



ETSI White Paper No. 28

MEC in 5G networks

First edition – June 2018

ISBN No. 979-10-92620-22-1

Authors:

Sami Kekki, Walter Featherstone, Yonggang Fang, Pekka Kuure, Alice Li, Anurag Ranjan, Debashish Purkayastha, Feng Jiangping, Danny Frydman, Gianluca Verin, Kuo-Wei Wen, Kwihoon Kim, Rohit Arora, Andy Odgers, Luis M. Contreras, Salvatore Scarpina

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org



About the authors

Sami Kekki

Huawei – Editor

Rohit Arora

Hewlett Packard Enterprise

Luis M. Contreras

Telefonica

Yonggang Fang

ZTE

Walter Featherstone

Viavi Solutions

Danny Frydman

Saguna

Feng Jiangping

Huawei

Kwihoon Kim

ETRI

Pekka Kuure

Nokia

Alice Li

Vodafone

Andy Odgers

Quortus

Debashish Purkayastha

Interdigital

Anurag Ranjan

Intel

Salvatore Scarpina

TIM

Gianluca Verin

Athonet

Kuo-Wei Wen

ITRI



Contents

About the authors	2
Contents	3
Introduction	4
Support for Edge Computing in 3GPP	5
Deployment of MEC in 5G	6
5G System architecture & MEC	6
MEC deployment scenarios	9
Traffic steering	10
UE and application mobility	12
Capabilities exposure	13
Charging	15
Regulatory requirements	15
UE application interface	16
MEC Use Case Examples	18
MEC for third-party cloud service providers	18
MEC for Serverless Computing and Cloud Integration for Massive IoT Devices	19
MEC for Enterprise Users	20
MEC for “Industrial IoT”	20
Conclusions	22
List of abbreviations	23
References	25



Introduction

Edge computing as an evolution of cloud computing brings application hosting from centralized data centres down to the network edge, closer to consumers and the data generated by applications. Edge computing is acknowledged as one of the key pillars for meeting the demanding Key Performance Indicators (KPIs) of 5G, especially as far as low latency and bandwidth efficiency are concerned. However, not only is edge computing in telecommunications networks a technical enabler for the demanding KPIs, it also plays an essential role in the transformation of the telecommunications business, where telecommunications networks are turning into versatile service platforms for industry and other specific customer segments. This transformation is supported by edge computing, as it opens the network edge for applications and services, including those from third parties.

ETSI ISG MEC (Industry Specification Group for Multi-access Edge Computing) is the home of technical standards for edge computing. The group has already published a set of specifications (Phase 1) focusing on management and orchestration (MANO) of MEC applications [2, 3], application enablement API [4], service Application Programming Interfaces (APIs) [5, 6, 7, 8] and the User Equipment (UE) application API [9]. The MANO and application enablement functions contribute to enabling service environments in edge data centres, while the service APIs enable the exposure of underlying network information and capabilities to applications. One of the key value-adding features of the MEC specification is this ability for applications to gain contextual information and real-time awareness of their local environment through these standardized APIs. This local services environment is a flexible and extendable framework, as new services can be introduced by following the API guidelines in [10], when creating new service APIs. And finally, the UE application API lets the client application in the UE interact with the MEC system for application lifecycle management.

5G networks based on the 3GPP 5G specifications [11] are a key future target environment for MEC deployments. The 5G system specification and its Service Based Architecture (SBA) leverage the service-based interactions between different network functions, aligning system operations with the network virtualization and Software Defined Networking paradigms. These very same characteristics are shared by MEC specifications. In addition, 3GPP 5G system specifications define the enablers for edge computing, allowing a MEC system and a 5G system to collaboratively interact in traffic routing and policy control related operations. MEC features together with these complementary technical enablers of the 5G system allow integration of these systems to create of a powerful environment for edge computing.

In the following sections of the white paper, we illustrate and explain ways to deploy and integrate MEC in the 5G system. The emphasis of the document is on the opportunities for MEC to benefit from the edge computing enablers of the 5G system specification, and for 3GPP ecosystem to benefit from the MEC system and its APIs as a set of complementary capabilities to enable applications and services environments in the very edge of mobile networks.



Support for Edge Computing in 3GPP

In the 5G system specifications there is a set of new functionalities that serves as enablers for edge computing. These enablers are essential for integrated MEC deployments in 5G networks. This white paper is focused primarily on utilizing these edge computing enablers. The full list of enablers with brief explanations can be found in clause 5.13 of [10].

1. **Local Routing and Traffic Steering:** the 5G Core Network provides the means to select traffic to be routed to the applications in the local data network. A PDU Session may have multiple N6 interfaces towards the data network. The UPFs that terminate these interfaces are said to support PDU Session Anchor functionality. Traffic steering by the UPF is supported by Uplink Classifiers that operate on a set of traffic filters matching the steered traffic, see clause 5.6.4.2 of [10] or alternatively by IPv6 multi-homing, where multiple IPv6 prefixes have been associated with the PDU session in question, see clause 5.6.4.3 of [10].
2. The ability of an Application Function to influence UPF (re)selection and traffic routing directly via the Policy Control Function (PCF) or indirectly via the Network Exposure Function (NEF), depending on the operator's policies, see clause 5.6.7 of [10].
3. The Session and Service Continuity (SSC) modes for different UE and application mobility scenarios. Description of the SSC modes 1, 2 and 3 is found in clause 5.6.9 of [10]
4. Support of Local Area Data Network (LADN) by the 5G Core Network by providing support to connect to the LADN in a certain area where the applications are deployed. The access to a LADN is only available in a specific LADN service area, defined as a set of Tracking Areas in the serving PLMN of the UE. LADN is a service provided by the serving PLMN of the UE, see section 5.6.5 of [10].



Deployment of MEC in 5G

MEC as it is deployed currently in the 4th generation LTE networks, is connected to the user plane via one of the options described in the ETSI White Paper [MEC deployments in 4G and evolution towards 5G](#) [11]. With LTE networks already having been deployed for a number of years, it was necessary to design the MEC solution as an add-on to a 4G network in order to offer services in the edge. Consequently, the MEC system as defined in [1] and in the related interface specifications, is to a large extent self-contained, covering everything from management and orchestration down to interactions with the data plane for steering specific traffic flows.

With 5G, the starting point is different, as edge computing is identified as one of the key technologies required to support low latency together with mission critical and future IoT services. This was considered in the initial requirements. The system was designed from the beginning to provide efficient and flexible support for edge computing to enable superior performance and quality of experience.

The design approach taken by 3GPP allows the mapping of MEC onto Application Functions (AF) that can use the services and information offered by other 3GPP network functions based on the configured policies. In addition, a number of enabling functionalities were defined to provide flexible support for different deployments of MEC and to support MEC in case of user mobility events. The new 5G architecture is described and explained in more detail in the next clause.

5G System architecture & MEC

The 5G system architecture specified by 3GPP and described in [10] has been designed to cater for a wide set of use cases ranging from a massive amount of simple IoT devices to the other extreme of high bit rate, high reliability mission critical services. Supporting all the use cases with the same and common architecture has required significant changes in design philosophies both for the RAN and the core network.

One significant architectural change was made to the communications between the core network functions that until now have relied on a point-to-point paradigm. In the 5G system specification there are two options available for the architecture; one with the traditional reference point and interface approach and the other where the core network functions interact with each other using a Service Based Architecture (SBA). In this white paper the emphasis is on the SBA option of the 5G system architecture.

