International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5003

(02/2022)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Signalling requirements and protocols for IMT-2020 – Signalling requirements and architecture of IMT-2020

Signalling requirements and architecture for federated multiaccess edge computing

Recommendation ITU-T Q.5003

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS	Q.4100–Q.4139
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
Signalling requirements and architecture of IMT-2020	**Q.5000–Q.5019**
Protocols for IMT-2020	Q.5020–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.5003

Signalling requirements and architecture for federated multiaccess edge computing

Summary

Recommendation ITU-T Q.5003 describes signalling requirements and architecture for federated multiaccess edge computing (MEC). This Recommendation specifies signalling requirements, signalling architecture with reference points and security considerations for federated MEC.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.5003	2022-02-13	11	11.1002/1000/14925

Keywords

Federated MEC, MEC platform, multiaccess edge computing.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.5003

Signalling requirements and architecture for federated multiaccess edge computing

1 Scope

This Recommendation describes the application layer architecture and architectural requirements for the federated multiaccess edge computing (MEC). The scope of this Recommendation covers:

– Signalling architecture;

– Signalling requirements.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 multiaccess edge computing [b-ETSI GS MEC 001]: System which provides an IT service environment and cloud-computing capabilities at the edge of an access network which contains one or more type of access technology, and in close proximity to its users.

3.1.2 MEC application [b-ETSI GS MEC 001]: Application that can be instantiated on an MEC host within the MEC system and can potentially provide or consume MEC services.

3.1.3 MEC platform [b-ETSI GS MEC 001]: Collection of functionality that is required to run MEC applications on a specific MEC host virtualization infrastructure and to enable them to provide and consume MEC services, and that can itself provide a number of MEC services.

3.1.4 MEC service [b-ETSI GS MEC 001]: Service provided via the MEC platform either by the MEC platform itself or by an MEC application.

3.1.5 lifecycle management [b-ETSI GS MEC 001]: Set of functions required to manage the instantiation, maintenance and termination of an MEC application instance.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 federated MEC: A group of multiaccess edge computing systems that belong to several multiaccess edge computing providers, and which jointly provide a unified service across these providers to respond to requests received from application providers by exchanging resources from all of the individual multiaccess edge computing systems.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

COTS Commercial-Off-The-Shelf

FE Functional Entity

HW Hardware

IaaS Infrastructure as a Service

IP Internet Protocol

MA MEC Aggregation

MAL MEC Aggregation Layer

MEC Multiaccess Edge Computing

MeML MEC Management Layer

MIL MEC Infrastructure Layer

MNO Mobile Network Operator

MPL MEC Platform Layer

PaaS Platform as a Service

QoE Quality of Experience

SaaS Software as a Service

SDK Software Development Kit

SLA Service Level Agreement

SW Software

UE User Equipment

URL Uniform Resource Locator

5 Conventions

None.

6 Overview

Multiaccess Edge Computing (MEC) providers have been developing the MEC services and platform separately using different technologies for different vertical domains, which may bring significant drawbacks. They have to deal with specific signalling flows for different interfaces to interwork with different service platforms, which may significantly increase the complexity for the MEC providers. Therefore, there is a strong necessary to specify an architecture with a signalling convergence to provide unified MEC services across different MEC providers, which can be fulfilled by federated MEC.

Federated MEC is a model which can provide a unified MEC service across MEC providers by exchanging the resources (e.g., cloud-computing resources, network capabilities) of each MEC system and requests from application providers.

Federated MEC mainly provides the following three functionalities:

– Authenticating, authorizing each MEC system and sharing its capabilities: This is needed for MEC providers to authenticate and authorize each other and share information related to each MEC system's catalogue with network resources, computing resources, etc.

– Discovering appropriate MEC systems: When a user moves to another region during MEC service or an application provider requests to interconnect with another application provider, it is supported that each MEC provider discover different MEC systems based on the registered information to maintain the quality that MEC service can originally provide.
– Communicating between MEC systems: After discovering, communicating between MEC systems is supported. Basically, the content type delivered over the communication is not limited, and it can also support the delivery of application packages and application contexts, or the exchange of some media (text, audio or video).

In this Recommendation, the architectural model and signalling requirements for federated MEC are specified in clause 7; the relevant security considerations in clause 8; and selected use cases for federated MEC are described in Appendix I.

