5GAA Automotive Association

MEC for Automotive in Multi-Operator Scenarios

5GAA Automotive Association
Technical Report

CONTACT INFORMATION:

Lead Coordinator – Thomas Linget
Email: liaison@5gaa.org

MAILING ADDRESS:

5GAA c/o MCI Munich
Neumarkter Str. 21
81673 München, Germany
www.5gaa.org

VERSION:	1.0
DATE OF PUBLICATION:	03.03.2021
DOCUMENT TYPE:	Technical Report
CONFIDENTIALITY CLASS:	P (Public use)
REFERENCE 5GAA WORKING GROUP:	Working Group 2
DATE OF APPROVAL BY 5GAA BOARD:	11.01.2021

Contents

Foreword

This Technical Report has been produced by 5GAA.

The contents of the present document are subject to continuing work within the Working Groups (WG) and may change following formal WG approval. Should the WG modify the contents of the present document, it will be re-released by the WG with an identifying change of the consistent numbering that all WG meeting documents and files should follow (according to 5GAA Rules of Procedure):

x-nnzzzz

(1) This numbering system has six logical elements:

(a) x: a single letter corresponding to the working group:

where x =

T (Use cases and Technical Requirements)

A (System Architecture and Solution Development)

P (Evaluation, Testbed and Pilots)

S (Standards and Spectrum)

B (Business Models and Go-To-Market Strategies)

(b) nn: two digits to indicate the year. i.e. ,17,18 19, etc

(c) zzzz: unique number of the document

(2) No provision is made for the use of revision numbers. Documents which are a revision of a previous version should indicate the document number of that previous version

(3) The file name of documents shall be the document number. For example, document S-160357 will be contained in file S-160357.doc

1 Scope

Edge Computing is an important topic in Vehicle-to-Everything (V2X) use cases, as many such cases ultimately require guarantees of low latency and high reliability. The use cases involve a large amount of regional data which needs to be processed and dispatched locally instead of being uploaded over the internet to its cloud services which, at scale, becomes time- and cost-intensive without generating much added value. Based on the use cases selected in Task 1 [36], the present document includes architecture and deployment models in the event that Edge Computing is used for these V2X use cases. The present document also describes how interoperability and service continuity can be solved.

2 References

[1] 5GAA XW2-190099, Draft MEC4AUTO TR 'Architecture and deployment of Edge Computing for V2X'

[2] 5GAA XW2-190102, 'MEC4AUTO TR architecture wish list for future contributions', Intel, Ericsson, Verison and Mitsubishi, MEC4AUTO call#17 December 2019

[3] ETSI white paper N°24: MEC Deployments in 4G and Evolution Towards 5G, February 2018

[4] ETSI white paper N°28: MEC in 5G networks, June 2018

[5] ETSI GS MEC 003 V2.1.1 (2019-01), Multi-access Edge Computing (MEC); Framework and Reference Architecture

[6] 5GAA_XWI2 190090, 'MEC deployment options in ETSI', Mitsubishi, November 2019

[7] 5GAA_XW2-190021 Interworking between MNOs

[8] SGAMBELLURI, Andrea, TUSA, Francesco, GHARBAOUI, Molka, et al. Orchestration of network services across multiple operators: The 5G exchange prototype. In: 2017 European Conference on Networks and Communications (EuCNC). IEEE, 2017. p. 1-5.

[9] ETSI GS MEC 021 V2.1.1 (2020-01), 'Multi-access Edge Computing (MEC); Application Mobility Service API'

[10] 3GPP TR 23.725 Study on enhancement of Ultra-Reliable Low-Latency Communication (URLLC) support in the 5G Core network (5GC)(Release 16) V16.2.0

[11] 3GPP TS 23.501 3GPP System Architecture for the 5G System V. 15.3.0, 2018-09-17

[12] 5GAA_A-200250, '5G Automotive Association; Working Group System Architecture and Solution Development; V2X Application Layer Reference Architecture', March 2020

[13] 3GPP, 'TR 23.786 - Study on architecture enhancements for the Evolved Packet System (EPS) and the 5G System (5GS) to support advanced V2X services', June 2019

[14] 3GPP, 'TS 23.286 - Application layer support for Vehicle-to-Everything (V2X) services; Functional architecture and information flows', March 2020

[15] 3GPP, 'TS 23.287 - Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services', Dec. 2019

[16] 3GPP, 'TS 23.502 - Procedures for the 5G System (5GS)', Dec. 2019

[17] 3GPP, 'TS 23.288 - Architecture enhancements for 5G System (5GS) to support network data analytics services (Release 16)', Dec. 2019

[18] 3GPP, 'TR 23.764 - Study on enhancements to application layer support for V2X services', March 2020

[19] AECC, 'Technical Report v2.0 - Automotive Edge Computing Consortium (AECC) - Technical Solution Working Group (WG2) - Driving Data to the Edge: The Challenge of Data Traffic Distribution', Jul. 2020, Link

[20] 3GPP, 'TS 23.682 - Architecture enhancements to facilitate communications with packet data networks and applications', Mar. 2012 (Rel. 11)

[21] The Linux Foundation, 'Cloud Native Computing Foundation ('CNCF') Charter', Dec. 2018, Link

[22] Microsoft Azure, 'What are public, private, and hybrid clouds? Understanding your options', Link

[23] Docker, 'What is a Container? A standardised unit of software', Link

[24] RedHat, 'What's a service mesh?', Link

[25] Mike Preston, 'The Declarative Power of APIs', Oct. 2018, Link

[26] API Evangelist, 'Imperative, Declarative, and Workflow APIs', Jul. 2019, Link

[27] ETSI GR MEC 017 V1.1.1 (2018-02), 'Mobile Edge Computing (MEC); Deployment of Mobile Edge Computing in an NFV environment'

[28] ETSI GS NFV-IFA 014: 'Network Functions Virtualisation (NFV); Management and Orchestration; Network Service Templates Specification

[29] ETSI white Paper No. #32, ' Network Transformation;(Orchestration, Network and Service Management Framework)', October-2019, available at https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_White_Paper_Network_Transformation_2019_N32.pdf

[30] SGAMBELLURI, Andrea, TUSA, Francesco, GHARBAOUI, Molka, et al. Orchestration of network services across multiple operators: The 5G exchange prototype. In: 2017 European Conference on Networks and Communications (EuCNC). IEEE, 2017. p. 1-5

[31] 5GAA XW2-200059: 'NFV framework for MEC deployment', May 2020

[32] 3GPP, 'TS 23.558 - Architecture for enabling Edge Applications (Rel. 17)', V0.4.0, August 2020

[33] ETSI White Paper n.36, Harmonising standards for Edge Computing - A synergised architecture leveraging ETSI ISG MEC and 3GPP specifications', July 2020, Link

[34] 3GPP, 'TS 23.222 - Common API Framework for 3GPP Northbound APIs (Rel. 17)', V17.1.0, July 2020

[35] 5GAA A-200094, 'V2XSRA Application Layer Reference Architecture', https://5gaa.org/wp-content/uploads/2020/06/5GAA_A-200094_V2XSRA-Application-Layer-Reference-Architecture-final.pdf

[36] 5GAA TR XW2-200023, 'Use cases and initial test specifications review', 5GAA MEC4AUTO TR (Task 1)

[37] National Institute of Standards and Technology. NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, Available online (retrieved 12 Aug 2020)

[38] 'Presidency of the Council: 'Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety. The text on the Regulation which the Presidency submits for approval as a General Approach appears in annex,' 201 pages, 11 June 2015, PDF'. Archived from the original on 25 Dec. 2015. Retrieved 30 Dec. 2015

[39] 3GPP TR 28.814, 'Management and orchestration; Study on enhancements of Edge Computing management', Rel' 17, August 2020

[40] ETSI GR MEC 035, Study on inter-MEC systems and MEC-cloud systems coordination

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	Third-Generation Partnership Project
5GAA	5G Automotive Association
5GC	5G Core
5GS	5G System
AC	Application Client
AECC	Automotive Edge Computing Consortium
AF	Application Function
AM	Asset Management
AMF	Access and Mobility Management Function
API	Application Programming Interface
APN	Access Point Name
AR/VR	Augmented Reality and Virtual Reality
AS	Application Server
ASP	Application Service Provider
CAPIF	Common API Framework
CNCF	Cloud Native Computing Foundation
CO	Central office
CSF	Cyber Security Framework
BDT	Background Data Transfer
BSM	Basic Safety Message
DHCP	Dynamic Host Configuration Protocol
DN	Data Network
DNN	Data Network Name
DNS	Domain Name System
EAS	Edge Application Servers
ECS	Edge Configuration Server
ECSP	Edge Computing Service Provider
EDN	Edge Data Network
EEA	European Economic Area
EEC	Edge Enabler Client
EES	Edge Enabler Servers
ECU	Electronic Control Unit
eNB	evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
E2E	End-to-End
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
ETSI ISG	ETSI Industry Specification Group
IMA	Intersection Movement Assist
IoT	Internet of Things
IP	Internet Protocol
IPX	IP Exchange
I-UPF	Intermediate UPF
IVE	In-Vehicle Entertainment
GDPR	General Data Protection Regulation
GRX	GPRS roaming exchange
GSMA OPG	GSM Association Operator Platform Group
GW	Gateway
HTTP	Hypertext Transfer Protocol
IQN	In-advance Quality of Service Notification
KPI	Key Performance Indicator
KVM	Kernel VM
LAN	Local Area Network
LBO	Local Breakout
LCM	Life Cycle Management
MANO	Management and Orchestration

ME	Mobile Edge
MEC	Multi-access Edge Computing
MEO	Multi-access Edge Orchestrator
MEP	MEC Platform
MEAO	Mobile Edge Application Orchestrator
MEPM	MEC Platform Manager
MNO	Mobile Network Operator
MSP	Mobility Service Provider
NAT GW	Network Address Translation GW
NEF	Network Exposure Function
NFV	Network Function Virtualisation
NG-RAN	Next Generation RAN
NIST	National Institutes of Standards and Technology
NMS	Network Management System
NS	Network Services
OBU	Onboard Unit
OEM	Original Equipment Manufacturer
PCF	Policy Control Function
PDN	Packet Data Network
PDU	Protocol Data Unit
PGW	PDN Gateway
PoP	Point-of-Presence
PSA	PDN Session Anchor
QoS	Quality of Service
RAN	Radio Access Network
RSU	Road Side Units
RTA	Road Traffic Authority
SA	Service Architecture
SAE	System Architecture Evolution
SGW	Serving Gateway
SCEF	Service Capability Exposure Function
SIPTO	Selective IP Traffic Offload
SMF	Service Management Function
SMS	Short Message Service
SLA	Service Level Agreement
SoA	State of Art
SP	Service Provider
SSC	Session and Service Continuity
ToD	Tele-operated Driving
UE	User Equipment
ULCL	Uplink Classifier
UPF	User Plane Function
URLLC	Ultra-Reliable Low-Latency Communication
V2X	Vehicle-to-Everything
VAE	V2X application enabler
VI	Virtualisation Infrastructure
VIM	Virtualisation Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Functions
VNFM	Virtual Network Function Manager
VRU	Vulnerable Road Users
WAN	Wide Area Network
WG	Working Groups
WI	Work Item

4 Definition of Edge Computing

Edge Computing refers to a broad set of techniques designed to move computing and storage out of the remote cloud (public or private) and closer to the source of data. For the emerging class of '5G Applications' this is often a matter of necessity. Locating such applications in a traditional cloud does not allow one to meet certain stringent requirements, such as roundtrip latency. In other cases, such as the Internet of Things (IoT) and Vehicle-to-Everything communication, the amount of data is expected to increase rapidly. Edge Computing can mitigate this by collecting and processing data closer to the user.

Multi-access Edge Computing (MEC) enables successful deployment of new use cases and various services that can be customised according to the customer requirements and demands. Some key applications and use cases are: video content delivery optimisation, video stream analytics and video surveillance, augmented reality and virtual reality (AR/VR), enterprise applications enablement and local breakout, applications with critical communication needs such as road traffic safety and control, autonomous cars, industrial IoT and healthcare, connected cars, IoT applications and gateway, location and context-aware services, as well as smart city applications.

The current prevalent distributed computing software development model uses a client-side to initiate server requests and a remote server-side to process these requests (the client-server model). This allows application developers to take advantage of centralised compute and storage and has been a major driver of the emergence of cloud computing. However, for MEC applications, developers need to identify features of their applications that require processing at the edge as distinct from features that require high compute power, or that do not require near real-time response and can, therefore, be deployed at a central location. Applications have to be designed in a way which supports distributed processing, synchronisation of contexts, and multi-level load-balancing.

To provide these new services and make the most out of MEC, it is also important for application developers and content providers to understand the main characteristics of the MEC environment and the additional services which distinguish MEC from other 'edge computes', namely: extreme user proximity, ultra-low latency, high bandwidth, real-time access to radio network and context information, and location awareness.

The automotive market is one of the key vertical segments driving the introduction of Edge Computing. Figure 4-1 below depicts a typical automotive scenario, where multiple vehicles, potentially belonging to different car OEMs and other devices (e.g. smartphones and other Vulnerable Road Users, VRUs) are connected to infrastructure (Road Side Units, RSUs) and a cellular network (RAN). The client application instances are generically able to communicate with server applications, i.e. at edge clouds, remote clouds, and/or OEM/private clouds.

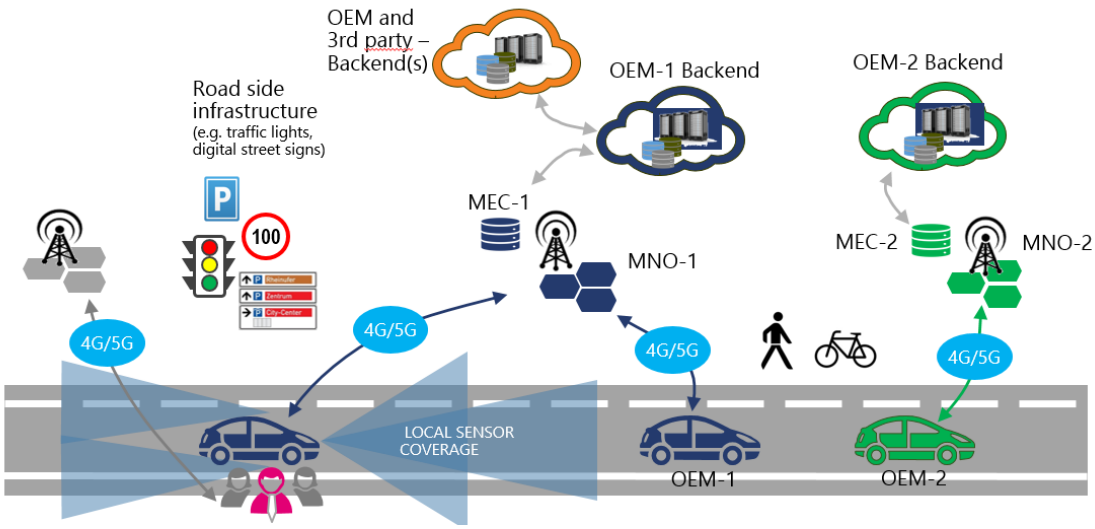

Figure 4-1 - Edge Computing support for automotive scenarios (MEC4AUTO perspective)

4.1 The application perspective (three-tier paradigm)

As a general concept, from an application perspective, the adoption of Edge Computing is introducing a three-tier paradigm shift, i.e. moving from a 'traditional' client-server model of application development. In fact, the emergence of Edge Computing (e.g. MEC) transforms this environment, by introducing an intermediate element at the network edge

(see Figure 4.1-1 below), as an additional MEC point-of-presence (PoP), usually distinct from a traditional remote cloud PoP (e.g. even on a different continent). Different levels of edge deployment are possible, also related to different business models and cloud ownerships; in all such cases, the introduction of MEC is providing additional flexibility to the application developer to specifically design components at the network edge when developing applications.

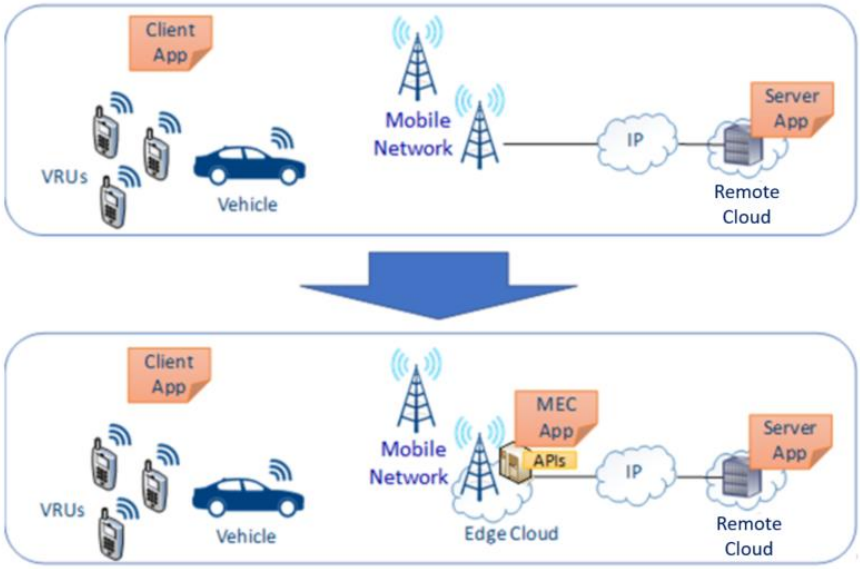

Figure 4.1-1: Example of three-tier paradigm shift from an application development perspective

This results in a new development model with three 'locations': client, near server (at the edge cloud), far server (in a remote cloud). An example is depicted in the above Figure 4.1-1. The client location can be a traditional smartphone (VRU) or other wireless connected compute elements in a car, or again roadside infrastructure. Moreover, the model is quite new to most software developers, not only because of the introduction of an intermediate application instance (at the edge), but also for the possibility for the MEC application to consume data and edge services locally (e.g. exposed through RESTful APIs by the MEC platform), as shown in the Figure 4.1-1.

5 Overview of Edge Computing architecture principles for V2X (SoA)

5.1 Relation to 5GAA V2X Application Architecture

5GAA WG2 has defined a V2X Application Layer Reference Architecture [12]. Figure 5.1-1 is part of that architecture and depicts the Mobile Network Operator (MNO) Edge Cloud providing MEC capabilities.

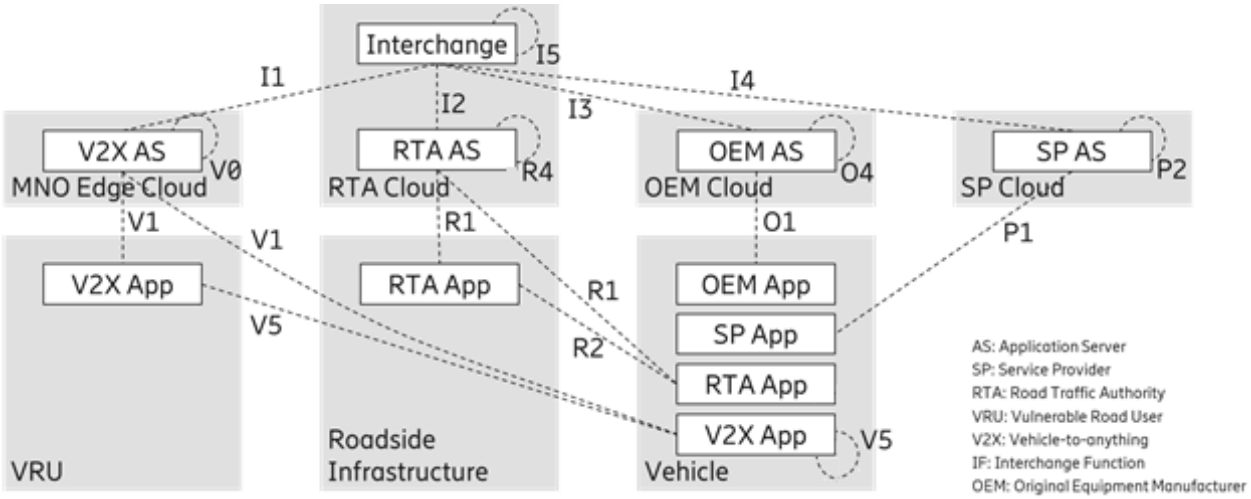

Figure 5.1-1: 5GAA V2X application architecture deployment view including an MNO Edge Cloud for MEC [12]

Figure 5.1-1 does not explicitly show cardinalities expressing how many entities of each exist, but for every cloud entity shown – MNO, Road Traffic Authority (RTA), OEM, and Service Provider (SP) – different instances belonging to the same domain (e.g. company) or different domains can exist. The V0 interface therefore represents inter-MEC communication of Application Servers (ASs) within the same and across different MNOs. On the client side, application instances run at VRUs, roadside infrastructure, and in vehicles. From the server side, potentially all clouds can host application instances. The V1, R1, O1, and P1 interfaces are used between these client applications and ASs, and are realised over mobile radio networks. Details of this realisation are not in the scope of the application architecture, but it is obvious that this is to be done through the 3GPP Uu interface. Additionally, the V5 and R2 application interfaces are included, allowing direct communication between client applications, e.g. using the PC5 interface on radio. V0, R4, O4, and P2 interfaces are used to communicate between ASs, where this is possible (e.g. because they belong to the same service and/or are managed by the same entity, such as an OEM). Alternatively, interfaces I1 to I4 enable communication through an 'interchange' and different interchange nodes can interact through the I5 interface. Details of the interfaces have not been specified in [12]. Figure 5.1-1 shows the interchange to be in the RTA Cloud but this is just an example and other options can be found in [12].

Currently, the architecture assumes that different clouds host ASs directly related to them, e.g. RTA clouds hosting RTA ASs. Cloud computing promotes the idea of relaxing this private cloud approach and allowing other hosting models, including but not limited to Edge Clouds.

5.2 ETSI MEC architecture and deployment options

5.2.1 ETSI MEC architecture

Multi-access Edge Computing is a general framework that enables the implementation of MEC applications as software-only entities that run on top of a virtualisation infrastructure located in or closer to the network edge. The MEC framework is split into the following general entities: system-level MEC entities, host-level MEC entities and network-level MEC entities [5].

The reference service architecture for MEC is shown in Figure 5.2.1-1, as described in [5]

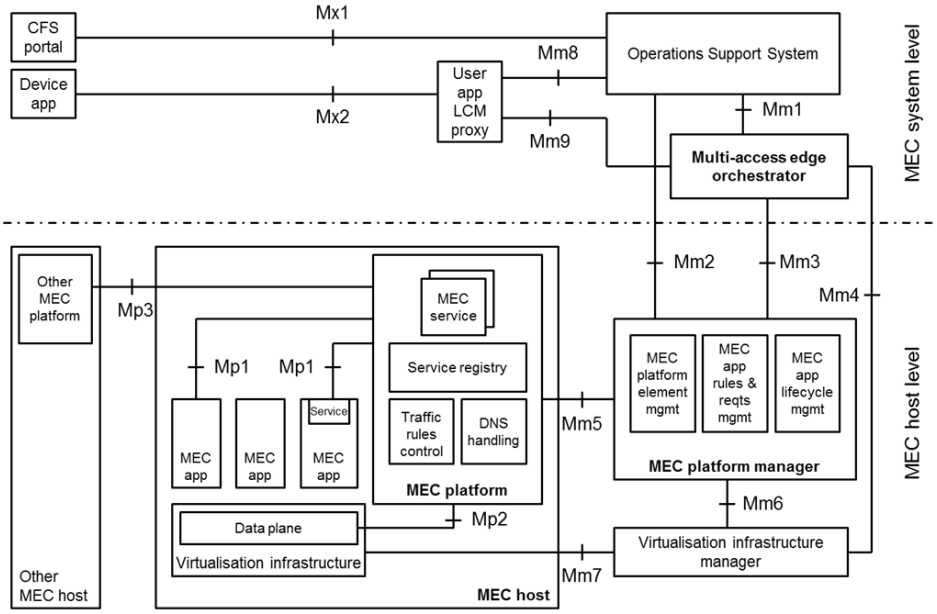

Figure 5.2.1-1: MEC reference service architecture [5]

The general components of the architecture are by the figure above for MEC hosts and the MEC management that are necessary to run MEC applications within an operator network, or a subset of an operator network.