With the SBA, there are functions that consume services and those that produce services. Any network function can offer one or more services. The framework provides the necessary functionality to authenticate the consumer and to authorize its service requests. The framework supports flexible procedures to efficiently expose and consume services. For simple service or information requests, a request-response model can be used. For any long-lived processes, the framework also supports a subscribe-notify model. The API framework defined by ETSI ISG MEC is aligned with these principles and in fact does exactly the same for MEC applications as the SBA does for network functions and their services. The functionality needed for efficient use of the services includes registration, service discovery, availability notifications, de-registration and authentication and authorization. All this functionality is the same in both the SBA and the MEC API frameworks.

In the figure below the 3GPP 5G system with its SBA is shown on the left, while the MEC system architecture is on the right. In the remainder of this white paper the focus is on describing how to deploy the MEC system in a 5G network environment in an integrated manner where some of the functional



entities of MEC (blue boxes in MEC system part) interact with the network functions of the 5G core network.

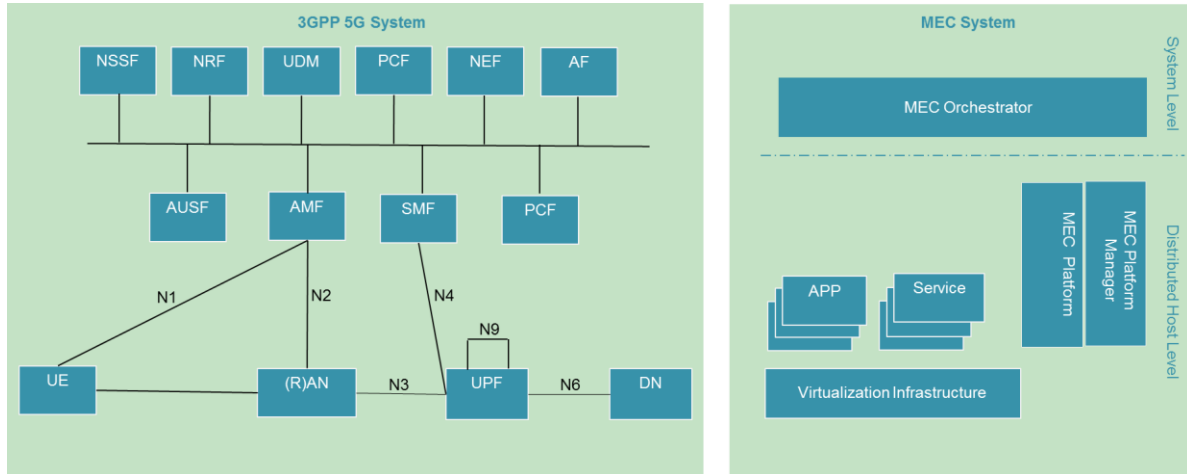


Figure 1. 5G Service-Based Architecture and a generic MEC system architecture

The network functions and the services they produce are registered in a Network Resource Function (NRF) while in MEC the services produced by the MEC applications are registered in the service registry of the MEC platform. Service registration is part of the Application Enablement functionality [4]. To use the service, if authorized, a network function can directly interact with the network function that produces the service. The list of available services can be discovered from the NRF. Some of the services are accessible only via the NEF, which is also available to untrusted entities that are external to the domain, to access the service. In other words, the NEF acts as a centralized point for service exposure and also has a key role in authorizing all access requests originating from outside of the system.

In addition to AF, NEF and NRF, there are a number of other functions that are worth introducing. The procedures related to authentication are served by the Authentication Server Function (AUSF).

One of the key concepts in 5G is Network Slicing that allows the allocation of the required features and resources from the available network functions to different services or to tenants that are using the services. The Network Slice Selection Function (NSSF) is the function that assists in the selection of suitable network slice instances for users, and in the allocation of the necessary Access Management Functions (AMF). A MEC application, i.e. an application hosted in the distributed cloud of a MEC system can belong to one or more network slices that have been configured in the 5G core network.

Policies and rules in the 5G system are handled by the PCF. The PCF is also the function whose services an AF, such as a MEC platform, requests in order to impact the traffic steering rules. The PCF can be accessed either directly, or via the NEF, depending whether the AF is considered trusted or not, and in the case of traffic steering, whether the corresponding PDU session is known at the time of the request.

The Unified Data Management (UDM) function is responsible for many services related to users and subscriptions. It generates the 3GPP AKA authentication credentials, handles user identification related information, manages access authorization (e.g. roaming restrictions), registers the user serving NFs (serving AMF, Session Management Function (SMF)), supports service continuity by keeping record of SMF/Data Network Name (DNN) assignments, supports Lawful Interception (LI) procedures in outbound roaming by acting as a contact point and performs subscription management procedures.



The User Plane Function (UPF) has a key role in an integrated MEC deployment in a 5G network. UPFs can be seen as a distributed and configurable data plane from the MEC system perspective. The control of that data plane, i.e. the traffic rules configuration, now follows the NEF-PCF-SMF route. Consequently, in some specific deployments the local UPF may even be part of the MEC implementation.

The following figure shows how the MEC system is deployed in an integrated manner in 5G network.

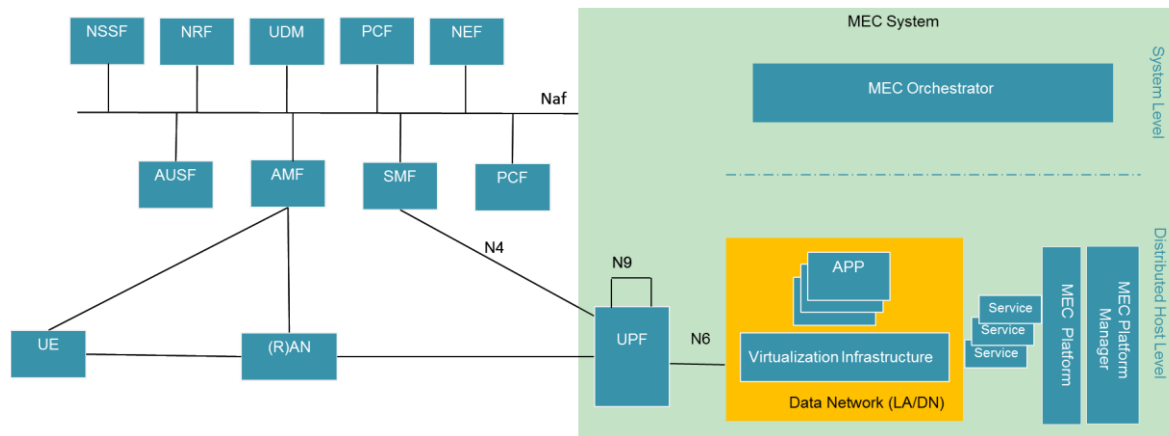


Figure 2. Integrated MEC deployment in 5G network

In the MEC system on the right-hand side of Figure 2 the MEC orchestrator is a MEC system level functional entity that, acting as an AF, can interact with the Network Exposure Function (NEF), or in some scenarios directly with the target 5G NFs. On the MEC host level it is the MEC platform that can interact with these 5G NFs, again in the role of an AF. The MEC host, i.e. the host level functional entities, are most often deployed in a data network in the 5G system. While the NEF as a Core Network function is a system level entity deployed centrally together with similar NFs, an instance of NEF can also be deployed in the edge to allow low latency, high throughput service access from a MEC host.