Note that the concept of MEC federation is also discussed in the other SDOs, e.g., GSMA OPG and ETSI ISG MEC; and there are other relevant specifications [b-GSMA] [b-ETSI GS MEC 035] being developed.

7 Architecture and signalling requirements

The MEC system is responsible for 1) serving MEC service and application providers' request to host their instances in the network edge; and 2) supporting an end-user to access via user equipment (UE) the MEC services and applications deployed in the MEC infrastructure.

In order to serve the UE registered or moving to different MEC systems, the MEC service and application providers need to interact with the different MEC systems via different interfaces, contract, policies, Service Level Agreement (SLA), etc.

In federated MEC, the interactions with MEC service and application providers are aggregated and the different MEC systems federate to deploy the MEC services and applications with no intervention at on-demand locations covered by different MEC providers.

This clause specifies the architectural model for federated MEC, including signalling requirements for interactions among different functional entities and between different MEC systems.

7.1 Architectural model for federated MEC

The architectural model for federated MEC consists of four layers, including several functional entities in each layer:

– MEC aggregation layer (MAL) is responsible for serving the MEC service and application providers' demands towards different MEC systems;
– MEC management layer (MeML) is responsible for the management of MEC services and applications;
– MEC platform layer (MPL) is responsible for provisioning and control of the connectivity to MEC services and applications;
– MEC Infrastructure Layer (MIL) is responsible for the management of the virtualized infrastructure.

In the architectural model of federated MEC, there are six reference points defined to serve the interactions among the layers and external entities (i.e. MEC services and applications and UE):

– MS reference point, for interactions between MEC services and applications and MAL;
– MA reference point, for interactions between MAL and MeML;
– MM reference point, for interactions between MAL and MeML;
– MM*e* reference point, for interactions between MeMLs of different MEC systems;
– MP reference point, for interactions between MPL and MIL;

– MP*e* reference point, for interactions between MPLs of different MEC systems;

– MI reference point, for interactions between MIL and UE.

The architectural model for federated MEC is illustrated in Figure 7-1.

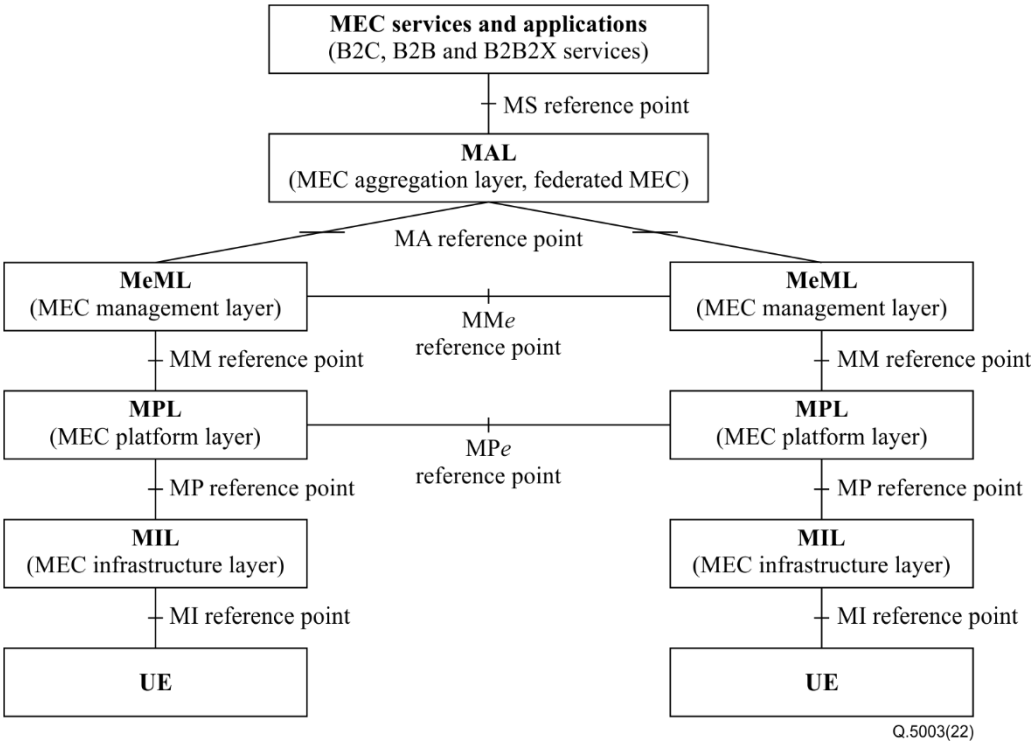

Figure 7-1 – Architectural model for federated MEC

7.1.1 Functional entities and requirements

This clause defines functional entities that require for each predefined layer.

