

- Hosted MEC applications running different types of workloads, e.g. Machine Learning (ML), data analytics, sensor measurement fusion from vehicles and the environment, privacy enforcement for data streams destined to a cloud (e.g. face blurring in video streams from on-board cameras), etc. Different MEC applications can either share data directly, or also through the MEC V2X API.
- Offloading processing-demanding tasks from vehicles to the network, e.g. relevant to computation-hungry applications such as Augmented Reality (AR), Virtual Reality (VR), Artificial Intelligence (AI), etc.
- Providing a common application framework for independent deployment across service providers, through the adoption of interoperable RESTful APIs, thus, also enabling cost-effective and efficient application lifecycle and V2X service provisioning.

A.36.3 Related requirements

- [Framework-05]
- [AppEnvironment-01], [AppEnvironment-04]
- [Connectivity-01], [Connectivity-03]
- [V2X-05], [V2X-06], [V2X-07]

A.37 Future Home

A.37.1 Description

Industry analyst forecasts, such as [i.26], predict the Future Home to be dominated by managed services. In-home devices and services offered via a subscription from a provider such as, cable operator, mobile operator, utilities, security providers, over-the-top players (Amazon, etc.), etc. Industry research groups (such as Cables Labs, [i.27], [i.28], [i.29] and [i.30]) envision Future Home applications, such as Mixed reality gaming and media, VR over distance, Holographic education, Health management, etc. that require a combination of low-latency/high-bandwidth communications, supported by local in-home edge computing, that also interfaces and interacts with remote applications and services.

The long-term vision of the Future Home is driven by a primary use-case that covers mixed-reality, interactive gaming. This is a representative use case of the other Future Home use cases and applications [i.27].

In a home, a set of users (e.g. a family composed of parents and kids) engage in an immersive game. The game relies on a headset that every player wears. The headset is lightweight since the game requires that players can move easily and quickly, such as running from one room to another. Thus, the headset is a wireless device, with minimal compute capabilities. Sensors might be embedded in the headset (or otherwise positioned on the player), including one or more cameras, that capture the player's viewpoint. Users may wear a neckband power unit to supply headset with power.

Even though the headset is lightweight, the headset still requires a board range of functionality/components, including wireless receiver(s)/transmitter(s), rendering engine, mixed-reality display, memory, CPU, etc. In addition to the headset, it may be possible to utilize other devices and resources that a player may be carrying or wearing. This includes the players smartphone.

From the perspective of a single player, the headset projects a virtual environment on top of the actual home environment. Both the virtual and physical environments are perfectly aligned; walls, doors and bigger objects appear in the virtual environment as part of the game, but textures, etc. are replaced with game content/context. For example, a futuristic space-ship look applied to all walls and objects of the home. Other players also appear in the virtual environment, but their clothing and appearance are adapted according to the game context. The positions of users and their movements are perfectly modelled so that a user's arm or finger can be used to interact with the virtual environment. The position of objects and their movements are also perfectly modelled, e.g. it is possible for a user to move an object such as a chair and these moved objects are modelled and moved accordingly in the game virtual environment. From the perspective of the headset, virtual and real players are perfectly aligned; real and modelled objects are also perfectly aligned.

Figure A.37.1: Future home scenarios

The game is played within predefined boundaries: while certain rooms and locations of the house can be used for the game, others (such as the yard or the bathroom, home office, etc.) are not. Similarly, certain objects and persons are not part of the game even though they are physically located within the home. Players can select these boundaries, choosing what to include and exclude in a game instance.

The player also receives visual and audio notifications about other players leaving or joining the game. New players can easily join the game (at start or while playing). New players may include visitors to the home that are not typical occupants (e.g. friend, neighbour, or relative). A player can also navigate through different menus and items to select accessories for the game. Virtual accessories can appear on players' bodies or in the virtual environment perfectly synchronized with players' movements.

While some of the home in-habitants engage in the immersive game, others are not part of the game. These other, non-player users may use services or applications, such as teleconferencing or immersive education, that rely on the same network and system infrastructure. These other applications do not interfere with the game experience.

A.37.2 Use of MEC

Future homes will witness the co-existence of different kind of connectivity and access technology. Traditional MNO (5G and beyond), Cable operators (802 technology) may deploy connectivity solutions inside the home. The last mile can be provided by traditional cable operators or by MNO using wireless backhaul. The Customer Premises Equipment (CPE) may be owned by any of the service providers or users may outright buy and own such CPE. A generic customer owned CPE may support multiple access technology and connect to different last mile solutions. The CPE may also include Edge Computing capability. As business model evolves, the CPEs with edge computing capability may be owned by a single entity or multiple entities. An overlay network maybe created to provide connectivity service to the diverse compute and storage nodes.

Gaming service may be provided by MNO, Cable operator or other third-party Game service provider. The CPE inside home with Edge Computing capability will host some parts of the gaming service and interact with other services in the distant cloud.

As it is evident from the use case, the requirements to provide the service inside home, may need to support low latency and high throughput communication. Different kinds of devices and sensors may be present inside home. Some devices may have computing capability, including non-MEC computing resources (i.e. devices not under orchestration control by the MEC System). MEC Applications should be able to utilize those available computing capabilities, by distributing tasks on those resources. A typical task may be managing and processing multiple sensor outputs and generate immediate response. MEC system may provide capability via the MEC API framework to discover and utilize non-MEC computing resources. MEC System may also manage and allocate network resources to the devices and sensors to maintain low latency and high throughput communication. MEC System may support dynamic redirection, allocating QoS to application, allocating network slice per application, etc.

Modelling and 3D mapping of home requires a static model and a dynamic model. Video cameras and sensors, used to create the 3D VR model, may be mobile or static. These cameras may capture images of the surrounding and the players to create the VR environment. The dynamic model senses, captures and tracks moving elements. Then the dynamic model is imposed on the static model. Precise indoor positioning of static and moving objects is a key element of this game. Multiple sensors may track moving objects and provide it to the gaming application running inside home. MEC System may support precise indoor positioning and modelling by collecting data from the ambient environment through different sensors.

A.37.3 Related requirements

- [CustomerPremiseEdge-01], [CustomerPremiseEdge-02], [CustomerPremiseEdge-03], [CustomerPremiseEdge-04], [CustomerPremiseEdge-05]

A.38 Future Vertical Applications

A.38.1 Description

As enterprises develop and services increase, many branches are set up in different locations, and some staff often go on business trips. They require fast, secure, and reliable network connections with the headquarters. On traditional dial-up networks, they use phone lines leased by the Internet Service Provider (ISP) and apply for a dial string or IP addresses from the ISP. This results in high costs. Besides, leased lines cannot provide services for remote users especially the staff on business trips.

A Virtual Private Dial-up Network (VPDN) allows a private network dial in service to span across to remote access servers (defined as the L2TP Access Concentrator(LAC)).When a Point-to-Point Protocol (PPP) client dials into a LAC, the LAC determines that it should forward that PPP session on to an L2TP Network Server (LNS) for that client. The LNS then authenticates the user and starts the PPP negotiation. Once PPP setup has completed, all frames are sent through the LAC to the client and the LNS.