In this white paper it is assumed that MEC is deployed on the N6 reference point, i.e. in a data network external to the 5G system. This is enabled by flexibility in locating the UPF. The distributed MEC host can accommodate, apart from MEC apps, a message broker as a MEC platform service, and another MEC platform service to steer traffic to local accelerators. The choice to run a service as a MEC app or as a platform service is likely to be an implementation choice and should factor in the level of sharing and authentication needed to access the service. A MEC service such as a message broker could be initially deployed as a MEC app to gain time-to-market advantage, and then become available as a MEC platform service as the technology and the business model matures.

Managing user mobility is a central function in a mobile communications system. In a 5G system it is the Access and Mobility Management Function (AMF) that handles mobility related procedures. In addition, the AMF is responsible for the termination of RAN control plane and Non-Access Stratum (NAS) procedures, protecting the integrity of signalling, management of registrations, connections and reachability, interfacing with the lawful interception function for access and mobility events, providing authentication and authorization for the access layer, and hosting the Security Anchor Functionality (SEAF). With the SBA, the AMF provides communication and reachability services for other NFs and it also allows subscriptions to receive notifications regarding mobility events.



Similarly to the AMF, the Session Management Function (SMF) is in a key position with its large number of responsibilities. Some of the functionality provided by the SMF includes session management, IP address allocation and management, DHCP services, selection/re-selection and control of the UPF, configuring the traffic rules for the UPF, lawful interception for session management events, charging and support for roaming. As MEC services may be offered in both centralized and edge clouds, the SMF plays a critical role due to its role in selecting and controlling the UPF and configuring its rules for traffic steering. The SMF exposes service operations to allow MEC as a 5G AF to manage the PDU sessions, control the policy settings and traffic rules as well as to subscribe to notifications on session management events.

Until now the SBA has been discussed with its network functions and their roles in the 5G system. While they play an essential role in enabling the flexible integration of MEC in the next generation system, there are a few additional high-level concepts worth listing that are essential in providing high performance MEC services with an unparalleled quality of experience.

- Concurrent access to local and central Data Networks (DN) in a single PDU session
- Selection of the User Plane Function for a PDU session close to the UE's point of attachment
- Selection/establishment of a new UPF based on UE mobility and connectivity related events received from the SMF, see the "UE and application mobility" section
- Network Capability Exposure to allow MEC (AF) to request information about UE(s) or request actions towards UE(s), see the "Capabilities exposure" section
- Possibility for MEC (AF) to influence traffic steering for a single UE or a group of UEs, see the "Traffic steering" section
- Support for LI and Charging for MEC in the edge cloud, see the "Regulatory requirements" and "Charging" sections
- Indication about LADN availability for UEs (Local Access Data Network) for specific and local MEC services

MEC deployment scenarios

Logically MEC hosts are deployed in the edge or central data network and it is the User Plane Function (UPF) that takes care of steering the user plane traffic towards the targeted MEC applications in the data network. The locations of the data networks and the UPF are a choice of the network operator and the network operator may choose to place the physical computing resources based on technical and business parameters such as available site facilities, supported applications and their requirements, measured or estimated user load etc. The MEC management system, orchestrating the operation of MEC hosts and applications, may decide dynamically where to deploy the MEC applications.

In terms of physical deployment of MEC hosts, there are multiple options available based on various operational, performance or security related requirements. The following figure gives an outline of some of the feasible options for the physical location of MEC.

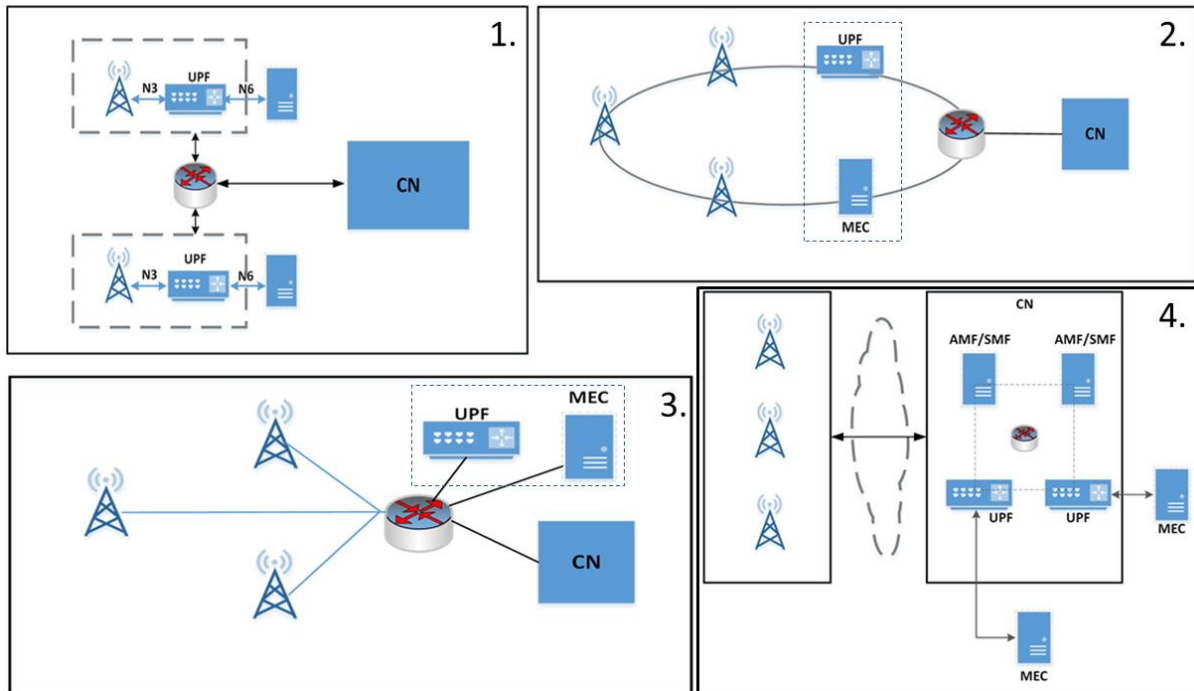


Figure 3. Examples of the physical deployment of MEC.

1. MEC and the local UPF collocated with the Base Station.
2. MEC collocated with a transmission node, possibly with a local UPF
3. MEC and the local UPF collocated with a network aggregation point
4. MEC collocated with the Core Network functions (i.e. in the same data centre)

The options presented above show that MEC can be flexibly deployed in different locations from near the Base Station to the central Data Network. Common for all deployments is the UPF that is deployed and used to steer the traffic towards the targeted MEC applications and towards the network.

Traffic steering

Traffic steering in MEC refers to the capability of the MEC system to route traffic to the targeted applications in a distributed cloud. Whilst in a generic MEC architecture as defined in [1], traffic steering is controlled by the MEC platform through configuring the data plane via the Mp2 reference point. In a 5G integrated deployment the role of the data plane is delegated to the User Plane Function (UPF). A UPF plays the central role in routing the traffic to desired applications and network functions. In addition to the UPF, there are a few related procedures specified by 3GPP that are used to enable flexible and efficient routing of the traffic to applications. One such procedure is the Application Function (AF) influence on traffic routing as described in clause 5.6.7 of [10]. It allows an AF to influence the selection and re-selection of a local UPF as well as request services to configure the rules to allow the traffic steering to a data network.