7.1.1.1 MEC aggregation layer

The MAL is responsible for different service providers' requirements over heterogeneous MEC with the functions described in Figure 7-2 and below.

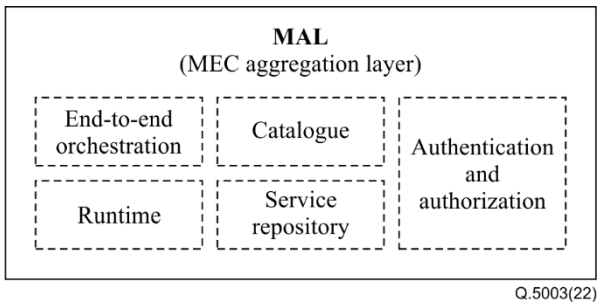

Figure 7-2 – Functional entities for the MEC aggregation layer

– The end-to-end orchestration FE supports the lifecycle management of MEC infrastructure resources, platform functions, services and applications over the federation of heterogeneous operator specific MEC platform and management layers. The FE supports necessary functionalities for the services and application providers to deploy and manage their applications, such as to upload, update and delete application images with necessary information. These functionalities are performed with related FEs in MeML and MPL; For the direct interaction between MeMLs and between MPLs of federated MEC systems when, for example, supporting consistent user experience across the MEC provider's coverage or

connecting services deployed on different MEC system and so on is required, the FE supports the discovery and selection of appropriate MEC system, datacentres and MEC platforms.

– Catalogue FE manages the collection of operator specific MEC infrastructure resources, platform functions capabilities.

– Runtime FE manages the runtime information of federated MEC. The FE handles, over MeML, services and application providers' requests to subscribe the event notification and run time information related to the network and MEC resources.

– Service repository FE manages and handles the federated MEC services.

– Authentication and Authorization FE manages authentication of the operator specific federated MECs.

7.1.1.2 MEC management layer

The MeML provides functionalities which are required for MEC network resource allocating tasks such as allocating cloud and network resources for each required MEC service (that may be in the same or a different MEC provider); see also Figure 7–3. MeML communicates with other MeML in a federated MEC system through an Exchange reference point between them, for example, for the direct delivery of an onboard application package to allow services and application providers of an MEC system to deploy their applications using the MEC resources and services of other federated MEC systems. Discovery and selection of appropriate target MEC systems and necessary information to establish the connection between the MeMLs is provided by end-to-end orchestration FE in the MAL.

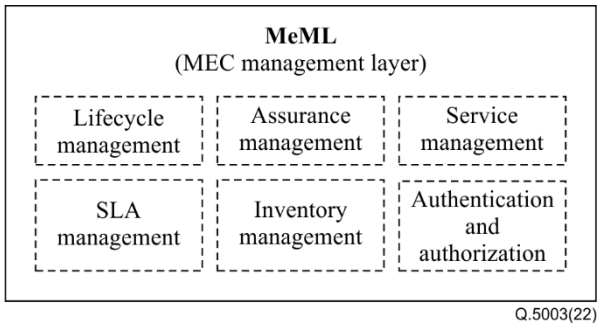

Figure 7-3 – Functional entities for the MEC management layer

– The lifecycle management FE supports the on-boarding, instantiation, configuration, scaling and termination of the MEC application and services over the MEC platform. For federated MEC application and service deployment and management, application images and related information are provided by the end-to-end orchestration FE in the MAL or by the MeML of the peering federated MEC associated with the application provider directly. When UE moves, including in roaming scenarios, to the area where the required MEC service or services are not enabled, the FE supports the relocation of MEC instance(s) over MPL between federated MEC systems as well as in an MEC system.

– The assurance management FE provides a data collection, analytics, and report functionality that supports monitoring and tracking resource usage and application status, and so on. The FE reports runtime MEC information including network information and event notification to the subscribed services and application providers via the runtime FE in MAL. When the services and application provider is associated with another federated MEC system, the FE forwards the information to the MeML of the federated MEC system.

