ETSI GS MEC 003 V4.1.1 (2025-05)

Multi-access Edge Computing (MEC); Framework and Reference Architecture

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-0003v411Arch

Keywords
architecture, MEC

ETSI

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

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

Siret N° 348 623 562 00017 - 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 provides a framework and reference architecture for Multi-access Edge Computing that describes a MEC system that enables MEC applications to run efficiently and seamlessly in a multi-access network. The present document also describes the functional elements and the reference points between them, and a number of MEC services that comprise the solution. It finally presents a number of key concepts related to the multi-access edge architecture.

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.

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

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

[3] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV); Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

[4] ETSI GS NFV-IFA 008: "Network Functions Virtualisation (NFV); Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

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

[6] ETSI GS MEC 040: "Multi-access Edge Computing (MEC); Federation enablement APIs".

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] Void.

[i.3] OpenStack®: "OpenStack++ for Cloudlet Deployment".

NOTE: The OpenStack® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. ETSI is not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

[i.4] Void.

[i.5] ETSI GR MEC 017: "Mobile Edge Computing (MEC); Deployment of Mobile Edge Computing in an NFV environment".

[i.6] ETSI TS 123 501: "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 Release 17)".

[i.7] ETSI GR MEC 035: "Multi-access Edge Computing (MEC); Study on Inter-MEC systems and MEC-Cloud systems coordination".

[i.8] GSMA™ Official Document OPG.02: "Operator Platform: Requirements and Architecture", v6.0, February 2024.

[i.9] ETSI TS 123 558: "5G; Architecture for enabling Edge Applications (3GPP TS 23.558 Release 17)".

[i.10] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310 Release 17)".

[i.11] IETF RFC 9334: "Remote Attestation Procedures".

[i.12] ETSI GR NFV-SEC 007: "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".

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:

AGW API Gateway

NOTE: For client applications.

CFS Customer Facing Service

4 Overview

The present document presents a framework and a reference architecture to support the requirements defined for Multi-access Edge Computing in ETSI GS MEC 002 [1].

The framework described in clause 5 shows the structure of the Multi-access Edge Computing environment.

The reference architecture described in clause 6 shows the functional elements that compose the multi-access edge system, including the MEC platform and the MEC management, as well as the reference points between them.

The functional elements and reference points listed in clause 7 describe the high-level functionality of the different functional elements and reference points.

Clause 8 describes the high-level functionality of a number of MEC services, comprising the solution for Multi-access Edge Computing.

Annex A describes at a high-level a number of key concepts that underlie the principles used to develop the framework and reference architecture described in the present document.

5 Multi-access Edge Computing framework

Multi-access Edge Computing enables the implementation of MEC applications as software-only entities that run on top of a Virtualisation infrastructure, which is located in or close to the network edge. The Multi-access Edge Computing framework shows the general entities involved. These can be grouped into system level, host level and network level entities.

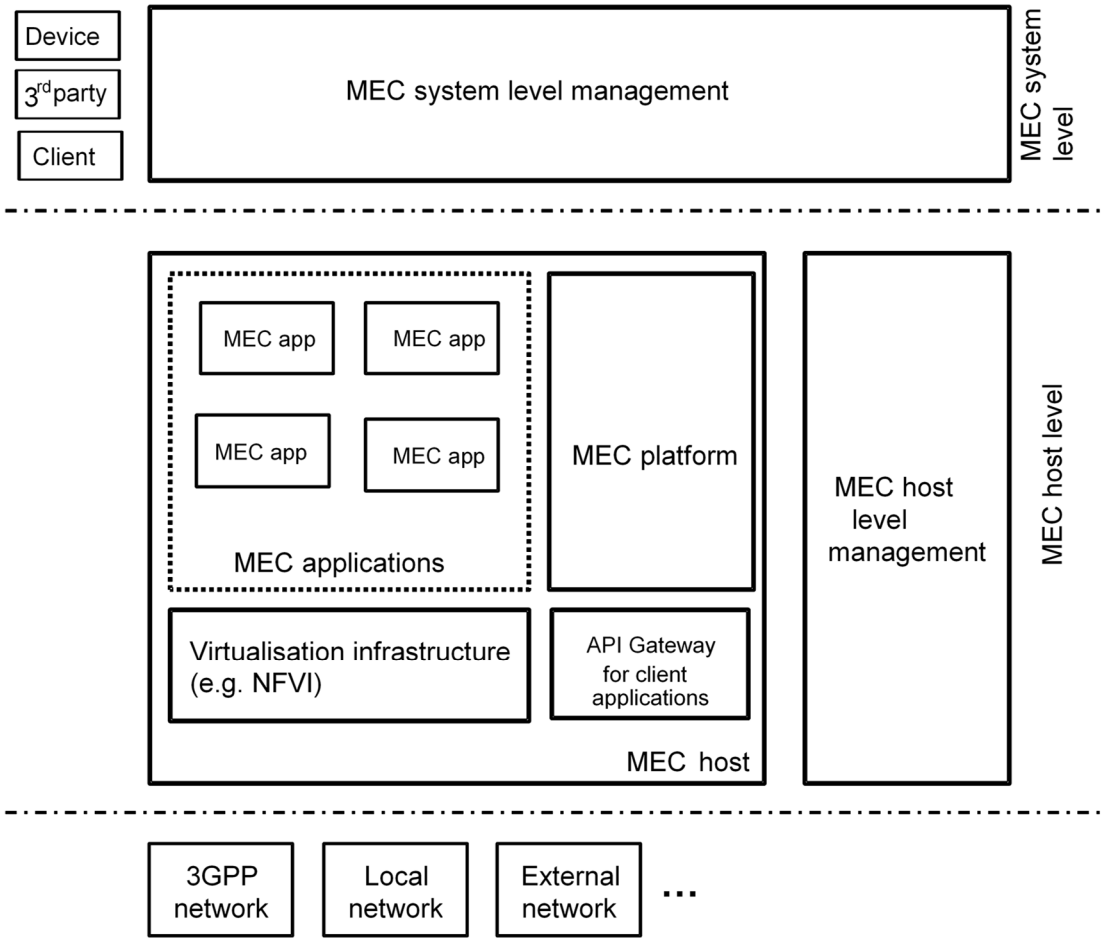

Figure 5-1: Multi-access Edge Computing framework

Figure 5-1 illustrates the framework for Multi-access Edge Computing consisting of the following entities:

- MEC host, including the following:
  - MEC platform;
  - MEC applications;
  - virtualisation infrastructure;
  - API gateway for client applications;

- MEC system level management;
- MEC host level management;
- external related entities, i.e. network level entities.

6 Reference architecture

6.1 Generic reference architecture

The reference architecture shows the functional elements that comprise the multi-access edge system and the reference points between them.

Figure 6-1 depicts the generic multi-access edge system reference architecture. There are three groups of reference points defined between the system entities:

- reference points regarding the MEC platform functionality (Mp);
- management reference points (Mm); and
- reference points connecting to external entities (Mx).

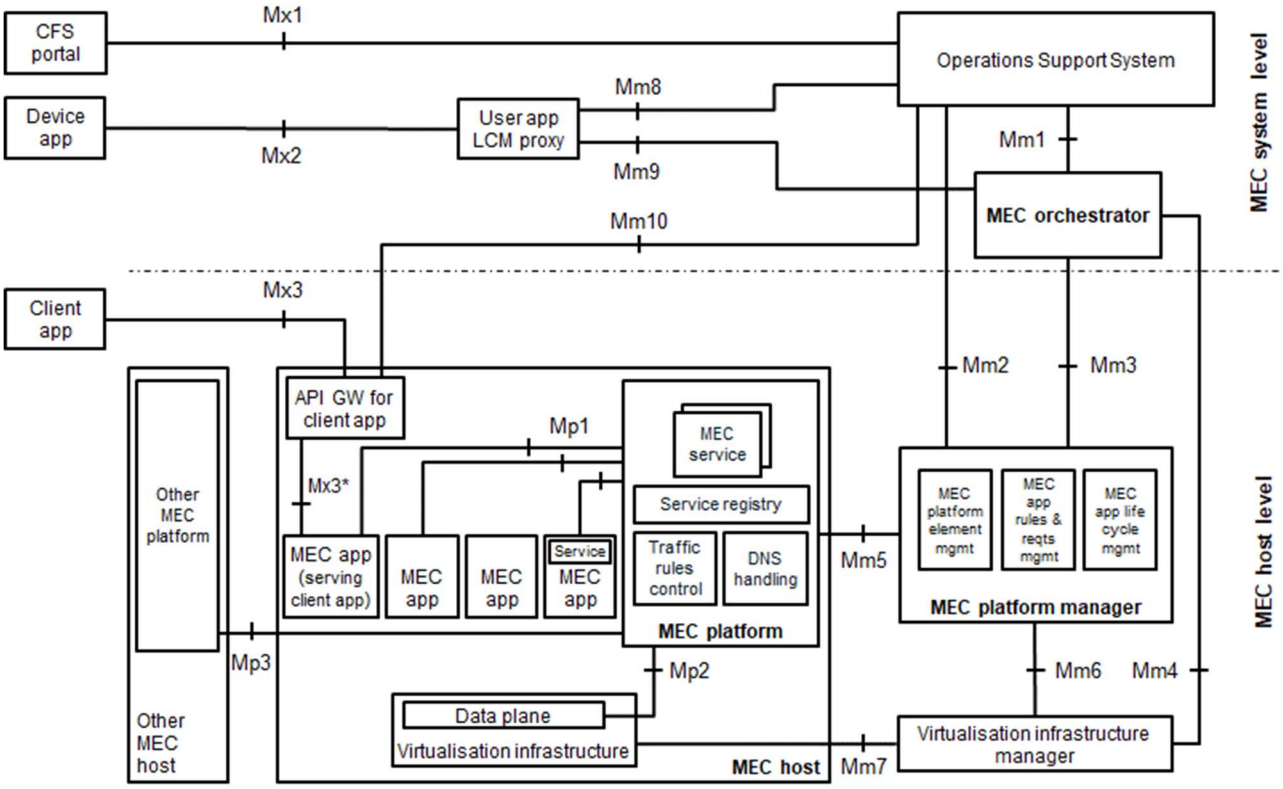

Figure 6-1: Multi-access edge system reference architecture

The multi-access edge system consists of the MEC hosts and the MEC management necessary to run MEC applications within an operator network or a subset of an operator network. Customer Facing Service (CFS) portal, device applications and client applications are external entities to the MEC system.