The Layer 2 Tunnelling Protocol (L2TP) is a Virtual Private Dial-up Network (VPDN) tunnelling protocol and expands applications of the Point-to-Point Protocol (PPP) to allow remote dial-up users to access the network of an enterprise headquarters.

Based on PPP negotiation, L2TP sets up tunnels between branch users and enterprise headquarters over the dial-up network, so that remote users can access the headquarters network. The PPP over Ethernet (PPPoE) technology further expands the application scale of L2TP and can establish L2TP tunnels between remote users and the headquarters over the Ethernet and Internet.

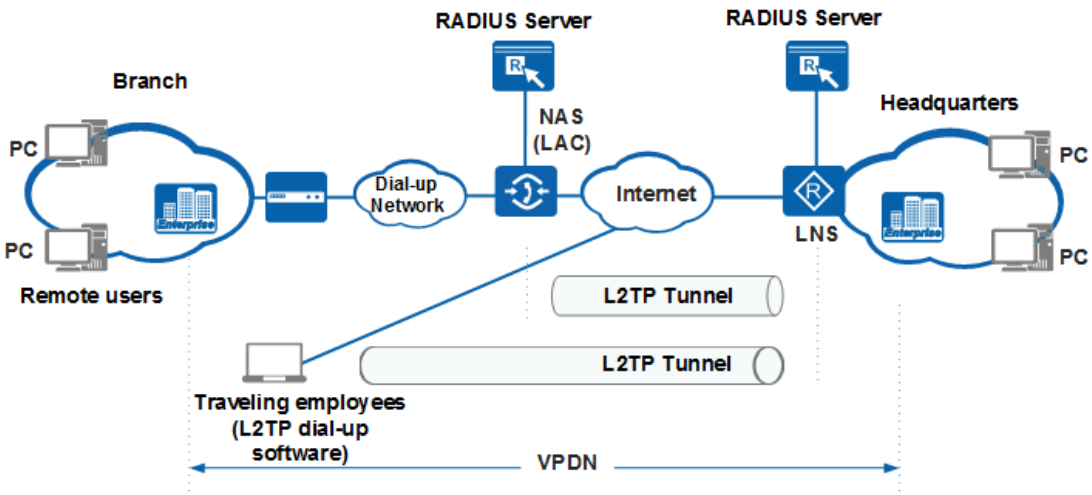


Figure A.38.1: Typical networking for constructing a VPDN network using L2TP

With the development of mobile network, the application of VPDN in 3G/4G is also very large. Many vertical industries based on mobile networks require operators to provide VPDN services, such as Banks, brokers, public sector governments, etc.

Figure A.38.2 shows the LTE L2TP VPDN networking architecture.

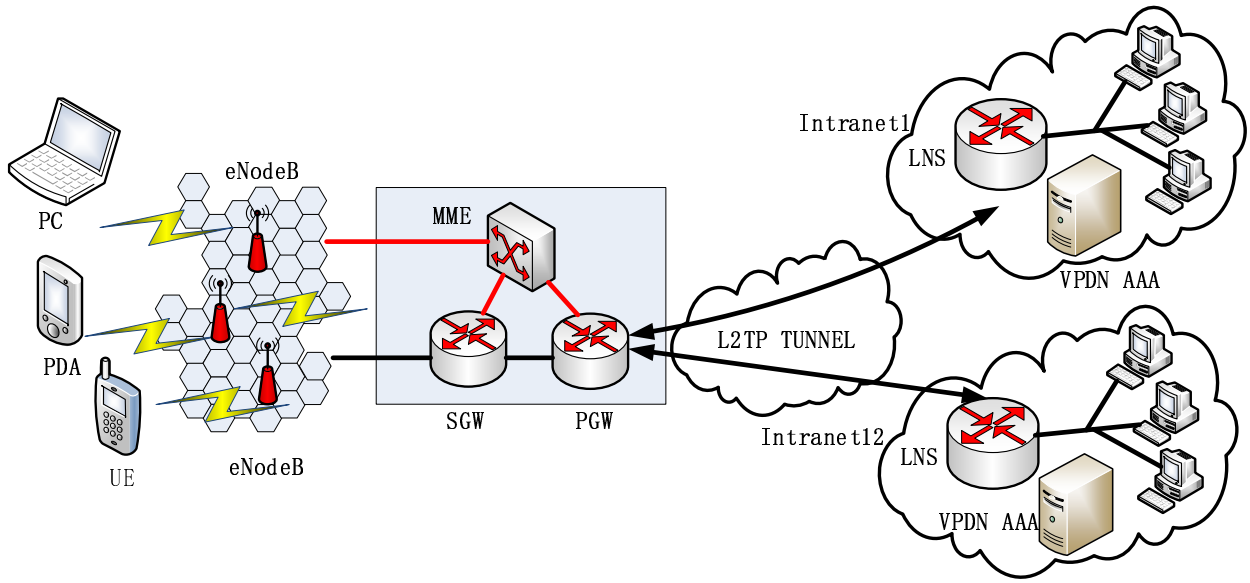


Figure A.38.2: LTE L2TP VPDN networking architecture

For 4G/LTE network, PGW establishes connection with VPDN platform or enterprise access gateway through L2TP tunnel of Layer 2 to provide customers with private network services. The terminal does not establish PPP connection with the network. PGW will act as the agent to negotiate and establish PPP connection with LNS, and perform L2TP session access for users.

With the commercial use of 5G, the application of 5G VPDN also begins to appear. Figure A.38.3 shows the networking of 5G VPDN L2TP. There are many 5G VPDN application messages on the Internet.

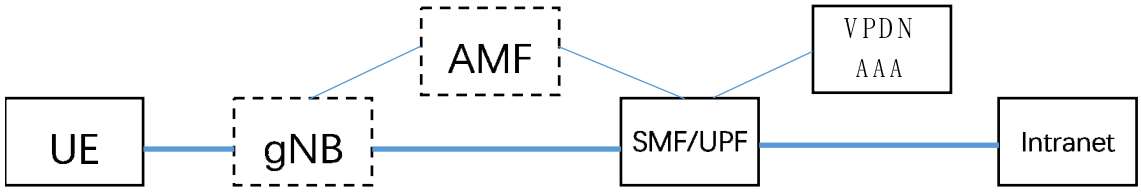


Figure A.38.3: 5G VPDN L2TP networking architecture

VPDN is very important for the Vertical Industries and Vertical Industries also need MEC with high speed, low latency. The integration of MEC and 5G VPDN will help Vertical Industries to improve efficiency quickly and effectively.

A.38.2 Use of MEC

MEC Hosts can provide hosting environment for vertical industry customers. If MEC group integrates VPDN functions into MEC, which means MEC Host simultaneously provides VPDN related functions, such as LNS and VPDN AAA, then it can simplify the work of customers. Customers do not need to carry out complex communication and coordination in front of MEC supplier team and VPDN team, only the MEC team is needed to solve the problems of MEC hosting and VPDN at the same time, which can greatly improve customers' user experience and promote the commercial scale of MEC. It will be easier for customers to connect with 5G or beyond, and the service based on 5G/MEC can be used more quickly.

The integration of MEC and VPDN is designed for industries with high security requirements, fast speed and low delay requirements. Anyway the integration of MEC and VPDN is beneficial to MEC.