– SLA management supports service-level agreement monitoring risk management tools.

– Inventory management FE manages MEC infrastructure resources, platform functions, service and application metadata and status, availabilities and so on; The FE supports direct delivery of onboard application packages to the other federated MEC system's lifecycle management FE through a reference point Exchange between MeMLs, allowing services and application providers of an MEC system to deploy their applications using the MEC resources and services of other federated MEC systems.
– The service management FE manages service information such as service profile, request handling, interaction management and so on.
– The authentication and authorization FE manages the authentication of MAL and authentication of itself to MAL, and it authorizes the MAL to interact with the operator specific federated MEC.

7.1.1.3 MEC platform layer

The MPL provides functionalities which are required for MEC service processing tasks such as service discovery and service availability via other platforms (that may be in the same or a different MEC provider); see also Figure 7–4. The MPL communicates with other MPLs of federated MEC systems through an exchange reference point between them, as an example, for connecting services deployed on another MEC system platform. The discovery and selection of an appropriate MEC system platform and necessary information to establish the connection between them is provided by the end-to-end orchestration FE in the MAL.

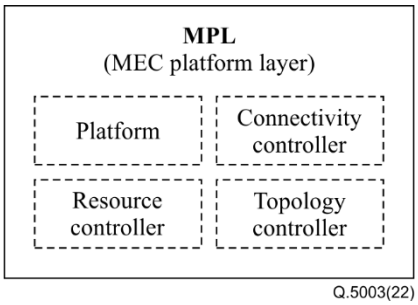

Figure 7-4 – Functional entities for the MEC platform layer

– The platform functions FE supports operator platform specific functions that may contain operator specific APIs and IaaS/PaaS/SaaS functions. When a service request from the serving local MEC application is not locally available, the FE connects the local MEC application to the services on the appropriate other federated MEC system through an exchange reference point between MPLs. Discovery and selection of the appropriate federated MEC system and platform is performed by the MAL and MeML.
– The connectivity controller FE supports the MEC platform to control an operator's specific connectivity resources.
– The resource controller FE supports the MEC platform to control an operator's specific compute, network and storage resources considering the resource sharing policy between services or MEC service providers, and so on. The FE reports runtime MEC information including network information and event notification to the assurance FE in MeML for the use of subscribed service and application providers.
– The topology controller FE maintains both the physical network and virtual network.

7.1.1.4 MEC infrastructure layer

The MIL provides a procedure for allocating and releasing virtualized (compute, storage and networking) resources of the virtualization infrastructure; see also Figure 7–5.

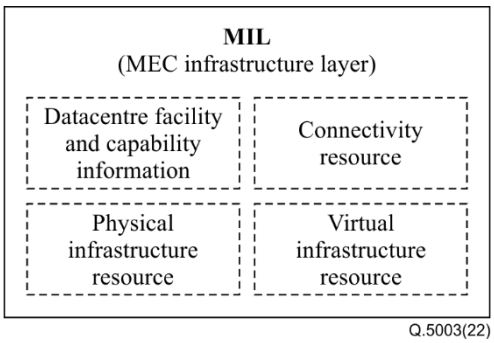

Figure 7-5 – Functional entities for the MEC infrastructure layer

– Datacentre facility and capability information FE manages various infrastructure information such as racks, shelves, network topology, HVAC capabilities and so on.

– Connectivity resource FE provides connectivity resource between multiaccess networks.

– Physical infrastructure resource FE manages resource information such as acommercial-off-the-shelf (COTS) servers, networks or storage hardware with special-purpose hardware components (e.g., AI inferencing accelerator).

– Virtual infra resource FE supports virtualized computing resources including virtual machine and container, network resources and storage resources that can be pooled and shared between services or dedicated to specific services. For the use of subscribed service and application providers, the FE collects and reports requested runtime MEC information including network information and event notification to the resource controller FE in the MPL.

7.1.1.5 UE

UE provides capabilities and an SDK that support specific capabilities and equipment to interact with the MPL; see also Figure 7–6.