The **MEC host** is an entity that contains a MEC platform and a Virtualisation infrastructure which provides compute, storage, and network resources, for the purpose of running MEC applications. The MEC host is further described in clause 7.1.1.

The **MEC platform** is the collection of essential functionality required to run MEC applications on a particular Virtualisation infrastructure and enable them to provide and consume MEC services. The MEC platform can also provide services. The MEC platform is further described in clause 7.1.2.

MEC applications are instantiated and run on the Virtualisation infrastructure based on configuration or based on requests validated by the MEC management. MEC applications are further described in clause 7.1.3.

The MEC management comprises the MEC system level management and the MEC host level management.

The MEC system level management includes the **MEC orchestrator** as its core component, which has an overview of the complete MEC system. The MEC system level management is further described in clause 7.1.4.

The MEC host level management comprises the **MEC platform manager** and the **Virtualisation infrastructure manager**, and handles the management of the MEC specific functionality of a particular MEC host and the applications running on it. The MEC host level management is further described in clause 7.1.5.

The **API gateway for client applications** is an entity that controls access to MEC applications by client applications. The API gateway is further described in clause 7.1.10.

6.2 Reference architecture variant for MEC in NFV

6.2.1 Description

MEC and Network Functions Virtualisation (NFV) are complementary concepts. The MEC architecture has been designed in such a way that a number of different deployment options of MEC systems are possible. A dedicated Group Report, ETSI GR MEC 017 [i.5], provides an analysis of solution details of the deployment of MEC in an NFV environment.

In clauses 6.2.2, 7.1.8 and 7.2.4 of the present document, a MEC architecture variant is specified that allows to instantiate MEC applications and NFV virtualised network functions on the same Virtualisation infrastructure, and to re-use ETSI NFV MANO components to fulfil a part of the MEC management and orchestration tasks.

6.2.2 Architecture diagram

Figure 6-2 depicts a variant of the multi-access edge system reference architecture for the deployment in an NFV environment [2].

In addition to the definitions for the generic reference architecture in clause 6.1, the following new architectural assumptions apply:

- The MEC platform is deployed as a VNF.
- The MEC applications appear as VNFs towards the ETSI NFV MANO components.
- The Virtualisation infrastructure is deployed as an NFVI and is managed by a VIM as defined by ETSI GS NFV 002 [2].
- The MEC Platform Manager (MEPM) is replaced by a MEC platform manager - NFV (MEPM-V) that delegates the VNF lifecycle management to one or more VNF Managers (VNFMs).
- The MEC Orchestrator (MEO) is replaced by a MEC Application Orchestrator (MEAO) that relies on the NFV Orchestrator (NFVO) for resource orchestration and for orchestration of the set of MEC application VNFs as one or more NFV Network Services (NSs).

The new reference points shown in figure 6-2 are further described in clause 7.2.4.

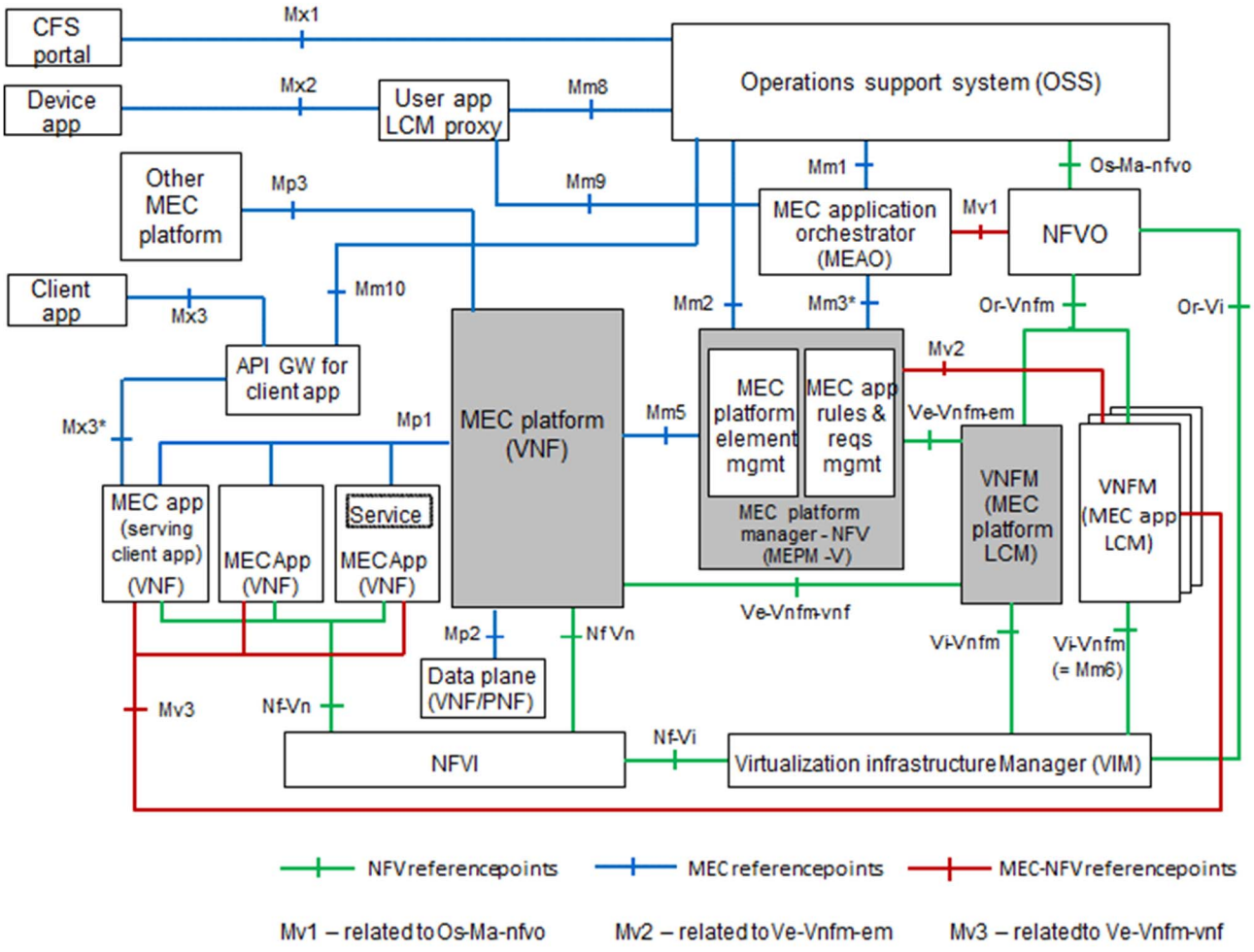

Figure 6-2: Multi-access edge system reference architecture variant for MEC in NFV

6.3 Reference architecture variant for MEC federation

6.3.1 Description

The MEC architecture has been designed in such a way that a number of different MEC system deployment options are possible. ETSI GR MEC 035 [i.7] provides an analysis of solutions for enabling inter-MEC system communication, as described in clause 9 of the present document. ETSI GR MEC 035 [i.7] also introduces the concept of a MEC federation, defined as "*a federated model of MEC systems enabling shared usage of MEC services and applications*" (see also clause 3.1 of [i.7]). In this environment, different stakeholders collaborate for joint business purposes, and "federate" their edge computing resources, by offering/exposing their MEC service capabilities, not only for mutual consumption, but also offering those to application developers and end customers (e.g. vertical market segments). The solutions identified by ETSI GR MEC 035 [i.7] are also influenced by the Operator Platform Requirements and Architecture (see GSMA™ Official Document OPG.02 [i.8]).

In clause 6.3.2 of the present document, a variant of the generic MEC architecture is presented that enables the establishment of a MEC federation and, through that, interworking between a MEC system and another MEC system or non-MEC system.

6.3.2 Architecture diagram

Figure 6-3 depicts a variant of the multi-access edge system reference architecture for the deployment in a MEC federation.

In addition to the definitions for the generic reference architecture in clause 6.1, the **MEC Federator** (MEF) functional element is introduced, including **MEC Federation Broker** (MEFB) and **MEC Federation Manager** (MEFM) functionalities. The MEF provides the functionality required to interface with other MEFs and in that capacity can act as a broker between MEFs. It interfaces to at least one MEO.