When a VPDN service is forward by SMF/UPF to MEC system:

1) SMF/UPF acts as LAC: L2TP Access Concentrator.

2) MEC system acts as LNS: L2TP Network Server (Specifically, the MEC system here should be the MEC host).

So SMF/UPF should know the IP address of the LNS. SMF can get LNS IP address from VPDN AAA, if SMF is not preconfigured such kinds of information. Anyway how does SMF get IP is not the point of this article.

3) MEC System should support LNS AAA function for user authentication and authorization.

Figure A.38.4 is the procedure chart of MEC system supporting 5G VPDN.

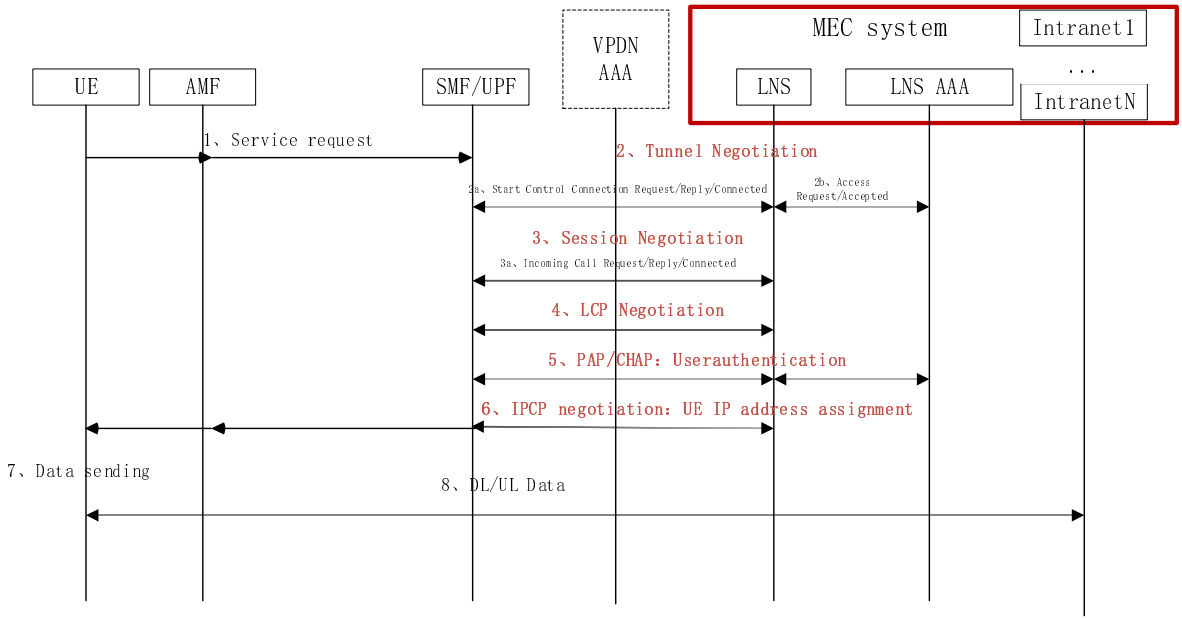


Figure A.38.4: Procedure chart of MEC system supporting 5G VPDN

1. 5G VPDN users send service request, launch PPP connection between it and SMF/UPF(LAC), carrying VPDN service special user name and password.

   1a. SMF/UPFLAC conducts authentication for users through VPDN AAA server, and verifies that users have VPDN service access authority.

   1b. VPDN AAA returns the corresponding tunnel attributes according to Request, including LNS IP, tunnel type, tunnel password, etc.

NOTE: 1a1b is conditional optional. If SMF/UPF is preconfigured with the corresponding information, these two steps do not exist.

2. SMF/UPF(LAC) initiates the request of establishing a tunnel according to the interaction with LNS, and L2TP tunnel between SMF/UPF(LAC) and LNS/MEC is established.

3. Session for users in the tunnel is established based on the negotiation between SMF/UPF(LAC) and LNS/MEC.

4. LCP Negotiation: SMF/UPF(LAC) sends LCP options and verification information obtained through negotiation with users to LNS.

5. PAP/CHAP: LNS initiates authentication request for user account to LNS AAA server.

6. IPCP negotiation: LNS assigns IP address and relevant information to users.

7. 5G VPDN Users initiate the data service.

8. UL/DL Data: SMF/UPF(LAC) routes the user data to the enterprise network deployed in MEC through L2TP tunnel.

A.39 V2X multi-stakeholder scenario

A.39.1 Description

Category: operator and third-party services

This use case includes a typical MEC federation scenario for V2X services as illustrated in Figure A.39.1, where multiple MNOs, multiple OEMs, and multiple MEC systems are involved. In the scenario, V2X application client instances may be running on vehicular UEs connected to MNO's network which is equipped with a MEC system. Such V2X application client instances, hosted by Vehicular UEs connected to different MNOs' networks, may communicate with each other via MEC application instances hosted in the MEC system.

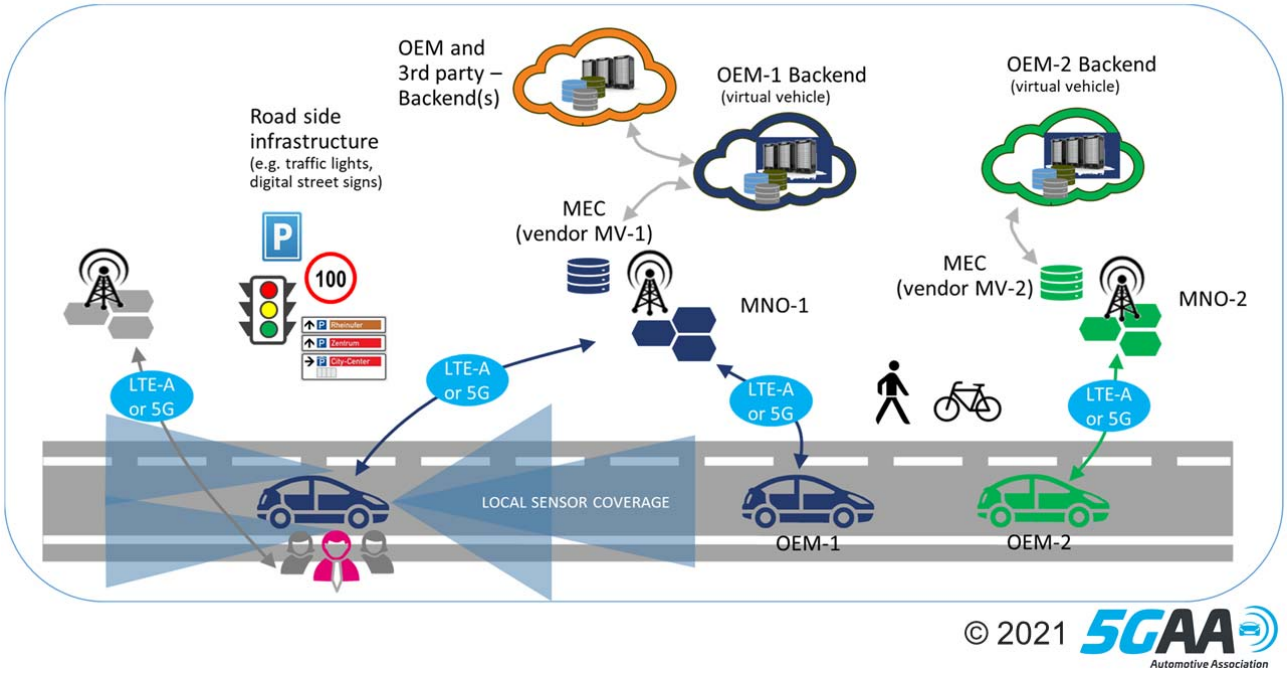


Figure A.39.1: Typical V2X multi-stakeholder scenario
(Source: 5GAA member's symposium in Turin, November 2019)