The toolset offered by a 5G network can be used by the AF, which, in the case of MEC, maps to Functional Entities (FE) of the MEC system. When a MEC application is instantiated, no traffic is routed to the application until the application is ready to receive traffic and the underlying data plane is configured to



route the traffic towards it. This configuration is done by the MEC platform. When deployed in a 5G network, a MEC FE such as a MEC platform, is in the role of a 5G AF towards the 5G core network. It interacts with the PCF to request traffic steering by sending information that identifies the traffic to be steered. The PCF will transform the request into policies that apply to targeted PDU session(s) and provides the routing rules to the appropriate Session Management Function (SMF). Based on the received information, the SMF identifies the target UPF, if it exists, and initiates configuration of the traffic rules there. If no applicable UPF exists, the SMF can insert one or more UPFs in the data path of the PDU session.

In the integrated deployment as described above the data plane functionality of the (generic) MEC architecture is now the responsibility of the UPF. This UPF is influenced by MEC through control plane interactions with 5G core network functions, rather than via a specific reference point that is termed Mp2 in the MEC architecture.

The SMF can also configure the UPF with different options for traffic steering. In the case of IPv4, IPv6, IPv4v6 or Ethernet, the SMF may insert an Uplink Classifier function (UL CL) in the data path. The UL CL can be configured with the traffic rules to forward the uplink traffic towards different targeted applications and network functions, and in the downlink direction it will merge the traffic destined to the UE(s). Alternatively, for PDU Sessions using IPv6 or IPv4v6, and if supported by the UE, the SMF may use the Multi-homing concept for traffic steering. In such a case, the SMF would insert a Branching Point function in the target UPF and configure it to split the UL traffic to a local application instance and the services in the central cloud based on the Source Prefixes of the IP data packets.

The 3GPP 5G system offers a flexible framework for AFs by enabling traffic steering based on a wide set of different parameters. This allows generic traffic rule setting or specific rule setting for certain specific UE(s). The parameters that can be used in traffic steering requests may contain, for instance, information to identify the traffic (DNN, S-NSSAI, AF-Service-Identifier, 5 tuple etc.), a reference ID to preconfigured routing information, a list of DNAs, information about target UE(s), indication about application relocation possibilities, temporal validity condition (timeframe when routing condition is valid), spatial validity condition (location of UE e.g. geographic area), notification type for user plane management notifications and AF transaction ID (enables modifications to the routing rule).

In addition to selecting the UPF and configuring the traffic steering rules, the 5G system also provides efficient tools for MEC Functional Entities, e.g. tools for a MEC platform, or a MEC orchestrator, to monitor the mobility events that relate to users of MEC application instances in local clouds. MEC FEs can subscribe to user plane path management event notifications from SMF(s), in which case it would receive notifications about path changes, e.g. when the Data Network Access Identifier (DNAI) for a particular PDU Session changes. The MEC management functions can use these notifications to trigger traffic routing configuration or application relocation procedures.

The discussion above assumes that the MEC system, with the relevant Functional Entities supported there, are trusted by the 3GPP network and that policies allow direct access from AFs to the 5G Core Network Functions. There are cases however, where a MEC FE needs to request services from the Network Exposure Function (NEF), for example when MEC is not considered trusted and the policy does not allow direct interaction with the 5G Core NFs. Also, whenever the request targets, or may target multiple PCFs, it would be required to go via the NEF.



UE and application mobility

The MEC system combines the environments of networking and computing at the edge of the network to optimize the performance for ultra-low latency and high bandwidth services. One direct consequence of hosting the applications at the edge, possibly even very close to the radio nodes, is the exposure of those applications to UE mobility. The UEs, whether traditional handheld devices or vehicles equipped with V2X systems, are expected to be mobile, and their movements may render the location of the currently used edge application host non-optimal in the long run, even though the underlying network maintained the service continuity between the endpoints. For the MEC system to maintain the application requirements in a mobile environment, application mobility is required. In practice, this means that the application instance that is serving the user is changed to a new location. And consequently, for stateful applications, the user context also needs to be transferred. In wide area MEC deployments it can be anticipated that the MEC hosts in the system are provisioned and configured with the application supported across the system, thus reducing the likelihood that an application needs to be relocated from one host to another. This, however, does not yet remove the need for a user context transfer between the source and the target MEC host for stateful application services.

An application service may be categorized as either a stateful or a stateless service. Application mobility for a stateful service requires transferring and synchronizing the service state between the original and relocated application instance in order to provide service continuity. Service state synchronization highly depends on the implementation of the application itself, thus requiring support from the application developer. In other words, the application must be designed in such a way that multiple instances of the application can run concurrently, and state (context) of the application instance can be captured in the source instance and copied to another instance independently from the operation of the instance itself. Then the service produced by the relocated application instance in the target MEC host can continue in a seamless manner from the state of the application instance in the source MEC host at the time of UE disconnection from that. The support of application mobility for a stateless service, on the other hand, is relatively simple as most likely it will not need service state (application context) transfer and synchronization between the original instance in the source and the instance in the target.

Application mobility is a unique feature of the MEC system. It is necessary to be able to relocate a user's context and/or application instance from one MEC host to another to continue offering an optimized service experience for the user. Application mobility is a part of service continuity support, in which the service to the UE will resume once the user's context and/or application instance has been relocated to another MEC host. The following figure illustrates the basic scenario for application mobility in an integrated MEC deployment in a 5G network.

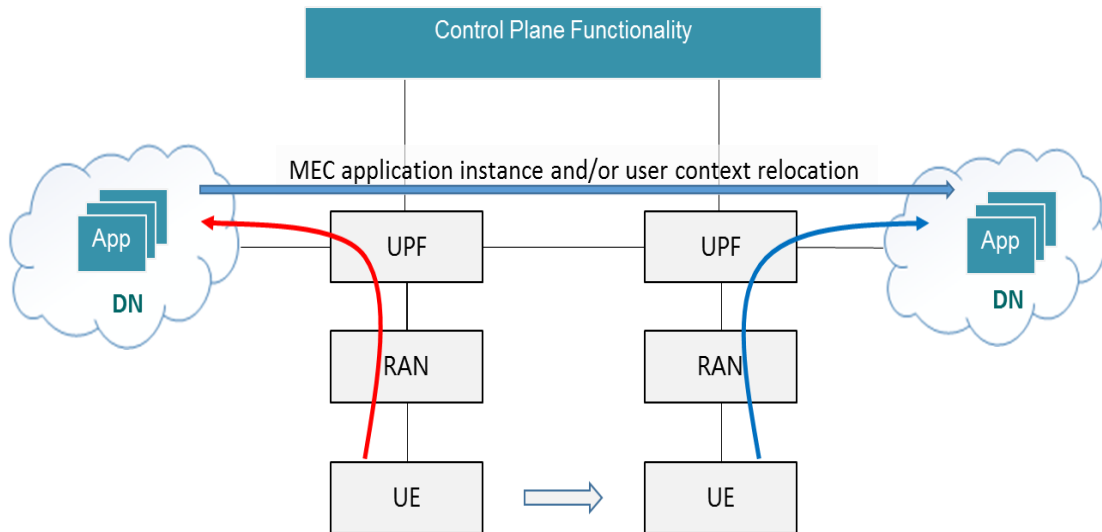


Figure 4. The principle of MEC application mobility.

The MEC application mobility feature is a work in progress in ETSI ISG MEC. The current definitions of the feature are grouped into procedures that may or may not apply depending on the characteristics of the application, environment and capabilities of the MEC host, MEC orchestrator and also of the MEC application itself. The procedures that are currently being developed are application mobility enablement, detection of UE movement, validation of application mobility, user context transfer and/or application instance relocation, and post-processing of application relocation. Ways in which a mobile UE application client may contribute to the enablement of the application mobility service to achieve the service continuity of the application are also being considered.