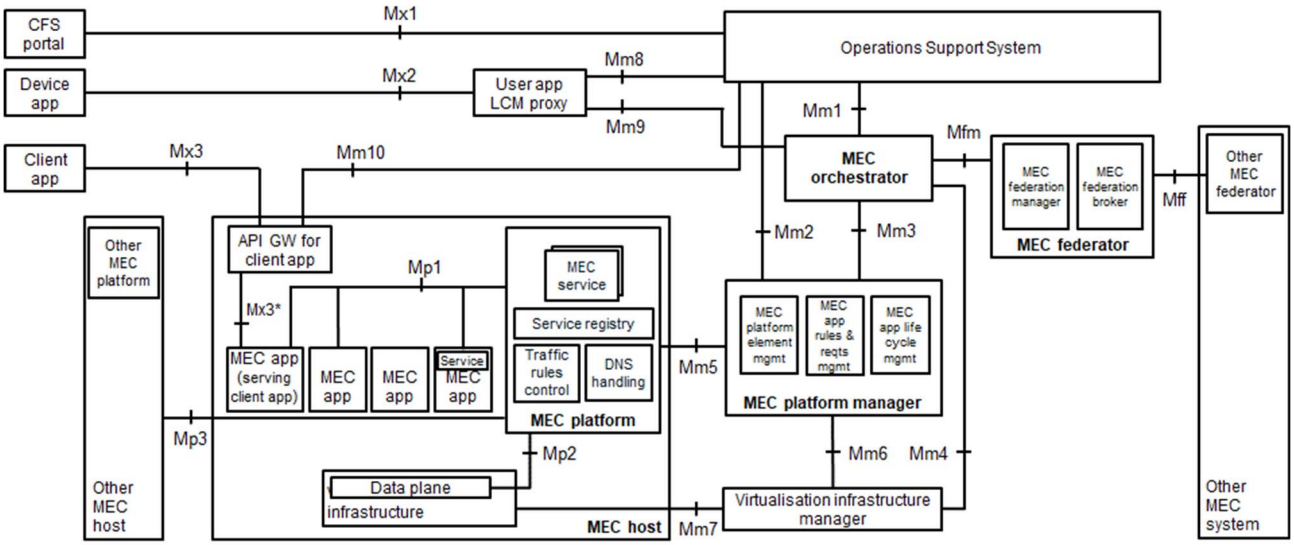

Figure 6-3: Multi-access edge system reference architecture variant for MEC federation

NOTE: Non-MEC systems may support Mff reference point. How this is implemented in the other system is out of the scope of the present document.

6.4 Reference architecture variant for Support for Security Monitoring and Management

6.4.1 Description

In clause 6.4.2 of the present document, a variant of the generic MEC architecture is presented that enables support for Security Monitoring and Management for ETSI MEC.

6.4.2 Architecture diagram

Figure 6.4 depicts a variant of the multi-access edge system architecture for SMM support. The SMM Function (SMMF) is introduced that provides the functionality of Security Monitoring and Management for the MEC system.

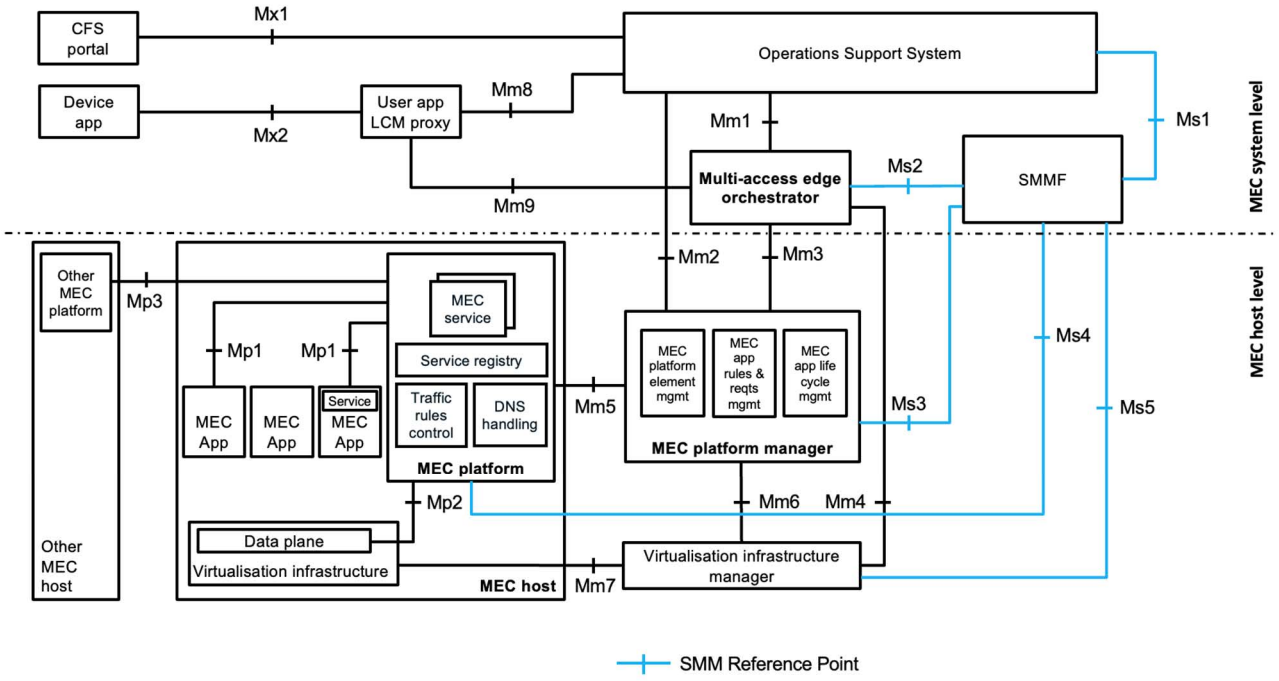

Figure 6.4: Multi-access edge system reference architecture variant for Support for SMM

7 Functional elements and reference points

7.1 Functional elements

7.1.1 MEC host

The MEC host is an entity that contains the MEC platform and a Virtualisation infrastructure which provides compute, storage and network resources for the MEC applications. The Virtualisation infrastructure includes a data plane that executes the traffic rules received by the MEC platform and routes the traffic among applications, services, DNS server/proxy, 3GPP network, other access networks, local networks and external networks.

7.1.2 MEC platform

The MEC platform is responsible for the following functions:

- offering an environment where the MEC application instances can discover, advertise, consume and offer MEC services (see clause 8), including, when supported, MEC services available via other platforms (that may be in the same or a different MEC system);
- receiving traffic rules from the MEC platform manager, applications, or services and instructing the data plane accordingly. When supported, this includes the translation of tags representing Ues in the traffic rules into specific IP addresses;
- receiving DNS records from the MEC platform manager and configuring a DNS proxy/server accordingly;
- hosting MEC services, possibly including services that are described in clause 8;
- providing access to persistent storage and time of day information;
- support for MEC application instance registration to the platform, enabling instances to provide their runtime information.

The MEC platform may be accompanied by API gateway functionality for MEC application instances to access the MEC service APIs.

7.1.3 MEC application

A MEC application is instantiated and run as a virtualised software application, within for instance a Virtual Machine (VM) or OS containers provided as part of the application package as a software image(s), on top of the Virtualisation infrastructure of the MEC system. Once instantiated, a MEC application instance can also potentially interact with the MEC platform to consume and provide MEC services (described in clause 8).

In certain cases, a MEC application instance can also interact with the MEC platform to perform certain support procedures related to the lifecycle of the application, such as indicating availability, preparing relocation of user state, etc. A MEC application instance can register to the MEC platform to provide its runtime related information. Registration enables discovery also in case the instance is not instantiated by the MEC management.

MEC applications can have a certain number of rules and requirements associated to them, such as required resources, maximum latency, required or useful services, etc. These requirements are validated by the MEC system level management and can be assigned to default values if missing.

7.1.4 MEC system level management

7.1.4.1 MEC orchestrator

The MEO is the core functionality in MEC system level management.

The MEO is responsible for the following functions:

- maintaining an overall view of the MEC system based on deployed MEC hosts, available resources, available MEC services, and topology;
- on-boarding of application packages, including checking the integrity and authenticity of the packages, validating application rules and requirements and if necessary adjusting them to comply with operator policies, keeping a record of on-boarded packages, and preparing the Virtualisation infrastructure manager(s) to handle the applications;
- selecting appropriate MEC host(s) for application instantiation based on constraints, such as latency, available resources, and available services;
- triggering application instantiation and termination;
- triggering application relocation as needed when supported;
- coordinating with the OSS the application instantiation lifecycle management operations.

7.1.4.2 Operations Support System (OSS)

The Operations Support System (OSS) in figure 6-1 refers to the OSS of an operator. It receives requests via the CFS portal and from device applications for instantiation or termination of applications, and decides on the granting of these requests. Granted requests are forwarded to the MEO for further processing.

When supported, the OSS also receives requests from device applications for relocating applications between external clouds and the MEC system.

7.1.4.3 User application lifecycle management proxy

A user application is a MEC application that is instantiated in the MEC system in response to a request of a user via an application running in the device (device application).