This use case also includes another scenario where a car moves across coverage areas of different MNOs. As illustrated in the figure the V2X application client, hosted by the vehicular UE connected to MNO 1's network, communicates with an application instance running on a MEC host. When the vehicular UE moves into the coverage of MNO 2's network, the service is expected to continue via MNO 2's network. The quality of service is also expected to be the same as when the vehicular UE connected to MNO 1's network.

A.39.2 Use of MEC

An application developer has a commercial relationship with MNO#1. Through the federation agreements, it is possible to also deploy the application developer's App in the MEC systems of MNO#2, MNO#3 to access their respective subscribers. Through its existing federation agreements, MNO#1 provides capabilities to allow the App developer to use an appropriate deployment approach based upon their commercial strategy.

A possible use case for MEC federation can be associated to a national roaming like scenario where vehicular UEs of MNO#1 could utilize the services offered by the MEC system of MNO#2 if this operator has a complementary coverage footprint. A vehicular UE is the subscriber of MNO#1 but the "best" edge location (e.g. in terms of latency) for the MEC App to be used is in the MEC system of MNO#2. The MEC system of MNO#1, through its federation agreement, identifies that the best edge location is in MNO#2. Then, the MEC system of MNO#1 redirects the App to the MEC system of MNO#2 to ensure the best possible service.

A.39.3 Related requirements

- [Federation-01], [Federation-02], [Federation-03], [Federation-04], [Federation-05], [Federation-06]

A.40 Multi-player immersive AR game

A.40.1 Description

Augmented Reality (AR) provides an interactive experience of a real-world environment mixed with computer-generated perceptual information and contents.

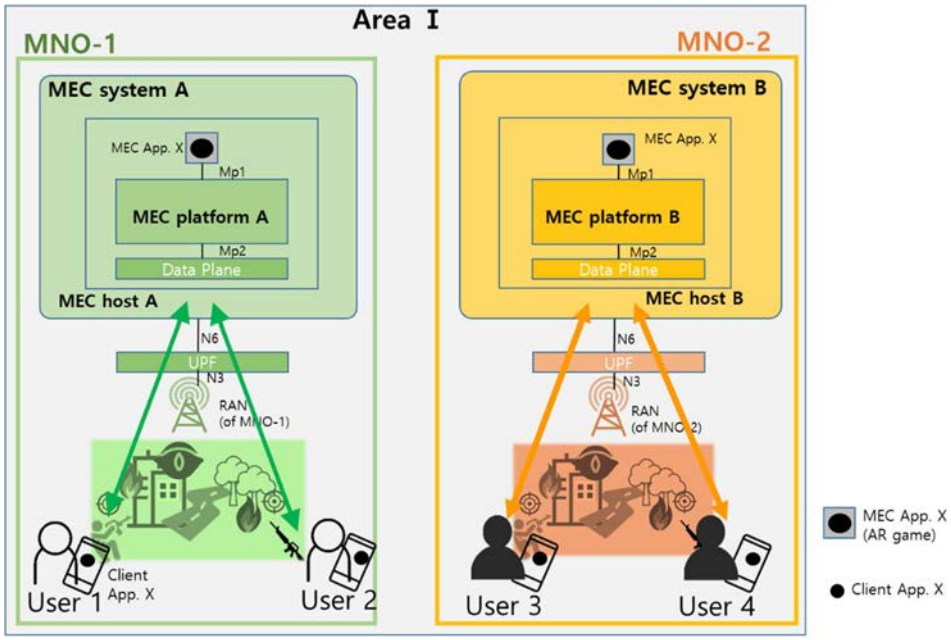
Entertainment looks to become one of the biggest applications of immersive AR content. Sport, music, etc. applications will target the attendees of a specific event to provide on-site entertainment services. Also, this introduces a new class of games, in which the physical environment, where the users are located, becomes an integral part of the game.

AR games incorporate diverse scenarios based on real-world settings and users' context such as viewpoint and player actions to provide them with fully immersive experience. Network latency and data rate play critical roles in delivering uninterrupted gaming experience. In this regard, one of the biggest hurdles in expanding AR applications widely is the need for E2E QoS assurance with high-bandwidth and low-latency. Battery capability of the mobile device is another indispensable consideration because running AR applications requires intensive computing resource use which results in massive battery consumption.

However, with the emergence of 5G and MEC, those are becoming less and less of obstacles. MEC is envisioned as a promising means to deliver better Quality of Experience (QoE) for immersive AR applications by reducing the delay and by addressing computation-intensive and battery-consuming tasks offloaded from the mobile devices.

Here, in this use case, a location-based immersive AR game is considered, whose scenario is designed to be played by all players at a specific geographical area. MEC fits well to these kinds of location-based immersive AR games in a sense that they are played by users in a certain location.

Without a MEC federation, however, there is a limitation in providing interactive AR application with users connected to different MNOs. For example, a multiplayer interactive AR game can be supported only when the users joining the game are connected to the same MNO. Users of different MNOs cannot join the multiplayer interactive AR game even when they are located nearby. This scenario is illustrated in Figure A.40.1.



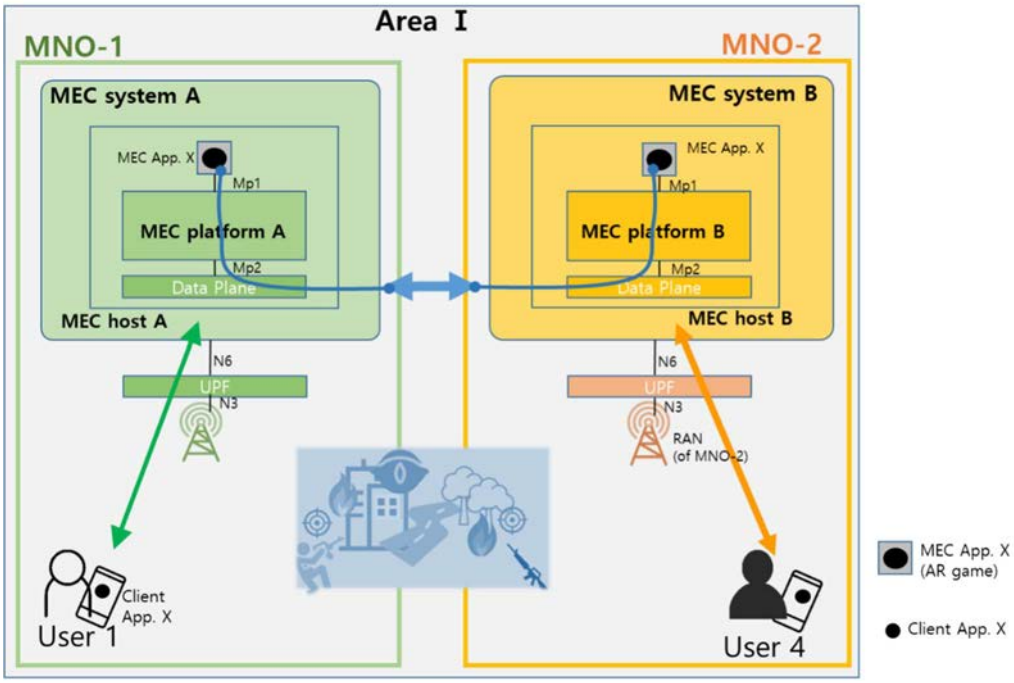
NOTE: In this environment:
- User 1 and user 2 of MNO-1 can play together by the help of MEC platform A.
- User 3 and user 4 of MNO-2 can play together by the help of MEC platform B.
- User 1 and User 4 connected to different MNOs cannot play together even when they are located nearby.