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

The **MEC platform** is the collection of essential functionalities required to run MEC applications on a particular virtualisation infrastructure and enable them to provide and consume MEC services. The MEC platform is providing the following basic functionalities for the MEC system:

- MEC platform is offering an environment where the MEC applications can discover, advertise, consume and offer MEC services, including, when supported, those available via other platforms (that may be in the same or a different MEC system);
- MEC platform is receiving traffic rules from the MEC platform manager, applications, or services, and instructing the data plane accordingly. When supported, this includes the translation of tokens representing user equipment (UE) in the traffic rules for specific IP addresses;
- MEC platform is receiving domain name system (DNS) records from the MEC platform manager and configuring a DNS proxy/server accordingly;
- MEC platform is hosting MEC services;
- MEC platform is providing access to persistent storage and time of day information.

MEC applications are instantiated on the virtualisation infrastructure of the MEC host based on configuration or requests validated by the MEC management. MEC applications are running as virtual machines (VM) on top of the virtualisation infrastructure provided by the MEC host, and can interact with the MEC platform to consume and provide MEC services

The MEC management comprises the MEC system-level management and the MEC host-level management and is derived from so-called management and orchestration (MANO) principles of the virtual network functions (VNFs). The MEC system-level management includes the **multi-access edge orchestrator** as its core component, which has an overview of the complete MEC system.

This orchestrator is responsible for the following functions:

- Maintaining an overall view of the MEC system based on deployed MEC hosts, available resources, available MEC services, and topology;

- On-boarding of application packages, including checking the integrity and authenticity of the packages, validating application rules and requirements, and if necessary adjusting them to comply with operator policies, keeping a record of on-boarded packages, and preparing the virtualisation infrastructure manager(s) to handle the applications;
- Selecting appropriate MEC host(s) for application instantiation based on constraints, such as latency, available resources, and available services;
- Triggering application instantiation and termination.

The MEC host-level management comprises the **MEC platform manager** and the **virtualisation infrastructure manager**, and handles the management of the MEC-specific functionality of a particular MEC host and the applications running on it.

The MEC platform manager is responsible for the following functions:

- Managing the life cycle of applications including informing the multi-access edge orchestrator of relevant application-related events;
- Providing element management functions to the MEC platform;
- Managing the application rules and requirements including service authorisations, traffic rules and DNS configuration, and resolving conflicts between different applications.

The virtualisation infrastructure manager is responsible for the following functions:

- Allocating, managing and releasing virtualised (compute, storage and networking) resources of the virtualisation infrastructure;
- Preparing the virtualisation infrastructure to run a software image: the preparation includes configuring the infrastructure, and can include receiving and storing the software image;
- Collecting and reporting performance and fault information about the virtualised resources;
- When supported, performing application relocation: for application relocation from/to external cloud environments, the virtualisation infrastructure manager interacts with the external cloud manager to perform the application relocation.

5.2.2 ETSI MEC architecture in NFV

In this section, we discuss some aspects of the integration and deployment of MEC in ETSI's network function virtualisation (NFV) architecture framework. The motivation behind the ETSI NFV concept and architecture is to improve the management and interoperability of network services by defining and orchestrating/chaining multiple virtual network functions, thereby reducing the cost of deployment [27]. The general NFV framework is shown in Figure 5.2.2-1.

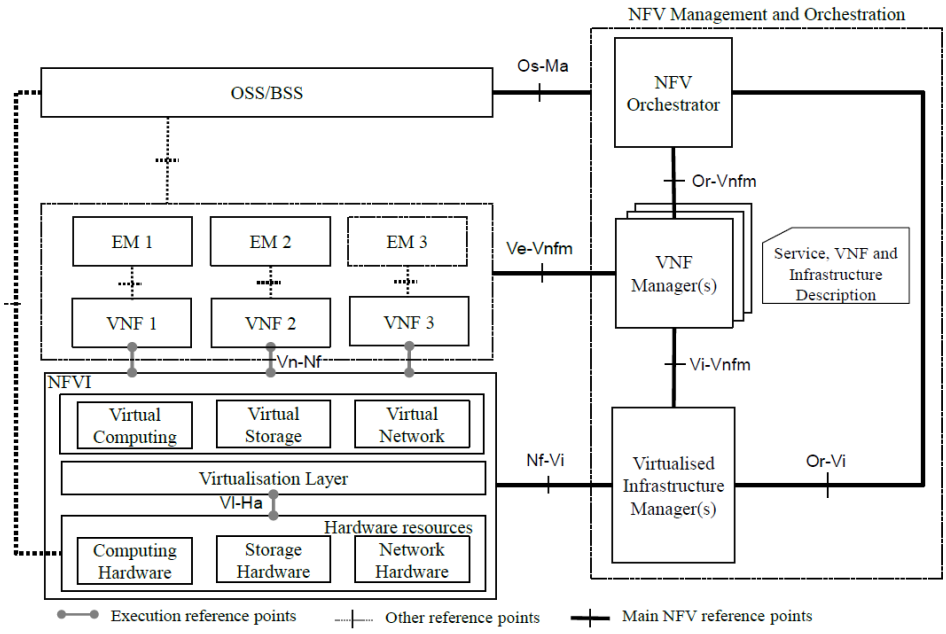

Figure 5.2.2-1: NFV reference service architecture [27]

The basic assumptions taken in [26] regarding the integration of the MEC and NFV architectures are given in the following:

1. The mobile edge platform (MEPM) is deployed as a virtual network functions using the procedures defined by ETSI NFV group.

2. The ME applications appear like VNFs towards the ETSI NFV MANO components.

3. The virtualisation infrastructure is deployed as a network function virtualisation infrastructure (NFVI) (using the NFV terminology) and its virtualised resources are managed by virtual infrastructure management (VIM), as defined by the ETSI NFV group.

Regarding the management plane of the MEC architecture, it is assumed that the ME application's VNFs will be managed individually, allowing the MEC node to delegate certain 'orchestration' and life cycle management (LCM) tasks of the ME applications to the network function orchestrator (NFVO) and virtual network function manager (VNFM) functional blocks.

The MEPM, as defined in the MEC reference architecture, is mapped onto the NFV, resulting in a 'MEPM-V' that delegates the LCM of the MEPM part to one or more VNFM(s).

Life cycle management of VNFs consists of various procedures such as: on-boarding, enablement, instantiation, termination, querying, disablement and deletion.

The Mobile Edge Orchestrator (MEO), as defined in the MEC reference architecture is transformed into a Mobile Edge Application Orchestrator (MEAO) that uses the NFVO for resource provisioning for the MEPM and for orchestrating the set of ME applications as one or more NFV Network Services [27].

The overall architecture of MEC in an ETSI-NFV environment is recalled in Figure 5.2.2-2 below where MEC-specific interfaces, NFV specific interfaces and some new joint MEC-NFV interfaces are presented.

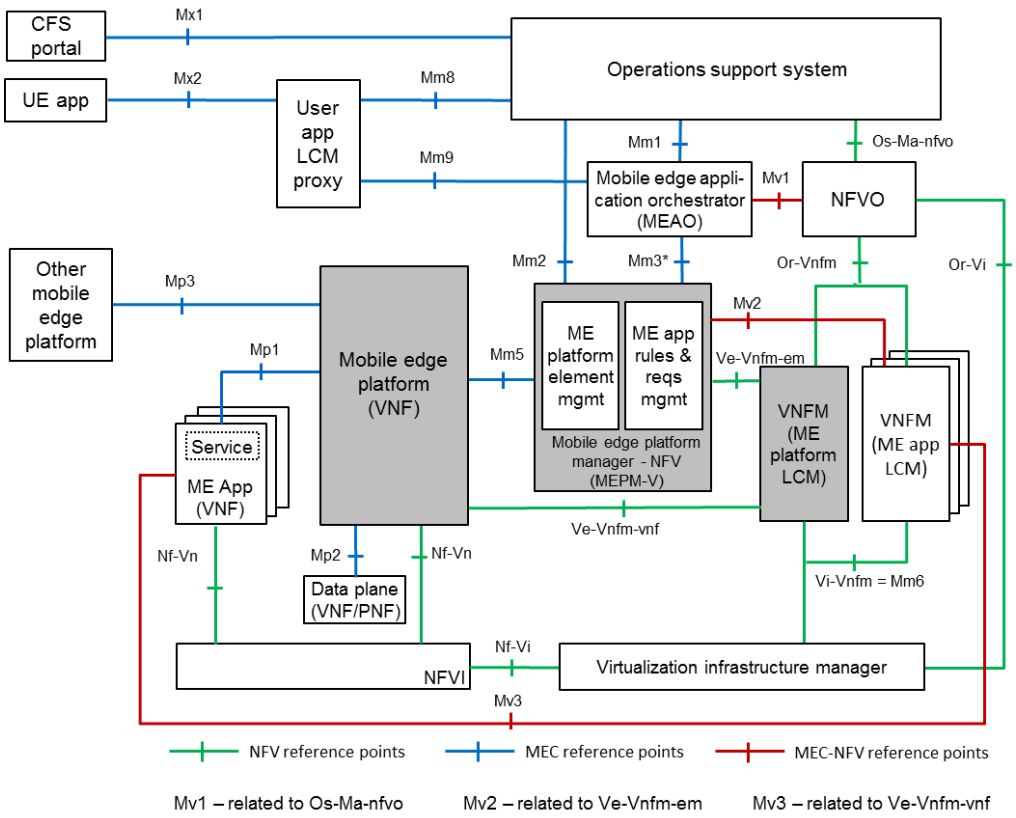

Figure 5.2.2-2: MEC architecture in NFV environment

The blue reference points in the figure are the standard MEC reference points, the green reference points are the standard ETSI-NFV reference points while the red ones are new hybrid reference points that are coordinating the MEC and ETSI-NFV architectural elements. These new reference points (Mv1, Mv2 and Mv3) are introduced to support the management of ME apps and the MEPM as VNFs.

5.2.3 ETSI MEC deployment options

The MEC service architecture seen above is essentially an application layer architecture where the MEC system, host, platform and their related management plane are built upon infrastructure virtualisation that is external to 3GPP networks. State-of-the-art deployment options for MEC are viewed as ways to promote interworking between the MEC application architecture and the access/core network of the MNO. If the MEC is considered as an application function (AF), this interworking may be viewed as a means of exposing MNO information to the MEO. In cases involving NFV deployment of MEC, the management entities of the NFV architecture may be used to find the point of presence (PoP) of the virtual mobile edge app or the MEPM-V. Next, we present some deployment options for the MEC system in 4G and 5G networks, focusing essentially on 5G networks.

In [6] we have presented different deployment options for MEC systems in 4G and 5G networks. For 4G networks, the following deployment options are possible:

- **Bump-in-the-wire approach**: The MEC platform and applications may be deployed in between the access and core network. In this case, the MEC platform sits on the S1 interface of the 4G system architecture. The MEC host's data plane has to process user traffic encapsulated in GTP-U packets, thus requiring the appropriate handling of these tunnels. A dedicated solution may be required (e.g. the MEC GW) to handle operations such as lawful interception and charging. In this solution, low latency is supported by installing the MEC platform all the way down to the eNB, or in locations that ensure minimal latency.
- **Distributed EPC approach:** The MEC platform and applications are located in this deployment through the operator's evolved packet core network (EPC). Different options are possible for the distributed EPC approach: the MEC host is external to the 3GPP network and the MEC data plane is behind the SGi interface. In order to steer U-plane traffic towards the MEC system, two elements – the local DNS of MEC and the PDN Gateway (PGW) of a distributed EPC – play critical roles. Another option of the distributed EPC is to deploy MEC hosts close to the Serving Gateway (SGW) and PGW of the EPC [6]. A last option the MEC host is collocated with the SGW (local breakout, or SGW-LBO). In this case, the MEC platform is a **trusted application of the operator EPC** and the SGW-LBO may be hosted in the MEC platform.

For 5G networks, the MEC system orchestrator (MEAO) exchanges information with the MNO network by the means of network exposure function or NEF. In this case, the MEAO may be viewed as a trusted application function of the MNO, see Figure 5.2.3-1.

The User Plane Function (UPF) of the 5G [4] core network takes care of steering the user plane traffic towards the targeted MEC applications in the PDN network. The locations of the data networks and the UPF are a choice of the network operator who 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.

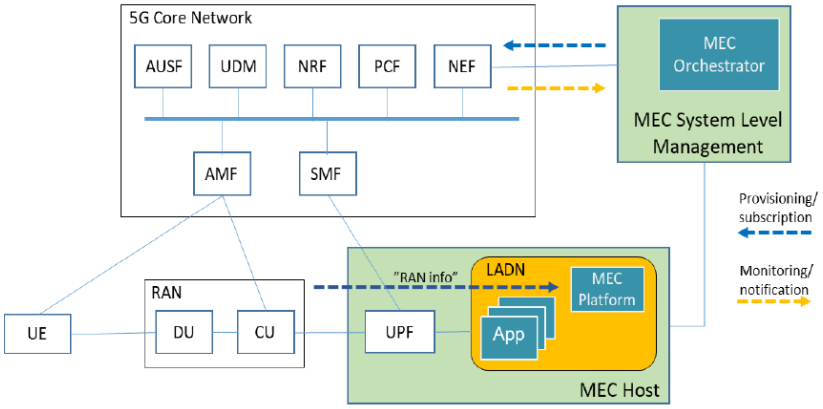

Figure 5.2.3-1: Capabilities exposure between MEC and NEF [4]

For NFV deployment of MEC, the MEC platform is considered as a virtual network function and a trusted application function (AF) of the MEC within the MNO operator, and may exchange information directly with the core network through a network exposure function.

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

1. Cell site deployment of MEC where the MEC and the local UPF collocated with the Base Station.
2. Central office (CO) deployment of MEC where the MEC collocated with a first network aggregation point that is a local or intermediary UPF I-UPF: this approach is similar to the distributed core network deployments of the 4G network.
3. Main CO deployment of MEC where the MEC and the local UPF are collocated with a second network aggregation point: an approach that is equivalent to the bump-in-the-wire approach of the 4G network.
4. Core CO deployment of MEC where the MEC collocated with the core network functions.

The state-of-the-art deployment options of MEC, as described above, consider the deployment of MEC service architecture in a single MNO network. The MEC system control plane (i.e. the MEAO or the V-MEPM) obtains information from the core network through NEF to determine the PoP of the MEC application in the network.

5.2.4 Multi-MNO MEC deployment options

The MEC multiple operator deployment case is more challenging since multiple operators need to agree on some basic common deployment options, and the interworking between 4G and 5G deployments of MEC nodes should be considered. Two options may be considered from ETSI standardisation, the MEC application mobility and the multi-domain MEC orchestration based on NFV framework [30].

The MEC application mobility feature can be found in the recent ETSI ISG MEC deliverable [9]. The main idea of the application mobility is to relocate the UE and application context between the different operators using a common control plane functionality that is deployed/agreed between them.

The Figure 5.2.4-1 illustrates the principle of MEC application mobility that should be extended to the multi-MNO case.

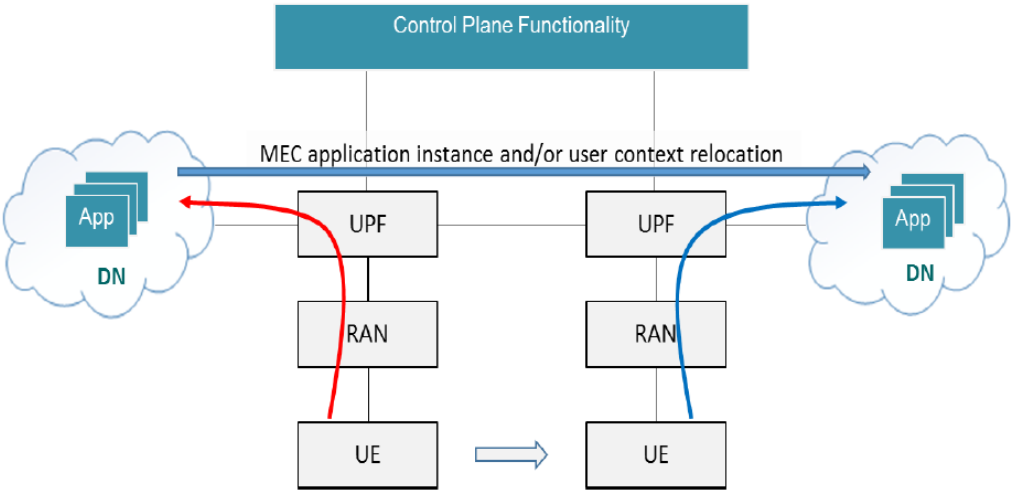

Figure 5.2.4-1: MEC application mobility

Among the options presented in [7], some common interworking or pairing between MEC hosts at different levels seems to be promising, but further studies are needed on this.

5.3 AECC architecture

The Automotive Edge Computing Consortium (AECC) was founded in 2017 to bring together industry stakeholders to drive the evolution of edge network architectures and computing infrastructures for connected vehicles. A key goal is to more efficiently support high-volume data services. The vision is a future where all connected vehicles can exploit the benefit of big data for intelligent driving, improved safety, and reliability.

The AECC Technical Report [18] summarises all findings of the Technical Solution Working Group and is being continuously updated. It provides architectures for several aspects:

- The hierarchical data-processing architecture states that vehicles are connected through Access Networks to reach Edge and/or Central servers.
- The cellular network architecture consists of the 3GPP 4G architecture, including QoS features, and the 5G architecture, where QoS is included by default. The core network can either be a 5G Core or a 4G Evolved Packet Core (EPC), but in both cases the RAN can be a mix of 5G New Radio and 4G LTE cells.
- The distributed computing reference model allows computing infrastructure operators to offer their resources (computing, network, storage) through a common AECC service. Services provided by server applications instantiated on those resources are also exposed through this common AECC service.
- The vehicle system reference model provides a four-layer view on the vehicle in this context. The lowest layers are its sensors and actuators and its computing and communication hardware. Those are vehicle specific. The ‘base software’ is located on top of that, and includes an operating system and hardware abstraction. This provides a run-time environment to further applications on the top layer. This layer includes ‘native’ applications that are, for example, installed by default at vehicle delivery, relying only on the base software. Further applications can then be installed either relying on the vehicle-specific base software or using a common ‘run-time environment’.

So far, AECC, considers six key issues and proposes solutions for them. Often several solutions are proposed that together form a migration path starting from today’s 4G network, over non-standalone 5G towards standalone 5G. Solution proposals also try to take into account that some network features, even when standardized, might not be immediately deployed. The six key issues and their solutions are:

- **Edge Data Offloading:**
  This key issue relates to three tightly coupled aspects: how are Edge Servers connected to 3GPP networks, how can data be routed to/from different Edge and Centre Servers, and how can routes to Edge Servers be dynamically adapted as the vehicle moves. The first aspect includes the two general options to either reach Edge Servers through gateways (PGW in 4G EPC, PSA UPF in 5G Core) or the interface between RAN and Core (S1 in 4G, N3 in 5G). The latter is not among the solutions promoted in the concluding statements for this key issue.
  For the issue of routing traffic to/from Edge and Centre Servers, using multiple Access Point Names

(APNs) in 4G EPC is one alternative. The same principle is also possible with 5G Core, where APNs are called Data Network Names (DNNs). Furthermore, the 5G Core offers the option to use Uplink Classifiers and/or IPv6 Multi-homing for this traffic separation.
The different Session and Service Continuity modes offered by the 5G Core and related 4G EPC features like Selective IP Traffic Offload (SIPTO) are discussed to dynamically adapt the route, especially the gateway, between vehicle and Edge Servers.

- **Mobility Service Provider (MSP)[1] Server Selection:**
  This key issue discusses how a vehicle, for a certain service or set of services, can determine the 'best' server(s) to communicate with. Four solutions are proposed corresponding to the entities making the decision: cellular network, IP network, selection function from MSP, or vehicle.
  When the cellular network decides, it can exploit its knowledge of the vehicle location (e.g. serving cell or tracking area) to manipulate certain data traffic. This way, for example, Domain Name Service (DNS) queries can be re-routed to an MNO DNS server providing replies according to the current vehicle location. The MNO needs respective information about server locations and addresses from the MSP.
  The IP network-based approach uses anycast where, for example, a connection request traverses the IP network until it reaches any server with the matching anycast address, and this server will then reply to the request and engage in further communication. This solution is not discussed in the concluding recommendations.
  For the selection function solution, DNS can also be used, but in this case the DNS server would be within MSP, not MNO control. The MSP could therefore configure the DNS server to provide responses according to the geographical deployment of (Edge) Servers, for example. The server could also offer interfaces to the vehicle allowing it to indicate its location. The selection-function-based solution is recommended as a baseline, as it can be implemented immediately by MSPs without requiring changes in the mobile radio network or vehicle.
  For the vehicle-based solution, the vehicle system receives information about available servers from the MSP. It then selects one based, for example, on its current location. This solution, together with the cellular network one, is recommended as an improvement to the baseline solution.
- **Vehicle System Reachability:**
  Reaching a vehicle that does not maintain an active connection with a corresponding server is often challenging. Either such connection does not exist, or it can no longer be used because of vehicle-side IP address changes in the gateway or MNO, for example. Three solutions are proposed: Short Message Service (SMS), push notifications, and Service Capability Exposure Function (4G EPC)/Network Exposure Function (5G Core) (SCEF/NEF). For the first solution, a server can use SMS to reach a vehicle through its mobile phone number. The vehicle software must handle the SMS content accordingly to trigger an application for example to contact its corresponding server.
  For push notifications, the vehicle would always – when possible and served by a mobile network – maintain a connection to a push notification server and be known by a unique ID there. The different applications and services can be made aware of this ID. Whenever an application-specific server is not able to reach a vehicle but needs to do so, it can invoke the push service with the unique ID to deliver information to the vehicle. This information can either be the actual data it wanted to send to the vehicle or a request to be contacted for further data exchange.
  3GPP 4G specifications define the SCEF and 5G Core specifications cover the NEF that is fully compatible with the SCEF regarding features supporting reachability. Further associations, such as methods specified by oneM2M on how to invoke the interfaces provided by SCEF/NEF to deliver a small amount of data similar to an SMS to a vehicle, can either carry the actual information that needs to be delivered or trigger the vehicle to contact a specific server for more information about why it was paged.
  Push notifications are the preferred solution, as they are agnostic to the access technology. If only cellular networks are considered, SMS is the preferred solution for now, to be eventually replaced by more powerful SCEF/NEF.
- **Access Network Selection:**
  This key issue deals with selecting from a set of available access technologies, typically cellular and WiFi, and deciding which one to use for what, when multiple options are available. A sophisticated set of solutions is described. Due to the limited relevance for 5GAA they are not further described here but can

[1] The term „MSP' is used by AECC to refer to any kind of service provider but stressing the fact that it is in automotive and transport (mobility) context.

be found in [18]. The preferred solution is to let the vehicle decide based on measured quality of the available access technologies and application preferences. For data traffic steering, the multi-path variants of common transport layer protocols are preferred, such as Multi-path TCP and Multi-path QUIC.

- **Provisioning and Configuration Update:**
  Many of the issues and solutions presented above, as well as further topics, require semi-static information to be maintained and updated. The systems involved in this include the vehicle, the network and different MSPs. Examples for such information include APNs and QoS parameters, or server host names, but also data traffic steering policies for access network selection or opportunistic data transfer, as discussed below. The following solutions are considered: pre-configuration, configuration through the cellular network, configuration through (MSP) application servers, configuration through a common, generic AECC application server, and a generic application server that is not necessarily related to AECC, including methods to identify such a server. These methods can use the Dynamic Host Configuration Protocol (DHCP) or pre-configuration. A mix of these solutions where certain solutions are preferred for different kinds of configurations. Further details can be found in [18].
- **Opportunistic Data Transfer:**
  This issue relates to the challenge of transmitting large data volumes, a key topic of AECC, and potential costs related to that. Often the data does not need to be immediately transmitted, but the network is not aware of the temporal and/or geographical constraints on when related up- or downloads should be completed. The three proposed solutions are access control and barring, Background Data Transfer (BDT) according to 3GPP specifications [19], and dynamic policy adaptation.
  Different combinations of the solutions and availability of corresponding features in the network are key to deciding what to use. Furthermore, the decision can depend on the actual application. Further details can be found in [18].