The user application lifecycle management proxy allows device applications to request on-boarding, instantiation, termination of user applications and when supported, relocation of user applications in and out of the MEC system. It also allows informing the device applications about the state of the user applications.

The user application lifecycle management proxy authorizes requests from device applications in the device (e.g. UE, laptop with internet connectivity) and interacts with the OSS and the MEO for further processing of these requests.

The user application lifecycle management proxy is only available when supported by the MEC system.

7.1.5 MEC host level management

7.1.5.1 MEC platform manager

The MEC platform manager is responsible for the following functions:

- managing the lifecycle of applications including informing the MEO of relevant application related events;
- providing element management functions to the MEC platform;
- managing the application rules and requirements including service authorizations, traffic rules, DNS configuration and resolving conflicts.

The MEC platform manager also receives Virtualised resources fault reports and performance measurements from the Virtualisation infrastructure manager for further processing.

7.1.5.2 Virtualisation infrastructure manager

The Virtualisation infrastructure manager is responsible for the following functions:

- Allocating, managing and releasing Virtualised (compute, storage and networking) resources of the Virtualisation infrastructure.
- Preparing the Virtualisation infrastructure to run a software image. The preparation includes configuring the infrastructure and can include receiving and storing the software image.
- When supported, rapid provisioning of applications, as described in "Openstack++ for Cloudlet Deployments" [i.3].
- Collecting and reporting performance and fault information about the Virtualised resources.
- When supported, performing application relocation. For application relocation from/to external cloud environments, the Virtualisation infrastructure manager interacts with the external cloud manager to perform the application relocation, for example using the mechanism described in "Adaptive VM Handoff Across Cloudlets" [i.3], possibly through a proxy.

The functionality provided by the Virtualisation infrastructure manager in the present document and the functionality provided by the Virtualised infrastructure manager described in ETSI GS NFV 002 [2], clause 7.2.5, overlap to a large extent.

7.1.6 Device application

Device applications as defined in the present document are applications in the device (e.g. UE, laptop with internet connectivity) that have the capability to interact with the MEC system via a user application lifecycle management proxy, as defined in clause 7.1.4.3.

7.1.7 Customer Facing Service (CFS) portal

The Customer Facing Service (CFS) portal allows operators' third-party customers (e.g. commercial enterprises) to select and order a set of MEC applications that meet their particular needs, and to receive back service level information from the provisioned applications.

7.1.8 Specific functional elements in the MEC in NFV architecture variant

7.1.8.1 Overview

The MEC in NFV architecture variant introduces two specific functional blocks which replace the MEO and the MEPM in the generic architecture. These specific blocks realize MEC-specific functionality and delegate tasks that can be fulfilled by ETSI NFV MANO to the related MANO functional blocks NFVO and VNFM.

7.1.8.2 MEC application orchestrator

The MEAO has the same responsibilities as the MEO (see clause 7.1.4.1), however, it delegates the management of the set of MEC applications to an NFVO which manages these as part of one or more NFV network services. Similarly, it can delegate the management of the MEC application VNF packages to the NFVO.

7.1.8.3 MEC platform manager - NFV

The MEPM-V has the same responsibilities as the MEPM (see clause 7.1.5.1), however, it does not perform LCM actions itself, but delegates these to a VNFM. Also, it does not receive Virtualised resources fault reports and performance measurements directly from the VIM, but these are routed via the VNFM.

7.1.8.4 NFVO

This functional block, as defined by ETSI GS NFV 002 [2], is responsible for managing the lifecycle of the network services that include the MEC application instances, treating each MEC application instance as a VNF instance.

7.1.8.5 VNFM (MEC platform LCM)

This functional block, as defined by ETSI GS NFV 002 [2], is responsible for managing the lifecycle of the MEC platform using standard NFV LCM procedures.

7.1.8.6 VNFM (MEC application LCM)

This functional block, as defined by ETSI GS NFV 002 [2], is responsible for managing the lifecycle of the MEC applications, treating each MEC application instance as a VNF instance. There may be more than one instance of this block in a deployment. Likewise, this block may be the same as the VNFM (MEC platform LCM) as defined in clause 7.1.8.5.

7.1.9 MEC federator

The MEC federator enables a MEC federation between MEC systems. It is applicable in the reference architecture variant for MEC federation, as depicted in clause 6.3.2.

Each MEF enables information exchange with at least one other MEF through support of the Mff reference point. Furthermore, a MEF may serve as a single point of contact (again via the Mff reference point) for multiple MEFs in the MEC federation, thereby acting as a broker between different MEFs. Such a MEF is considered to be "broker capable" and in that case contains MEFB functionality.

MEFs are considered as "manager capable", containing MEFM functionality and supporting the Mfm reference point. A MEF with MEFM and MEFB functionality is both "manager capable" and "broker capable". There may be more than one MEF that is "broker capable" in an overall MEC federation.

The MEF provides the federation enablement service which is further specified in ETSI GS MEC 040 [6].

7.1.10 API gateway for client applications

A client application is an application software running on a device in order to utilize functionality provided by one or more MEC application(s).

The API Gateway for client applications (AGW) provides access control to the APIs/services provided by the MEC applications to client applications. It serves as an endpoint to security related signalling whereby the client applications request and obtain access to the MEC applications. The AGW may revoke this authorization upon certain conditions (e.g. DOS). The AGW may be managed by the OSS in order to obtain and apply security-related configuration (if any) for MEC applications it is protecting.

The AGW is only available when supported by the MEC system.

7.1.11 Support for Security Monitoring and Management (SMM)

Security Monitoring and Management (SMM) refers to functionality employed by MEC network operators or communication service providers to continually assess and preserve the security of their network deployment (physical, virtualized or hybrid).

The MEC system may provide support for SMM. The MEC operator can integrate their existing SMM system to collect security-related data and generate any alerts that indicate a potential security issue in the MEC system.

The SMM Function (SMMF) is a function that realizes SMM functionality for the MEC system. The interfaces between the SMM and the MEO, MEP, MEPM, VIM, and OSS allow the collection of security-related data for further analysis of potential attacks to the MEC system and transmission of SMM-related messages. The SMMF may be managed by either the MEC operator's existing system or by the OSS.

SMM is only available when supported by the MEC system.

7.2 Reference points

7.2.1 Reference points related to the MEC platform

Mp1: The Mp1 reference point between the MEC platform and the MEC applications provides service registration, service discovery, and communication support for services. It also provides other functionality such as application instance registration, application availability, session state relocation support procedures, traffic rules and DNS rules activation, access to persistent storage and time of day information, etc. This reference point can be used for consuming services and providing service specific functionality.

Mp2: The Mp2 reference point between the MEC platform and the data plane of the Virtualisation infrastructure is used to instruct the data plane on how to route traffic among applications, networks, services, etc. This reference point is not further specified.

Mp3: The Mp3 reference point between MEC platforms is used for control communication between MEC platforms.

NOTE: Optionally control signalling can be exchanged between two MEC platforms in different MEC systems in order to facilitate feature specific inter-MEC system coordination. Such features include application mobility support and V2X support.

7.2.2 Reference points related to the MEC management

Mm1: The Mm1 reference point between the MEO and the OSS is used for triggering the instantiation and the termination of MEC applications in the MEC system. This reference point also supports coordination of application instantiation lifecycle procedures.

Mm2: The Mm2 reference point between the OSS and the MEC platform manager is used for the MEC platform configuration, fault and performance management.

Mm3: The Mm3 reference point between the MEO and the MEC platform manager is used for the management of the application lifecycle, application rules and requirements and keeping track of available MEC services.

Mm4: The Mm4 reference point between the MEO and the Virtualisation infrastructure manager is used to manage Virtualised resources of the MEC host, including keeping track of available resource capacity, and to manage application images.

Mm5: The Mm5 reference point between the MEC platform manager and the MEC platform is used to perform platform configuration, configuration of the application rules and requirements, application lifecycle support procedures, management of application relocation, etc. This reference point is not further specified.

Mm6: The Mm6 reference point between the MEC platform manager and the Virtualisation infrastructure manager is used to manage Virtualised resources e.g. to realize the application lifecycle management.

Mm7: The Mm7 reference point between the Virtualisation infrastructure manager and the Virtualisation infrastructure is used to manage the Virtualisation infrastructure. This is reference point is not further specified.

Mm8: The Mm8 reference point between the user application lifecycle management proxy and the OSS is used to handle device applications requests for running applications in the MEC system. This reference point is not further specified.

Mm9: The Mm9 reference point between the user application lifecycle management proxy and the MEO of the MEC system is used to manage MEC applications requested by device application. This reference point is not further specified.

Mm10: The Mm10 reference point between the AGW and the OSS is used for the security-related configuration for each MEC application whose services/APIs the AGW is protecting. It is only available when supported by the MEC system.

7.2.3 Reference points related to external entities

Mx1: The Mx1 reference point between the OSS and the customer facing service portal is used by the third-parties to request the MEC system to run applications in the MEC system. This reference point is not further specified.

Mx2: The Mx2 reference point between the user application lifecycle management proxy and the device application is used by a device application to request the MEC system to run an application in the MEC system, or to move an application in or out of the MEC system. It is only available when supported by the MEC system.

Mx3: The Mx3 reference point between the client application and the AGW is used to authorize access to the services/APIs MEC applications provide to client applications. It is only available when supported by the MEC system.