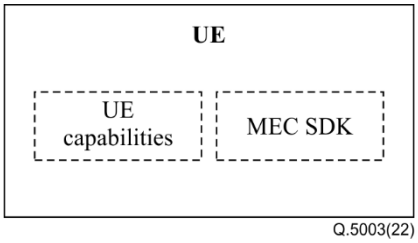

Figure 7-6 – Functional entities for UE

– The UE capabilities FE provides connectivity with the federated MEC by supporting the provisioning and discovery of MEC services and registration and authentication/authorization of the UE as an MEC client. It also supports retrieving UE-related information (e.g., UE location, application/connection status, measurement data) to the federated MEC for MEC service management such as triggering instantiation/termination of MEC applications or placing the MEC applications based on the UE location.

– MEC SDK FE provides a common software library for client-side MEC applications.

7.2 Signalling requirement for reference point MS

This clause describes the interface and messages between service providers and MEC aggregators which aims to deliver a service provider's services requirements to aggregators to distribute their services over multioperator MEC (e.g., service description and requirements — HW, SW, network requirement, etc).

– It is required that reference point MS enable service and application providers to exchange request/response messages with the MAL for the deployment of their services and applications over operator MECs.
– It is recommended that reference point MS allow service and application providers to provide the required information for the optimized orchestration and deployment of their services and applications. The information may include MEC infrastructure requirements, MEC platform requirements, preferred region and data centre to deploy and service availability related requirements, etc.
– It is required that reference point MS enable service and application providers to exchange request/response messages with the MAL for the instantiation, monitoring, updating and deleting their application instances.
– It is required that reference point MS allow service and application providers to access the published catalogues of the operator MECs. The catalogue may include the collection of the operator specific MEC infrastructure resources, MEC platform function capabilities, MEC network capabilities (e.g., capacity, latency), etc.
– It is required that reference point MS allow service and application providers to upload, update and delete application images with necessary information for the instantiations and management of their applications.
– It is recommended that reference point MS allow service and application providers to subscribe to the network information related notification service provided by the operator MECs. The network information may include UE location, radio network information, application instance to UE connection status and traffic throughput, etc.

7.3 Signalling requirement for reference point MA

This clause describes the interface and messages between the aggregator and each operator's MEC to distribute a service provider's service requirements over heterogeneous MEC (e.g., operator's MEC, Public Cloud, etc.).

– It is required that reference point MA allow the MAL to exchange request/response messages with the MeML for operator specific federated MEC resource and application information. The information may include collection of resource usage and application performance monitoring data, analytics and application status, etc.
– It is required that reference point MA allow the MAL to exchange request/response messages with the MeML for MEC service lifecycle management such as onboarding, instantiation, configuration, scaling and termination of the MEC application and services over one or more operator specific federated MEC platforms.
– It is required that reference point MA allow the MAL to interact with the MeML to handle service and application providers' MEC service requests. The MEC service request related information may include service profile and quality of service (QoS) requirements, etc.
– It is required that reference point MA enable the MAL and the MeML to authenticate each other.
– It is required that reference point MA allow MeML to authorize MAL to interact with the operator specific federated MEC.
– It is recommended that reference point MA allow MAL to exchange request/response messages with MeML, related to the discovery and selection of other federated MEC system, datacentres and MEC platforms, for the direct interaction between MeMLs and between MPLs of federated MEC systems through Exchange reference points.

7.4 Signalling requirement for reference point MM

This clause describes the interface and messages between the MeML and the MPL to manage and allocate each operator's cloud and network resources to an onboard service provider's services over each operator's MEC.

– It is required that reference point MM allow the MeML to exchange request/response messages with the MPL for the enforcement of MEC application and service lifecycle management such as onboarding, instantiation, configuration, scaling and termination of them on the corresponding MEC platform.

– It is required that reference point MM allow the MeML to provide executable application images to the MPL for the instantiation of one or more MEC applications on the selected MEC platform(s).

– It is recommended that reference point MM allow the MPL to report run time MEC information including network information and event notification to the runtime FE in the MAL for the use of subscribed service and application providers.

– It is recommended that reference point MM support the relocation of MEC instances between federated MEC systems as well as in an MEC system when it is required.

7.5 Signalling requirement for reference point MP

This clause describes the interface and messages between the MPL and the MIL to control and allocate virtualized HW, SW and network related resources.