Figure A.40.1: Illustration of a multiplayer interactive AR game scenario without a MEC federation

A.40.2 Use of MEC

By a MEC federation, a multiplayer interactive AR game can be enjoyed by users connected to different MNOs and this scenario is illustrated in Figure A.40.2. Two options may be possible in incorporating multiplayer interactive games under MEC federation environment.

The first option, illustrated in Figure A.40.2, is to coordinate multiple MEC application instances of same kind where each of them is providing game service to the users connected to an MNO equipped with its respective MEC system.



NOTE: Users of different MNOs, user 1 of MNO-1 and user 4 of MNO-2, can join a multiplayer interactive AR game and play together. The two AR game MEC application X instances coordinate for real-time synchronization.

Figure A.40.2: Illustration of (Option 1) a multiplayer interactive AR game scenario under a MEC federation

In Figure A.40.2, the two MEC application Xs instantiated on MEC hosts of MEC system A and MEC system B respectively, communicate and coordinate together for synchronizing the game scenario. Information to be exchanged between the two MEC applications for coordination mostly include users' game play actions such as players' position, movement, direction, game control and the status of game contents virtually created.

The coordination and synchronization mechanism are specific to application implementation. However, the basic idea of how the applications are associated is represented below since it is closely related to a MEC federation.

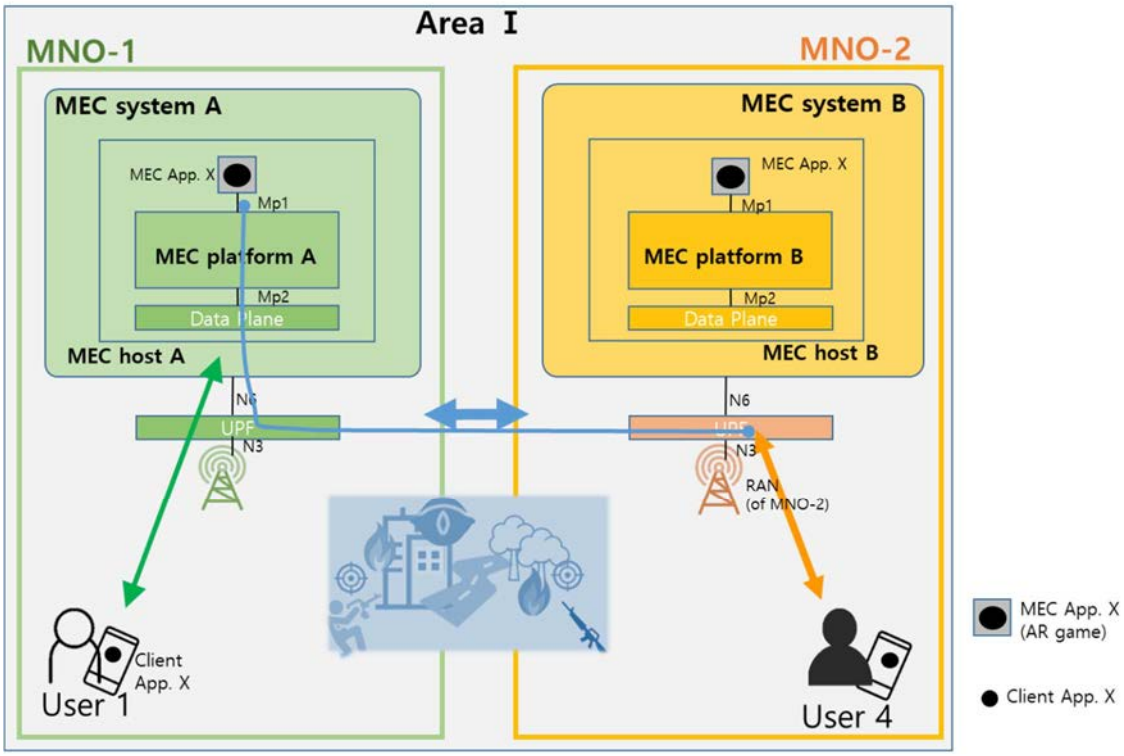
A user - e.g. user 1 - is a leader and needs to create a "multiplayer game room" to enjoy a multiplayer mode on a game server running on MEC host, MEC host A in this case. The leader can set a secret key for the multiplayer game room and share it with the desired users he wants to play together.

Thereafter, the MEC application X instantiated on MEC host A transfers the "multiplayer game room" information to other MEC application X instance on the other MEC hosts within the MEC federation, MEC host B in this example.

The desired user - user 4 in this case - can enjoy the multiplayer game by entering the "multiplayer game room" when he connects to the game server, i.e. the MEC application X running on MEC host B in this case.

Following MNO agreement, there exists a direct IP network between the associated MEC systems owned and operated by different MNOs.

In the other possible option, as illustrated in Figure A.40.3, one main application instance plays the main role in providing the game scenarios to all the users who joined the multiplayer mode including users connected to different MNOs.



NOTE: In this environment, users of different MNOs, user 1 of MNO-1 and user 4 of MNO-2 can join a multiplayer interactive AR game and play together. The MEC platform B switches the traffic from user 4 for MEC application X to MEC platform A.

Figure A.40.3: Illustration of (Option 2) a multiplayer interactive AR game scenario under a MEC federation

In Figure A.40.3, MEC application X running on the MEC host A of MNO-1, is the main application instance. This may be decided by the MEC application instance where a user - the leader, user 1 in this case - creates a multiplayer game room. Thereafter, this main instance - in this case, the MEC application X on MEC host A - transfers this information to other MEC application X instantiated on the other MEC hosts of the MEC federation, MEC host B in this example. The MEC application X running on MEC host B needs to set a traffic rule so that the traffic from user 4 to it can be switched to the main MEC application X instance - the one running on MEC host A in this case. In this way, both user 1 and user 4 can enjoy the multiplayer mode together while being served by MEC application X running on MEC host A. Following MNO agreement, there exists a direct IP network between the UPFs of different MNOs within the MEC federation.