7.2.4 Reference points related to the MEC in NFV architecture variant

Mm3*: The Mm3* reference point between MEAO and MEPM-V is based on the Mm3 reference point. Changes cater for the split between MEPM-V and VNFM (MEC applications LCM).

Mv1: The Mv1 reference point between the MEAO and the NFVO is related to the Os-Ma-nfvo reference point, as defined in ETSI GS NFV-IFA 013 [3].

Mv2: The Mv2 reference point between the VNF Manager that performs the LCM of the MEC application VNFs and the MEPM-V allows LCM related notifications to be exchanged between these entities. It is related to the Ve-Vnfm-em reference point as defined in ETSI GS NFV-IFA 008 [4].

Mv3: The Mv3 reference point between the VNF Manager and the MEC application VNF instance allows the exchange of messages e.g. related to MEC application LCM or initial deployment-specific configuration. It is related to the Ve-Vnfm-vnf reference point, as defined in ETSI GS NFV-IFA 008 [4].

The following reference points are used as they are defined by ETSI NFV:

Ve-Vnfm-em: This reference point connects the VNF Manager (VNFM) that manages the lifecycle of the MEC platform with the MEC Platform Manager - NFV (MEPM-V). It is the Ve-Vnfm-em reference point as defined in ETSI GS NFV-IFA 008 [4].

Ve-Vnfm-vnf: This reference point connects the VNFM that manages the lifecycle of the MEC platform with the MEC Platform VNF.

Nf-Vn: This reference point connects the MEC Platform VNF with the NFVI.

Nf-Vi: This reference point connects the NFVI with the VIM.

Os-Ma-nfvo: This reference point connects the OSS with the NFVO. It is primarily used to manage Network Services, i.e. a number of VNFs connected and orchestrated to deliver a service.

Or-Vnfm: This reference point connects the NFVO with the VNFM that manages the lifecycle of the MEC platform. It is primarily used for the NFVO to invoke VNF LCM operations.

Vi-Vnfm: This reference point connects the VIM with the VNFM that manages the lifecycle of the MEC platform. It is primarily used by the VNFM to invoke resource management operations to manage the resources that are needed by the VNF.

Or-Vi: This reference point connects the NFVO with the VIM. It is primarily used by the NFVO to manage resources capacity.

7.2.5 Reference points related to the MEC federation architecture variant

Mff: The Mff reference point between MEFs within the MEC federation is used for sharing information (e.g. MEC system information).

Mfm: The Mfm reference point between the MEO and the MEF enables sharing information of a MEC system.

7.2.6 Reference points related to the Support for SMM architecture variant

Ms1: The Ms1 reference point connects the SMMF and the OSS.

Ms2: The Ms2 reference point connects the SMMF and the MEC orchestrator.

Ms3: The Ms3 reference point connects the SMMF and the MEC platform manager.

Ms4: The Ms4 reference point connects the SMMF and the MEC platform.

Ms5: The Ms5 reference point connects the SMMF and the Virtualisation infrastructure manager.

8 MEC services

8.1 General

A MEC service is a service provided and consumed either by the MEC platform or a MEC application. When provided by an application, it can be registered in the list of services to the MEC platform over the Mp1 reference point (see clause 7.2.1).

A MEC application can subscribe to a service for which it is authorized over the Mp1 reference point.

A certain number of MEC services are necessary in order to fulfil the requirements defined in ETSI GS MEC 002 [1] and are described in clauses 8.2 to 8.4.

8.2 Radio Network Information

The Radio Network Information service, when available, provides authorized applications with radio network related information.

It exposes information to applications, such as:

- appropriate up-to-date radio network information regarding radio network conditions;
- measurement and statistics information related to the user plane;
- information (e.g. UE context and radio access bearers) related to Ues served by the radio node(s) associated with the MEC host;
- changes on information related to Ues served by the radio node(s) associated with the MEC host.

The radio network information is provided at the relevant granularity (e.g. per User Equipment (UE) or per cell, per period of time).

8.3 Location

The Location service, when available, provides authorized applications with location-related information.

It exposes information to applications, such as:

- the location of specific Ues currently served by the radio node(s) associated with the MEC host;
- information about the location of all Ues currently served by the radio node(s) associated with the MEC host;
- optionally, information about the location of a certain category of Ues currently served by the radio node(s) associated with the MEC host;
- a list of Ues in a particular location;
- information about the location of all radio nodes currently associated with the MEC host.

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

8.4 Traffic Management Services

The following optional Traffic Management services are supported:

- BandWidth Management (BWM) service.
- Multi-access Traffic Steering (MTS) service.

The BandWidth Management (BWM) service, when available, allows allocation of bandwidth to certain traffic routed to and from MEC applications and the prioritization of certain traffic.

The Multi-access Traffic Steering (MTS) service, when available, allows seamlessly steering/splitting/duplicating application data traffic across multiple access network connections.

9 Other considerations

9.1 Inter-MEC system communication

Inter-MEC system communication addresses the following high level requirements:

1) A MEC platform should be able to discover other MEC platforms that may belong to different MEC systems.

2) A MEC platform should be able to exchange information in a secure manner with other MEC platforms that may belong to different MEC systems.

3) A MEC application should be able to exchange information in a secure manner with other MEC applications that may belong to different MEC systems.

To enable the inter-MEC system communication, the following hierarchical inter-MEC system discovery and communication framework is assumed:

- MEC system level inter-system discovery and communication.
- MEC host level inter-system communication between the MEC platforms.

NOTE: It is for further study if MEC platforms in different MEC systems should be able to discover each other without the involvement of the MEC system level functional elements.

9.2 Security of the Mp3 reference point

MEC platforms may wish to exchange control information on the Mp3 reference point. To guard against attacks on this communication, the link between the two platforms should be first secured.

APIs offered over the Mp3 reference point shall support HTTP over TLS as defined in clause 6.22 of ETSI GS MEC 009 [5]. Since TLS is a client-server protocol, and the two MEC platforms could be viewed as peers, one platform may assume the role of the client (for example, the one initiating the communication), while the other assumes the role of the TLS server. The TLS authentication should be mutual and based on digital certificates at both the client and server side. The certificates should be provisioned and managed for each MEC platform by the MEC system they are part of, and the certificate profiles should follow the guidelines of clause 6.1 of ETSI TS 133 310 [i.10]. In case that the certificates are issued by different authorities (e.g. different MEC systems), these certificate management operations should allow for trust to be established between the authorities (i.e. MEC systems) with which the Mp3 communication is envisioned to take place (see for example clause 7.3 of ETSI TS 133 310 [i.10]).

Annex A (informative): Key concepts

A.1 MEC host selection

In order to run a MEC application in the MEC system, the MEO receives requests triggered by the OSS, a third-party, or a device application.

These requests provide information about the application to run, and possibly other information, such as the location where the application needs to be active, other application rules and requirements, as well as the location of the application image if it is not yet on-boarded in the MEC system.

The information considered by the MEO when selecting a MEC host(s) for a MEC application can include:

- deployment model of the application (e.g. whether it is one instance per user, one instance per host, one instance on each host, etc.);
- required Virtualised resources (compute, storage, network resources, including specific hardware support);
- latency requirements (e.g. how strict the latency constraints are, latency fairness between users);
- requirements on location;
- required MEC services that are needed for the MEC application to be able to run;
- MEC services that the MEC application can take advantage of if available;
- connectivity or mobility requirements (e.g. application state relocation, application instance relocation);
- required MEC features, such as VM relocation support or UE identity;
- required network connectivity (e.g. connectivity to applications within the MEC system, connectivity to local networks, or to the Internet);
- information on the operator's MEC system deployment or mobile network deployment (e.g. topology, cost);
- requirements on access to user traffic;
- requirements on persistent storage.

The MEO considers the requirements and information listed above and information on the resources currently available in the MEC system to select one or several MEC hosts within the MEC system, and requests the selected host(s) to instantiate the application.

NOTE: The actual algorithm used to select the hosts depends on the implementation, configuration, and operator deployment and is not intended to be specified.

Under certain circumstances (e.g. UE mobility events resulting in increased latency, load balancing decisions), and if supported, the MEO could decide to select a new host and initiate the transfer of an application instance or application-related state information from a source host to a target host, as described in clause A.4.

A.2 DNS support

The MEC platform provides access to DNS, which includes a name server and a proxy/cache function. The MEC platform receives the application DNS rules from the MEC management. Based on configuration or following an activation request from the MEC application, the MEC platform configures the mapping between an IP address and its FQDN into the DNS based on these rules.

A.3 Application traffic filtering and routing

The MEC platform allows the activation, update, and deactivation of the MEC application traffic rules, and applies these rules to the underlying data plane. This allows IP traffic routing or tapping to the MEC applications or to locally accessible networks (e.g. enterprise network, Internet access, etc.) according to the configured traffic rules.

Within the constraints set by the MEC management, an authorized MEC application can request the activation, update and deactivation of the MEC application traffic rules dynamically. For example, this allows the redirection of traffic of a certain UE to an enterprise network after the UE has been authenticated and authorized by the MEC application.

A.4 Support of application and UE mobility

A.4.1 Background: UE mobility

UE mobility is supported by the underlying 3GPP networks and can result in the UE moving to a radio node associated with a different MEC host due to handover events. The likelihood for MEC host changes due to UE mobility depends on the deployment options and the topology of the network.