– It is required that reference point MP allow the MPL to exchange request/response messages with the MIL to manage the infrastructure resources, such as setup and release of connectivity and physical/virtual infrastructure resources, etc., for the MEC applications and services running on the corresponding MEC platform.

– It is recommended that reference point MP enable the MPL to configure the QoS parameters of the specific MEC application traffic session provided by the connectivity resource in the MIL.

– It is recommended that reference point MP allow the MPL to enforce the routeing and traffic steering rules of MEC application traffic provided by the connectivity resource in the MIL.

– It is recommended that reference point MP allow the MPL to exchange request/response messages with the MIL to collect network related information and event notification. The information and event notification may include radio network performance information, charging and billing related data, network congestion, UE location and connection status, etc.

– It is recommended that reference point MP allow the MPL to exchange request/response messages with the MIL to collect physical/virtual infrastructure resource related information. The information may include infrastructure resource usage statistics, performance monitoring data, and a resource catalogue to be published by the MAL.

7.6 Signalling requirement for reference point MI

This clause describes the interface and messages between MEC service enabled UE and MEC. To guarantee stable QoS over multioperator MEC, the following factors have to be included: multiaccess capability, local breakout roaming scenario and MEC discovery over UE.

– It is required that reference point MI enable UE to exchange request/response messages with operator specific federated MEC via the connectivity resource in the MIL to discover, register to and trigger the MEC service(s). The messages may include UE ID, MEC application ID, required UE capabilities, selected application instance access point information (e.g., URL or IP address), etc.

– It is required that reference point MI enable UE to exchange request/response messages with operator specific federated MEC via the connectivity resource in the MIL to be authenticated and authorized itself.

7.7 Signalling requirement for reference point MM*e*

This clause describes the interface and messages between a neighbour operator's MeML to exchange service packet data or other messages (e.g., service requirements, service related data) if there is any necessity to sync up between different service servers based on each service's usage requirements.

– It is recommended that reference point exchange MM*e* exchange request/response messages to share and update the information of available regions for the MEC service(s). The information may include region ID, name, geographical location, etc.

– It is recommended that reference point MM*e* allow the MeML of the local MEC system to deliver the MEC application package(s) and to forward the lifecycle management messages directly to the peering MeML of a remote federated MEC, allowing service and application providers of an MEC system to deploy their applications using the MEC resources and services of other federated MEC systems. The local MeML may provide a MEC application instantiation request, MEC application requirements and service repository data related to the MEC application, etc. to the federated remote MEC.

– It is recommended that reference point MM*e* allow the MeML of remote peering MeML of the federated MEC to forward the network information and event notification, etc. to the MeML of the local MEC system which delivers the forwarded information to the associated application provider.

– It is recommended that reference point MM*e* exchange request/response messages, in roaming scenario, etc., to support UE to register to the visited MEC service(s). The messages may include the user profile and authentication information, etc.

7.8 Signalling requirement for reference point MP*e*

This clause describes the interface and messages between a neighbour operator's MPL.

– It is recommended that reference point MP*e* provide communication between the local MEC application and services on the peering federated MEC system.

– It is recommended that reference point MP*e* allow the MPL of the visited peer federated MEC to forward the network information (e.g., UE location and connection status), MEC resource usage/performance monitoring data and event notifications to the home MEC MPL, for the use of the MEC service and application provider.

8 Security considerations

This Recommendation provides signalling architecture and requirements for federated MEC environments. Thus, it is assumed that security considerations in general are based on the security framework from network function virtualization [b-ITU-T X.1046] and [b-ETSI GS NFV-SEC 022] and security requirements and architecture for network slice management and orchestration [b-ITU-T X.1047].

Appendix I

Use case of the federated MEC

(This appendix does not form an integral part of this Recommendation.)

I.1 Introduction

MEC is considered a key successful factor in the 5G era that can provide a low latency user experience and huge data volume. In particular, latency sensitive services such as V2X, remote medical services and VR/AR services which have become popular nowadays are expected to have benefits from being hosted in the distributed cloud close to mobile network users.

MEC services are typically envisaged as being offered and supplied by mobile network operators. Currently, these MEC systems have been developing separately and become difference verticals, which will significantly increase the complexity for application providers in extending the reach of applications.