5.4 Edge Computing support in 3GPP systems

From the point of view of the 4G 3GPP System Architecture Evolution (SAE), Application Servers (ASs) are located in a Packet Data Network (PDN) separated from the 3GPP 4G Evolved Packet Core (EPC) through the SGi interface terminating at the Packet Data Network Gateway (PGW) on the EPC side. The same is true for non-standalone 5G networks, where 4G EPCs are used. For standalone 5G networks (implemented with 5G Core) mostly interface and node names are different. For instance, instead of SGi, the respective interface is called N6 and the term PDN was replaced by the more generic one ‘Data Network (DN)’.

One requirement for MEC in the context of 3GPP specifications is the possibility to change the PGW (4G)/Protocol Data Unit (PDU) Session Anchor User Plane Function (PSA UPF) (5G) over which traffic is routed to a MEC-hosted AS. Changing the PGW is something originally not intended by the 4G EPC specifications, but it is possible, as described in Section 8.2.1. For the 5G Core, this functionality was explicitly added by introducing Session and Service Continuity (SSC) mode 3 and single PDU session with multiple PDU session anchors. SSC mode 1 and mode 2 are closely related to the limited capabilities of 4G EPC for changing PGWs. Furthermore, the possibility to use multiple PSA UPFs is introduced and Uplink Classifiers in UPFs are used to steer uplink traffic towards an intended PSA UPF. For the downlink, the routing within the DN must take care of that and this is not within the scope of 3GPP specifications.

Seamless end-to-end service continuity requires further measures outside of the domain covered by 3GPP RAN and Core specifications. To support this, the ‘AF influence on traffic routing’ API was introduced allowing Application Functions (AFs) to influence which traffic uses which PSA UPF, and to change this dynamically. This way, the network and application function can jointly decide how and when to change the PSA UPF(s).

3GPP Working Groups (e.g. SA6, CT3) also specify northbound interfaces to be used by AFs to provide information and influence network decisions on traffic routing and V2X policy/parameters provisioning. One of these is the Traffic Steering API mentioned above and further ones are listed in [36]. V2X-specific APIs have been studied in TR 23.786 [13], the corresponding normative work has been reflected in TS 23.287 [15], TS 23.288 [15], and TS 23.502 [16]. This includes solutions related to QoS sustainability analytics notification (aka in-advanced QoS Notification (IQN) in 5GAA) and QoS changes based on extended NG-RAN notification, to support alternative service requirements in 3GPP. Furthermore, it also describes the provisioning of V2X Authorisation Policy and parameters to the UE by PCF.

3GPP Service Architecture Working Group 6 (SA6) provides standards going beyond RAN, Core and User Equipment (UE). This allows the standardisation of V2X application layer functional architecture, including a V2X application enabler (VAE) to ensure the efficient use and deployment of V2X applications in 3GPP networks [14]. A study for further V2X-related enhancements within the scope of 3GPP SA6 Rel. 17 standardisation is ongoing [18].

5.4.1 Edge Computing in 3GPP SA5

The work-item FS_eEDGE_Mgt [39] is one of the activities related to Edge Computing in SA5. This work item discusses the use cases, requirements, and solutions for enhancing Edge Computing management. Aspects discussed in this work-item include lifecycle management of Edge Computing architecture elements, as defined in SA6 (see Figure 5.4.1-1 below). These architecture elements are: Edge Application Servers (EAS), Edge Enabler Servers (EES) and Edge Configuration Server (ECS). The management aspects also consider various deployment scenarios of the Edge Computing as well as the provisioning of EES and ECS and their fault supervision.

First, the work-item defines some generic relationships from the management perspective and between the stakeholders involved in a typical edge communication system (described in the Figure 5.4.1-1).

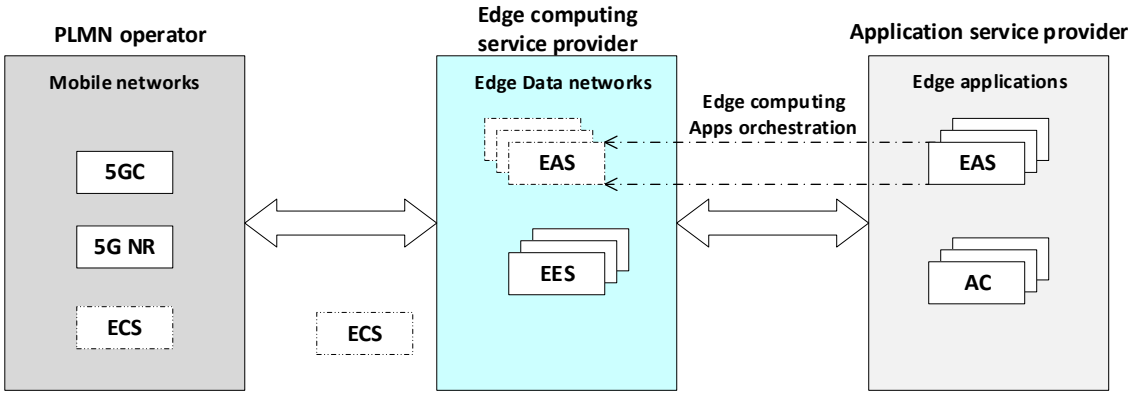

Figure 5.4.1-1: Relationship of service providers in the Edge Computing network deployment

The Application Service Provider (ASP) is responsible for the creation of Edge Application Servers (EAS) and Application Clients (AC). The Edge Computing Service Provider (ECSP) is responsible for the deployment of Edge Data Networks (EDN) that contain EAS and Edge Enable Server (EES) that provides the configuration information to Edge Enabler Client (EEC), enabling AC to exchange application data traffic with the EAS.

The ASP can have service agreement with one or more ECSP(s) and may request the ECSP to deploy one or more EAS in the EDN. Upon receipt of ASP's request, the ECSP should deploy the EAS(s), and then register the EAS(s) to the EES in the EDN. The ECSP can have service agreement with one or more PLMN operators and may request the PLMN operators to connect EAS and EES with 5GC network functions.

The Edge Configuration Server (ECS) may reside in PLMN operator or in ECSP, and provide functions needed for the edge enabler client (EEC) to connect with an EES.

The Figure 5.4.1-2 is describing some specific deployments of the Edge Computing entities and the interaction between the Edge Computing entities and the 5G Core Network elements.

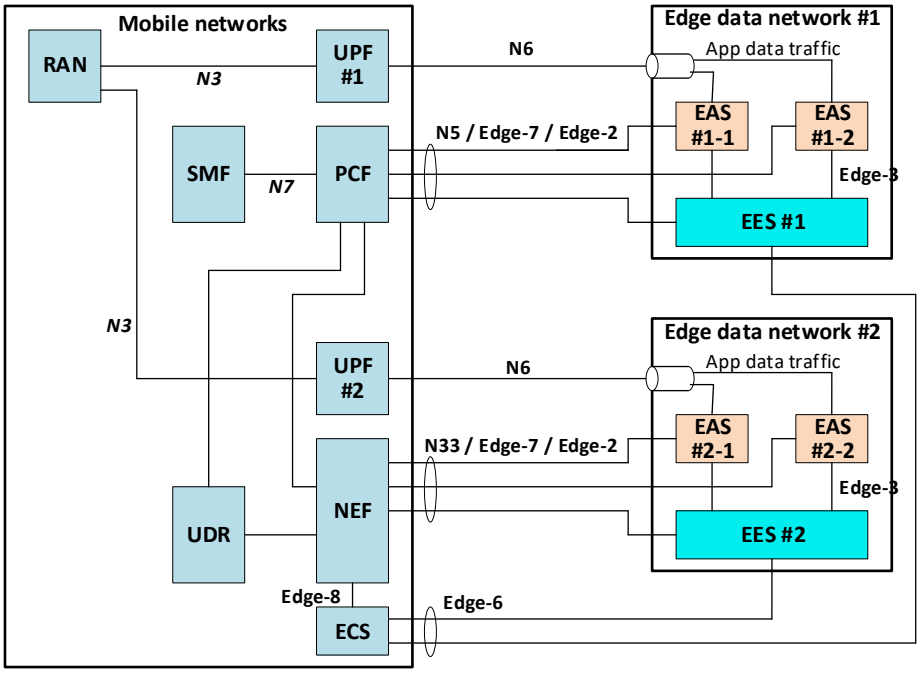

Figure 5.4.1-2: Edge Computing deployment example

The mobile networks are connected to two EDNs that each contains two EASs. In EDN #1, the EAS(s) are connected to the UPF via the N6 interface to carry the applications data traffic, while EAS(s) and EES are connected to the PCF via the N5/Edge-7/Edge-2 interfaces (see TS 23.501 [11], and the definition of Edge 2 and 7 in TS 23.558 [32], where the EES acts as a trusted AF in 5GC), on which information can be sent to the SMF to influence traffic routing. In the EDN #2, EAS(s) and EES are connected to NEF via the N33/Edge-7/Edge-2 interfaces (see TS 23.501 [11], where the N33 is the reference point between NEF and AF), on which information can be sent to the Service Management Function (SMF) via a Policy Control Function (PCF) to influence traffic routing that supports the traffic management in TS 23.558 [32]. The ECS residing in the mobile networks is connected to NEF in the mobile networks via N33/Edge-8 interface and EES via Edge-6 interfaces.

The management aspect of Edge Computing includes (but is not limited to) the following:

- Lifecycle management of EDN as a 3GPP Local Data Network.
- Lifecycle management of edge components including EAS, EES and ECS.
- Performance Assurance of edge components including EAS, EES and ECS.
- Fault Supervision of edge components including EAS, EES and ECS.
- Virtual resource management for edge components including EAS, EES and ECS.
- EDN capability management including the type and capabilities of EAS(s) available in the EDN.
- TS 23.814 [39] includes use cases and requirements for the management of Edge Computing, viewed as the instantiation, deployment and termination of EAS, EES and ECS. The instantiation/termination of the EAS involves interaction between the 3GPP OAM and the orchestration layer of the application, viewed as an ETSI MANO architecture in order to instantiate VNFs of the EAS and to connect or chain EAS VNFs and EES VNFs, and to connect EAS with the 5G Core functions. The instantiation/termination of ECS involves the PLMN OAM for the instantiation of VNFs of the ECS.

Regarding the deployment of Edge Computing systems, several entities are involved in the ecosystem, as defined in SA6 and including ASP, ECSP, PLMN Operator etc. The ASP consumes the edge services (e.g. infrastructure, platform) provided by the ECSP. As per the architecture defined in TS 23.558 [32], there can be multiple deployment variations. While some of the deployment models are well within the scope of SA5's work, some fall out of scope. The following figures capture various deployment models pertaining to EAS, EES and ECS management.

Figure 5.4.1-3: deployment options for edge communication system

In the above Figure 5.4.1-3 'Provided by' implies that the functionality is created by a particular entity. Whereas, 'Managed by' implies that the LCM, PA and FS of the functionality is carried out by a particular entity.

5.4.2 Edge Computing in 3GPP SA6

The work item EDGEAPP is a major activity in 3GPP SA6 that defines an architecture to enable applications to be hosted on the Edge[2] of the 3GPP network. One of the main areas focused on how to minimise the impact on deploying Edge-based applications on the 3GPP Core Network architecture – so that they do not need major App redevelopment.

Key requirements are:

- UE application portability – Changes in Application Clients compared to existing cloud environment are avoided.
- Service differentiation – The mobile operator is able to provide service differentiation (e.g. by enabling/disabling the Edge Computing functionalities).
- Flexible deployment – There can be multiple Edge Computing providers within a single PLMN operator network. The Edge Data Network can be a sub-area of a PLMN.
- Integration with 3GPP network – Capability exposure, such as location service, QoS, Application Function traffic influence the Edge Apps.
- Service continuity – Support for continuation of application context across Edge deployments

The figure below shows the EDGEAPP architecture developed by SA6.

[2] 3GPP does not use the term MEC but rather 'Edge (Computing)'. Within this section the term Edge will be used to match what is shown in the figures that were copied from 3GPP specifications.

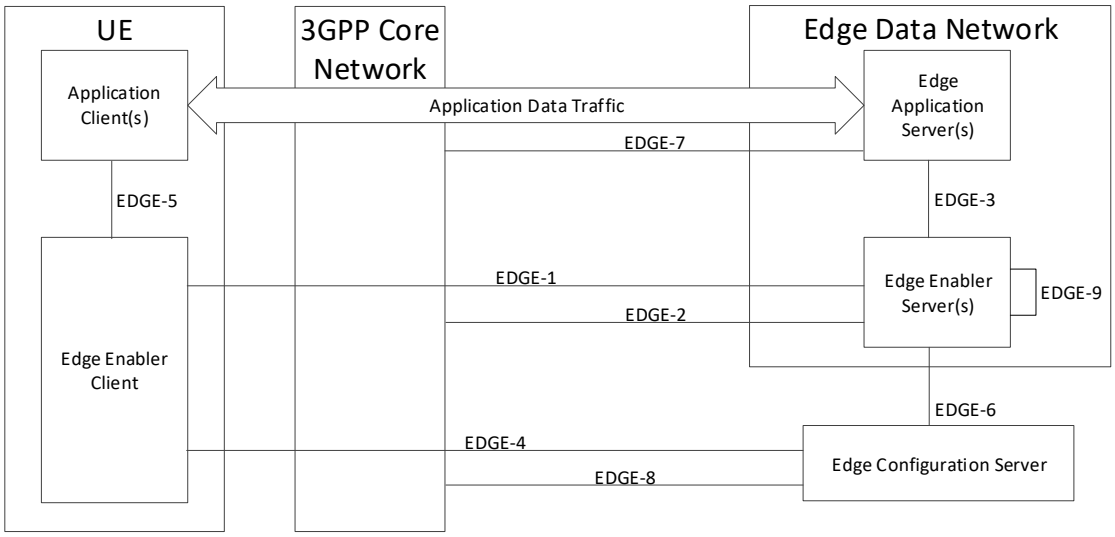

Figure 5.4.2.1– EDGEAPP architecture (ref. 3GPP TS 23.558 [32])

Whilst offering indirect support to Edge-unaware application clients, EDGEAPP offers additional benefits for edge-aware applications through direct interaction with the device hosted Edge Enabler Client. The architecture also enables the Common API Framework, or CAPIF [34], to be leveraged as a standardised means of providing and accessing APIs in the Edge Cloud.

Figure 5.4.2-2 below also provides a Synergised Mobile Edge Cloud architecture supporting different modes of operations and leveraging 3GPP and ETSI ISG MEC.

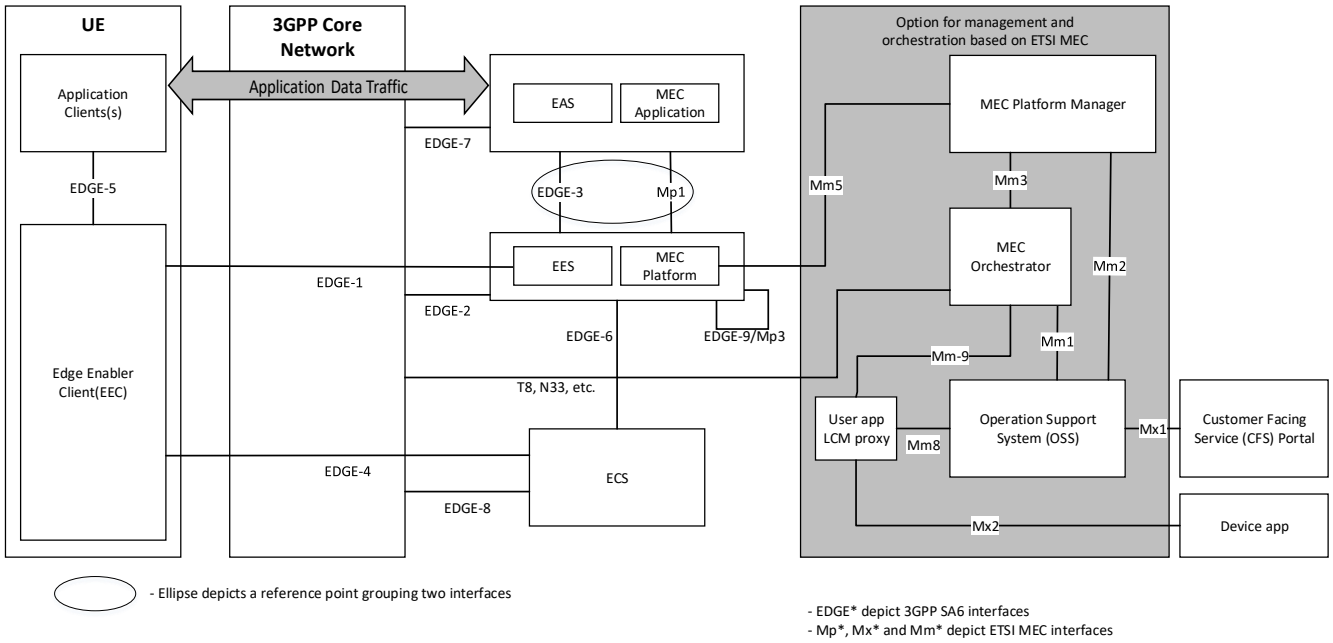

Figure 5.4.2-2 – Synergised Mobile Edge Cloud architecture [33], supported by 3GPP [32]and ETSI ISG MEC [5]

This above figure (taken from Annex C of 3GPP TS 23.558) represent a visual example for how the EDGEAPP architecture [32] and ETSI ISG MEC architecture [5] can complement each other. It is thus worth highlighting that all building blocks in the system are not duplicated; their implementations are coherent with a common synergised architecture, where MEC platforms (corresponding to EES) are capable of exposing service APIs to MEC Applications (corresponding to EAS), in order to enable advanced Edge services and use cases. In the context of MEC4AUTO, multi-MNO, multi-OEM and multi-vendor environments are targeted, so the above architecture is the starting point to consider the single-MNO architecture, aligned with 3GPP and ETSI MEC standards. Federation aspects, and related requirements, are instead driven by GSMA Operator Platform Group (OPG).

5.5 Cloud Native Computing Foundation

We expect MEC to be more than just 'normal' cloud computing where the only difference is the location of the hosts. Still, many things that are true for cloud computing in general should also apply to MEC. The Cloud Native Computing Foundation (CNCF), as part of the Linux Foundation, is a body bringing all stakeholders of cloud computing together to discuss and decide on recommendations in that field. This section explains, using broadly understandable terms and examples, the recommendations for cloud native technologies, according to how CNCF defines them:

"Cloud native technologies empower organisations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach." [20]

In the following, the statement and major terms used are further described:

Public, private, and hybrid clouds: According to [21] a public cloud provides computation, connectivity and storage resources to many businesses and other kind of organisations using it. Each public cloud is operated by a cloud service provider and the largest ones are typically referred to as hyperscale cloud providers (e.g. AWS, Microsoft, Google). Private clouds are operated by the same business or other kind of organisation that also uses it to run its applications on it. Hybrid is a mix of both where some applications or parts of them are on public and other on private clouds. MNOs providing MEC services to different businesses and other kinds of organisations would be considered as public clouds according to this definition. The term 'MEC' is therefore used to distinguish this from the hyperscale cloud providers.

Containers: Virtual Machines (VMs) represent the heaviest way of virtualisation in terms of required resources. They include the whole Operating System (OS) with applications running on top of it. Kernel VMs (KVMs) are an improvement where the Kernel of the OS is shared among the VMs running on top of it. This reduces the required memory, as the Kernel is only present once. Containers are an even more lightweight virtualisation solution and therefore considered state of the art, especially for hyperscale clouds. Docker [22] is the most commonly used open source software to create containerised applications. A container includes the application itself and all helper applications and libraries it requires to run. Such a Docker container can therefore be deployed to a cloud and executed without having to resolve further dependencies. Kubernetes is commonly used to manage tasks related to container deployment and further operations and maintenance tasks.

Microservices: Containers allow the creation and deployment of self-contained applications (services) that can cooperate with other services to provide an overall service. It is common to refer to the overall service as just 'the service' while the sub-parts constructing it are called 'microservices'. Microservices allow distributed software development and evolution where only interfaces between the microservices must be defined. Microservices can include the logic to discover each other, connect to each other and provide failover mechanisms.

Service meshes: As mentioned above, discovery, communication and failover can be part of the microservice implementation. Alternatively, this task can be decoupled from the microservice and handled by the service mesh [23]. Application developers therefore do not have to provide code for these tasks. The service mesh usually also takes care of performance monitoring allowing it to not use microservice instances that do not perform as required or have failed, and also to detect when they can be used again.

Immutable infrastructure: Besides the application itself, running in microservices, other parts of the container (e.g. libraries or even the OS hosting the container) might require updates or configuration changes. The paradigm of 'immutable infrastructure' demands that such changes are not made during runtime. Instead, new instances are deployed where these updates and/or changes have been done. Thanks to the service mesh, they are seamlessly integrated into running the overall service. Furthermore, compatibility is assured as only parts around the application were changed, not the application itself. In the event of undesired behaviour, the newly deployed microservices can be disabled and another configuration attempt can be done. For desired behaviour, old containers can be gradually replaced by new ones.

Declarative APIs: The opposite of declarative APIs are imperative APIs. They are invoked by their consumers to get an intended task done, step by step. A set of API calls with specific input parameters is used to prompt intended outputs to be then used in follow-up calls. Declarative APIs [24] [25] are used to get a certain task done without having to worry about the individual steps needed to reach the goal. An example would be 'warn other vehicles about a hazard' rather than 'construct message', 'negotiate required QoS for it with the network', 'determine area of interest', 'determine recipients in area of interest', etc.

6 High-level architectural considerations on MEC in multi-MNO scenarios

6.1 Reference architecture for MEC4AUTO scenarios

Figure 6.1-1 illustrates MEC4AUTO reference architecture used as a baseline for multi-MNO scenarios on MEC in Sections 6.3 and 6.4, as examples of deployments of Edge Computing architecture in Section 7.1, and as demos or trial implementations in Section 7.3.

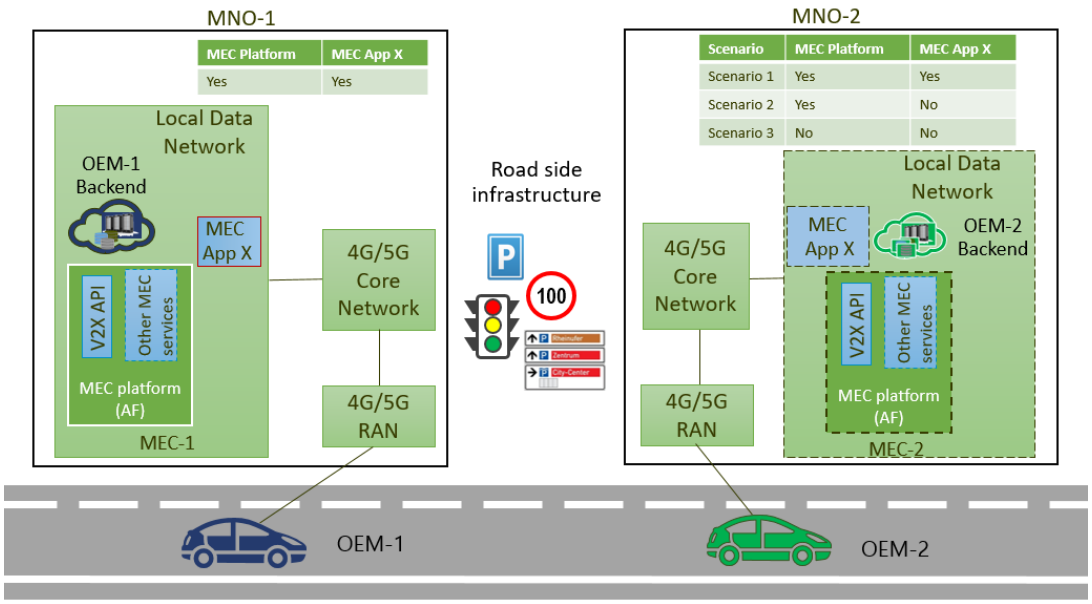

Figure 6.1-1 MEC4AUTO reference architecture

The dashed boxes in the figure depict different MEC4AUTO scenarios in which the second MNO can have the MEC platform and MEC application X, have only the MEC platform but without the application, or does not have any MEC platform and, thus, no application at all. The scenarios are explained in detail in Sections 6.3 and 6.4 below.