The detection of UE movement to a new serving cell is one of the triggers for application mobility, which may rely on the 5G Network Exposure Function (NEF) and the ability of the MEC functional entities to subscribe to relevant event notifications available there. The MEC platform may also subscribe to the Radio Network Information produced by the RNIS [5]. Through Radio Network Information the platform can identify UEs experiencing cell change and determine whether they are about to move out of the serving area of the current MEC host.

Applications running in the MEC system may produce a wide range of services from multi-media and gaming to machine type services like V2X. This variety creates significant complexity for application mobility support. The application/service providers should consider all aspects of the application lifecycle in the mobile environment, including the application mobility, when planning their application and its roll-out in the network edge.

Capabilities exposure

As previously highlighted, there is a specific function, namely the Network Exposure Function (NEF), to expose capability information and services of the 5G CN Network Functions to external entities. Such entities could include Application Functions (AF) such as MEC system functional entities. While 5G Service Based Architecture (SBA) also enables direct access to a Network Function for an authorized AF, there are many cases when services and capabilities are exposed over NEF. Those include the following:



- **Monitoring:** Allows an external entity to request or subscribe to UE related events of interest. The monitored events include a UE's roaming status, UE loss of connectivity, UE reachability and location related events (e.g. location of a specific UE, or identification of UEs within a geographical area). The AMF & UDM are the key entities in providing access to such event information.
- **Provisioning:** Allows an external entity to provision expected UE behaviour to the 5G system, for instance predicted UE movement, or communication characteristics.
- **Policy and Charging:** Handles QoS and charging policy for UE based requests made by an external party, which also facilitates sponsored data services. The PCF is the key entity with regard to Policy and Charging Control (PCC), although most NFs are involved to some degree in supporting the PCC framework.

Figure 5 illustrates an example of 5G capability exposure to the MEC system. In this case the MEC orchestrator (MEC system level management) appears as a 5G AF, providing centralized functions for managing the computing resources and operation of the MEC hosts. In addition, it offers orchestration of MEC applications running on MEC hosts. The MEC orchestrator as a 5G AF interacts with NEF and with other relevant NFs with regards to overall Monitoring, Provisioning, Policy and Charging capabilities. The MEC host, on the other hand, might be deployed at the edge of 5G RAN to leverage the advantages of MEC for optimizing the performance of applications and improving users' Quality of Experience. Therefore, it is possible that the MEC platform may need direct exposure to the Centralized Units (CUs) of the 5G RAN and potentially even the Distributed Units (DUs). For example, services offered by a MEC host such as the Radio Network Information Service (RNIS) [5] rely on exposure of the RAN capabilities, especially for the up to date radio information related to UEs. Such information could be used to help MEC applications running on the MEC host to optimize the services offered to those UEs. Directly exposing the radio information, such as received signal received power / quality, to the MEC platform also avoids unnecessary transmission latency and bandwidth consumption of routing messages to its consumers (i.e. MEC applications) via the Core Network. The exposure of local network information is a task of a local NEF instance deployed in the edge.

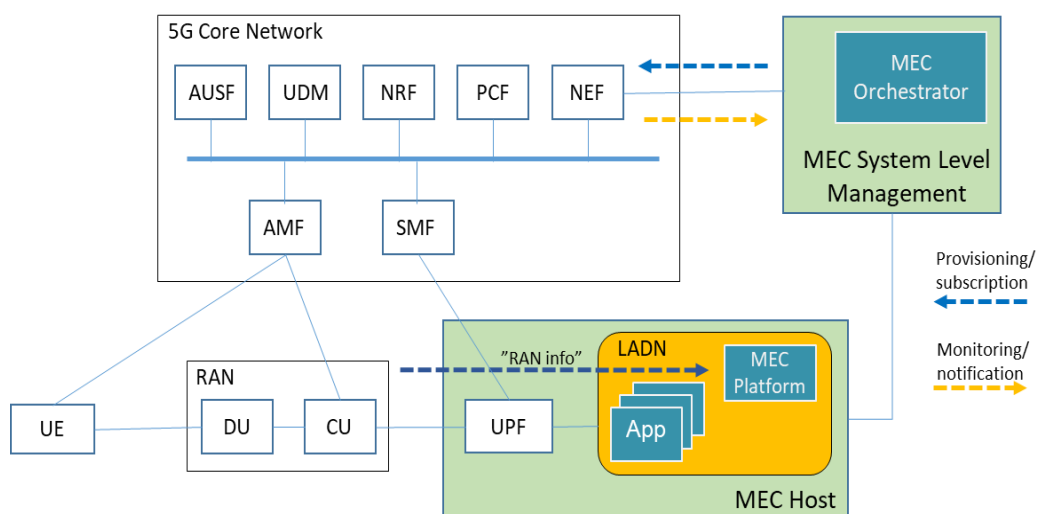


Figure 5. Capabilities exposure (MEC deployed in Local DN).



The MEC system is also able to leverage network capability information exposed by the 5G RAN to provide add-on services to MEC applications. For example, with access to real-time radio signal measurements, the MEC platform, or even a MEC service producing application, may calculate the precise position of a UE and expose it to MEC service consuming application via the MEC Location Service [6]. Such location information could even be provided back to the 5G network, for instance in relation to the NEF offered provisioning capability with regards to UE location predictions. Information can be used by the 5G system to optimize the service to the end user or be used as part of an overall Location-Based Service (LBS) offering, e.g. UE location-based marketing. This latter example illustrates the versatility of the SBA, where also the MEC functions/applications can produce services for the 5G system.

Charging

The integrated deployment of MEC in a 5G system relies on the UPF as the PDU session anchor and gateway to data networks where the MEC environment is deployed. Consequently, the same charging mechanisms and capabilities apply as apply to non-MEC applications.

The transformation of the telco networks into 3rd party service hosting environments where the application cloud becomes an integral part of the telco network calls for new approaches in charging principles and capabilities. Along with the tight integration between 5G NFs such as UPF and SMF and MEC, it is expected that the support of both online charging and offline charging will be relatively straightforward, which would allow 3GPP compliant MEC deployments with charging natively supported for MEC applications.

However more investigation is needed and ETSI ISG MEC looks at the 3GPP charging experts as the source of any new capabilities.

Regulatory requirements

5G Lawful Interception (LI) and Retained Data (RD) continue to play a crucial role in helping Law Enforcement Agencies (LEAs) to combat terrorism and serious criminal activity. LI enables a LEA to perform electronic surveillance on an individual (a target) as authorized by a judicial or administrative order. To facilitate the lawful intercept process, certain legislation and regulations require service providers and Internet service providers to implement their networks to explicitly support authorized electronic surveillance. Actions taken by the service providers include: provisioning the target identity in the network to enable isolation of target communications (separating it from other users' communications), duplicating the communications for the purpose of sending the copy to the LEA, and delivering the Interception Product to the LEA.

In the context of MEC, it is recommended to utilise the LI&RD at SMF and UPF based on the CUPS LI model (Control and User Plane Separation of EPC nodes) as specified in 3GPP Rel-14. The figure below shows an example 5G LI model that is currently under discussion in 3GPP. As explained in the previous sections, the UPF is effectively the data plane for the MEC hosts, thus it is an integral part of the MEC deployment in a 5G network. Consequently, the 3GPP LI&RD is natively supported for MEC application traffic as it is for any application traffic passing the UPF.