MEC applications can be impacted by UE mobility events and the possible scenarios are described in clause A.4.2.

A.4.2 MEC application scenarios for UE mobility

A.4.2.1 MEC applications not sensitive to UE mobility

Some MEC applications remain unaffected by UE mobility events, for example if their purpose is to only process traffic that goes through the local MEC host, or if the UE related state can be rapidly rebuilt after a handover.

A.4.2.2 MEC applications sensitive to UE mobility

A.4.2.2.1 Maintaining connectivity between UE and MEC application instance

Some MEC applications expect to continue serving the UE after a location change of the UE in the mobile network. In order to provide continuity of the service, the connectivity between the device application and the MEC application needs to be maintained. As the UE moves around the network, the traffic between the UE and the MEC application is routed so that it reaches the intended destination.

As the UE moves further away from the location of the MEC application, there could be an increased latency between the UE and the MEC application. Due to this reason or others (e.g. network congestion), for some MEC applications, it might become necessary to relocate the application state or application instance in order to satisfy the latency requirements.

A.4.2.2.2 Application state relocation

Application state relocation assumes MEC application support. As the UE moves around in the mobile network, another (target) MEC host might be identified as being a more appropriate location for the MEC application to serve the UE instead. If the application does not run yet on the target MEC host, the application can be instantiated before starting the application state relocation. Interaction between the two application instances on the source and target MEC hosts is enabled, e.g. to move the application state from one instance to the other. The exact data, the procedures, and the pacing of this interaction are dependent on the application design. At some point in time, the application state will have been fully transferred, the source instance will stop serving the UE, and the target instance will take over serving the UE.

A.4.2.2.3 Application instance relocation within the MEC system

In some cases, and when it is supported, it is preferable for some applications to move the serving application instance itself from the source host to the target host. This is done by having the MEO trigger the application instance relocation. In that case, the application instance runs in the source host, while it is copied over to the target host. When the process is complete, the instance then runs in the target host and takes over the traffic from the UE. This concept is exemplified by the "VM handoff" described in "Adaptive VM Handoff Across Cloudlets" [i.3].

A.4.2.2.4 Application instance relocation between the MEC system and an external cloud environment

In some cases, and when it is supported, the UE can request the MEC system to move application instances out of the MEC system to an external cloud environment, or from an external cloud environment to the MEC system. In that case, the application instance relocation is triggered between the MEC system and the external cloud environment under the supervision of the MEO.

A.5 Void

A.6 Data Plane

In the MEC reference architecture the Virtualisation infrastructure in the MEC host includes a data plane that executes the traffic rules received by the MEC platform, and routes the traffic among applications, services, DNS server/proxy, 3GPP network, local networks and external networks (as described in clause 7.1.1). The Data plane described in the present document is only a representation of the execution environment for the traffic rules and routing. Mapping of all or part of MEC data plane functionality to any functional element(s) of a real network architecture, e.g. UPF in ETSI TS 123 501 [i.6], implies a specific deployment option of MEC in such a network architecture.

A.7 API gateway support

The MEC platform may be accompanied by API gateway functionality supporting e.g. the following:

- Receiving the service API request from MEC application via a stable service connection endpoint. The IP address change of MEC service instances will not lead to the update of the service connection endpoint information.
- Load balancing for the multiple backend MEC service instances.
- Throttling API requests for better throughput based on the configuration.
- Monitoring the API requests. It can be used for statistics and charging.

A.8 Root of Trust support

The MEC host may be accompanied by a Root Of Trust (ROT) functionality. For a definition of a ROT see ETSI GS MEC 002 [1], clause A.43.2, and [i.12], Clause 4.1. The ROT can serve to increase the assurance that a MEC application package has not been tampered with or compromised, before instantiating it onto the MEC host.

A.9 Remote attestation concepts

A MEC deployment may support various instantiations of the IETF RATS architecture as described in IETF RFC 9334 [i.11]. The attestation is "remote" because the party verifying the integrity of an entity is remote (i.e. external to the system) with respect to the entity being evaluated.

The following "roles" are defined, along with an example implementation:

- Relying party. For a definition, see ETSI GS MEC 002 [1], clause A.43.2. A Relying party (e.g. OSS) is seeking assurances of the integrity of an application, in this case the MEC Application package. The OSS may require this information before requesting the MEO to instantiate the MEC Application.

- Verifier. For a definition, see ETSI GS MEC 002 [1], clause A.43.2. The Verifier is the entity that performs the checks between the received Evidence (containing measurements) and the Reference values of those measurements. The Verifier needs access to the Reference values.

- Attester. For a definition, see ETSI GS MEC 002 [1], clause A.43.2. The Attester is the entity that compiles Evidence consisting of measurements of the MEC Application package, and securely delivers them to the Verifier.

The following "artifacts" are defined, along with an example implementation

- Reference values. Also referred to as "known-good values", these measurements can be hashes of the binary software image computed in a secure environment on the known good software images and stored securely to prevent tampering.

- Evidence. Evidence comprises the measurements of the software being evaluated (i.e. the MEC Application package) and is produced by the Attester.

Example of the mapping of the IETF RATS architecture roles to MEC system entities is shown in the table A.9-1.

Table A.9-1: Example of the mapping of the IETF RATS architecture roles to MEC system entities

IETF RATS term	Role or Artifact	ETSI MEC entities it can map to (not exhaustive)
Relying party	Role	OSS
Verifier	Role	MEO
Attester	Role	VIM
Evidence	Artifact	Computed MEC Application image hash and the underlying infrastructure
Reference value	Artifact	Stored MEC Application image hash and the underlying infrastructure

There is flexibility in how cryptographic attestation capabilities might be implemented in support of assessing MEC application package integrity, and the following steps outline one common implementation. The cryptographic attestation steps described below follow the concepts outlined in IETF RFC 9334 [i.11], adapted to the MEC architectural entities accordingly:

Step 0: The MEO (in the Verifier role) is provisioned with the correct ("known-good") reference values for a given MEC application package and all components of the MEC host measurement infrastructure.

Step 1: The OSS (in its role as the Relying Party) wishes to verify the integrity of a MEC application package and issues a request to the MEO (in its role as Verifier) for a trust assessment. The MEO receives this request and issues an attestation request that is relayed through the MEPM and MEP, and targeted at the VIM (in its role as the Attester).

Step 2: The VIM securely collects and compiles evidence, which will include cryptographic measurements. This evidence will be signed by a ROT on the MEC platform.

Step 3: The VIM returns the evidence to the MEO, through the MEP and MEPM.

Step 4: The MEO (in its role as Verifier) validates that the received evidence is signed by an authentic ROT and then compares the received evidence with the stored reference values (from Step 0) to perform its trustworthiness checks. The MEO then informs the OSS of its assessment.

This would convey to the OSS that the measured component(s) have not been compromised, and that it is safe to instantiate a new MEC Application instance.

Annex B (informative): Relationship with 3GPP SA6 EDGEAPP architecture

B.1 Introduction

The architecture for enabling edge applications (also known as EDGEAPP architecture) is, as defined in ETSI TS 123 558 [i.9], an application layer architecture for enabling edge applications over 3GPP networks. Edge Application Servers (EASs) and the Edge Enabler Server (EES) are contained within the Edge Data Network (EDN). The Edge Configuration Server (ECS) provides configurations related to the EES, including details of the EDN hosting the EES. The UE contains Application Clients (Acs) and the Edge Enabler Client (EEC). The EAS(s), the EES and the ECS may interact with the 3GPP Core Network. An example for how the 3GPP SA6 (EDGEAPP) architecture and ETSI MEC architecture can complement each other is illustrated in Figure B.1-1, per the informative Annex C of ETSI TS 123 558 [i.9].

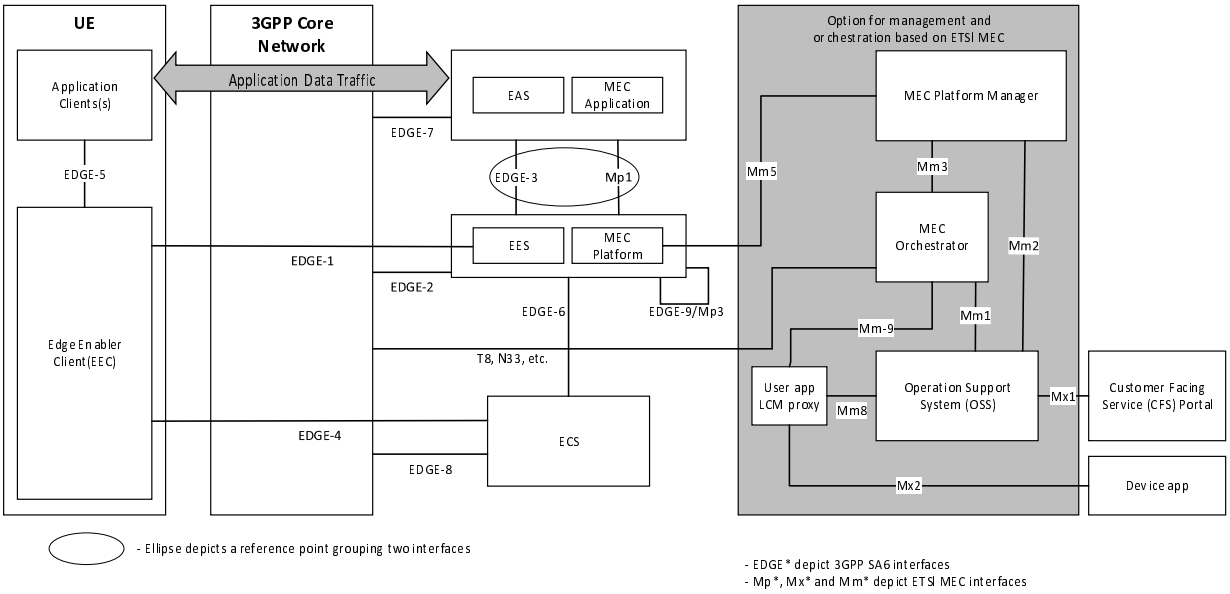

Figure B.1-1: Relationship between 3GPP SA6 (EDGEAPP) architecture and ETSI MEC architecture, per the informative Annex C of ETSI TS 123 558 [i.9]