6.2 Introduction to multi-MNO scenarios and assumptions

One of the main objectives of 5GAA MEC4AUTO is to provide guidance on how to realise and manage the interoperability of automotive services in a multi-Mobile Network Operator (MNO), multi-access Edge Computing (MEC) and multi-vehicle Original Equipment Manufacturer (OEM) environment.

More specifically, a challenge is how a vehicle which has radio access to MNO B can use a MEC application which is operated by MNO A without missing the MEC-KPIs (i.e. low latency).

The following, three main multi-MNO scenarios are considered within the 5GAA MEC4AUTO scope:

1. Both MNO A and MNO B have MEC platform and MEC application X.
2. Both MNO A and MNO B have MEC platform, but MEC application X is available only in MNO A.
3. Only MNO A has MEC platform and MEC application X is available only in MNO A.

Note that inter-MNO connectivity in Scenario 3 can be realised by means of two different options (see Section 6.3.3 and Section 6.4.3 for more details).

The general assumptions for the multi-MNO scenarios are:

- Client application X, running in a vehicle, needs to connect to MEC application X (server application) running on top of the virtualisation infrastructure supported by the MEC platform[3].

[3] MEC platform functionality issues are out of scope of Section 5.7 and will be considered in the Section 5.2

- The MEC platform can belong to either a 3GPP MNO or a third-party, e.g. an Edge Computing Service Provider (ECSP).
- All required business agreements are in place between the involved parties in order to allow the vehicle to access the requested MEC applications.

The following text currently uses 5G Core Network terminology but the basic principles are also valid for 4G Evolved Packet Core (EPC).

The rest of this chapter is organised as follows. Section 6.3 describes single-vehicle OEM use cases for these three scenarios. Then, Section 6.4 extends these considerations for multi-vehicle OEM use cases. Section 6.5 provides a list of open issues related to the presented multi-MNO scenarios. Section 6.6 summarises the chapter.

6.3 Single OEM use case for 3 main scenarios

6.3.1 Scenario 1: Both MNO A and MNO B have MEC platform and MEC application X

In Scenario 1 it is assumed that each operator has a MEC platform and MEC application X, as illustrated in Figure 6.3.1-1. MEC application X is a server application that can be a V2X application server (i.e. see-through application server, ToD application server, etc.) in 3GPP sense. When a vehicle with a client application X moves from MNO A to MNO B, the MEC application X can be accessed through MNO B infrastructure. It provides the shortest data path to the MEC application X and, as a result, supports low-latency requirements. In particular, the 5G Core Network selects a User Plane Function (UPF) close to the vehicle (called local UPF here and below) for low-latency purposes and executes the data traffic steering from the local UPF to the local Data Network via the N6 interface according to 3GPP TS 23.501, Section 5.13.

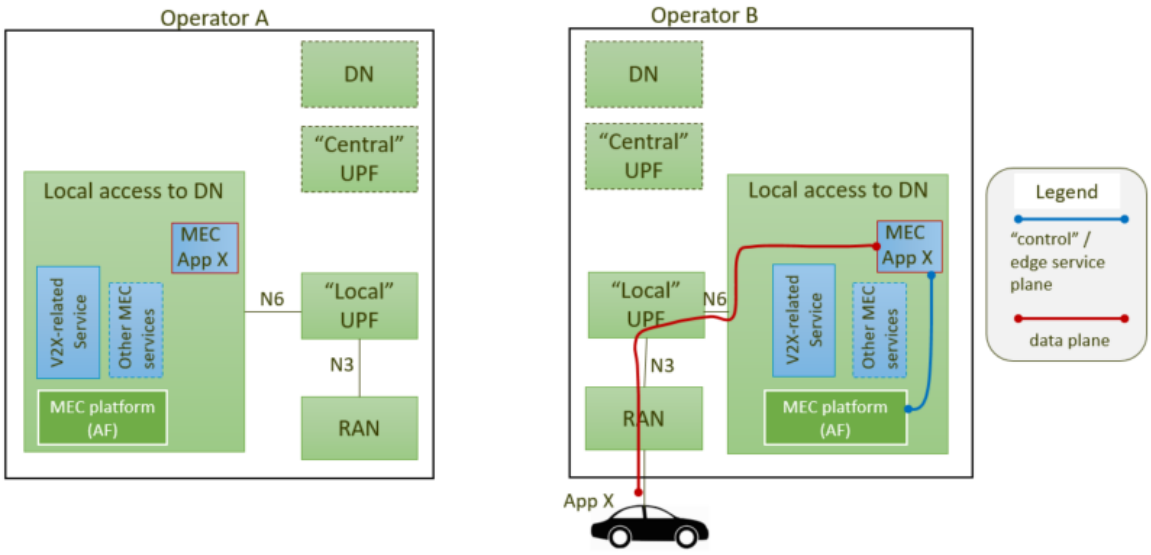

Figure 6.3.1-1 Illustration of Scenario 1 where both MNOs have MEC platforms and MEC application X (single vehicle OEM use case)

Scenario 1 supposes that MEC platforms are installed in all MNO networks to support all relevant applications, which is challenging from both a business and market penetration perspectives. This can be a viable solution in the long term, but it may be difficult to achieve in the short term, and time to market is the key question here.

6.3.2 Scenario 2: Both MNO A and MNO B have MEC platforms, but MEC application X is available only in MNO A

Scenario 2 assumes that each MNO has a MEC platform, as in the previous scenario, but MEC application X is available only in the MNO A premise, as shown in Figure 6.3.2-1.

Having the MEC application X available only in MNO A makes the existence of the MEC infrastructure in MNO B for that specific application/service practically irrelevant from a user plane connectivity perspective.

The data path can be arranged in a similar way as in Scenario 3 (see the next Section). For example, Figure 6.3.2-1 illustrates the connectivity by means of enabling direct 'horizontal communications' between the data networks of both operators (see details in Section 6.3.3.1).

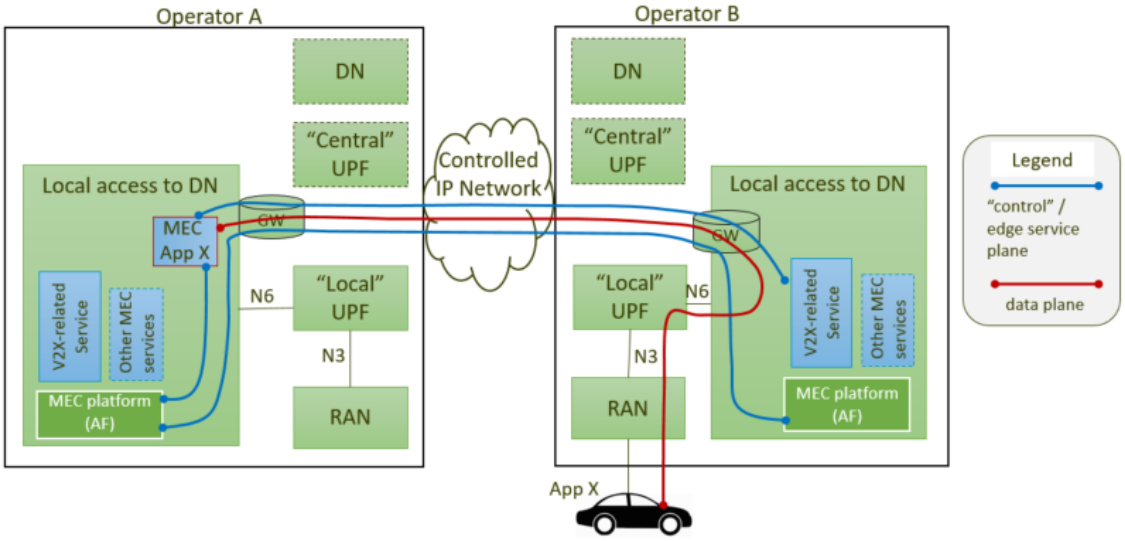

Figure 6.3.2-1 Illustration of Scenario 2 where both MNOs have MEC platforms, but MEC application is available only in MNO A (single vehicle OEM use case)

6.3.3 Scenario 3: Only MNO A has a MEC platform and MEC application X is available only in MNO A

There are two options in this scenario, namely Scenario 3A when interworking between MNOs is arranged by means of home-routed roaming with the use of the N9 interface for user plane traffic, and Scenario 3B is for when interworking is based on local 'pairing' between MNOs by means of a controlled IP network.

6.3.3.1 Scenario 3A: Inter-domain connectivity by means of N9 tunnelling

In Scenario 3A shown in Figure 6.3.3.1-1, the 5G Core Network of MNO B selects a UPF close to the vehicle (local UPF) and executes home-routed roaming towards the local UPF of MNO A via the N9 interface, as defined in 3GPP TS 23.501, Section 4.2.4. From the local UPF of MNO B, the data (user) plane traffic goes to the local Data Network towards MEC application X, which is supported by a MEC platform providing service-specific functionality.

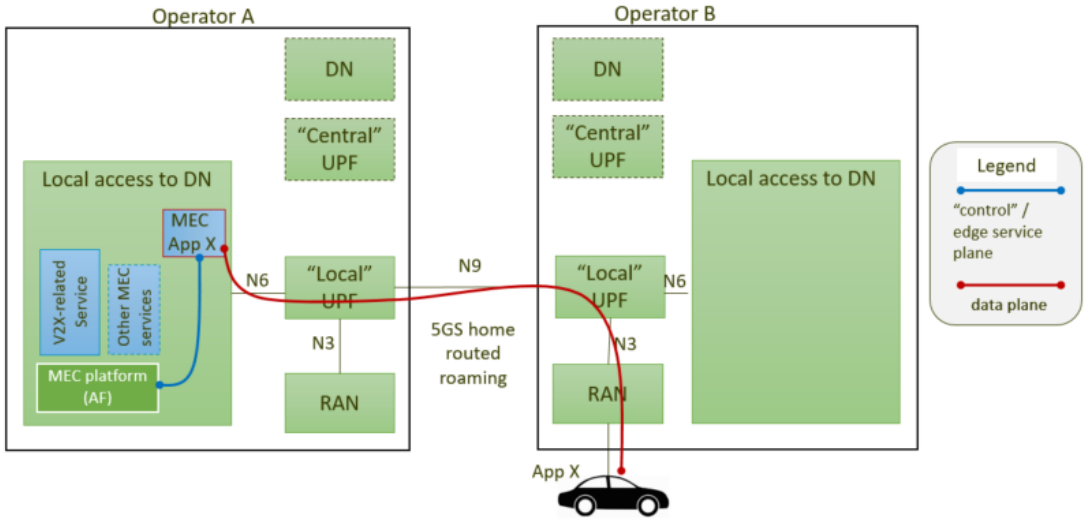

Figure 6.3.3.1-1 Illustration of Scenario 3 where only MNO A has a MEC platform and MEC application, and inter-MNO connectivity is by means of N9 tunnelling (single vehicle OEM use case)

Note that in the 3GPP TS 23.501 the N9 interface is the logical one in the 5G system architecture. The realisation of this logical interface is completed by means of the transport network using GRX/IPX IP interconnect that involves a number of GRX (GPRS roaming exchange)/IPX (IP exchange) providers and can cause extra latency.

6.3.3.2 Scenario 3B: Inter-domain connectivity by means of controlled IP network

In Scenario 3B shown in Figure 6.3.3.2-1, the data traffic related to the MEC application X is offloaded through local UPF of MNO B towards the Data Network (DN) of MNO A, where the MEC application X is located directly via a controlled IP network between MNOs. The controlled IP network is established by means of local 'pairing' links between operators' premises. The local 'pairing' links are terminated by GWs that can play the role of border GWs to DNs and can have some functionality (e.g. NAT GW functionality) supporting inter-domain connectivity over the controlled IP network.

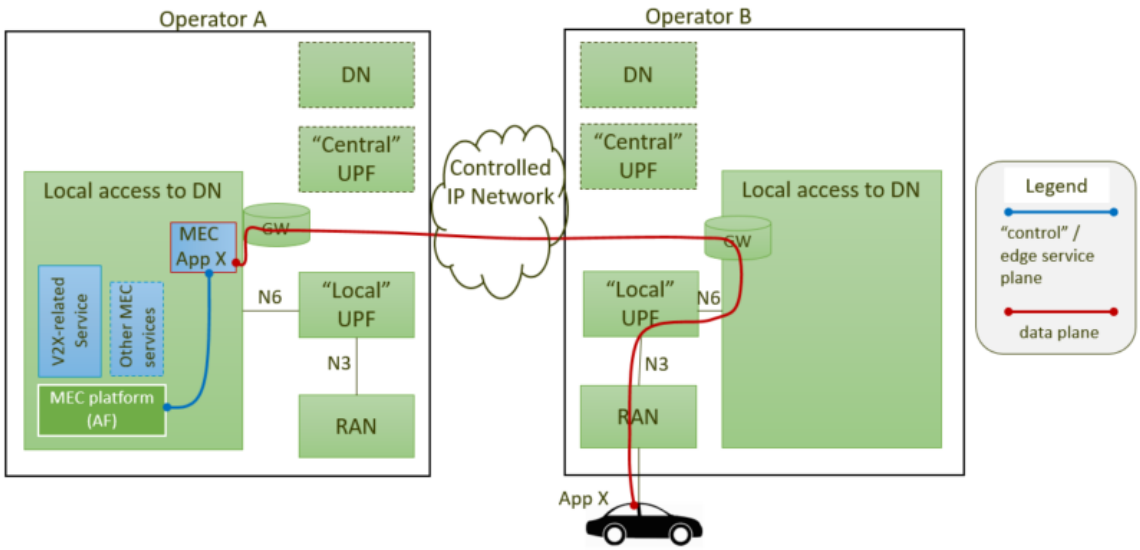

Figure 6.3.3.2-1 Illustration of Scenario 3 where only MNO A has a MEC platform and MEC application, and inter-MNO connectivity is by means of controlled IP network (single vehicle OEM use case)

6.4 Multiple OEMs vehicle use case for three main scenarios

In this section the three single vehicle OEM scenarios described above are extended for multiple vehicle OEM use cases from the viewpoint of interconnectivity.

6.4.1 Scenario 1: Both MNO A and MNO B have MEC platforms and MEC application Y

Scenario 1 for the multiple vehicle OEMs use case is illustrated in Figure 6.4.1-1. It is assumed that each client application communicates with the local server application (MEC application Y) by means of traffic offloading to the DN of each MNO via the N6 interface. Moreover, the server applications communicate with each other through a controlled IP network. The communication involves the Edge service (control) plane traffic between MEC platforms of both MNOs and between the MEC platform and local server application of each MNO.

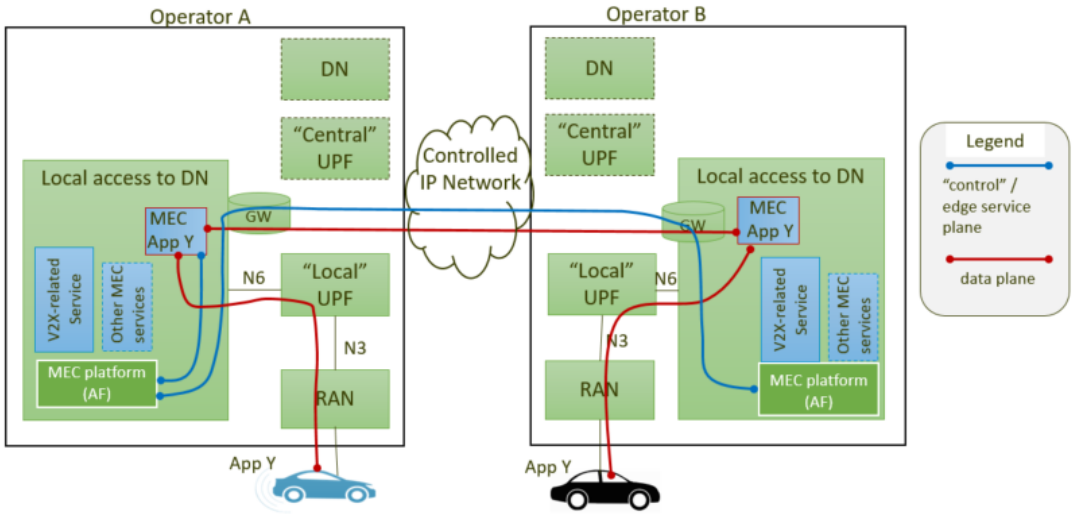

Figure 6.4.1-1 Illustration of Scenario 1 where both MNOs have MEC platforms and MEC application Y (multiple OEM vehicle use case)

6.4.2 Scenario 2: Both MNO A and MNO B have MEC platforms, but MEC application Y is available only in MNO A

Scenario 2 for the multiple OEMs use case is shown in Figure 6.4.2-1. It is similar to the scenario for the single OEM. Only the data path via the N6 interface between a client application of vehicles in MNO A and the local server application (MEC application Y) is additionally added. The client application of vehicles in MNO B communicates with the same server application in MNO B by means of a controlled IP network.

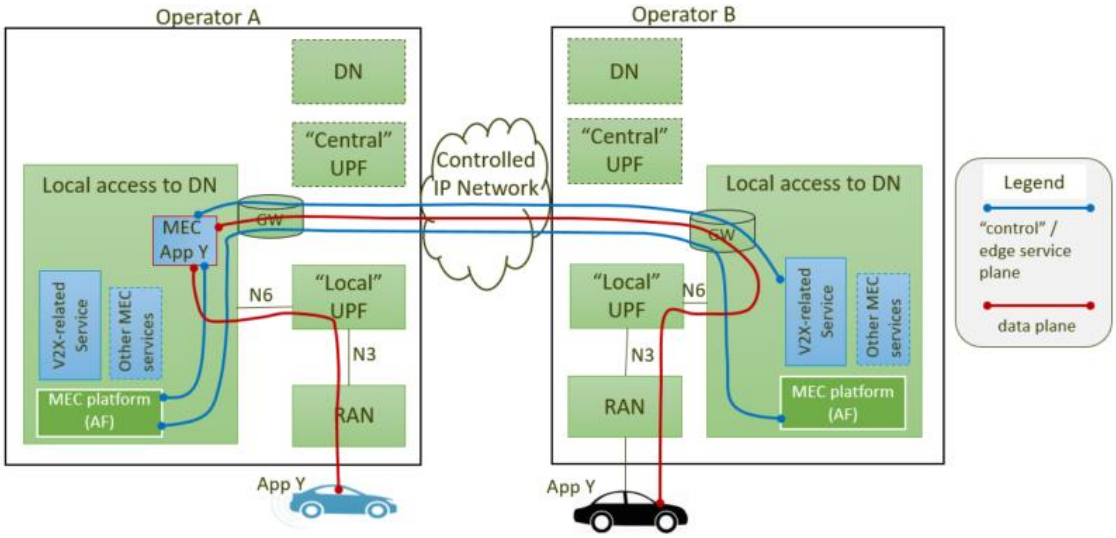

Figure 6.4.2-1 Illustration of Scenario 2 where both MNOs have MEC platforms, but MEC application Y is available only in MNO A (multiple vehicle OEMs use case)

6.4.3 Scenario 3: Only MNO A has a MEC platform and MEC application Y is available only in MNO A

6.4.3.1 Scenario 3A: Inter-domain connectivity by means of N9 tunnelling

Scenario 3A for the multiple OEMs use case is shown in Figure 6.4.3.1-1. As in the previous scenario, only the data path via the N6 interface between a client application of vehicles in MNO A and the local server application (MEC application Y) is added compared with the single vehicle OEM use case.

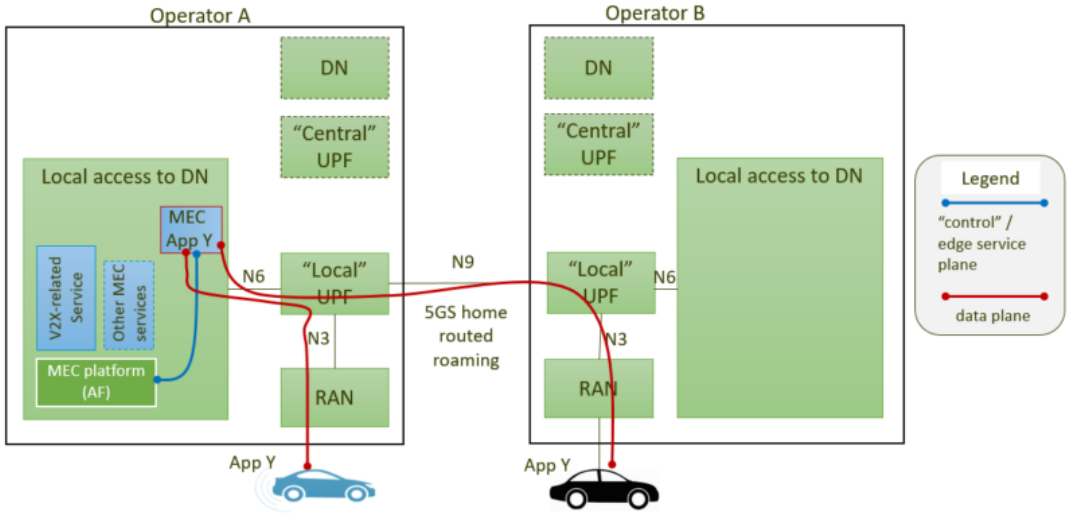

Figure 6.4.3.1-1 Illustration of Scenario 3 where only MNO A has a MEC platform and MEC application Y and inter-MNO connectivity is by means of N9 tunnelling (multiple vehicle OEMs use case)

6.4.3.2 Scenario 3B: Inter-domain connectivity by means of controlled IP network

Scenario 3B for the multiple OEMs use case is illustrated in Figure 6.4.3.2-1. As in scenario 3A, only the data path via the N6 interface between a client application of vehicles in MNO A and the local server application (MEC application Y) is added compared with the single vehicle OEM use case.

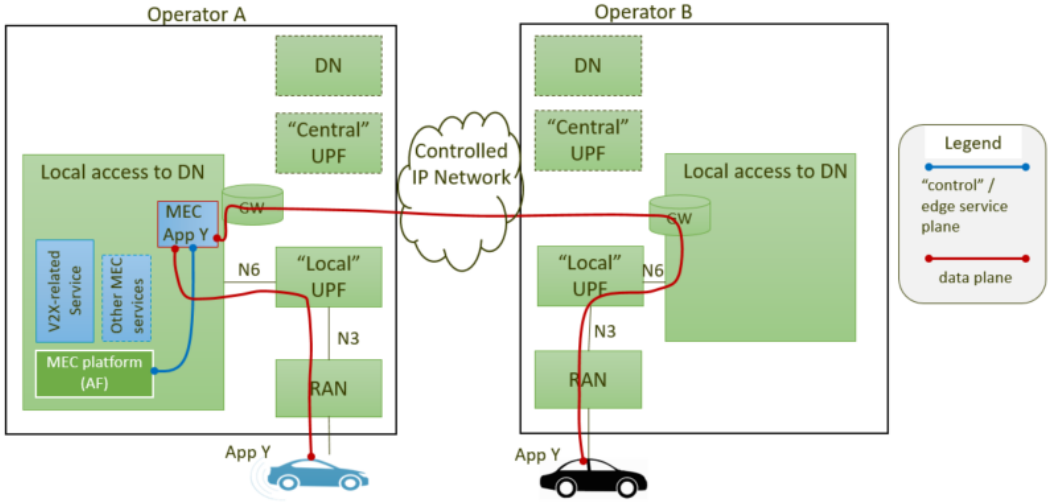

Figure 6.4.3.2-1 Illustration of Scenario 3 where only MNO A has a MEC platform and MEC application Y and inter-MNO connectivity is by means of a controlled IP network (multiple vehicle OEM use case)

6.5 Open issues

Some open issues related to the presented multi-MNO scenarios already identified by MEC4AUTO are:

- How quick (short-, middle-, or long term) can the different MEC4AUTO scenarios be deployed?
- The perspectives for MEC deployment based on N9 interface or local 'pairing' between the operators should be clarified.
- The different MEC4AUTO scenarios need to be compared in terms of complexity, latency budget and how realistic they are to be deployed.
- It should be clarified how difficult it is in practice to establish the required local 'pairing' links between operators, and the timeline for deployment that can be foreseen.