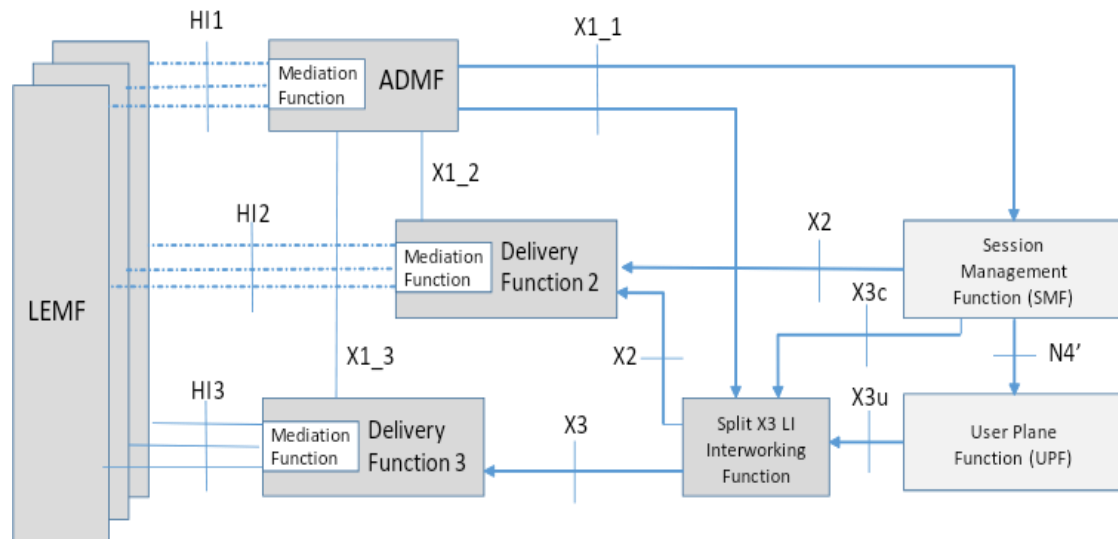


Figure 6. 5G Lawful Interception architecture (3GPP proposal).

UE application interface

In the MEC reference architecture there is one additional reference point of interest that has not been addressed in the previous sections of this white paper. The Mx2 reference point is between the device application and the User Application Lifecycle Management proxy. ETSI ISG MEC has defined a UE Application API over Mx2 reference point in [9]. This API allows the device application to request certain application lifecycle management actions in the MEC system, such as requesting a list of available MEC applications, and instantiation and termination of a new MEC application. Similarly, the API allows the device application to receive notifications of the change of the MEC application's IP address. The MEC applications that have been instantiated in a MEC host in response to a request of a user via a device application are referred to as user applications. In the context of this white paper, the assumption is that the deployment of the user application lifecycle management proxy does not directly impact the rest of the MEC system integration into the 5G system architecture, and any procedures resulting from requests over UE Application API get routed by the Operations Support System (OSS) towards the MEC system level management.

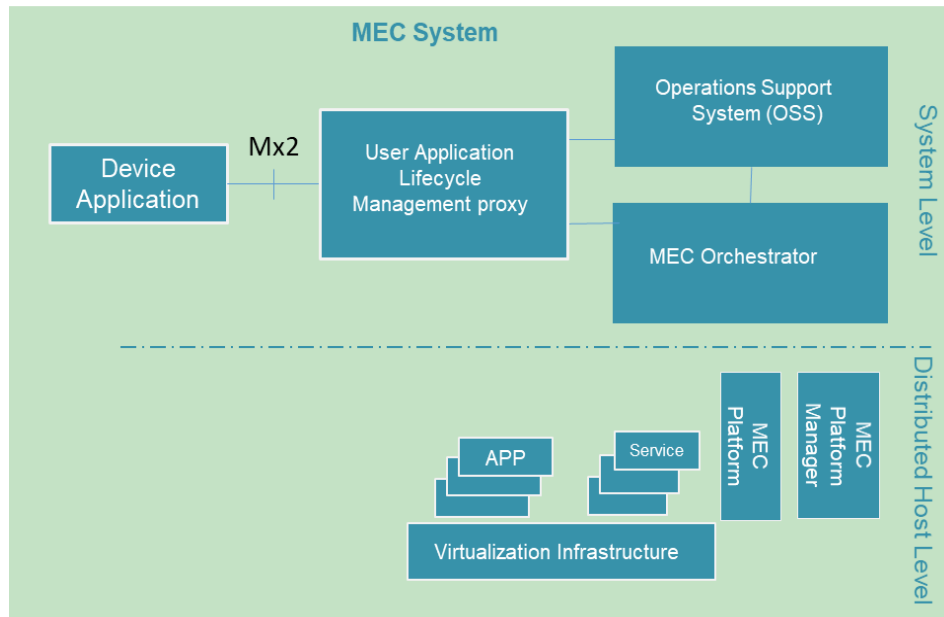


Figure 7. UE application API over Mx2 reference point

For MEC application mobility the UE Application API may be used to assist the MEC system in application/context relocation, as well as in application relocation between different MEC systems or between the MEC system and another cloud system. All these considerations are work in progress in ETSI ISG MEC.



MEC Use Case Examples

This section illustrates the benefits of deploying a MEC system in conjunction with a SBA based 5G network for a selected set of example use cases. In addition, the reader is recommended to consider the 5GAA™ white paper [Toward fully connected vehicles: Edge computing for advanced automotive communications](#) [12], which offers insight into how MEC can benefit Cellular V2X.

MEC for third-party cloud service providers

MEC services are typically envisaged as being offered and supplied by Mobile Network Operators. However, a MEC service can also be offered by the third parties. For instance, third party cloud service providers are entities offering MEC application hosting services and resources, while not being traditional network operators. Examples of such third-party providers willing to deploy edge cloud resources include: venue and facility owners or management companies, cell tower owners and neutral host vendors and vehicle fleet management companies (railway, automotive, etc.). Due to operational complexity, costs, or simply difficulty in deploying MEC in hard to reach areas (for example, due to real estate scarcity), MNOs may buy edge cloud services from such third-party providers to supplement their networks. Typically, MNOs are not involved in day to day management and operation of these third-party edge clouds.

The following diagram shows an example of how a third-party cloud service provider could leverage 5G network functions in harmony with the MEC architecture to provide an edge computing service.

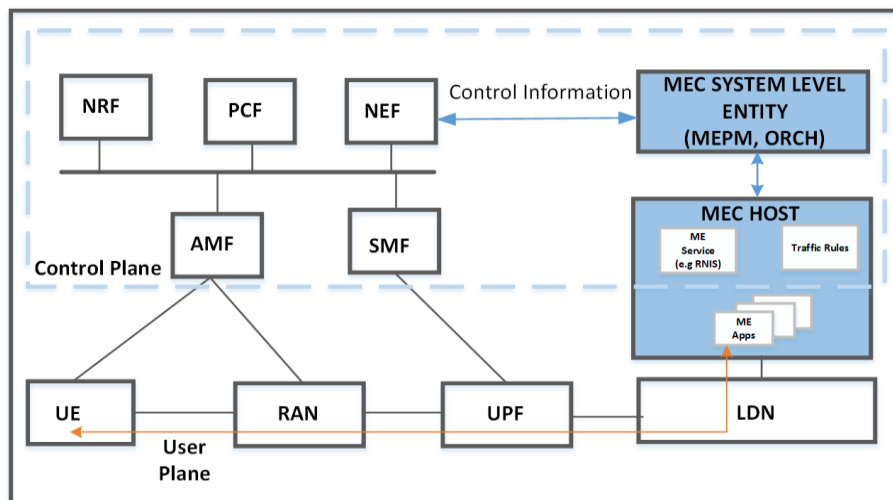


Figure 8. Third-party cloud for MEC in 5G network environment.