A.40.3 Related requirements

- [Federation-07], [Federation-08], [Federation-09]

A.41 Holographic Type Communications

A.41.1 Description

With the full commercialization of 5G, the quality of communication services has been comprehensively improved. At the same time, holographic technique is getting mature, and the holographic communication business will usher in explosive growth.

Holographic communication is a new type of communication. It uses holographic technology to capture images of people and surrounding objects in remote locations, transmits holographic data through the network, uses laser beam projection at the terminal, and re-constructs the hologram in real time. Figure A.41.1 shows the holographic communication network model. Computing and transmission are the two key points of holographic service.

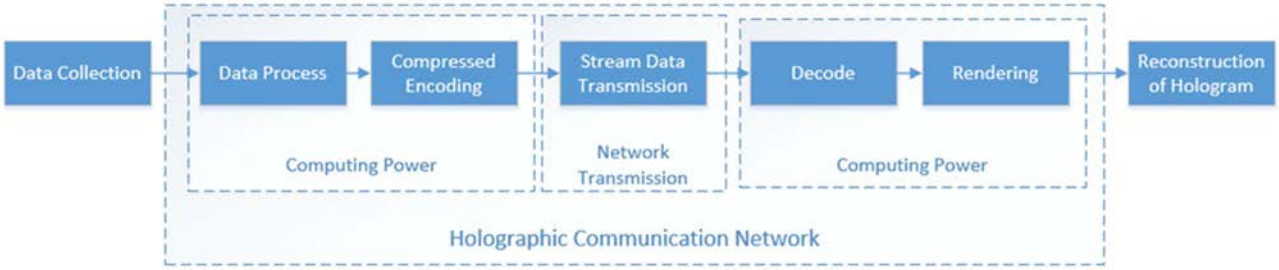


Figure A.41.1: Holographic communication network model

As shown in Figure A.41.1, the hologram needs to be encoded and compressed for network transmission, decoded and displayed at the terminal. Due to the huge amount of information and data contained in the hologram, the calculation time is too long, in addition to bringing a huge bandwidth burden, it will also cause a high Motion To Photons (MTP) delay.

If the MEC can be applied, it will greatly help the holographic communication. By placing the computing requirements of holographic communication on the MEC host, the burden on the terminal device (e.g. the computing and data storage) can be offloaded to the edge network thus the cost and power consumption of the terminal device are reduced. It also reduces the MTP delay and improves the quality of holographic communication.

In addition, if the MEC and UPF can be deployed closely to the access network, or even MEC and UPF can share some infrastructure with RAN, it will greatly shorten the transmission distance of holograms from the terminal to the network, reduce transmission loss, and improve the quality and effect of the overall communication.

A.41.2 Use of MEC

These holography-enabled terminal devices are assumed to be able to connect to MEC applications and maintain service continuity as users move. The MEC host uses general-purpose hardware, where specific network functions (e.g. on-premises UPF and RAN) can be instantiated to form an edge network to serve the UEs with extreme connection requirements (such as real-time high-definition holographic communication). The MEC host can have various forms to support holographic services with low latency and large bandwidth. Such as Network functions (e.g. on-premises UPF and RAN) and MEC are co-located or share the infrastructure. In this case, in addition to the basic edge computing services, the co-located network functions can provide some network capabilities, which can help edge network to provide extreme connection and computing services for holographic services.

The scenarios are shown in Figure A.41.2.

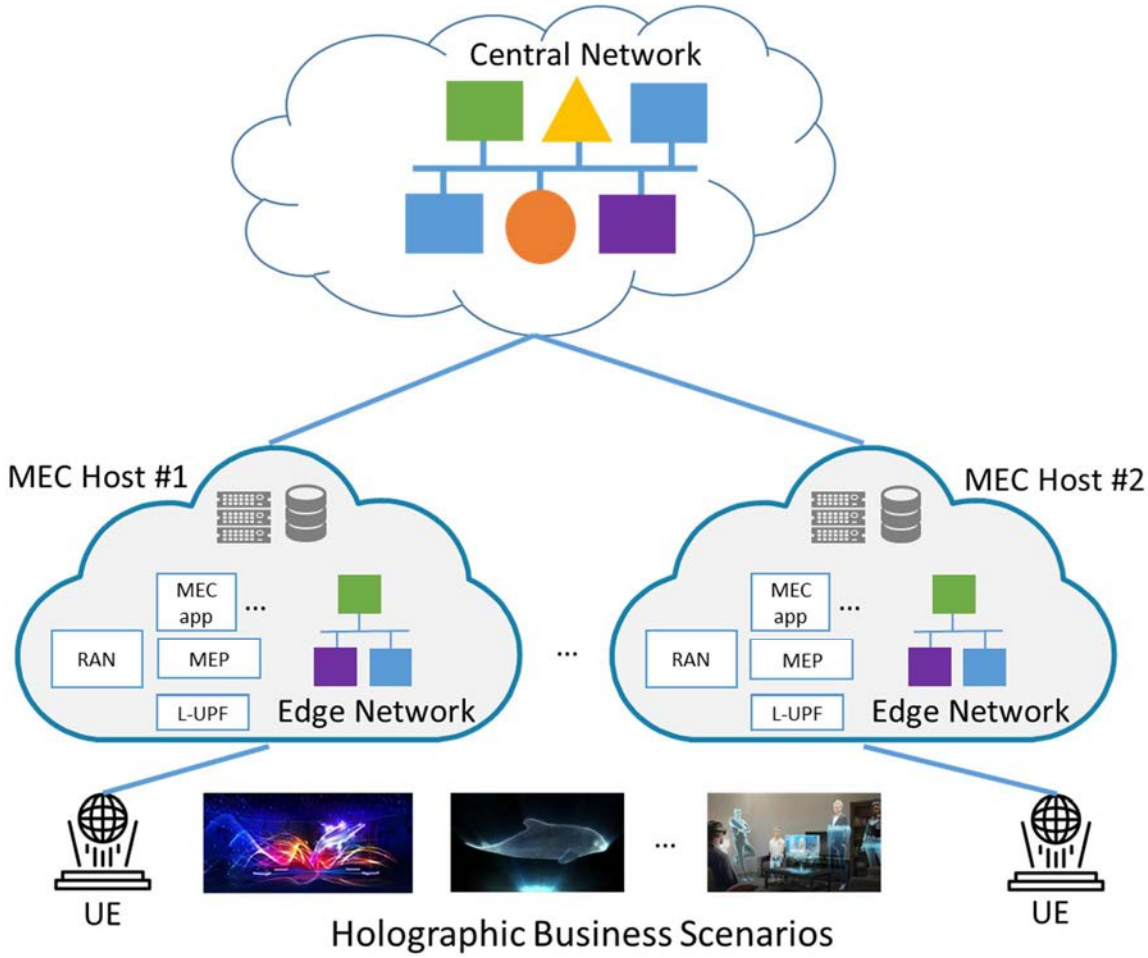


Figure A.41.2: Example diagram of holographic service deployment based on MEC

A.41.3 Related requirements

- [HTC service -01], [HTC service -02]

A.42 MEC Security Monitoring and Management (SMM)

A.42.1 Description

Category: operator and third-party services

Like any digital technology system, MEC may be susceptible to cybersecurity attacks by adversaries who seek to exploit and take advantage of system vulnerabilities for their own personal goals or objectives. One strategy to mitigate and detect such security threats for MEC is through the deployment of a SMM system.