B.2 Edge Enabler Server (EES)

Despite of the obvious differences between the MEC reference architecture and EDGEAPP architecture, the EES bears some similarities with the MEC platform. The EES provides supporting functions not only for EASs but also EECs residing in the Ues. The MEC platform offers supports to MEC applications (similar to EASs, where both can be considered as application servers in 3GPP nomenclature) via the Mp1 reference point; it is also involved in the MEC application management through connectivity to the MEC platform manager via the Mm5 reference point. While the MEC platform does not directly interact with the Ues, a device application (hosted in a device, for which a UE is provided as an example in clause 7.1.6) can issue a request (via Mx2 reference point to the user application lifecycle management proxy) to instantiate an application in the MEC system, or to move an instantiated application in or out of the MEC system.

As specified in ETSI TS 123 558 [i.9], table B.2-1 summarizes the APIs provided by the EES in support of the EASs.

Table B.2-1: APIs provided by the EES in support of EASs

API Name		Description	References
Eees_EASRegistration		The EAS Registration procedure allows an EAS to provide its information to an EES in order to enable its discovery by an EEC.	Clause 8.4.3 of ETSI TS 123 558 [i.9]
Eees_EASDiscovery		EAS discovery enables the EEC to obtain information about available EASs of interest from the EES.	Clause 8.5 of ETSI TS 123 558 [i.9]
EES capability exposure to EAS	Eees_UELocation	The EES exposes the UE location API to the EAS in order to support tracking or checking the valid location of the UE.	Clause 8.6.2 of ETSI TS 123 558 [i.9]
	Eees_ACRManagementEvent	The EES exposes application context relocation (ACR) management event notifications of one or more Ues to an EAS (e.g. in order to trigger the ACR).	Clause 8.6.3 of ETSI TS 123 558 [i.9]
	Eees_AppClientInformation	Application Client information exposure enables EASs to obtain information about capabilities of Acs from the EESs.	Clause 8.6.4 of ETSI TS 123 558 [i.9]
	Eees_UEIdentifier	EES exposes UE Identifier API to the EAS in order to provide an identifier uniquely identifying a UE.	Clause 8.6.5 of ETSI TS 123 558 [i.9]
	Eees_SessionWithQoS	The EES exposes the Session with QoS API to the EAS in order to support the setup of a data session between AC and EAS with a specific QoS and the modification of the QoS of this data session.	Clause 8.6.6 of ETSI TS 123 558 [i.9]
Eees_TargetEASDiscovery		This procedure is to fetch target EAS information, which may be utilized by a source EAS, which undertakes the transfer of application context information to a target EAS directly, or can be invoked by the source EES itself on deciding to execute application context relocation.	Clause 8.8.3.2 of ETSI TS 123 558 [i.9]
Eees_AppContextRelocation		The procedure is for the EEC to trigger the EES to initiate ACR.	Clause 8.8.3.4 of ETSI TS 123 558 [i.9]

An EAS utilizes the services of the EES whereas a MEC application utilizes the services provided by the MEC platform as specified in the present document. The EES and MEC platform can be collocated in an implementation (as also stated in the informative Annex C of ETSI TS 123 558 [i.9]), for example the APIs listed in table B.2-1 could be offered/exposed by an implementation offering both EES and MEC platform capabilities in support of EASs and MEC applications. Similarly, an EAS and MEC application can be collocated in an implementation (as also stated in the informative Annex C of ETSI TS 123 558 [i.9]), to utilize the services offered by both the EES and MEC platform. In summary, implementations (in particular those in which an EES and MEP are collocated) may be compliant to:

1) the 3GPP EDGEAPP specification (ETSI TS 123 558 [i.9]);

2) the ETSI MEC specifications; or

3) both sets of specifications.

The third option enables capabilities of both specifications to be offered and can avoid potential duplication of separately deploying EESs and MEC platforms.

Annex C (informative): Relationship with GSMA OP architecture

C.1 Introduction

The GSMA Official Document OPG.02 [i.8] in its Annex A has proposed a mapping of GSMA OPG requirements to ETSI MEC, among other external fora. In Annex A.1 of [i.8], the GSMA Official Document OPG.02 describes a mapping between the GSMA OP architecture and the ETSI MEC framework, which is illustrated by a diagram in Annex E.1.2, and is provided here in figure C.1-1.

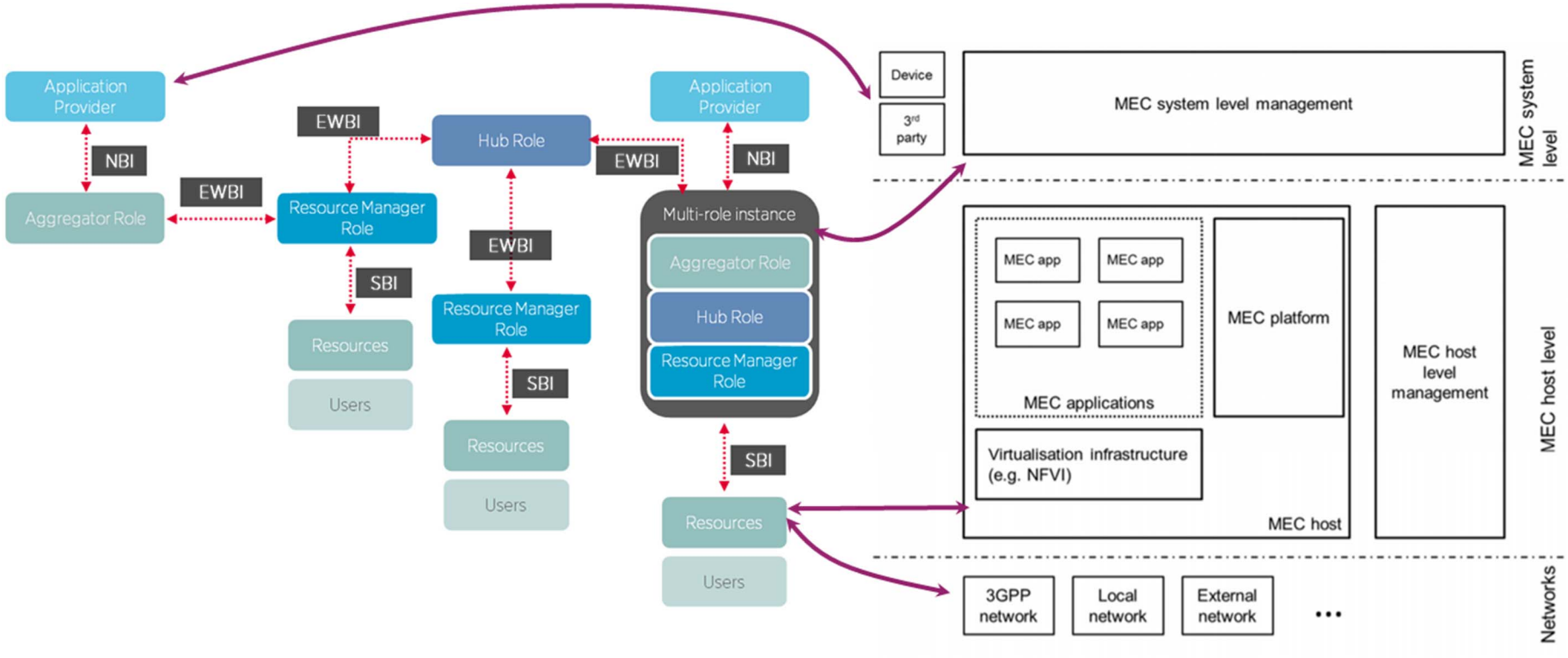

Figure C.1-1: Relationship between GSMA OP architecture and ETSI MEC framework, per Annex E.1.2 of [i.8]

This annex provides a more detailed mapping between the GSMA OP and ETSI MEC architectures. Figure C.1-2 shows the mapping of a subset of Operator Platform (OP) interfaces to reference points of the reference architecture variant for MEC federation, as specified in clause 6.3 of the present document. This takes into account the definitions of these OP interfaces, as provided in clause 3.5 of GSM Official Document OPG.02 [i.8]. The specific OP interfaces considered are the East-West Bound Interface (E/WBI), the Northbound Interface (NBI) and the Southbound Interface (SBI).