The 5G network provides a clear path to enable third party cloud service providers. The Network Exposure Function (NEF) may be used as the entry point in the 5G network for authorized third parties. Using this function, they may configure how appropriate application traffic in the user plane is directed towards MEC applications in Local Data Network (LDN). Also, the NEF may be used for exposing network information such as mobility, radio resource information, etc. to the MEC system. To summarize, the NEF can handle control plane functions for third-party service providers to manage MEC operation. Network information exposed by the NEF is consumed by MEC services and can be exposed to MEC applications. This allows a clear separation between the MNO and the third-party service provider.



User plane traffic is directed towards MEC applications by proper placement and configuration of UPF functions. Authorized third-party cloud service providers can influence the placement and configuration of UPF by using the control interface exposed through NEF.

MEC for Serverless Computing and Cloud Integration for Massive IoT Devices

MEC will enable serverless computing for a key 5G use case, namely, massive IoT devices, by hosting Function as a Service (FaaS) in the edge and supporting integration with the cloud service provider as shown below. In this implementation model FaaS could be implemented through cloud wrapper MEC application(s) running on one or more MEC hosts and provisioned with the required resources, managed locally via an MEC service application. The initial traffic steering from the MEC AF will set up the routes such that the packets from a range of IoT devices are directed to the correct cloud wrapper MEC applications.

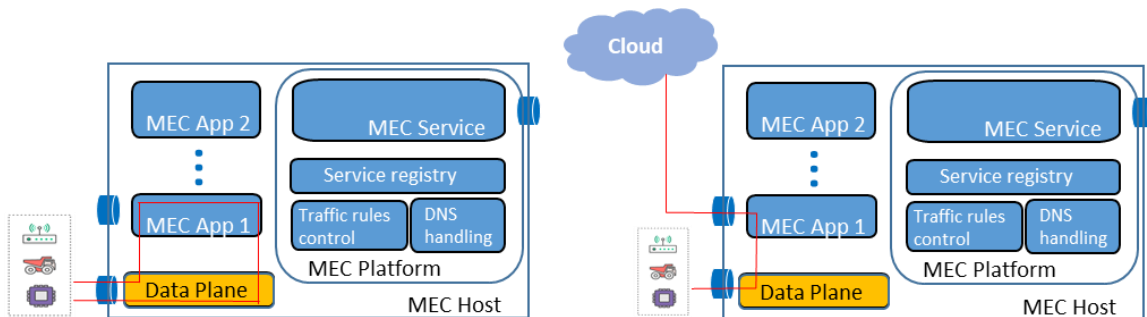


Figure 9. MEC host with and without break-out to cloud.

The egress traffic could be sent back to the IoT device, breakout to a cloud service provider from the cloud wrapper MEC application or transferred to another MEC application with the correct resources. The MEC application and/or MEC service may indicate to the AF to initiate traffic steering to an alternate MEC host with the required resources, if needed. Such indication can be made via traffic rule activation over the application enablement API.

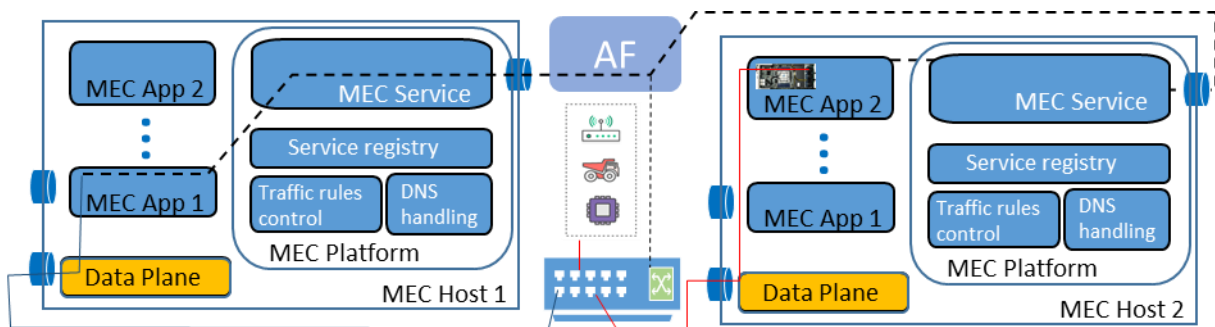


Figure 10. Traffic steering to alternative MEC host.



MEC for Enterprise Users

MEC is envisaged to play an important role in the way 5G penetrates enterprise connectivity and is used to support enterprise applications. Industry sectors such as healthcare, government institutions and fleet management are expected to benefit from MEC-based 5G applications.

However, in order to realize these benefits, the complexity and diversity of requirements associated with various types of enterprise use cases need to be addressed. Here, 5G capabilities, such as network slicing and flexible deployment of UPF, help enable flexible MEC-based deployment that is needed to host such different enterprise applications.

Deployment of MEC for enterprise applications in a corporate office environment could be applied as follows:

A corporate enterprise might require employees to access enterprise apps within the physical location of the corporation. The app can be used for tracking employees, sending training videos, security updates, etc. As explained in previous sections, MEC can exist as an AF within the 5G architecture. Within the 5G architecture, network slicing is very critical and will play an important role in the enterprise setting as well. This can be achieved through the NSSF function in 5G architecture. Within the corporate environment the requirements could be that the VPN connection to the corporate intranet should drop when the employee is out of the physical location. This can be provided by the UPF function in the 5G architecture. As the corporate location represents a limited physical area, the UPF serving that area can be collocated within the MEC site. Specific rules need to be configured in the PCF to provide traffic steering to the dedicated UPF when the enterprise users are trying to access the enterprise applications.

MEC for “Industrial IoT”

IoT has been one of the key drivers for the 3GPP 5G architecture and its requirements have been considered from the outset. There are multiple enablers specifically designed to serve a great variety of IoT use cases. For mission critical IoT services, there is the concept of URLLC (Ultra Reliable Low Latency Communications) that can be enabled by local processing in the Edge Cloud supported by the 5G architecture. The Edge Cloud is also a key component for Massive IoT, where huge amounts of data are processed near the source, where the data may originate from a massive number of sensors. Another key component that is extremely useful for IoT is network slicing, which allows offering dedicated resources for service tenants specifically tailored to their needs. The following presents a few Industrial IoT use cases that may well be deployed with MEC in 5G networks.

1. Security, safety, data analytics for Industrial IoT

This use case groups a number of innovative services for the operator or third party vendors based on the gathering of huge amounts of data (video, sensor information, etc.) from devices, analysed through a certain amount of processing to extract meaningful information before being sent towards central servers. Applications might run in a single location (i.e. on a single host) or be spread over a given area (e.g. campus coverage) or even in the whole network. In order to support the constraints of the operator or the third party requesting the service, the applications might have to be run on all requested locations (MEC hosts).

This use case describes an application running on a MEC host deployed close to the radio network that receives a very large amount of information from devices and sensors connected to the radio node associated with the MEC host. The application then processes the information and extracts the valuable



metadata, which it sends to a central server, likely deployed in a central cloud outside of the mobile network. A subset of the data might be stored locally for a certain period for a later cross-check verification.

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

Security, safety: monitoring of an area for specific events, such as abandoned luggage, authorized access (e.g. with face recognition), car park car monitoring, etc.

Big data: massive sensor data pre-processing, smart factory, etc.

For any of these scenarios the local information can be complemented for example with device location tracking.