6.6 Summary on multi-MNO scenarios on MEC

All presented scenarios are suitable and technically valid options for multi-MNO interworking for single and multi-OEM use cases and cover the need to inter-connect the two MNO domains with or without local MEC platforms and/or MEC applications.

In particular:

- Scenario 1 is a straightforward solution, but it requires that the MEC platform and relevant applications are installed in all MNO networks. It is a viable approach, but difficult to achieve in a short-term perspective due to business and market limitations.
- Scenario 2 has the MEC application X available only in MNO A which makes the existence of the MEC platform in MNO B practically irrelevant (from a connectivity perspective). In this case, Scenario 2 can be managed with options A and B considered for scenario 3 (‘only MNO A has MEC platform and the related application’).
- Scenario 3 (‘Only MNO A has a MEC platform and the MEC application is available only in MNO A’) can be managed with two deployment options:
    - Scenario 3A (‘N9 tunnelling’) requires some sort of roaming arrangement among operators within the same country that may result in unnecessary complexity and latency, but technically should be a valid option.
    - Scenario 3B (‘controlled IP network’) is perhaps easier to implement, but in any case needs the configuration of ‘direct’ links between the two data networks of the operators (upon related business agreement between the operators, obviously).

7 Deployments for use cases

7.1 Examples of Edge Computing architectures

The descriptions [36] of the use cases ‘See Through’ and ‘Intersection Movement Assist (IMA)’ explicitly state that connected vehicles and road infrastructure could be using mobile radio network subscriptions from different MNOs. The following is therefore valid for them and many other use cases where entities with potentially different MNO subscriptions interact.

Figure 6.3.2-1 depicts a ‘Controlled IP Network’ between two MNOs. Only two MNOs are shown but it equally applies for more than two MNOs. In the following, realisations for such an IP Network are presented.

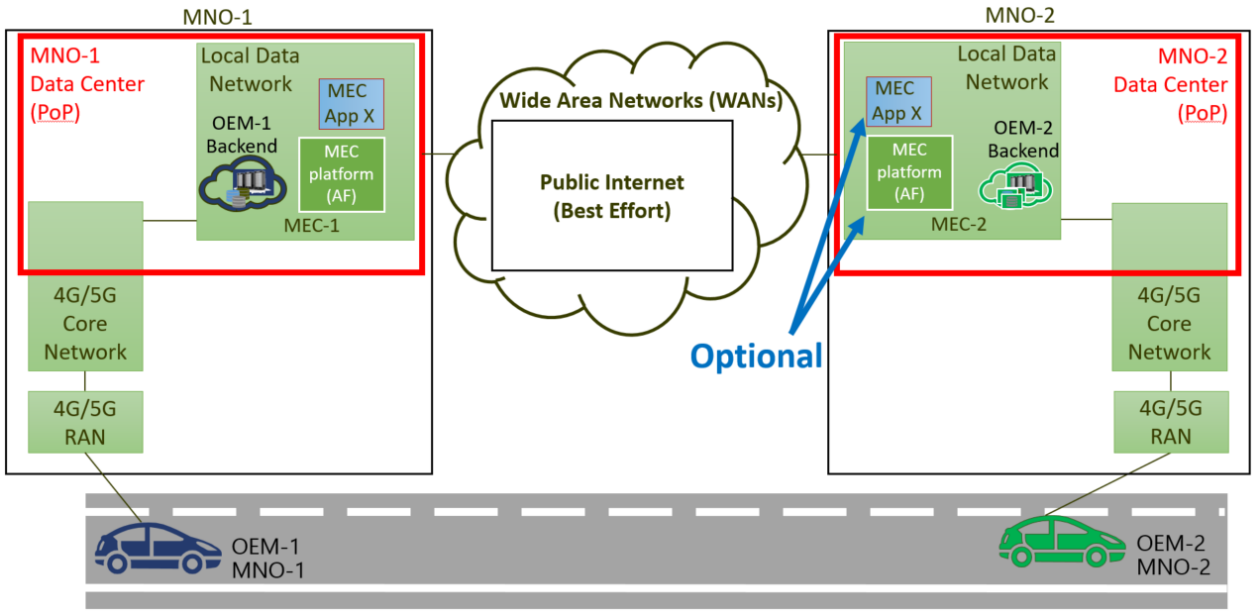

Figure 7.1-1: Two MNOs serving vehicles using a service where their MEC hosts need to exchange information. Realising the exchange through the public internet does not result in a controlled end-to-end path. MEC App X and MEC platform at MNO-2 are optional according to the three scenarios presented in Section 6.

The trivial potential solution of just using the public Internet to interconnect the two MNOs is shown in Figure 7.1-1. It is not a viable solution as it does not fulfil the requirement to have more than best-effort QoS between the MNOs. This requirement is concluded from the fact that end-to-end QoS is a strong motivator for MEC and should also be fulfilled in multi-MNO environments as e.g. encountered in the See Through and IMA use cases [36].

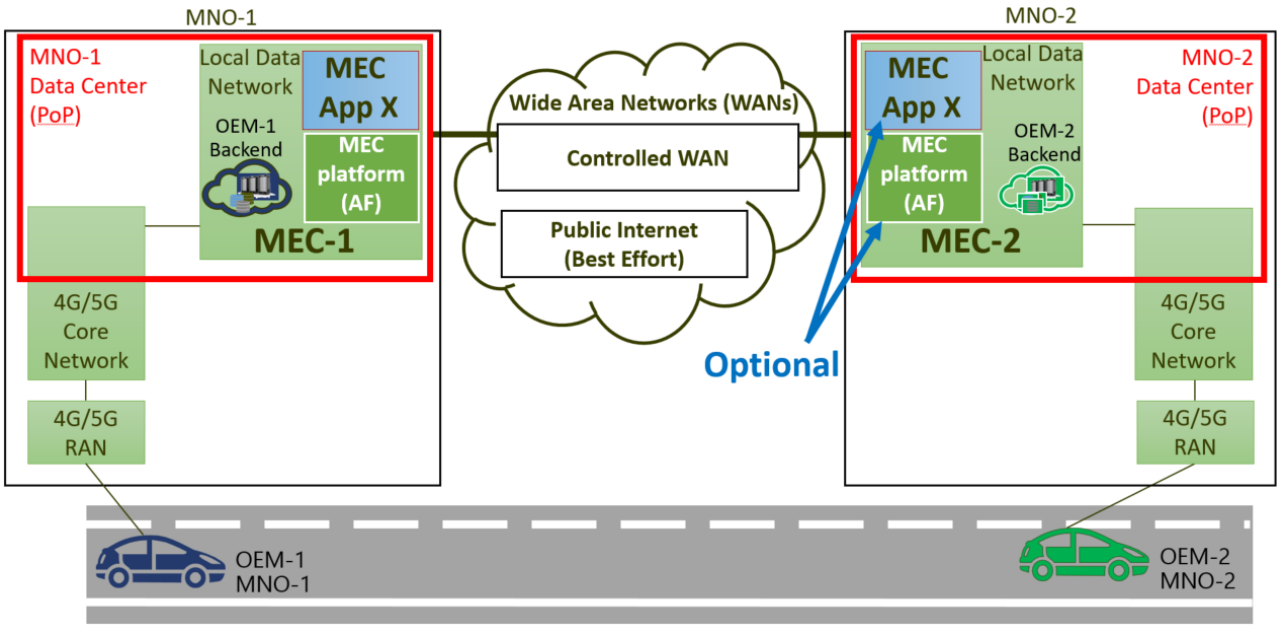

Figure 7.1-2: End-to-end QoS in a multi-MNO environment through controlled WAN(s)

Figure 7.1-2 presents an approach not just using the public internet. In this example, the MNOs sign an Service Level Agreement (SLA) with one or more appropriate Wide Area Network (WAN) providers to obtain a controlled connection between their PoPs. Each MEC platform usually resides within its own domain, e.g. an MNO-specific Local Area Network (LAN), so further security and routing means are required for the platforms and applications to communicate with each other. Communication between the MEC applications requires more network engineering than just mutual knowledge of IP addresses, as those addresses are usually not accessible outside of the respective MNO domains.

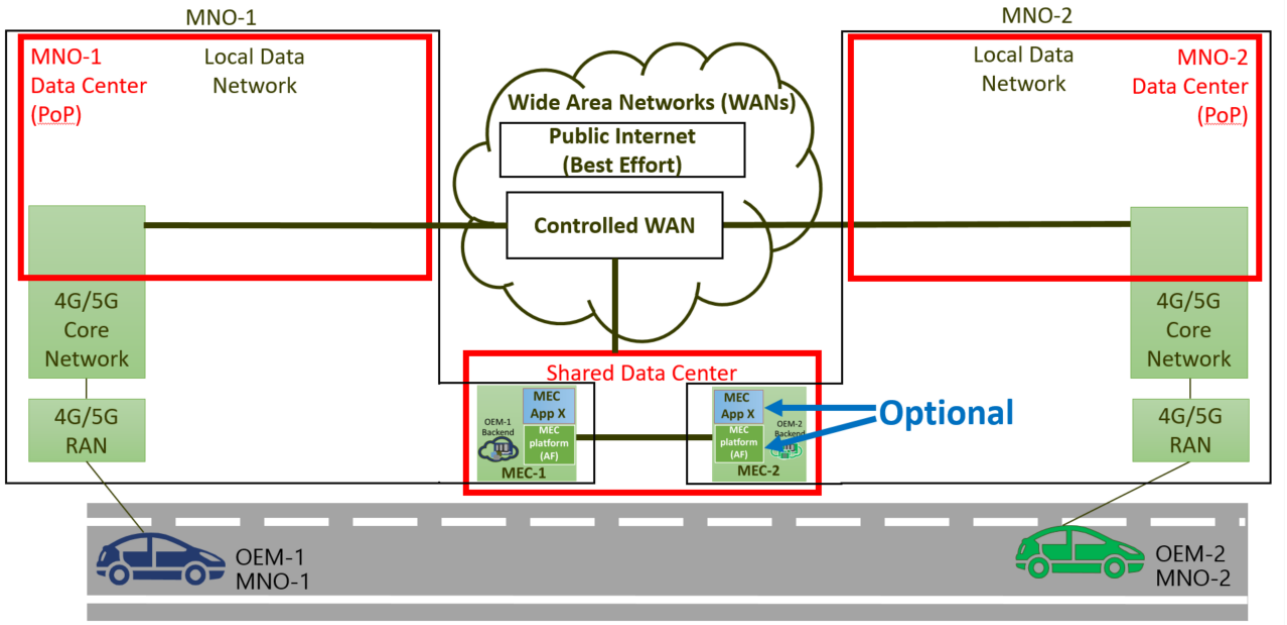

Figure 7.1-3: End-to-end QoS in a multi-MNO Environment through MEC hosting in a shared data centre

MEC platforms hosting MEC applications that need to interact could be placed in a shared data centre, as shown in Figure 7.1-3. Within the shared data centre and its controlled high-performance network, it is possible to maintain very high[4] QoS between the MEC applications. The remaining challenge is to assure similar control from the MNO PoPs to the shared data centre. For this, appropriate SLAs with WAN providers must be signed. It is not uncommon that one or both MNOs shown, or the shared data centre provider, could also be the WAN provider. It is also possible that different WAN

[4] In the sense that it would not become a bottleneck of the end-to-end path

providers are used for this connectivity, in which case SLA requirements have to be agreed across multiple parties. This is not expected to be a problem as it has been best the practice in the fixed carrier world for many years.

According to the three different scenarios described in Section 6 the MEC App X and MEC platform is optional at MNO-2. Scenario 3, where MNO-2 has no MEC App X and having no MEC platform appears to make no sense as MNO-1 would have little reason to move nodes to the shared data centre, preferring to opt for the solution depicted in Figure 7.1-2. But the figures show only two MNOs for the sake of simplicity and there could be further MNOs that moved nodes to the shared data centre, as in the MNO-1 case. MNO-2 would then still benefit from controlled connectivity towards these multiple MNOs even if, for Scenario 3, MNO-2 has no MEC Appx and MEC platform in the shared data centre.

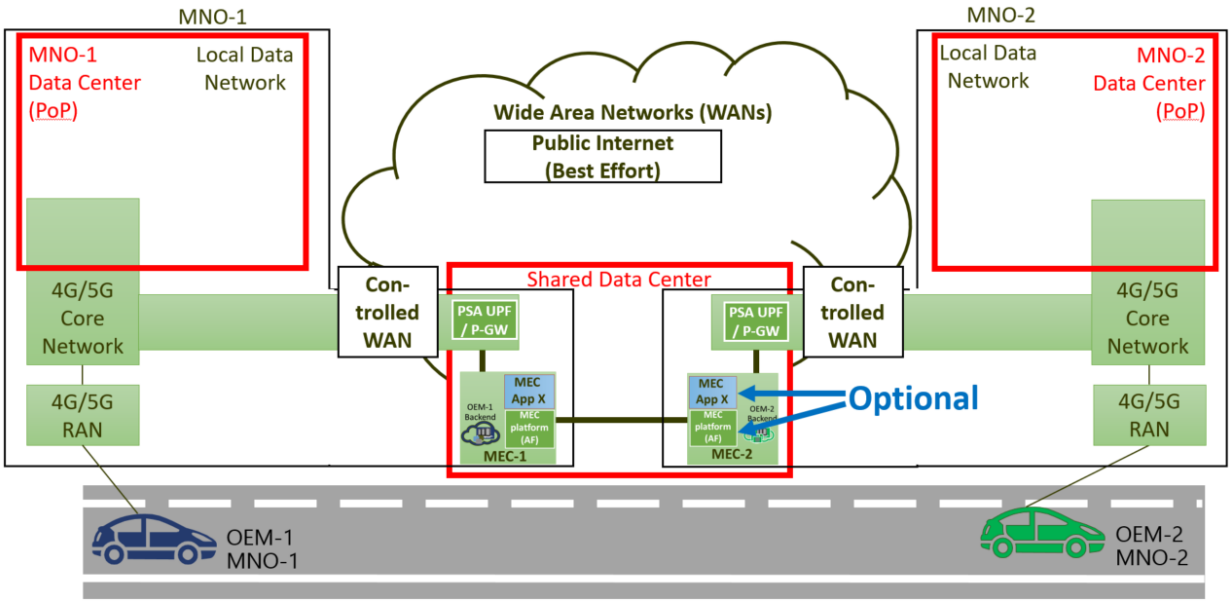

Figure 7.1-4: End-to-end QoS in a multi-MNO environment through gateway and MEC hosting in a shared data centre

Figure 7.1-4 presents a variant of the previous solution where not only the MEC platforms but also the 3GPP gateways are located in a shared data centre. In case of 5G Core the gateways are Protocol Data Unit (PDU) Session Anchor (PSA) User Plane Functions (UPFs). In the case of non-standalone 5GS or 4G EPS they are Packet Data Network Gateways (PGWs). All three scenarios, as described in Section 6, are possible where either MNO-1 and MNO-2 have the same MEC-related functions (MEC App X and MEC platform) deployed, or where MNO-2 has not all these functions deployed.

The precise realisations and involved transport networks required to realise this setup can be different for each MNO. But it is a generally valid assumption that MNOs can deploy parts of their core network, in this case gateways, in any data centre, also a shared one and that these gateways are connected through controlled[5] IP networks.

Three solutions were presented on how to build controlled environments for multi-MNO MEC. These are needed as a basis to preserve end-to-end QoS when multiple MNOs and their respective MEC platforms are involved in offering a service. The findings are equally applicable if only one MEC platform is involved but more than one MNO. There is no preference among the solutions. Their applicability depends on individual MNO properties like existing deployments and further services that they offer (e.g. if they are also in the data centre and/or WAN business) and what the services from other stakeholders (shared data centre and WAN provider) cost.

7.2 Application layer deployments for MEC4AUTO use cases

MEC4AUTO Task 1 [36] has defined five use cases to be investigated:

UC1: See Through
UC2: In-Vehicle Entertainment (IVE)
UC3: Intersection Movement Assist (IMA)

[5] Different stake holders like MNOs and WAN providers typically have network equipment like switches and routers in so-called Carrier Neutral Facilities where they can connect to each other. In public Internet context such interconnection is commonly called ‘peering’, aka ‘Network-to-Network Interface (NNI)’

UC4: Vulnerable Road User (VRU)
UC5: Vehicle Platooning

These use cases are quite different from the application layer perspective and their impact on Edge cloud deployment.

The application layer deployments in this chapter are based on the 5GAA Application Layer Reference Architecture [34]. The application layer deployments take both multi-MNO and multi-OEM aspects into account.

Three main scenarios are specified in this TR, see Chapter 6 above. Unless otherwise stated, the application layer deployments in this chapter are based on Scenario 1, i.e. both MNO-1 and MNO-2 have edge cloud and the applications are deployed in both edge clouds, see Figure 7.2-1 below.

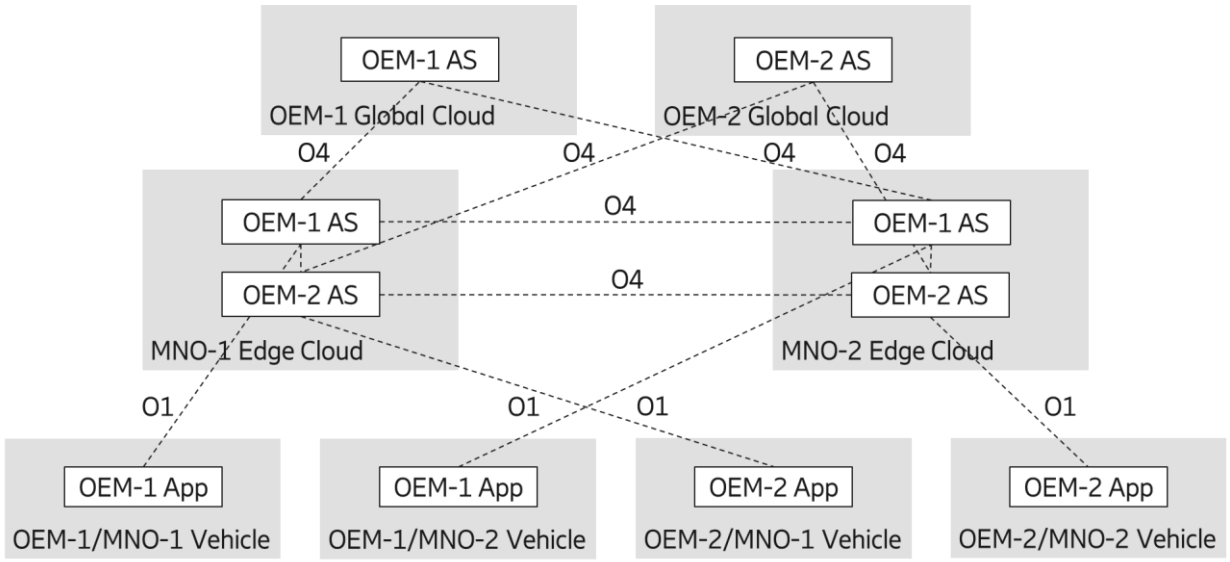

Figure 7.2-1: Application layer deployments according to 5GAA Application Layer Reference Architecture

The application layer deployments in this chapter can easily be transferred to the other two main scenarios.

7.2.1 UC1: See Through

The first use case is ‘See Through’, i.e. a vehicle with a front-facing video camera sends the video stream to the following vehicle. The following vehicle displays the video stream to the driver. The application layer deployment is shown in Figure 7.2.1-1 below.

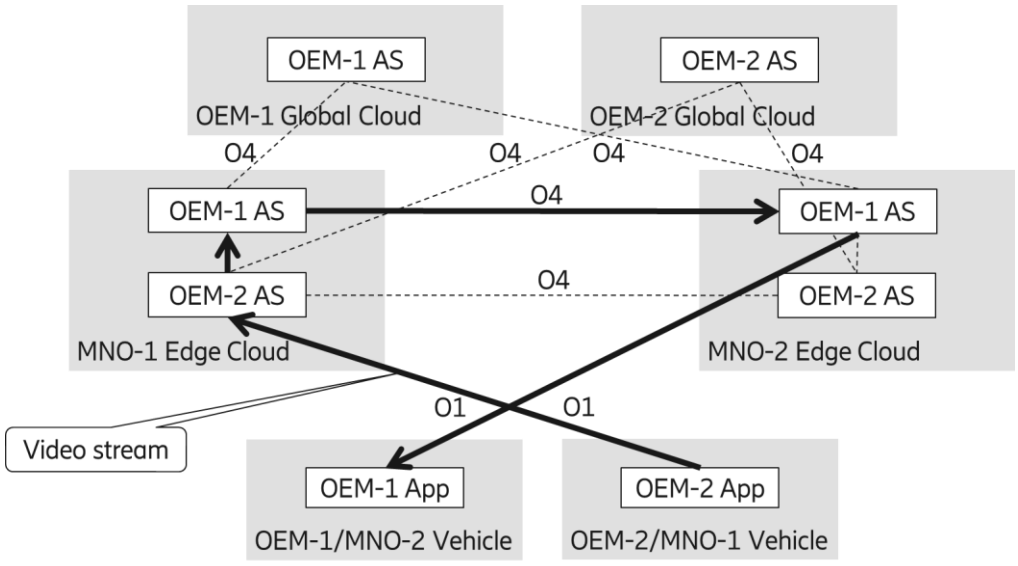

Figure 7.2.1-1: UC1: See Through

7.2.2 UC2: In-Vehicle Entertainment (IVE)

The second use case is ‘In-Vehicle Entertainment (IVE)’ and the assumption is that a video/audio stream is sent from the Edge Cloud to the vehicle. The application layer deployment is shown in Figure 7.2.2-1 below.

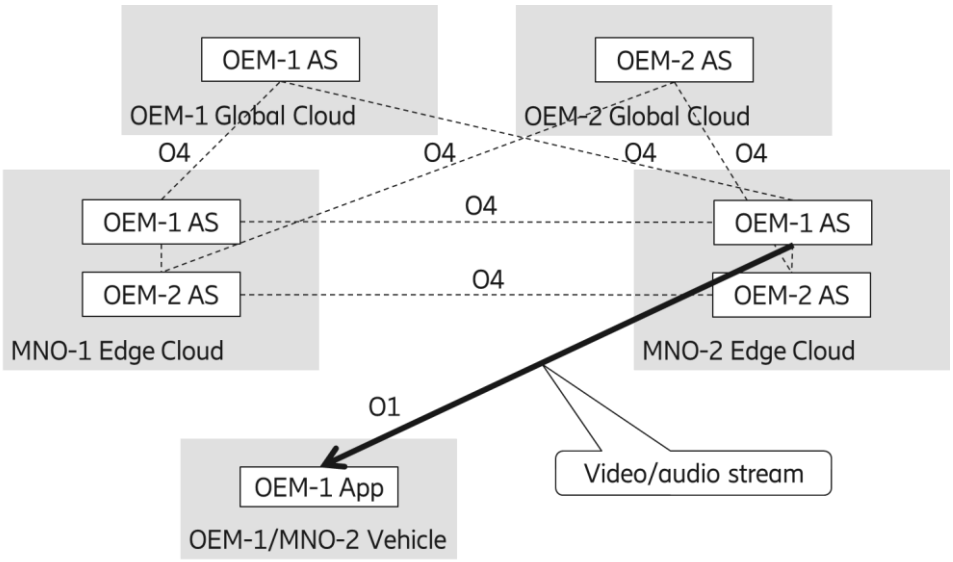

Figure 7.2.2-1: UC2: In-Vehicle Entertainment (IVE)

7.2.3 UC3: Intersection Movement Assist (IMA)

The third use case is ‘Intersection Movement Assist (IMA)’. All vehicles in an intersection exchange messages with all other vehicles at the intersection to improve traffic safety and traffic efficiency. Two different application layer deployment options for this use case are presented below.