To resolve this limitation, MEC providers need to adopt a federation model to interconnect each separated MEC with unified interfaces. The first approach is to make standardized APIs that will make application providers access various MEC systems effectively. In case of a single public cloud vendor, providing consistent QoE (quality of experience) is uncomplicated. However, it can be very useful to define standardized APIs in heterogeneous MEC systems created by multiple operators. Second, a federated MEC can help address poor MEC coverage. As the federated members share their network and resource capabilities and secure interfaces between their systems, the total MEC coverage can be extended and consistent service delivery can be guaranteed.

I.2 Federation for easy onboarding of application package

When an application provider deploys an application package to an MEC system, many discussions on technical procedures and steps are required in addition to business negotiations with the MEC provider. It requires a lot of time and resources for the application provider and it would be a big burden if the application provider decided to interact with several other MEC providers.

Federated MEC defines and provides standardized APIs to application providers, which can guarantee that technical steps for deployment are same, whether there is interaction with one MEC provider or several MEC providers.

In addition, once an application package is successfully onboarded in one MEC provider, the MEC provider can directly deliver this package to other federated members with the acceptance of the application provider. It will be very valuable to enrich business opportunities of the application provider. For example, if an application provider with a local business wants to expand its MEC-based services globally, the local MEC provider can deliver an application package to a global MEC provider, which can be deployed globally without the application provider's global on-site technical support.

I.3 Federation for supporting consistent user experience across the MEC provider's coverage

MEC aims to provide compute resources at the nearest place to the customer to improve the data transaction latency of contents or services to end users. As MEC systems are appropriate to provide a low latency and high-volume service within a limited range of areas, it would be difficult for MEC providers to facilitate their MEC systems in every location in a short period of time due to equipment installation costs.

When users are located in the MEC service enabled area, their MEC service is handled through the operator's MEC node directly. However, when users move to another area where MEC service or systems are not yet enabled (e.g., roaming scenario), they cannot utilize the reliable low latency based services continually even if they hope to receive the same QoS wherever they are.

In a case of federated MEC, federated MEC providers have already shared related information, such as edge computing resources, network capabilities and the locations of each MEC node, and have interfaces to communicate with each other. When one of the above-mentioned exception scenarios occurs, an MEC provider will be able to find which MEC providers are available and utilize their facilities to provide the same quality of service to users located in that area.

For example, assuming that MEC provider A covers region I and MEC provider B covers regions I and II, and that they support the same capabilities for a mobile service and federate with each other. Mostly, a user of MEC provider A connects with MEC provider A in region I. However, when the user moves to region II, MEC provider A can interwork with MEC provider B to maintain the services that the user is currently using.

I.4 Federation for connecting services deployed on a different MEC system

MEC systems are usually deployed along with mobile network operators, but only the mobile network operator does not have to be an MEC provider. There will be multiple MEC providers over the MEC infrastructure that network operator can physically provide. However. interaction between multiple MEC providers has not yet been considered, especially if MEC providers A and B are deployed on different MNO infrastructures.

On the other hand, the commercial needs that connect with various services are increasing. For example, a voice recognition service can work as a key feature within other services, such as a navigation service. In that case, the voice recognition service provider is not necessarily the same as the navigation service provider, and each service can cooperate under commercial and technical agreements. When it is decided to deploy each service in an MEC system, a different MEC provider can be selected by each service. In these MEC environments, a service-level agreement will be maintained.

Once the federation is performed, the federated members will share information about which application providers are deployed and will find the appropriate MEC system that the application provider wants to communicate with, even if each application is deployed on different MEC systems. Additionally, a communication path for an MEC-to-MEC system will be secured.

Bibliography

[b-ITU-T X.1046] Recommendation ITU-T X.1046 (2020), *Framework of software-defined security in software-defined networks/network functions virtualization networks*.

[b-ITU-T X.1047] Recommendation ITU-T X.1047 (2021), *Security requirements and architecture for network slice management and orchestration*.

[b-ETSI GS MEC 001] ETSI GS MEC 001 (2019), *Multi-access edge computing (MEC) terminology*.

[b-ETSI GS NFV-SEC 022] ETSI GS NFV-SEC 022 (2020), *Network functions virtualisation (NFV) release 2; Security; Access token specification for API access*.

[b-GSMA] GSM Association (2021), *Operator Platform Telco Edge Requirements*, v1.0.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022