2. Active device location tracking

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

The deployment of this use case in a MEC system provides an efficient and scalable solution with local measurement processing. It enables location-based services for enterprises and consumers (e.g. on opt-in basis), for example in venues, retail locations and traditional coverage areas where GPS coverage is not available.

3. Application computation off-loading

In the application computation off-loading use-case, an application in the MEC host executes compute-intensive functionalities with high performance on behalf of mobile devices. By providing rich computation resources on a MEC host, application computation can be off-loaded there, to be accelerated even if a user uses relatively low performance devices, satisfying the user experience regardless of the type of UE.

This use case is effectively used for especially computation-hungry applications such as graphical rendering (high-speed browser, Augmented Reality (AR), Virtual Reality (VR) and 3D gaming, etc.), pre-processing of data (sensor data cleansing, video analytics, etc.), and value-added services (language translation, log analytics, etc.). One example of application computation offloading is the Edge Accelerated Browser (EAB). Most parts of the browsing functions, such as Web content evaluation, rendering and optimized transmission, are off-loaded to the MEC application, while the UE just renders reconstituted browser graphics on its display. Again, by transferring any compute-intensive process from a UE to a MEC host to accelerate an application, a rich application experience is made available on various types of mobile devices.



Conclusions

ETSI has published the baseline MEC standards to allow a standards-based environment for cloud applications in the network edge. Application enablement API and the MEC service APIs are the essential components in the MEC specification for a unified, standards-based environment for context-aware cloud applications. With this set of APIs an application can produce its intended function and it can also produce services for other applications, and discover and consume services produced by other applications and the MEC platform. The APIs for application lifecycle management and for the UE application interface are the other essential part of the published MEC specification. These two APIs are for application lifecycle management. The APIs for MEC application mobility are an ongoing effort in ETSI ISG MEC. New MEC service APIs are also being developed for specific industry applications such as V2X to allow MEC better serve and add value to these applications.

The 3GPP 5G system specification of Rel-15 includes native enablers for edge computing. This white paper has illustrated the potential of these enablers for an integrated MEC deployment in 5G networks. The key components of this integration are the ability of MEC, as a 5G AF, to interact with the 5G system to influence the routing of the edge applications' traffic and the ability to receive notifications of relevant events, such as mobility events, in the 5G system for improved MEC deployment efficiency and end user experience. Moreover, the versatility of the 3GPP service exposure and API frameworks in principle also allows MEC to provide services to the 5G system.

This white paper has demonstrated the benefits of deploying MEC on the N6 reference point of the 5G system. This deployment is enabled by flexibility in UPF location. It is the UPF that implements the data plane for MEC hosts. This data plane is controlled by the SMF of the 5G system and is influenced by MEC as a 5G AF. Whether the physical deployment of MEC is in the RAN or in the core network or somewhere in-between, the role of the UPF remains; it is the data plane for the MEC host and it integrates the MEC application traffic in the 5G bearer stratum, thus enabling charging and LI&RD for that traffic.

The value of ETSI MEC standards remains the same regardless of the way in which MEC is deployed in the 5G system. ETSI MEC standards support a unified, standards-based application environment where the applications are exposed to all application enablement and network information and capabilities through standardized MEC APIs. To sum up, while there are many options to deploy, there is only one application environment for applications to experience.

Standardization of the APIs to expose the required 3GPP system capabilities assumed in this white paper is a work in progress in 3GPP. Interested parties are invited to contribute to this work.



List of abbreviations

3GPP	3 rd Generation Partnership Project
4G, 5G	4 th , 5 th generation of mobile networks
ADMF	Administration Function
AF	Application Function
AMF	Access and Mobility Management Function
API	Application Programming Interface
APN	Access Point Name
APP	Application
AR	Artificial Reality
AUSF	Authentication Server Function
CN	Core Network
CU	Centralized Unit (of RAN)
CUPS	Control/User Plane Separation
DNAI	Data Network Access Identifier
DNN	Data Network Name
DU	Distributed Unit (of RAN)
EAB	Edge Accelerated Browser
EPC	Evolved Packet Core network
ETSI	European Telecommunications Standards Institute
IoT	Internet of Things
IP	Internet Protocol
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
MEP	MEC Platform
MNO	Mobile Network Operator
NEF	Network Exposure Function
NFV	Network Functions Virtualization
NSSF	Network Slice Selection Function
NRF	Network Repository Function
PaaS	Platform as a Service
PCF	Policy Control Function
PDN	Packet Data Network
QoS	Quality of Service
RAN	Radio Access Network
RD	Retained Data
RNIS	Radio Network Information Service
SBA	Service Based Architecture
SMF	Session Management Function
S-NSSAI	Subscribed Network Slice Selection Assistance Information
UDM	Unified Data Management
UE	User Equipment
UL	Uplink



UL CL	Uplink Classifier
UPF	User Plane Function
V2X	Vehicle to Everything
VNF	Virtualized Network Function
VR	Virtual Reality



References

- [1] ETSI GS MEC 003 V1.1.1, “Mobile Edge Computing (MEC); Framework and Reference Architecture” (2016-03)
- [2] ETSI GS MEC 010-1 V1.1.1, “Mobile Edge Computing (MEC); Mobile Edge Management; Part 1: System host and platform management” (2017-10)
- [3] ETSI GS MEC 010-2 V1.1.1, “Mobile Edge Computing (MEC); Mobile Edge Management; Part 2: Application lifecycle, rules and requirements management” (2017-07)
- [4] ETSI GS MEC 011 V1.1.1, “Mobile Edge Computing (MEC); Mobile Edge Platform Application Enablement” (2017-07) ETSI GS MEC 011
- [5] ETSI GS MEC 012 V1.1.1, “Mobile Edge Computing (MEC); Radio Network Information” (2017-07)
- [6] ETSI GS MEC 013 V1.1.1, “Mobile Edge Computing (MEC); Location API” (2017-07)
- [7] ETSI GS MEC 014 V1.1.1, “Mobile Edge Computing (MEC); UE Identity API” (2018-02)
- [8] ETSI GS MEC 015 V1.1.1, “Mobile Edge Computing (MEC); Bandwidth Management API” (2017-10)
- [9] ETSI GS MEC 016 V1.1.1, “Mobile Edge Computing (MEC); UE Application Interface” (2017-09)
- [10] 3GPP TS 23.501 V15.1.0, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 15)” (2018-03)
- [11] ETSI White Paper “MEC deployments in 4G and evolution towards 5G”, February 2018 (http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf)
- [12] 5GAA White Paper “Toward fully connected vehicles: Edge computing for advanced automotive communications”, December 2017 (<http://5gaa.org/news/toward-fully-connected-vehicles-edge-computing-for-advanced-automotive-communications/>)







The Standards People

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

This White Paper is issued for information only. It does not constitute an official or agreed position of ETSI, nor of its Members. The views expressed are entirely those of the author(s).

ETSI declines all responsibility for any errors and any loss or damage resulting from use of the contents of this White Paper.

ETSI also declines responsibility for any infringement of any third party's Intellectual Property Rights (IPR), but will be pleased to acknowledge any IPR and correct any infringement of which it is advised.

Copyright Notification

Copying or reproduction in whole is permitted if the copy is complete and unchanged (including this copyright statement).

© ETSI 2018. All rights reserved.

DECT™, PLUGTESTS™, UMTS™, TIPHON™, IMS™, INTEROPOLIS™, FORAPOLIS™, and the TIPHON and ETSI logos are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ and LTE™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM™, the Global System for Mobile communication, is a registered Trade Mark of the GSM Association.