The first deployment option for IMA is vehicle OEM oriented. An OEM-1 vehicle uses its proprietary interface O1 to update its OEM-1 Application Server (AS). The OEM-1 AS updates all other OEM-1 vehicles at the intersection. Finally, the OEM-1 AS updates OEM-2 AS which in turn updates all OEM-2 vehicles at the intersection. The application layer deployment is shown in Figure 7.2.3-1below.

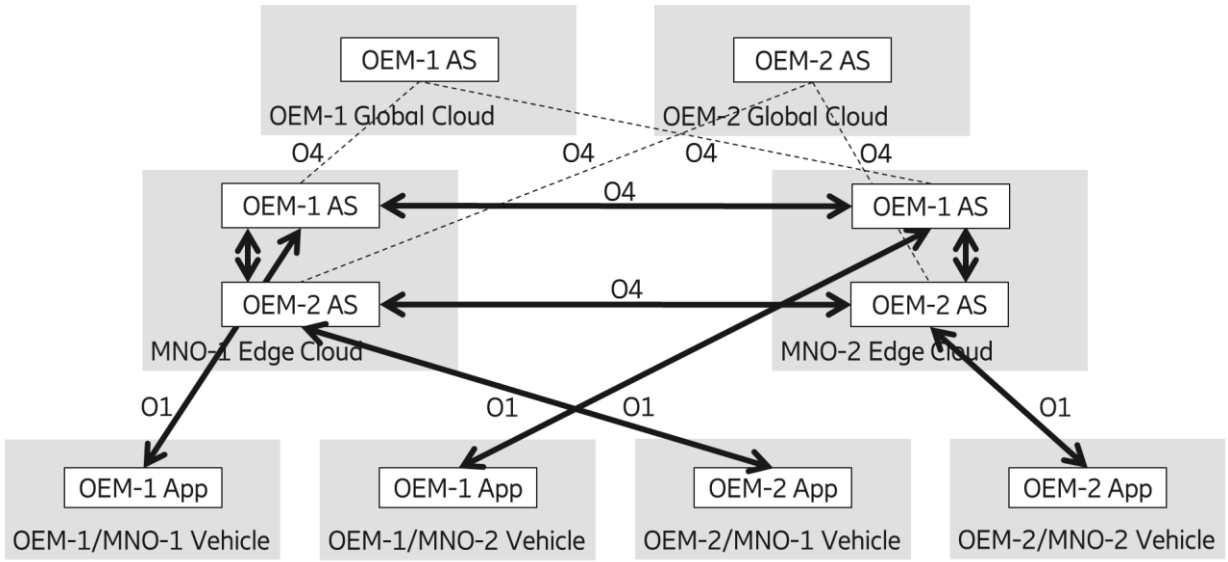

Figure 7.2.3-1: UC3: Intersection Movement Assist (IMA), vehicle OEM oriented

The second deployment option for IMA is C-ITS oriented. It is assumed that all vehicles have a V2X application that support standardised C-ITS messages for IMA. A vehicle uses a standardised interface V1 to update its V2X Application Server (AS). The V2X AS updates all other vehicles at the intersection. Finally, the V2X AS updates all

other V2X ASs, which in turn updates all V2X vehicles at the intersection. The application layer deployment is shown in Figure 7.2.3-2 below.

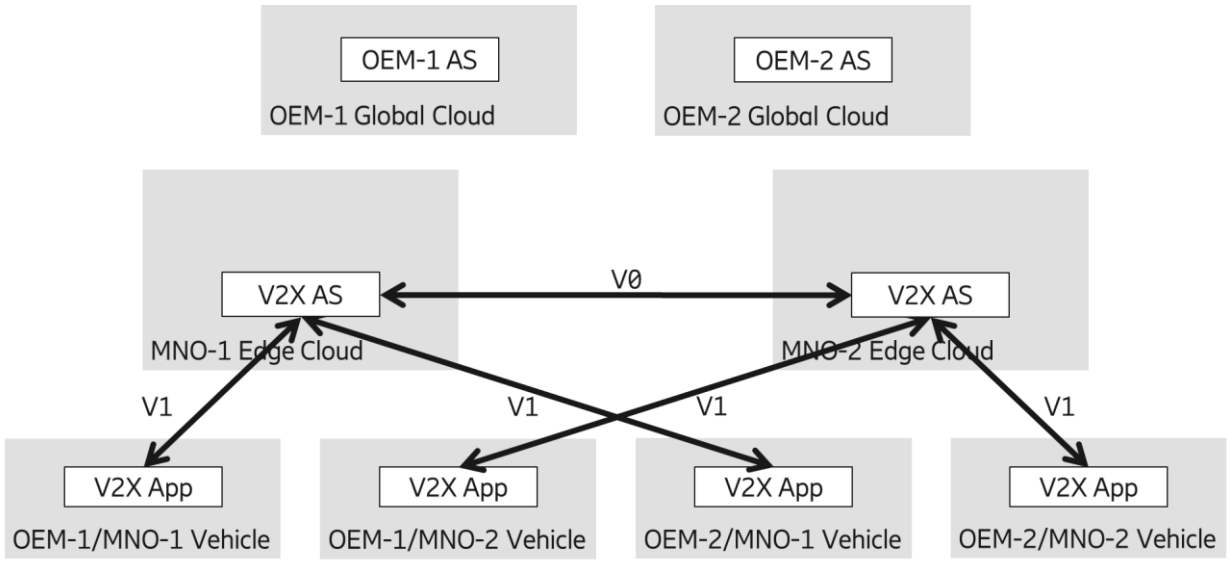

Figure 7.2.3-2: UC3: Intersection Movement Assist (IMA), C-ITS oriented

A challenge with this deployment option is to find a proper stakeholder for the V2X Application Server.

7.2.4 UC4: Vulnerable Road User (VRU)

The fourth use case is 'Vulnerable Road User (VRU)'. An OEM-2 vehicle with a front-facing video camera sends the video stream to its OEM-2 Application Server in the Edge Cloud. The OEM-2 AS analyses the situation. If a VRU is in danger, OEM-2 AS sends a warning message to the driver of the OEM-2 vehicle and all other OEM-2 vehicles in the vicinity. Finally, the OEM-2 AS updates OEM-1AS, which in turn updates all OEM-1 vehicles in the vicinity.

This type of VRU protection is not dependent on any device for the VRU. The deployments are based on the in-vehicle sensor-based approach of UC4. The infrastructure sensor-based approach of UC4 is a subset, where only the VRU warning is send in downlink but no video stream in uplink.

7.2.4.1 Deployment according to Scenario 1

In Scenario 1, both MNO-1 and MNO-2 have Edge Clouds and the ASs are deployed in both. The application layer deployment according to Scenario 1 is shown in Figure 7.2.4.1-1 below.

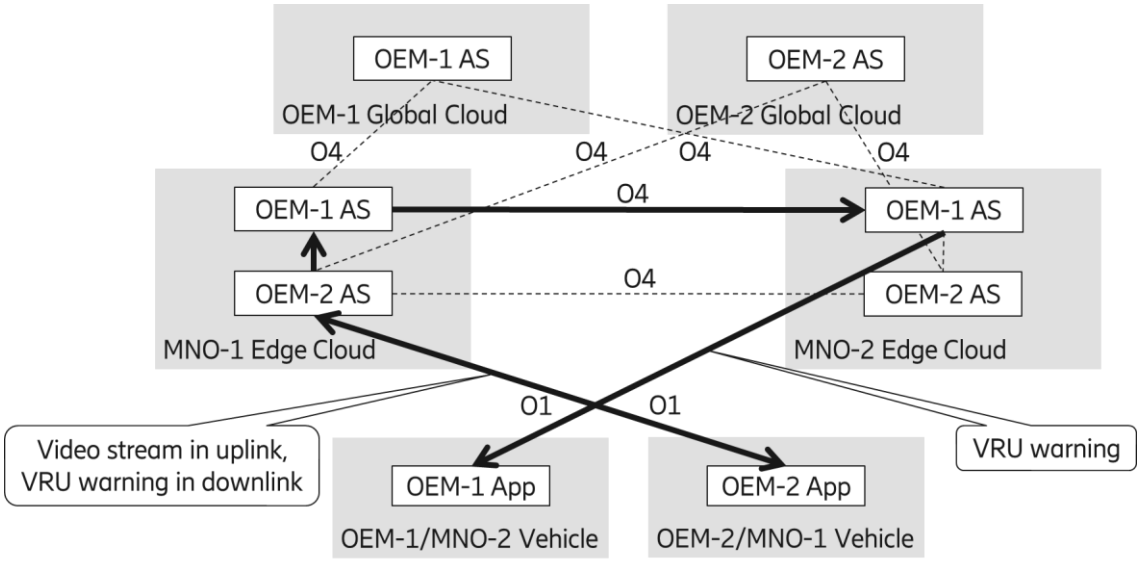

Figure 7.2.4.1-1: UC4: Vulnerable Road User (VRU), Scenario 1

7.2.4.2 Deployment according to Scenario 2

In Scenario 2, both MNO-1 and MNO-2 have Edge Clouds, but the ASs are only deployed in the MNO-1 case. The application layer deployment according to Scenario 2 is shown in Figure 7.2.4.2-1 below.

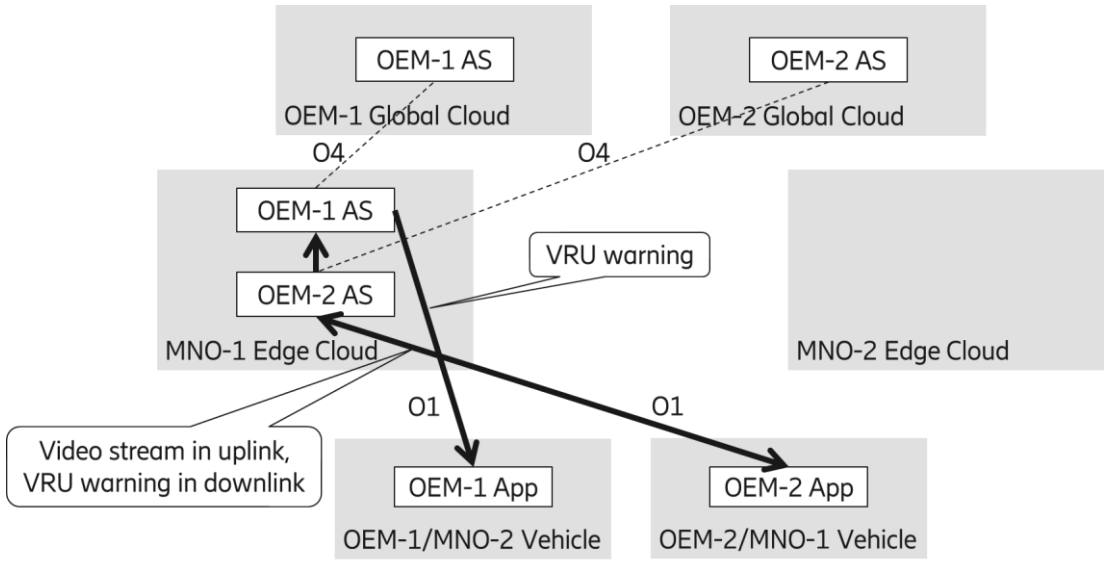

Figure 7.2.4.2-1: UC4: Vulnerable Road User (VRU), scenario 2

Note that according to '5GAA V2XSRA Application Layer Reference Architecture' [34], O1 denotes the endpoints of the application layer protocols between OEM AS and OEM App.

The endpoints of the application layer protocol message 'VRU warning' in Figure 7.2.4.2-1 above is OEM-1 AS in the MNO-1 Edge Cloud and OEM-1 App in the OEM-1/MNO-2 Vehicle. However, since the OEM-1/MNO-2 Vehicle is connected via the mobile network MNO-2, the application layer protocol message 'VRU warning' is routed via the mobile network MNO-2 by lower layer protocols.

7.2.4.3 Deployment according to Scenario 3

In Scenario 3, only MNO-1 has Edge Cloud and the ASs are deployed there. The application layer deployment according to Scenario 3 is shown in Figure 7.2.4.3-1 below.

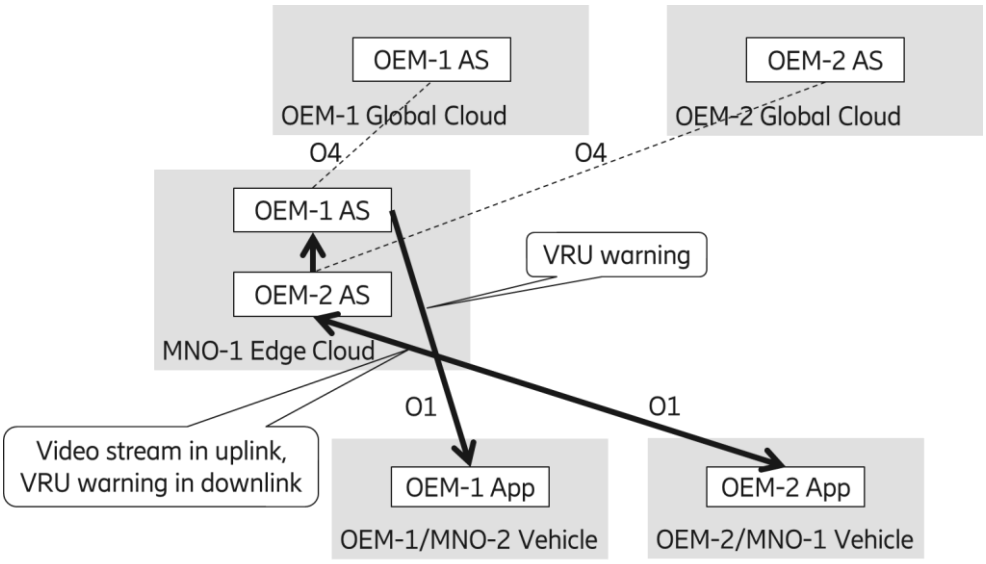

Figure 7.2.4.3-1: UC4: Vulnerable Road User (VRU), Scenario 3

The endpoints of the application layer protocol message 'VRU warning' in Figure 7.2.4.3-1 above is OEM-1 AS in the MNO-1 Edge Cloud and OEM-1 App in the OEM-1/MNO-2 Vehicle. However, since the OEM-1/MNO-2 Vehicle is

connected via the mobile network MNO-2, the application layer protocol message ‘VRU warning’ is routed via the mobile network MNO-2 by lower layer protocols.

7.2.5 UC5: Vehicle Platooning

The fifth use case is ‘Vehicle Platooning’. A head vehicle and a few member vehicles in a platoon exchange messages with other vehicles in the platoon to create, configure and control the platoon.

An OEM-1 vehicle uses its proprietary interface O1 to update its OEM-1 Application Server. The OEM-1 AS updates all other OEM-1 vehicles in the platoon. Finally, the OEM-1 AS updates OEM-2 AS which, in turn, updates all OEM-2 vehicles in the platoon. The application layer deployment is shown in Figure 7.2.5-1 below.

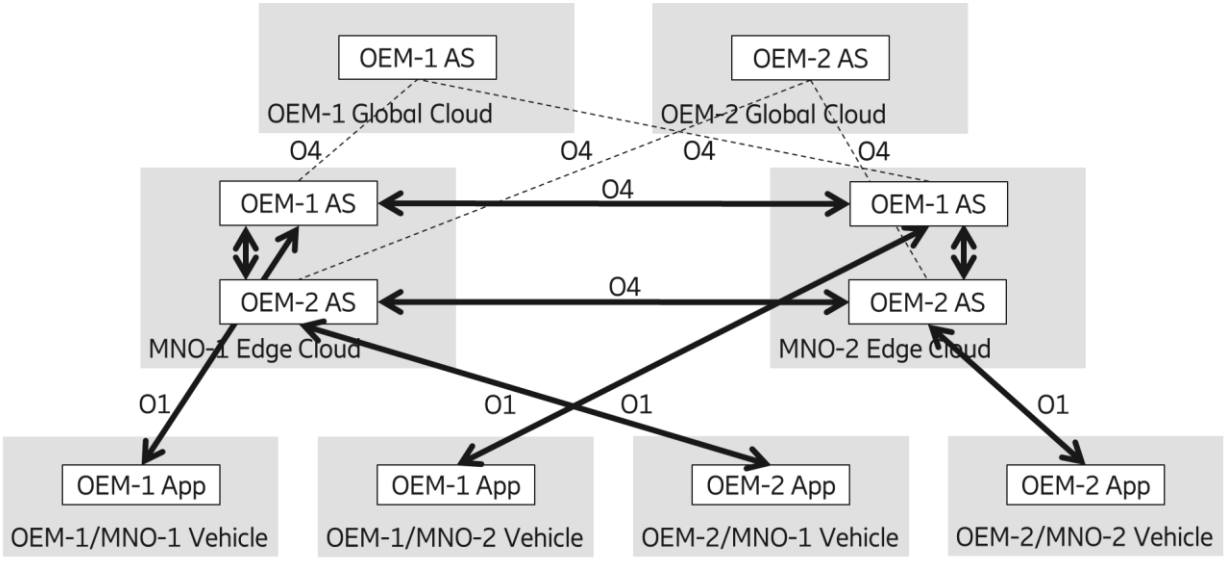

Figure 7.2.5-1: UC5: Vehicle Platooning

7.2.5.1 Deployment example (vehicle joining/leaving the platoon)

The main purpose of the platooning application is to determine/update the platoon head vehicle and establish communication between it and platoon members. Determining which vehicle is nominated platoon head is dependent on the scenario under consideration and may lead to different types of platooning use case, among which one can find the group start 5GAA use case [36].

When the platoon head is selected by the platooning application server of OEM-1, the application layer deployment for joining V2 and V3 of the OEM-2 to the platoon is given by the following:

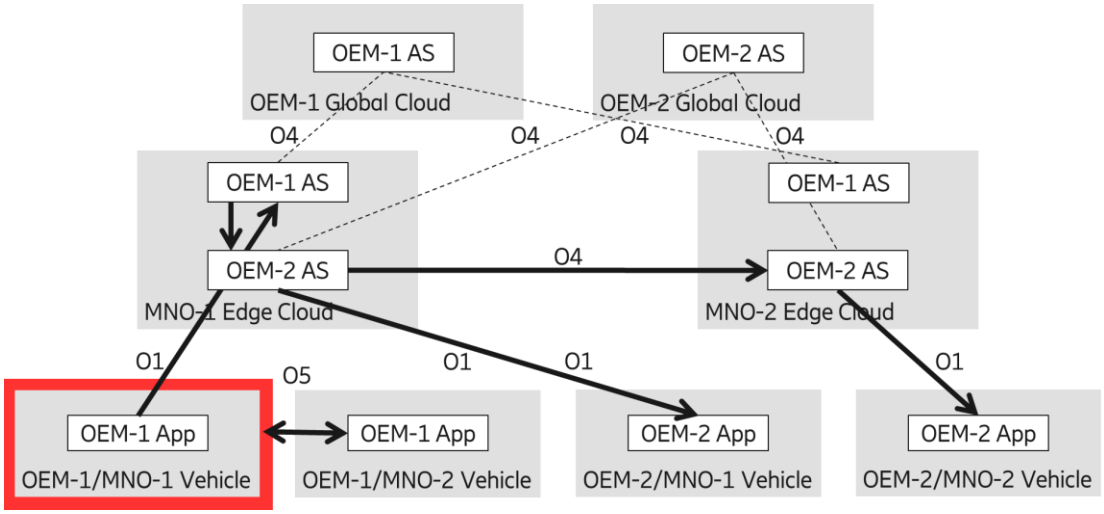

Figure 7.2.5.1-1: UC5: Vehicle Platooning deployment example (vehicle OEM-2 joining the platoon)

7.2.5.2 Deployment example (changing the platoon head vehicle)

Another important deployment aspect of the platooning use case is the change of the platoon head. In the example below, the platoon head is changed from the vehicle of OEM-1/MNO-1 to a vehicle in OEM-2/MNO-2.

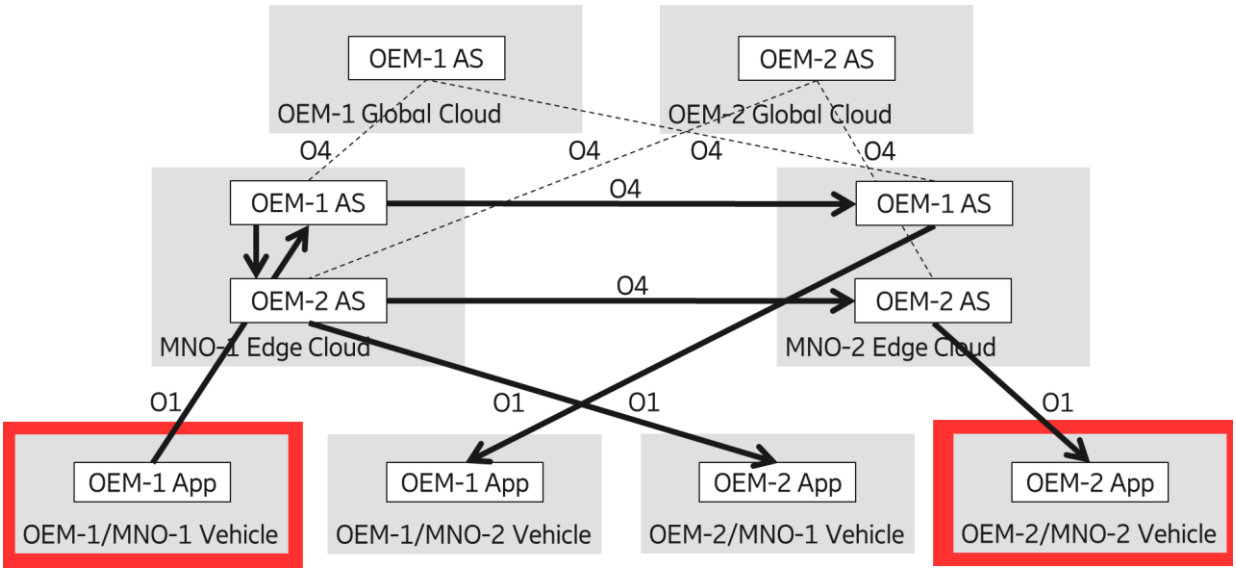

Figure 7.2.5.2-1: UC5: Vehicle Platooning deployment example (platoon head change from OEM-1 to OEM-2)

One possible way to reduce the complexity of the deployment is to build some form of application server federation of the OEM AS. In this case, the deployment flow is provided by the figure below. The OEM- 1 and OEM-2 establish 'agreements' and are considered as members of an AS federation. So, OEM-2 can communicate with OEM-1 App and vice versa. In this case the deployment is simplified but the challenge is still to investigate the business aspects for this OEM AS federation model.