ETSI GR MEC 041 [i.31] describes a scenario where an IoT botnet initiates a Distributed Denial of Service (DDOS) attack onto the MEC system. The DDOS attack causes a MEC application with no pre-defined resource usage limit to consume a large, disproportionate amount of virtual infrastructure resources, causing other MEC applications to be unable to obtain the resources they require to function properly. An SMM system resource usage could detect this anomaly, and request the MEC system to take appropriate actions such as terminating the application instance.

A.42.2 Use of MEC

The following terms are defined for Security Monitoring and Management (SMM):

- Security Monitoring specified in ETSI GS NFV-SEC 024 [i.32]: Functionality that collects and performs analysis of relevant events from across the MEC system which allow the SMM system to make informed security management decisions.
- Security Management specified in ETSI GS NFV-SEC 024 [i.32]: Functionality that applies security policy to a MEC system based on both predefined default policy and active analysis of information provided through security monitoring.
- SMM System: A system that implements Security Monitoring and Security Management for the MEC system.
- MEC System entity: Any MEC system functional element in the Multi-access edge system reference architectures of ETSI GS MEC 003 [i.33] (e.g. MEO, MEP and MEC apps).
- SMM alert: notification that a specific attack has been directed at the MEC system as determined by the SMM system based upon Security Monitoring.

SMM system support for MEC provides the MEC operator additional visibility into the MEC system and the ability to detect anomalous behaviour or activity. The heightened awareness of the MEC system through monitoring and detection allows the operator to respond to potential security threats in a timely manner. The operation of SMM can be described using the following basic components:

- Security Profile: A set of security-related data a MEC entity can deliver to the SMM system as well as what security directives it will respond to and how.
- Security Directive: A set of actions a MEC entity can perform in response to an SMM alert notification.
- Security Policy: Configuration information describing the actions (i.e. directive) undertaken upon determination that a certain event(s) occurred, based on the data collected (according to the security profile).

Examples of data that could be part of a security profile include:

- Actual MEC application resource usage (e.g. compute, storage, network from VIM); consistency check with pre-defined usage limits in MEC AppD (as described in ETSI GS MEC 010-2 [i.34]) from MEO.
- Logs of security-related event types of a MEC entity involving user password changes, failed logons, failed access, security or privacy attribute changes as described in NIST SP800-53v5 [i.35].
- Telemetry data such as statistics, events, records, and configuration data as described in IETF RFC 9232 [i.36].
- MEC application security events such as instantiation, attestation, termination, deletion, unsuccessful access attempts, and generated errors or exceptions.
- Logs of security-related event types of a MEC entity involving importing, exporting, creation and deletion of certificates and keys.

SMM system use for MEC consist of collecting security monitoring related data from MEC entities, according to their security profile. Then, the SMM system analyses that data, looking for events and patterns that may indicate the presence of an adversarial activity. The SMM then applies the relevant security policy, which may result in security directives being sent to the MEC entity that needs to take an action as per policy (e.g. MEC application, or MEO, to trigger termination of possibly compromised application instance).

The SMM details described above are intended to be configurable to allow maximum flexibility and personalization of how the MEC operator may choose to deploy and run the SMM system.

A.42.3 Related requirements

- [SMM-01], [SMM-02], [SMM-03], [SMM-04], [SMM-05], [SMM-06], [SMM-07]

A.43 Cryptographic attestation for MEC applications

A.43.1 Description

Category: operator and third-party services

Like any digital technology system, MEC is susceptible to cybersecurity attacks by adversaries who seek to exploit and take advantage of system vulnerabilities for their own goals or objectives. Authentication, authorization and encryption are traditionally the basis of secure data and control flow on a MEC system. These assume that the peers of every message exchange are implicitly trustworthy. However, MEC applications could become compromised as described in ETSI GR MEC 041 [i.31] through multiple means such as software exploits, privilege escalations, or leaked credentials, to cite a few. These may lead to various adversary actions such as data exfiltration and/or establishment of a backdoor and thereby subvert other security measures and practices. It is therefore useful to condition the operations of MEC applications on a positive trust assessment to complement traditional authentication and authorization flows. It is beneficial to securely verify the provenance of MEC applications with respect to an established and trusted baseline state, at various stages in the App lifecycle management.

One strategy to address this gap in MEC is through the deployment of a cryptographic attestation framework.

A.43.2 Use of MEC

The following terms are defined for attestation:

- Attestation: The process of providing a digital signature for a set of measurements securely stored in some medium, and then having the requester validate the signature and the set of measurements (this definition is based on NIST CSRC [i.37]).
- Measurement: Also referred to as a "software integrity measurement", is a digest computed over critical system components, e.g. firmware, kernel modules, executables and/or other programs.
- Cryptographic attestation: Employment of cryptographic protocols to authenticate verification data (e.g. signatures over measurements or code) using a root of trust technology.
- Root of trust: Highly reliable hardware, firmware, or software components that perform specific, critical security functions. They are inherently trusted, secure by design and provide a firm foundation from which to build security and trust (this definition is based on NIST CSRC [i.37]).
- Attester: An entity whose attributes shall be evaluated in order to determine whether the entity is trustworthy. (this definition is based on IETF RFC 9334 [i.38]).
- Relying party: An entity that depends on the validity of information about another entity. (this definition is based on IETF RFC 9334 [i.38]).
- Verifier: An entity that evaluates the validity of evidence about an Attester (this definition is based on IETF RFC 9334 [i.38]).

Following is a summary of the high-level workflow utilizing a cryptographic attestation framework. Measurements are collected from a target MEC application's software stack prior to its deployment on a MEC system and stored as reference values. Over the MEC application lifecycle, a relying party (e.g. the MEO) may request a trust assessment of a MEC application instance (attester). In servicing this request, measurements are securely taken of the software stack of the MEC application instance and attested using a root of trust entity. These measurements are presented to a verifier entity as evidence of the MEC application instance's current operational state. The verifier entity validates the authenticity of the received evidence and appraises the provided measurements against their reference values to determine whether the MEC application instance is in the intended state and thereby trustworthy. The result of this trust assessment is fed back to the relying party.

A.43.3 Related requirements

- [ATT-01], [ATT-02], [ATT-03]

A.44 MEC APP Gateway

A.44.1 Description

Category: operator and third-party services

Like any digital technology system, MEC systems may be susceptible to cybersecurity attacks by adversaries who seek to exploit and take advantage of system vulnerabilities for their own goals or objectives. One strategy to mitigate such security threats for MEC is to employ an APP Gateway (APP-GW) to ensure secure access to MEC applications by legitimate client applications.

Some MEC applications (e.g. V2X) have high security needs due to the sensitivity of associated content and/or the criticality of proper operation for legitimate users. For example, a vehicle-to-infrastructure edge service that provides hazard alerts in near real time to drivers can involve safety-of-life. Such a service collects information from vehicles and roadside sensors to recognize high-risk situations in advance and sends alerts and warnings to the vehicles in the area. It is essential for such information to originate from valid sources that reflect true and current local road conditions.

