ETSI GS MEC 002 V3.1.1 (2023-04)

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-0002v311TechReq

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

Important notice

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

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

This Group 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 at https://docbox.etsi.org/Reference.

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

[i.1] ETSI 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] "Byte Caching in Wireless Networks". IEEE 32nd International Conference on Distributed Computing Systems. Franck Le; Mudhakar Srivatsa; Arun K. Iyengar Macau. China; June 2012.

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

[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; 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 (3GPP TS 23.501)".

[i.23] ETSI TS 123 502: "5G; Procedures for the 5G System (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.

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
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
MADP	Multiple Access Data Proxy
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
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 VNFs (Virtual Network Functions) 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.