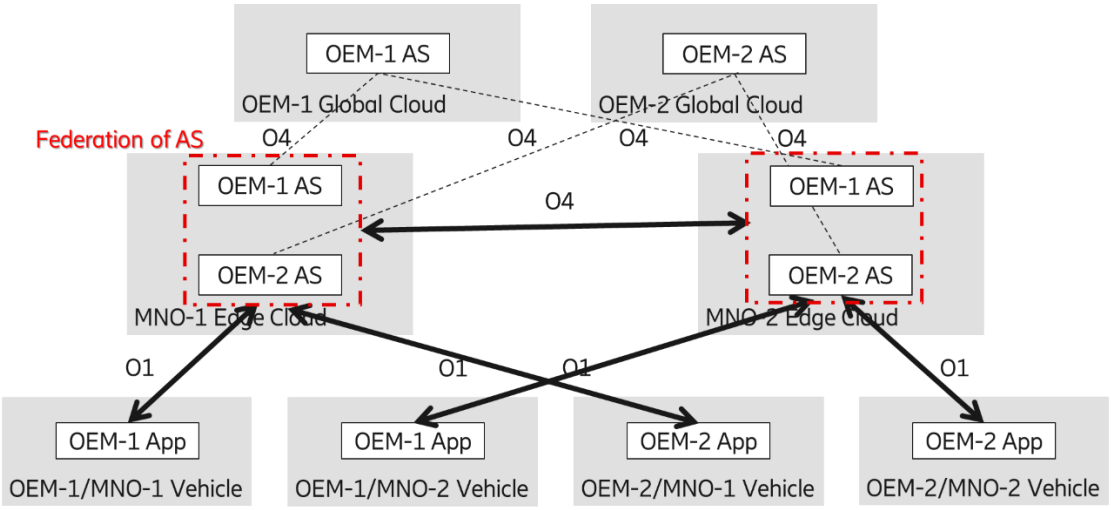

Figure 7.2.5.2-2: UC5: Vehicle Platooning deployment with federated OEM AS

7.3 Examples of demonstration/trial implementations

The architectural considerations in this Technical Report are mainly related to the specific goal of MEC4AUTO to demonstrate interoperability in multi-MNO scenarios. In fact, a target for a MEC4AUTO demo trial should consider multiple MNOs, which in general either:

1. Do not have a MEC but accept their networks interconnecting with other MNOs in their region, or
2. Do have their own MEC deployment.

In practice, for the purpose of demos/trials, interoperability can be achieved if:

- Interconnection exists between MNOs in a region,
- Edge Apps can run on different MNOs and MEC systems without bias (and consume different service APIs),
- MEC systems can be managed/orchestrated properly.

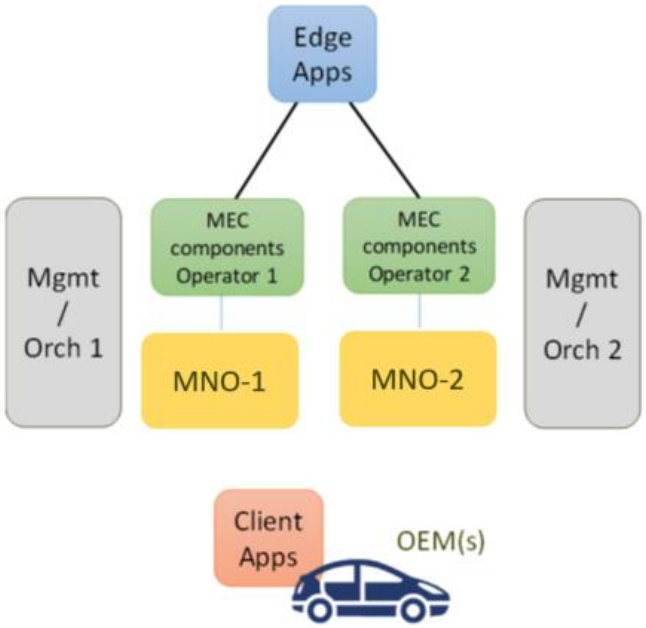

Figure 7.3-5: Interoperability scenario in multi-MNO environment

In general, when considering the simplest multi-MNO scenario with two MNOs (depicted in the above Figure 7.3.1), we can make the following deployment considerations:

- The same Edge App should be able to run seamlessly in any MNO and MEC system (and consume different service APIs at the edge nodes)
- The Edge Apps are reachable from the client side (running in the vehicle) through an IP address
- Both MEC systems should be managed/orchestrated properly
- Two cases may arise:
    - MEC-2 system is not present: in this case, the App might not be in a low latency environment (the E2E path is therefore not optimal)
    - MEC-2 is present: in this case, the MEC4AUTO architecture components should enable this low latency connection at the physical level

In the case of two operators having their own MEC systems (which in general are different, and coming from different MEC infrastructure providers), the target for interoperability is that MEC application A should be able to run in operator environment A, or in operator environment B (Figure 7.3-2 below); otherwise, the ability to consume MEC services in infrastructure B would be lost. Here, the implicit assumption is that every MNO has distributed 3GPP components (e.g. UPF in 5G system).

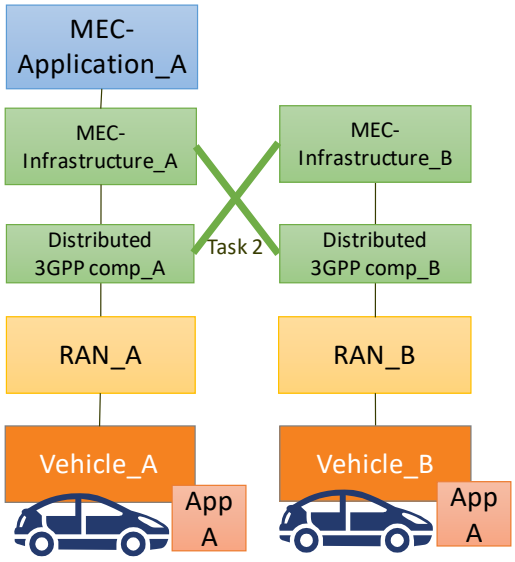

Figure 7.3-6: Possible connections between MNO A (left) and MNO B (right)

The most challenging scenario is clearly when only one MNO has its own MEC infrastructure. So, in this case the actual challenge is not technical but rather business-related, needing to convince all interested operators (MNOs indicated in Figure 7.3-3 below) that they must interconnect with another MNO's MEC system on a low, distributed network level. The consequence, otherwise, is to lose low latency benefits provided by Edge Computing. Here, the implicit assumption or pre-requisite is also that every MNO has distributed 3GPP components (e.g. UPF in the 5G system).

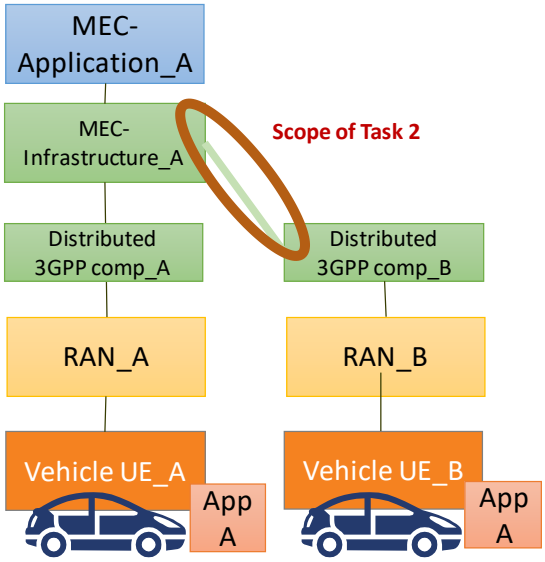

Figure 7.3-7: Possible connection, where MNO B has no MEC infrastructure

A third case, to be avoided, is when only one MNO has a MEC system deployed in its network, but the roaming operator is unwilling to provide a MEC connection. In this case, a MEC-enabled C-V2X service cannot be provided in an interoperable way across different systems.

8 Interoperability and service continuity for Edge Computing

8.1 State of requirement

Because vehicles are designed to move around, and often at high speeds, it poses a particular technical challenge in delivering a reliable MEC-V2X architecture with widely accessible and uninterrupted application services as part of the emerging Internet of Vehicles.

To ensure V2X service continuity, the network domain solution and application domain solution should be considered at the same time.

As described in [10] – network domain when the application is relocated – the N6 connection between the 5GC and Data Network (DN) will need to be re-established. To support the upper layer session and service continuity, one of the solutions is to keep the connection between the 5GC and AF before the new N6 connection is fully ready. This solution enables the runtime between the AF and 5GC to be coordinated, which supports application relocation without breaking the upper layer session and affecting the continuity of the Ultra-Reliable Low-Latency Communication (URLLC) services. Another solution is to release the connection between the AF and DN before the new N6 is established. As long as the interruption time is tolerable, the service continuity can still be guaranteed. Both of these two solutions can meet the requirement of service continuity for different kinds of C-V2X services.

In the application domain, the application server should complete the data migration from the source node to the destination node as soon as it gets accurate information about the destination node, ensuring that the service will not be interrupted while the user/vehicle is moving.

8.2 MEC service continuity based on N9 forwarding tunnel

8.2.1 Network domain solution

In 3GPP, how to support Session and Service Continuity (SSC) has been discussed. In TS 23.501[11], SSC modes and single PDU session with multiple PDU session anchors in the 5G System architecture were designed. SSC Mode 1 is impractical because vehicle mobility UE requires to frequent UPF change. SSC Mode 2 can meet low latency service requirements, but service interruptions occur during session and IP switching. In SSC Mode 3 and single PDU session with multiple PDU session anchors, the Network ensures that the UE suffers no loss of connectivity, which can meet the latency-sensitive demands of URLLC services.

Based on the single PDU session with multiple PDU session anchors, 3GPP offers one of possible solution (the single MNO), as shown in Figure 8.2. 1-1, which establishes a N9 tunnel between the source UPF and the destination UPF, thus ensuring that the application on the source Edge node can continue to provide timely application services for the departing vehicle, while striving to create a time buffer for the switching of the MEC application service. The architecture of this solution is as follows [10]:

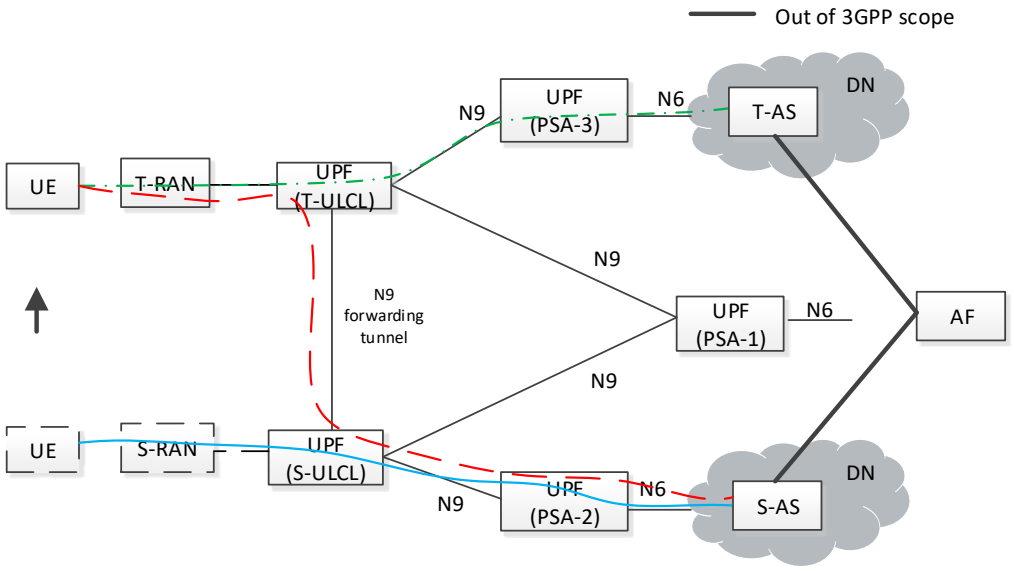

Figure 8.2.1-1: Architecture with N9 forwarding tunnel between source and target ULCL

The following illustrates the states for the N9 forwarding that are described in the Figure 8.2.1-1:

- Blue path-starting state: initially UE is connected to Source RAN (S-RAN) and has a PDU Session established with a remote PDU Session Anchor (PSA-1). The network has inserted an Uplink Classifier (S-ULCL) that directs selected traffic to a local PDU Session Anchor (PSA-2). Traffic from UE to the S-AS on the following path: S-RAN, S-ULCL, PSA-2, S-AS.
- Red path-intermediate state: the UE's location has changed from S-RAN to T-RAN, but since the upper-layer data has not been prepared on the T-AS the UE still accesses the S-AS through the N9 tunnel. Uplink traffic from existing sessions (between UE and Source AS) on the following path: T-RAN, T-ULCL, S-ULCL, PSA-2. Similarly, S-ULCL is configured to forward all downlink traffic for this UE coming from S-AS into the N9 forwarding tunnel towards T-ULCL.
- Green path-final state: the application service completes the redirection, and the traffic can be transmitted from UE to the T-AS through T-ULCL and PSA3.

The high-level procedural steps to support session and service continuity via the N9 tunnel are:

1. SMF selects a UPF as Target Uplink Classifier (T-ULCL) and establishes an N9 forwarding tunnel between T-ULCL and Source Uplink Classifier (S-ULCL).

2. The SMF updates the newly created N9 tunnel information to T-ULCL, RAN, PDU Session Anchor 1 (PSA-1), so that all uplink and downlink traffic between the UE and PSA-2 must pass through the N9 forwarding tunnel, and the uplink and downlink traffic between the UE and PSA-1 directly passes T-ULCL to PSA-1 (S-ULCL is used as the intermediate UPF).

3. SMF selects a UPF as PSA-3.

4. The SMF notifies the AF of changes in the local UPF (change from PSA-2 to PSA-3), which also includes the T-AS pointed to by PSA-3. The T-AS IP address can be configured at AF.

5. The AF triggers the S-AS to redirect the UE to a T-AS, using the upper layer (IP layer or HTTP layer) redirection mechanism. Based on the redirection, the UE starts to use a new destination IP address to lead T-ULCL to direct the traffic to PSA-3.

6. Traffic monitoring in the N9 forwarding tunnel can be performed by S-ULCL or T-ULCL, both of which can notify SMF.

7. SMF releases UPF and PSA-2 as S-ULCL.

8.2.2 Application domain solution

Referring to the MEC architecture in ETSI [5], and based on the network capability exposure of 5G network, the MEC platform and MEC application, combined with the network domain solution mentioned in the previous sub-section, an Edge Computing service continuity proposal can be formed. As shown in Figure 8.2.2-1, the entire proposal is mainly divided into three stages: application service retention, application instantiation and data migration, and application service redirection.

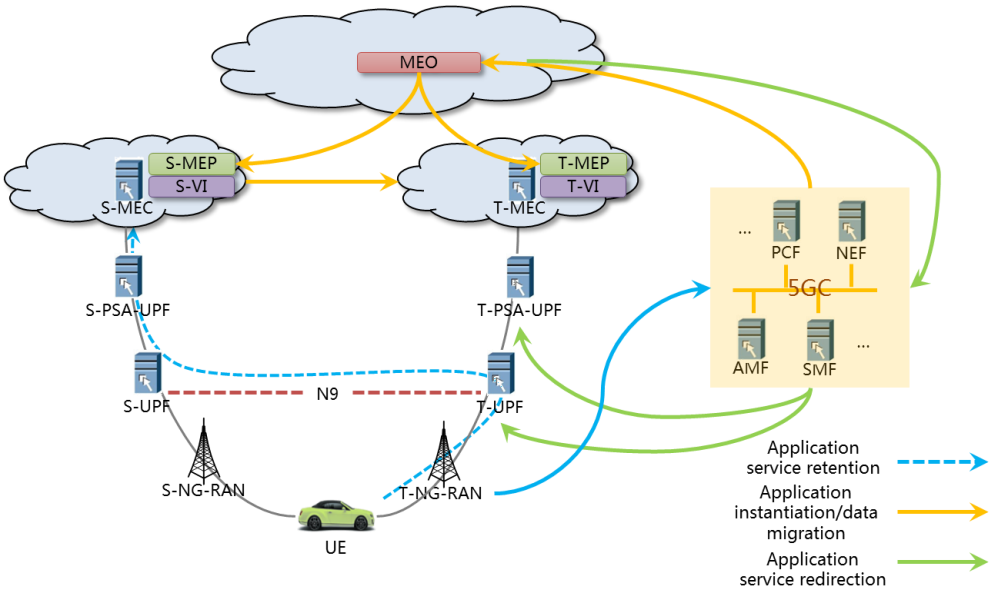

Figure 8.2.2-1: Process diagram for service continuity

Referring to ETSI, the key network elements/functions in the architecture are described as follows:

MEO: The MEC Orchestrator is the core functionality in MEC system-level management which is responsible for the following functions:

- Maintaining an overall view of the MEC system based on deployed MEC hosts, available resources, available MEC services, and topology;
- On-boarding of application packages, including checking the integrity and authenticity of the packages;
- Validating application rules and requirements, and if necessary adjusting them to comply with operator policies, keeping a record of on-boarded packages, and preparing the virtualisation infrastructure manager(s) to handle the applications;
- Selecting appropriate MEC host(s) for application instantiation based on constraints, such as latency, available resources, and available services;
- Triggering application instantiation and termination;
- Triggering application relocation as needed when supported.

MEP: The MEC Platform is the collection of essential functionality required to run MEC applications on a particular virtualisation infrastructure, enabling them to provide and consume MEC services. The MEC platform can also provide services.

VI: Virtualisation Infrastructure

VIM: The Virtualisation Infrastructure Manager is responsible for the following functions:

- Allocating, managing and releasing virtualised (compute, storage and networking) resources of the virtualisation infrastructure;
- Preparing the virtualisation infrastructure to run a software image, which includes configuring the infrastructure, and can include receiving and storing the software image;
- When supported, rapid provisioning of applications;
- Collecting and reporting performance and fault information about the virtualised resources;
- When supported, performing application relocation from/to external cloud environments, where the virtualisation infrastructure manager interacts with the external cloud manager to perform the application relocation.

Comparing the architecture with N9 forwarding tunnel, the MEO and MEC act as the AS and the AF can be deployed on the AS.

8.2.2.1 Application service retention

When UE's position changes and switches from source RAN to target RAN, the SMF decides to target UPF, configures forwarding rules and establishes an N9 forwarding tunnel from the target UPF to the source UPF, in order to maintain application service continuity. A UE uplink message will be forwarded to the source MEC application service via the N9 forwarding tunnel.

The schematic is shown in Figure 8.2.2.1-1:

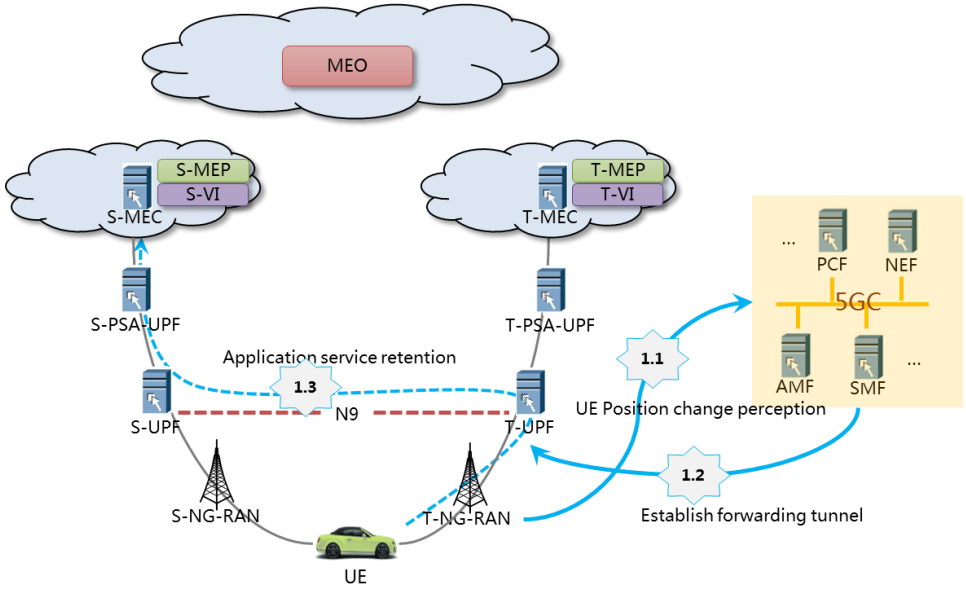

Figure 8.2.2.1-1: Process diagram for application service retention

<1.1 UE position change perception> The UE moves from the S-NG-RAN to the T-NG-RAN, and the 5GC 'senses' the position change of the UE on the RAN side.

Note: In the 5G network, the UE movement will cause the path switch signalling send to AMF. AF can subscribe for UE's mobility information from AMF through NEF.

<1.2 Establishing forwarding tunnel> The 5GC selects a UPF as the T-UPF for the UE according to the location of the UE, and configures the T-UPF forwarding rule to establish the N9 forwarding tunnel from the T-UPF to the S-UPF for the vehicle.

<1.3 Application Service retention> Vehicle uplink messages will be forwarded to the original S-MEC application service via the N9 tunnel, keeping application services constant.

8.2.2.2 Application instantiation and data migration

The MEO maintains an overall view and understanding of the MEC system based on deployed MEC hosts and the available resources, MEC services and topology (the relationship between MEC service areas and cells).

When the UE switches to target RAN, the MEO chooses the target MEC, triggers application instantiation, and applies data migration from source MEC to target MEC.

The schematic is shown in Figure 8.2.2.2-1:

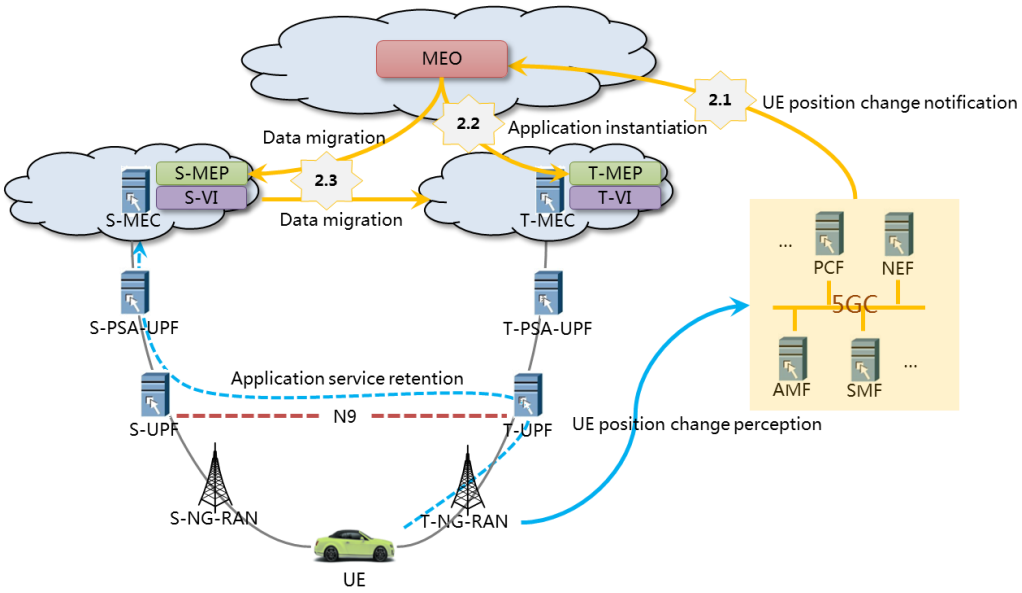

Figure 8.2. 2.2-1： Process diagram for application instantiation and data migration

<2.1 UE Position Change Notification> 5GC (via AMF, PCF, NEF) notifies the MEO of the changed UE position on the RAN side.

Note: In 3GPP TS 23.502 (V16.3.0), AF can subscribes UE Mobility information (Cell-ID) through Namf_EventExposure service carried by the Namf interface. So the MEO can get the UE's position change information (Cell-ID) from the 5GC.

<2.2 Application instantiation> The MEO selects the new Edge node, T-MEC, for the UE according to the position of the UE. If there is no corresponding application instance on the T-MEC, the application instantiation on the T-MEC will be triggered. The MEC Platform Manager (MEPM), VIM, T-MEP, and T-VI will collaborate together to prepare resources to complete the instantiation of T-MEC applications.

<2.3 Data Migration> If the T-MEC has the corresponding application instance, or the application is instantiated, the application data migration is triggered, and the corresponding application data deployed on the S-MEC is synchronised to the T-MEC application through the MEP. Based on the architecture shown in [5], there is an interface Mp3 between MECs, which can allow the data synchronisation between different MECs. So T-MEC and S-MEC can finish the synchronisation through Mp3 interface.