For this type of V2X MEC application, it is important to ensure that V2X sources are actually geographically located in the area that they are providing reports on. This capability could be implemented within the authentication and authorization process carried out by the APP-GW, for example, by leveraging a MEC device location service. In this way, attacks on the MEC (V2X) system by sophisticated adversaries located in other regions/countries can be mitigated. More generally, the APP-GW allows for customization (e.g. by leveraging other MEC services) of the authentication and authorization process towards a particular MEC application.

Client applications may seek to access MEC applications via various types of connections (5G, Wi-Fi®, wired) that have their own access control protocols at the lower layers. To mitigate client application access related potential security vulnerability, the APP-GW can provide a service (currently not specified by MEC) for authentication and authorization of client applications. This encompasses signaling that takes place before application-specific user traffic is exchanged, and is suitable for all MEC applications requiring this additional access control.

Most importantly, the APP-GW provides a straightforward mechanism for MEC application providers to specify their requirements for client application authentication and authorization (if any) while, at the same time, lifting the burden of secure implementation of such access control from the MEC application developer(s) within their MEC application. In this way, the MEC service provider/operator can ensure secure and consistent implementation of access control for all of its MEC applications. Additionally, the operator can monitor MEC application access by clients and potentially terminate connections that are identified as security threats (e.g. malware, spyware, privilege escalation, and lateral movement) to the MEC system.

A.44.2 Use of MEC

The operation of an APP-GW can be described as follows:

- APP-GW is configured by or via MEC management to use an AA entity or not, subject to the access control needs of individual MEC applications.
- The AA entity is configured by the MEC application provider for authentication and authorization of its users (details out of scope).
- APP-GW may be configured by or via MEC management to also utilize other MEC services as appropriate within the authentication and authorization process, based on MEC application needs.
- Client application obtains an access token from AA entity after it authenticates.
- Access token is stored securely on the device running the client application.
- Client application presents the access token when initiating MEC application access via APP-GW.
- APP-GW verifies the access token, potentially using the AA entity.

- Upon successful authentication and authorization, the APP-GW forwards traffic between client application and MEC application.
- The AA entity and interaction with the client application and APP-GW are out of scope of ETSI MEC specifications.
- MEC system monitors access from client applications via reports from APP-GW and directs APP-GW to terminate connections that are identified as potential security threats.

A.44.3 Related requirements

[AGW-01], [AGW-02], [AGW-03], [AGW-04], [AGW-05].

A.45 Authentication and Key Management for Applications (AKMA) function support

A.45.1 Description

Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS) is standardized in ETSI TS 133 535 [i.39] to enable applications to leverage the authentication of the UE performed by the 5GS and to use it for further authentication and authorization by an application and to bootstrap the necessary application security keys to the UE. For an application to support AKMA its Application Server (AS) component (complimentary to the UE hosted client application component) presents itself as an Application Function (AF) of the 5GS. Such an AF can interact with the 5G core in order to provide services. See clause 6.2.10 of ETSI TS 123 501 [i.22] for further detail and clause 4.2.2 of ETSI TS 133 535 [i.39] for the additional functional requirements of an AF supporting AKMA.

AKMA can be selected to be used between a UE and AF after completion of the 5GS primary authentication procedure (as required for UE access to a 5GS). It is then necessary to derive an AKMA Application Key (K_{AF}) that is specific to the UE and AF (i.e. the session key for encryption and decryption of the communication traffic). For access to an AF that is not anonymous, the UE is identified by its Subscription Permanent Identifier (SUPI) or Generic Public Subscription Identifier (GPSI) depending on the level of trust, e.g. the SUPI is not exposed to an untrusted AF.

With AKMA selected, the associated key material (AKMA Anchor Key (K_{AKMA}) with associated AKMA Key IDentifier (A-KID)) is generated in the UE and the AUthentication Server Function (AUSF). The UE stores the AKMA key material required for subsequent service requests with the AF. On the contrary, the AUSF need not store the AKMA key material it generates after it delivers it and the UE identifier to the selected AKMA Anchor Function (AAnF). Then when the UE subsequently initiates communication with the AF, the AF will obtain the required AKMA Application key (K_{AF}) and UE identifier from the appropriate AAnF (if the AF does not already have an active context associated with the A-KID received from the UE) by providing its AF identifier along with the A-KID that it received from the UE in the session establishment request. The AF will then provide K_{AF} to the UE.

ETSI TS 133 535 [i.39], clause 4.7, also describes the use of an Authentication Proxy (AP) between the UE (hosting the client application) and the AS. In such a scenario, the AP takes the role of the AKMA capable AF with the AS(s) being placed behind the AP. The AP role is to help the AS(s) execute AKMA procedures to save the consumption of signalling resources and AAnF computing resources, thereby enabling the AS(s) to delegate the security tasks. Furthermore, the AP provides assurance to the ASs that received requests originate from a Mobile Network Operator (MNO) subscriber that has been authorized. The interface (Ua*) between the UE and AP (acting as the AF) utilizes K_{AF} and can be HTTP based, with the AP acting as a reverse proxy to handle the communication between the UE and the AS. The interface (AP-AS) between the AP and AS is HTTP based.

A.45.2 Use of MEC

It is proposed that AKMA functionality can be applied to MEC, specifically that the MEC Platform (MEP) can support the AAnF function by acting as an AP between UE hosted client application and MEC hosted server applications. In such a deployment, the UE identifier, along with the K_{AF}, will be passed to the MEP (as an AF) in the AKMA Application Key Get response from the AAnF (see clause 6.2.1 of ETSI TS 133 535 [i.39]).

In such a deployment, the MEP acting as the AKMA AP may interact directly with the AAnF if it is within the MNO's trust domain, otherwise interactions are via the MNO's NEF. In the former case, the UE identifier obtained from the AAnF will be in the form of either a SUPI or GPSI according to local policy. In the latter case, it will be in the form of a GPSI (specifically in the form of an External Identifier that is an AF specific UE identifier, ETSI TS 123 501 [i.22]).

A.45.3 Related requirements

- [UEIdentity-07]

Annex B (informative): Operator trusted MEC applications

Operator trusted MEC applications can be viewed as extensions of the MEC platform functionality, such as allowing a tighter integration with the core network, by providing services to the MEC platform.

In addition to the MEC application capabilities, the operator trusted MEC applications will have advanced privileges to provide information to the MEC platform securely.

Due to the privileged role, it is required that such applications and the platform are mutually authenticated and authorized and that the communication between these entities cannot be eavesdropped on by third parties.

The role of the operator trusted MEC applications is not specifically to report on or modify the performance of the radio network but also to extend the functions of the existing trusted core network functions. The interface between such application and the core network elements are external to the platform. Some examples might be:

- distributed policy control;
- distributed quality of service;
- providing information on transport tunnel allocation.

History

Document history		
V1.1.1	March 2016	Publication
V2.1.1	October 2018	Publication
V2.2.1	January 2022	Publication
V3.1.1	April 2023	Publication
V3.2.1	February 2024	Publication
V4.1.1	June 2025	Publication