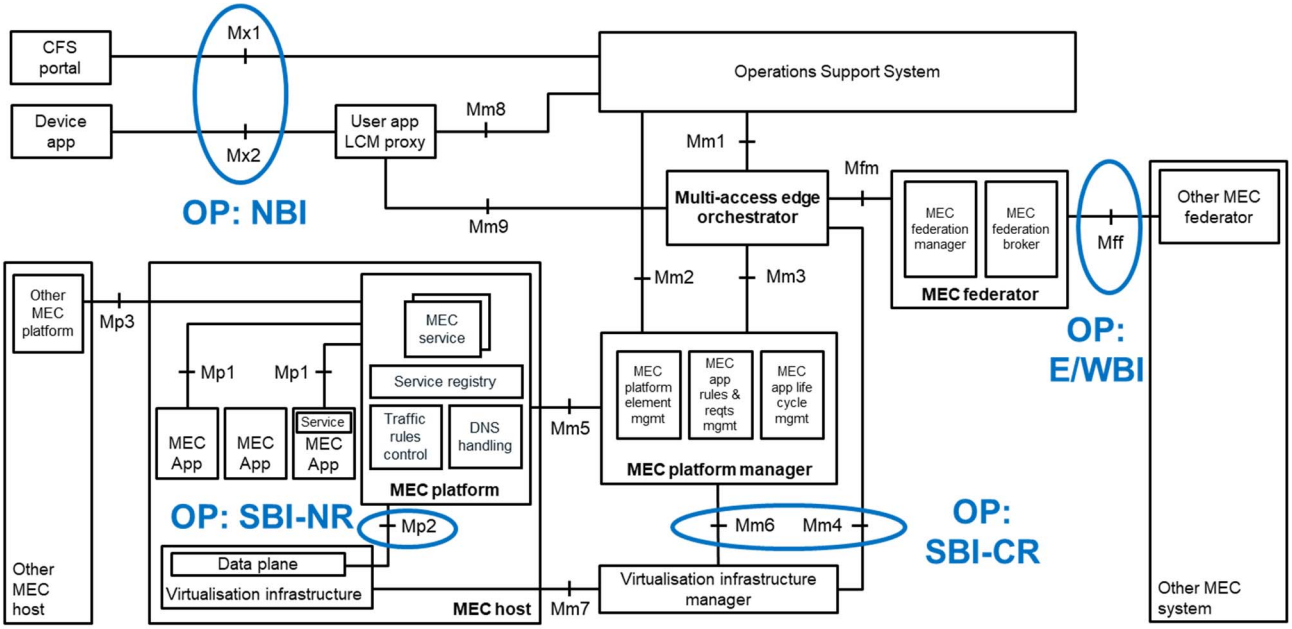

Figure C.1-2: Mapping between the E/WBI, NBI and SBI interfaces of the GSMA OP architecture to reference points of the reference architecture variant for MEC federation

C.2 E/WBI

As documented in clause 3.5.4 of [i.8], the E/WBI connects partner OP instances with the primary goal of allowing Application Providers of an OP to utilise the edge cloud services of another OP. The E/WBI is not exposed to the Application Providers and is primarily driven by the Federation Manager Role within the OP.

The E/WBI in GSMA OP architecture can be mapped to the Mff reference point of the MEC federation variant of the ETSI MEC reference architecture, as presented in clause 6.3.2 of the present document.

C.3 NBI

As documented in clause 3.5.1 of GSMA Official Document OPG.02 [i.8], the NBI is the interface between the developers and an OP.

The NBI in GSMA OP architecture can be mapped to reference points Mx1 and Mx2 of the ETSI MEC reference architecture, as defined in clause 6.1 of the present document.

Annex D (informative): Relationship with both 3GPP SA6 EDGEAPP and GSMA OP reference points

Following the separate analysis on the relationship the ETSI MEC reference architecture has with 3GPP SA6 EDGEAPP (Annex B of the present document) and GSMA OP architectures (Annex C of the present document), Table D-1 provides a cross-SDO mapping, indicating correspondences with OP interfaces, as proposed by GSMA Official Document OPG.02 [i.8].

Table D-1: Relationship between OP interfaces and reference ETSI MEC and 3GPP SA6 EDGEAPP reference points

GSMA OP interface	ETSI MEC relevance	3GPP relevance SA6/SA5	In scope of ETSI MEC specifications	Comments
E/WBI	Mff	SA6: Federation is in Rel-18 scope (EDGEAPP)	Yes	ETSI GS MEC 040 [6] Mp3 is not considered relevant for OP compliance. Action: Requires alignment between 3GPP and ETSI MEC.
NBI	Mp1 (e.g. for network event support) & Mx*X*/Mm*X* (e.g. for MEC application LCM)	SA6: EDGE-3 [i.9] SA5: Provisioning MnS	Yes	Action: Requires alignment between 3GPP and ETSI MEC (e.g. Mp1/EDGE-3, Mx*X*/Provisioning MnS and Mm*X*/Provisioning MnS).
SBI-NR (SBI - Network Resources)		SA6: EDGE-2/8 [i.9]		Non-overlapping, no alignment needed between 3GPP< and ETSI MEC.
SBI-CHF (SBI - Charging Functions)		SA5: Edge Converged Charging		Non-overlapping, no alignment needed between 3GPP and ETSI MEC.
SBI-CR (SBI - Cloud Resources)	Mm*X*	SA5: Provisioning MnS		See note.
UNI (User Network Interface)		SA6: EDGE-1/4 [i.9]		Non-overlapping, no alignment needed between 3GPP and ETSI MEC.
NOTE: Regarding the SBI-CR OP interface, although it is open to multiple architectures (as indicated in clause 3.5.2.1.2 of GSM Official Document OPG.02 [i.8]) and considering the current industry solutions, the ETSI ISG NFV architecture is deemed to be of highest relevance, because of its current alignment with 3GPP, but also considering the similarities of MEC and NFV.				

Annex E (informative): Change History

Date	Version	Information about changes
February 2021	3.0.1	Baseline for phase 3
March 2021	3.0.2	MEC(21)000065r8 MEC003 - Introduction of MEC Federation Manager and MEC Federation Broker in ETSI MEC architecture, includes figure 6.3.2-1
April 2021	3.0.3	MEC(21)000107r3 MEC003 - informative Annex on 3GPP/ETSI MEC alignment on EES/MEP
May 2021	3.0.4	MEC(21)000194r2 MEC003 - informative Annex on relationship with GSMA OP architecture
September 2021	3.0.5	MEC(21)000265r5 MEC003 - Correspondence with OP interfaces
October 2021	3.0.6	MEC(21)000451r3 MEC003 Federation architecture consolidation MEC(21)000475r1 MEC003 GSMA OPG PRD reference
October 2021	3.0.7	MEC(21)000476 MEC003 editorial change app to application MEC(21)000480r1 MEC003 Federation reference point descriptions
October 2021	3.0.8	MEC(21)000481r2 MEC003 Federator description MEC(21)000493r1 MEC003 Federation architecture Annex C MEC(21)000503 MEC003-alignment on the abbreviations
December 2021	3.0.9	MEC(21)000624r1 MEC003 prepare for publication by removing some unfinished content Editorial changes to prepare publication, clean-up done by editHelp!
March 2022	3.1.2	Base line derived from published 3.1.1 MEC(22)000015 MEC003v321 Restore content removed by MEC(21)000624r1 MEC(22)000031r1 MEC 003 MEC application description update
May 2023	3.1.3	MEC(23)000136r1 MEC 003 Application instance registration MEC(23)000137r1 MEC 003 Application LCM coordination
September 2023	3.1.4	MEC(23)000326 MEC 003 - Add security for the Mp3 reference point
December 2023	3.1.5	MEC(23)000505r1 MEC003 - closing some Editor's Notes on MEC Architecture
February 2024	3.1.6	MEC(24)000067r2 MEC003 finalization
February 2024	3.1.7	Final draft v3.1.7 is similar to Stable draft v3.1.6, and ready to be sent to MEC RC for review.
March 2024	3.1.8	Final draft 3.1.8 is similar to 3.1.7 as there were no comments during the RC for review. It is ready to go to MEC RC for approval.
June 2024	4.0.1	Start of work.
June 2024	4.0.2	MEC(24)000298r1 MEC 003 Add API gateway for client applications
October 2024	4.0.3	MEC(24)000361r1 MEC003-update to the figure in clause 6.2
October 2024	4.0.4	MEC(24)000426r1 MEC003- replacement of API Gateway MEC(24)000427r2 MEC003- update figure 6.2 MEC(24)000428r1 MEC003- update figure 6.3
November 2024	4.0.5	MEC(24)000399r3 MEC003 - Add Root of Trust MEC(24)000463r1 MEC003- Add SMM
December 2024	4.0.6	Rapporteur's clean-up. Stable Draft.
March 2025	4.0.7	MEC(25)000029 MEC003 SMM Diagram Edit MEC(24)000019r1 MEC003 Add AGW to MEC framework

History

Document history		
V1.1.1	March 2016	Publication
V2.1.1	January 2019	Publication
V2.2.1	December 2020	Publication
V3.1.1	March 2022	Publication
V3.2.1	April 2024	Publication
V4.1.1	May 2025	Publication