8.2.2.3 Application service redirection

When application instantiation and data migration finish, the MEO generates new application service routing rules. The 5GC updates corresponding UPF triage rules and makes it work. The UE's uplink message will be forwarded to target MEC applications via UPF.

The schematic is shown in Figure 8.2.2.3-1:

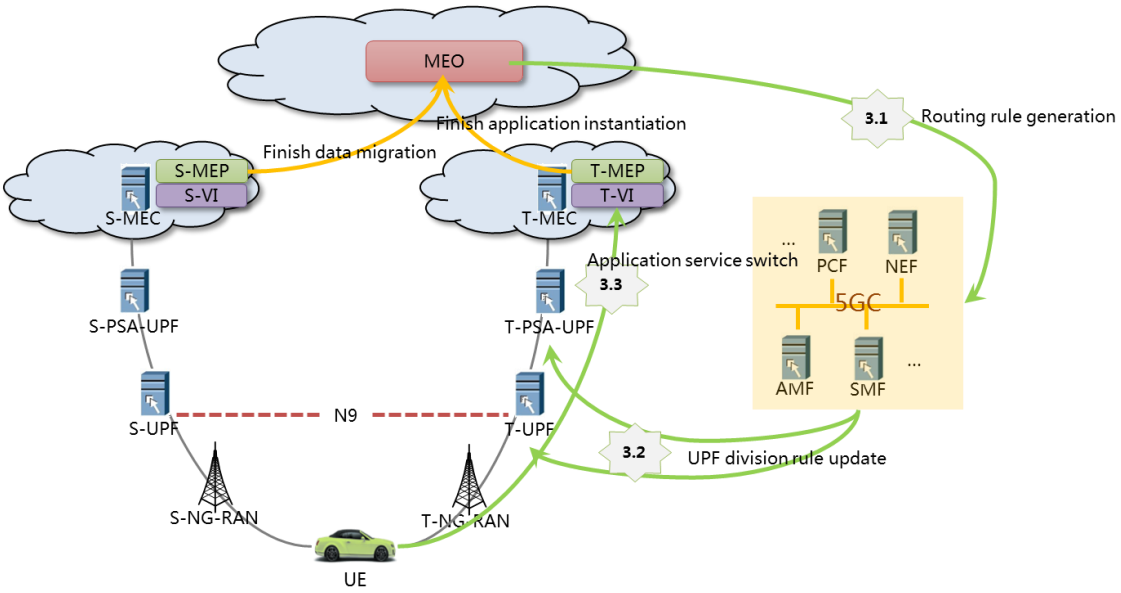

Figure 8.2. 2.3-1： Process diagram for application service redirection

<3.1 Routing Rule Generation> After application instantiation and data migration are completed, the MEO will trigger the application redirection for the network based on the T-MEC information and the network will form the new routing rules for the UE to forward the traffic to the application deployed on T-MEC.

<3.2 UPF Offload Rule Update> 5GC (through NEF, PCF, SMF) updates the corresponding UPF offload rule and makes it effective.

<3.3 Application Service Switching> At this time, the UE uplink data is forwarded to the application deployed on the T-MEC through the UPF in order to complete the redirection of the MEC application service.

8.3 Summary on MEC service continuity

The 3GPP enables to address the various continuity requirements of different UE applications and services, with different Session and Service Continuity modes. With single PDU session with multiple PDU session anchors, the network ensures that the UE suffers no loss of connectivity. A connection through new a PDU session anchor point is established before the previous connection is terminated in order to support seamless session and service continuity. Single PDU session with multiple PDU Session anchors is more appropriate for Edge use cases taking into account that 1) The mobility of vehicles/UE leads to frequent UPF change; 2) The Edge application is sensitive to the latency; 3) Support for Edge application relocation is needed so the SSC is not broken.

This section considers the network-level support for session continuity via the N9 forwarding tunnel [10]. Based on this, the application-level solutions explore how to support application service retention, instantiation, data migration, and service redirection between Edges. Note that these considerations are valid for supporting continuity between Edges within a single MNO network. The multi-MNO case is something for further study and should take into account outcomes of an ongoing ETSI study on inter-MEC systems and MEC-cloud systems coordination **Error! Reference source not found.**.

9 MEC security guidance

The purpose of this section is to provide general guidance for the secure implementation of MEC in a Cellular Automotive Connected Vehicle environment.

9.1 Security scope

Embedded security on Onboard Unit (OBU) or Electronic Control Unit (ECU) systems interacting with MEC systems call for a holistic security approach. Embedded security concerns are out of the scope of this document. The security boundary as defined in this MEC Security document shall be only address systems and networks within the MEC itself and the associated security services provided by the MEC.

The sections below will identify key security controls or requirements where compensating measures must be implemented for an overall secure system.

9.2 MEC4AUTO Shared Responsibility Security Model

Where systems are virtualised, many potential parties provide portions of an overall compute solution. Organisations have established a Shared Responsibility Security Model to deal with this. That is the security of the MEC is a collaboration between many parties.

MEC4AUTO Shared Responsibility Security Model

Security and compliance is a shared responsibility between the MNO, the MEC tenant application provider and the application user. This shared model can help relieve local security concerns among application users and MEC tenant application providers because the MEC operates, manages and controls the components from the host operating system and virtualisation layer down to the physical security of the facilities in which the MEC services operate. The application user and MEC tenant application provider assume responsibility and management of the tenant applications and services not provided by the MEC (including software updates and security configurations), other associated application software and firmware, as well as configuration of security services from the MEC tenant application provider.

9.3 Security boundary

One of the primary organising principles in Security Architecture is to define all the elements that are to be secured by the system. In the MEC case, the security boundary is defined by the MEC system itself and the associated security services that the MEC hosts for connected vehicles' OBUs and/or ECUs.

Note: It is assumed that the MEC provider secures the MEC as a cloud provider would normally secure its infrastructure. So these sections will primarily cover the security of MEC4AUTO security services. The overall MEC security would be covered by the MEC provider's own shared responsibility security agreement (and thus outside the scope of this document).

There are many use cases where vehicles will be interacting with different combinations of MNOs and connected vehicles. Example use cases will be described below.

9.3.1 Security boundary single OEM use case

The security boundary for the single MNO MEC non-roaming case is illustrated in Figure 9.3.1 below as a blue box.

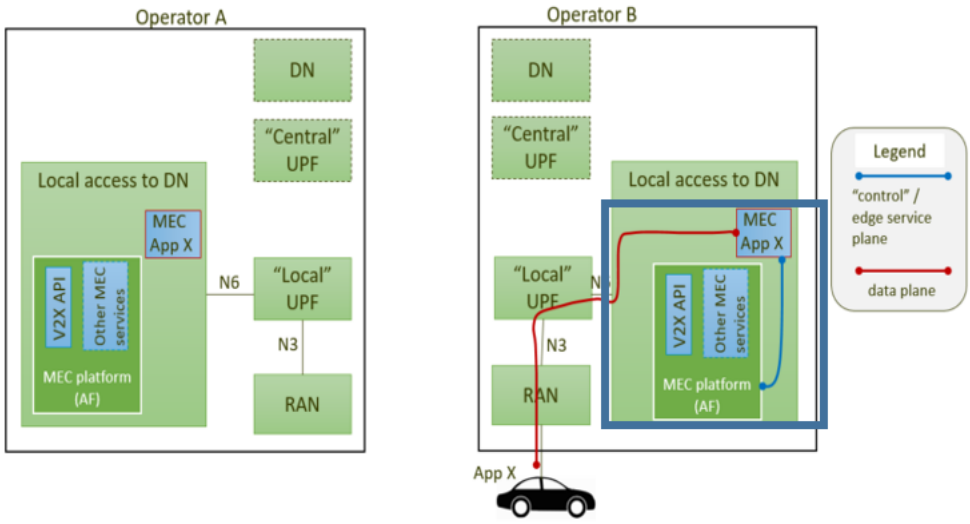

Figure 9.3.1-8: Illustration of a scenario where both MNOs have MEC platforms and MEC application X (single vehicle OEM use case)

9.3.2 Security boundary single OEM multi-MNO MEC use case

The security boundary for multi-MNO MEC joint security services case is illustrated below in Figure 9.3.2-1 as a set of blue boxes.

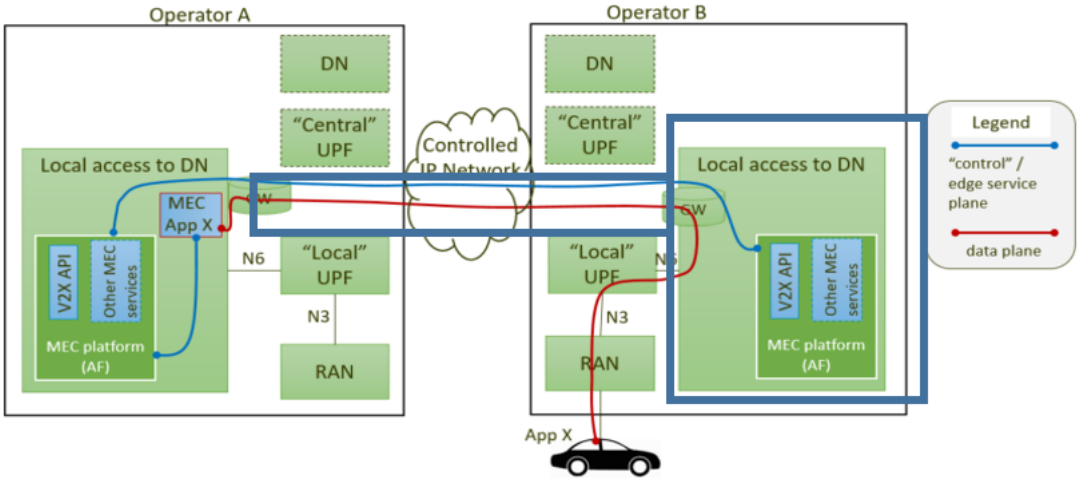

Figure 9.3.2-9: Illustration of a scenario where both MNOs have MEC platforms, but MEC application is available only in MNO A (single vehicle OEM use case)

9.3.3 Security boundary multi-MNO MEC roaming use case

The security boundary for multi-MNO MEC joint security services case is illustrated in Figure 9.3.3-1 as a set of blue boxes below.

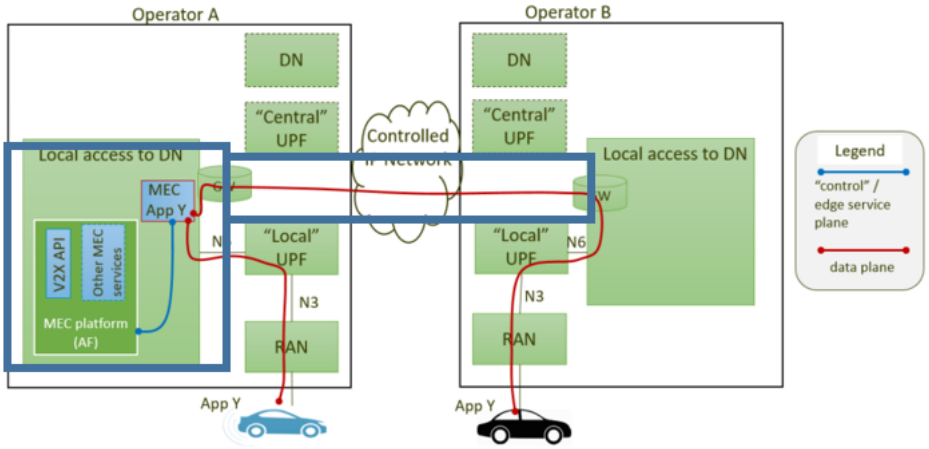

Figure 9.3.3-1 Illustration of a scenario where only MNO A has a MEC platform and MEC application Y and inter-MNO connectivity is by means of a controlled IP network (single vehicle OEM use case)

It is important to note that the security services proposed below do not extend to the N9 interface (which would be Local UPF to Local UPF in the above diagram). Therefore there is no guidance proposed for securing the N9 interface because it was deemed outside the security boundary of the MEC4AUTO area of concern.

9.4 MEC security approach

In line with the holistic security approach, the guidance of the US National Institutes of Standards and Technology (NIST) Cyber Security Framework (CSF) is leveraged for high-level guidance of areas of concern for MEC security. The NIST CSF was originally published in February 2014 in response to US Presidential Executive Order 13636, 'Improving Critical Infrastructure Cybersecurity', which called for the development of a voluntary framework to help organisations improve the cybersecurity, risk management, and resilience of their systems. NIST conferred with a broad range of partners from government, industry, and academia for over a year to build a consensus-based set of sound guidelines and practices.

The NIST CSF is often used in the evaluation of current and proposed system architectures where there is a need to identify security areas of concern and the corresponding security controls or requirements to be implemented to secure the proposed architecture. Using a framework helps to prevent duplication of security requirements and guides architectures to ensure that they have 'all bases covered' in the secure implementation.

Given that this TR is intended for an international audience, the NIST CSF guidance will be augmented by guidance from the European Union Agency for Cybersecurity (ENISA), particularly in the areas of privacy.

The NIST CSF is divided into five broad security areas: identify, protect, detect, respond and recover. With the inclusion of ENISA guidance primarily in conjunction with General Data Protection Regulation (GDPR), which is a regulation in EU law on data protection and privacy in the Member States and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to give control to individuals over their personal data and simplify the regulatory environment for international business by unifying the regulation within the EU [37].

With the inclusion of ENISA guidance there are six broad areas of high-level security functional guidance: identify, protect, detect, respond, recover and privacy. Here is a broad description of each security functional area.

- **Identify** – This is described as 'develop an organisational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities' [37]. The organisational understanding means that the MEC provider identifies and fully understands the systems, people, assets, data and capabilities of the MEC system and its associated security services.
- **Protect** – This is described by the constituent sub-categories (some not implemented in MEC) which are 'access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology [37]. Of these, the MEC provider is primarily concerned with access control, information protection processes and procedures, and MEC maintenance.

- **Detect** – This is described in three categories that comprise the ‘detect’ function: anomalies and events, security continuous monitoring, and detection processes. One of the prime requirements in security is ‘anomaly and misbehaviour detection’.
- **Respond** – This is described as all of the security functions around: response planning, communications, analysis, mitigations, and improvements. Although ‘response planning’ is important in MEC, ‘security implementation communication’ is by far the most important, while MEC cloud governance and laws are still in their infancy. It is reasonable to assume that responses within MEC security services would be limited to disconnection and communication responses only.
- **Recover** – This is described as all of the security functions around: recovery planning, improvements, and communications. As with the detect security function, communication with connected vehicles and entities will be critical in recovery of security services.
- **Privacy** – In MEC security implementations, the GDRP principles will be utilised to protect subscriber entity privacy. Given consent by subscriber entities, contractual compliance, data control, official authority interactions, public interest, and legitimate intent will all be covered in this ‘security functional area’. With these areas covered there will be other privacy services provided by the MEC to allow in order to comply with privacy best practice.

9.5 Detailed security functions within MEC

Within the MEC4AUTO Shared Responsibility Security Model there are specific security services that the MEC shall provide. These security services should align with established cybersecurity best practices. In MEC4AUTO we call upon guidance from NIST CSF for the functional areas ‘identity’, ‘protect’, ‘detect’, ‘respond’ and ‘recover’, while for ‘privacy we adopt the broad GDRP guidance.

Each Security Guidance Domain will be explored in more detail below.

Identify:

- Entity Management – In line with NIST CSF Asset Management (ID.AM), the vehicles, data, personnel, devices, systems, and facilities that enable the MNO(s) to achieve MEC functionality are identified and managed consistent with their relative importance to business objectives and the MNO’s risk strategy.
- Risk Assessment (Identity Security) – The MNOs understand the cybersecurity risk to MEC operations (including services, functions, and service availability), MNO assets, and individuals. The security guidance contained in this document is intended to be Risk Informed and Risk Managed. MNO(s) are encouraged to keep up to date with cybersecurity risk and threat intelligence such as published by OWASP and other global sources.

Protect:

- Access Control – To physical and logical MNO and MEC assets and their associated facilities. It is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to activities and services. A policy of least privilege shall be implemented for all MEC access and control.
- Data Security – Information and records (data) are managed consistent with the MNO’s risk strategy, privacy policy and applicable laws in order to protect the confidentiality, integrity, and availability of information.
- Information Protection – Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained by the MNO and used to manage protection of information systems and assets. Consumer privacy related information shall be protected at levels consistent with applicable laws or MNO privacy guidance.

Detect:

- Anomalies and Events – Anomalous activity shall be detected in a timely manner and the potential impact of events is understood. The MNO MEC provider shall detect misuse and malicious behaviour against services hosted by the MEC, where possible with regard to privacy constraints.

  Guidance on specific data-centric misbehaviour detections include consistency and plausibility checks:
  1) Consistency: Consistency-based misbehaviour detection leverages historical data aggregation to evaluate whether newly received messages (e.g. Basic Safety Message (BSM) in the SCMS) are consistent with the majority of the previous ones. For example, the average vehicle speed (historical) in a geographical area, and a specific threshold value defines an acceptance interval. Thus, if a newly received BSM’s speed value is out of this interval, it would be deemed suspicious. However, the consistency check relies on the ‘honest majority’ premise: the boundaries of what is normal or misbehaviour cannot be reliably defined if there is a large amount of misbehaviour in the dataset.

2) Plausibility: Plausibility-based misbehaviour detection leverages relationship models between different data fields within the messages to evaluate if they are plausible against these models. As an example, a speed plausibility check would start by computing the expected speed of a vehicle from two consecutive messages by calculating the travelled distance per time difference between them. Next, it would compare the obtained value with the actual speed value from the current message: if the difference between expected and actual speed values is larger than a certain threshold, the corresponding vehicle would be deemed as suspicious. Although more primitive than the consistency check approach, plausibility checks can be performed over messages from individual vehicles, and the honest majority premise is not required. Nevertheless, plausibility checks' effectiveness relies on a proper balance of the capability of handling subtle events and the generalisation of the considered data models. The ultimate goal is to maximise privacy while protecting the MEC infrastructure (cybersecurity).

- Security Continuous Monitoring: The MEC and related assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. MNO/MEC best practice shall be to provide automated monitoring for non-major attacks and malicious activity. Furthermore, the MNO MEC operator shall guard against larger cybersecurity attacks or campaigns and provide a minimal level of MEC services to function during a major cyber-attack. The MNO monitors its networks broadly and can respond to macro-events. However, it is unrealistic to expect MNOs to respond or mitigate every event. It is important to remember that MEC cybersecurity resides in a Shared Responsibility Security Model.

Respond:

- Response Planning – MNO MEC response processes and procedures are executed and maintained to ensure timely responses to detected cybersecurity events. Cybersecurity best practice is to have a security incident response plan that acknowledges the reality of MNO MEC Shared Responsibility paradigm.
- Response Communications – Response activities are coordinated with internal and external entities (OEMs and subscribers), as appropriate, to include external support from governmental agencies.
- Mitigation – MNO MEC cybersecurity activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Recover:

Response Planning – MNO MEC cybersecurity recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Privacy:

MEC privacy security services may vary depending on location and MNO, but given broad agreement on certain privacy controls, it is prudent to provide certain MEC privacy preserving functions. GDPR and laws inspired by GDPR such as CCPA are considered models upon which most MNO MEC operators should turn for privacy guidance.

The following privacy principles as per GDPR and other guidance inspired by GDPR are as follows.

1) If the data subject has given consent to the processing of his or her personal data;
2) To fulfil contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;
3) To comply with a data controller's legal obligations;
4) To protect the vital interests of a data subject or another individual;
5) To perform a task in the public interest or in official authority;
6) For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or his/her rights according to the Charter of Fundamental Rights (especially in the case of children).

- Anonymity Services – The MNO MEC shall provide anonymity services as applicable by law or MEC service (e.g. safety messaging)
- Personal Privacy Data Management – The MNO shall allow (where applicable by law) a mechanism for subscribers to manage privacy data.
- Do Not Track Services – The MNO shall allow (where applicable by law) a mechanism for subscribers to invoke services to prevent tracking.

9.6. MEC4AUTO security summary

It was determined that the architectural arrangement is securable with appropriate services and controls outlined in the above-named security services. Only the case of network interconnection across the N9 interface (as shown in Figure

6.3.3.1-1) was deemed beyond the securable boundary. A security solution for this scenario can be developed, but it is out of scope of this TR and should be considered for further study.

This allows for MNO-to-MNO secure interoperability across the controlled IP network, gateway to gateway (as shown in Figure 6.4.1-1).

MNOs and subscribers acknowledge the security value in adopting strong security guidance in their MEC environments. Many MNOs are directed to align their cybersecurity risk management and reporting practices to existing cybersecurity best practices in order to achieve a secure MEC system and organisational risk posture. MNOs can strengthen their cybersecurity by leveraging MEC security services as part of their enterprise risk-managed services. They can leverage the above MEC Security Best Practices to enhance future validations by third-party assessors like GSMA or equivalent.

10 Conclusions

Edge Computing is an important topic in V2X use cases, as many of them require low latency and reliability. The use cases involve a large amount of regional data that need to be processed and dispatched locally instead of uploading to the cloud, which is time and budget consuming without generating any added value. After having analysed selected use cases of interest [36], this document discussed the architecture and deployment aspects when Edge Computing is used for V2X use cases. It also described how interoperability and service continuity can be solved, in particular by providing guidance on how to realise and manage the interoperability of automotive services in a multi-MNO, multi-vehicle OEM and multi-MEC vendor environments.

The MEC4AUTO reference architecture was presented, by considering three main multi-MNO scenarios:

1. Both MNO A and MNO B have a MEC platform and MEC application X.
2. Both MNO A and MNO B have a MEC platform, but MEC application X is available only in MNO A.
3. Only MNO A has a MEC platform and MEC application X is available only in MNO A.

This report also provided some examples of Edge Computing architectures, realising the multi-MNO communication in different ways (i.e. the exchange through the public internet or controlled WAN, or through MEC Hosting in a shared data centre). Some application layer deployments for MEC4AUTO use cases from [36] were also presented.

Finally, some MEC security guidance was provided to allow secure multi-MNO interoperability on the MEC. In particular, security boundaries were determined for the main multi-MNO scenarios.

According to this analysis of the scenarios, some preliminary considerations were made:

- Scenario 1 is a straightforward solution, but it requires that the MEC platform and relevant MEC applications are installed in all MNO networks. It is a viable approach, but difficult to achieve in the short term due to business and market limitations.
- Scenario 2 has the MEC application X available only in MNO A, which makes the existence of the MEC platform in MNO B practically irrelevant (from a connectivity perspective). In this case, Scenario 2 can be managed with options A and B considered for Scenario 3 (‘only MNO A has a MEC platform and the related application’).
- Scenario 3 (‘only MNO A has a MEC platform and the MEC application is available only in MNO A’) can be managed with two deployment options:
    - Scenario 3A (‘N9 tunnelling’) requires some sort of roaming arrangement among operators within the same country that may result in unnecessary complexity and latency impacts, but it should be a technically valid option.
    - Scenario 3B (‘controlled IP network’) is perhaps easier to implement, but needs the configuration of ‘direct’ links between the two operator data networks (upon related business agreement between the operators, obviously).

Based on the above considerations, MEC4AUTO identified some open issues related to the multi-MNO scenarios presented:

- How quickly (short-, middle-, or long term) can the different MEC4AUTO scenarios be deployed?
- The perspectives for MEC deployment based on N9 interface or local ‘pairing’ between the operators should be clarified.
- The different MEC4AUTO scenarios need to be compared in terms of complexity, latency budget and how realistic they are to be deployed.
- It should be clarified how difficult it is in practice to establish the required local ‘pairing’ links between operators. What is the timeline for deployment that can be foreseen?

For that purpose, the group should further discuss possible follow-up activities, including the demonstrations reported and anticipated in the final MEC4AUTO deliverable.


5GAA
Automotive Association