ETSI GR MEC 024 V2.1.1 (2019-11)

Multi-access Edge Computing (MEC); Support for network slicing

Disclaimer

The present document has been produced and approved by the Multi-access Edge Computing (MEC) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/MEC-0024NWslicing

Keywords
MEC, slicing

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Multi-access Edge Computing (MEC).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document focuses on identifying the MEC functionalities to support network slicing. It first analyses the relevant network slicing concepts as defined by external organizations. Next, it collects relevant use cases based on the identified network slicing concepts when applied in the context of MEC and it evaluates the gaps from the defined MEC functional elements. When necessary, the present document identifies new MEC functionalities or interfaces as well as changes to existing MEC functional elements, interfaces and requirements. It will also recommend the necessary normative work to close these gaps if identified.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

[i.1] ETSI GS MEC 001: "Multi-access Edge Computing (MEC); Terminology".

[i.2] NGMN Alliance: "5G White Paper", February 2015.

[i.3] NGMN Alliance: "Description of Network Slicing Concept", January 2016.

[i.4] Open Networking Foundation: "Applying SDN Architecture to 5G slicing", ONF TR-526, April 2016.

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

[i.6] 3GPP TR 28.801: "Telecommunication management; Study on management and orchestration of network slicing for next generation network".

[i.7] ETSI TS 128 530: "5G; Management and orchestration; Concepts, use cases and requirements (3GPP TS 28.530)".

[i.8] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.9] ETSI GS NFV-IFA 013: "Network Function Virtualization (NFV); Management and Orchestration; Os-Ma-Nfvo reference point - Interface and Information Model Specification".

[i.10] ETSI GR MEC 017: "Mobile Edge Computing (MEC); Deployment of Mobile Edge Computing in an NFV environment".

[i.11] ETSI GS MEC 010-2: "Multi-access Edge Computing (MEC); MEC Management; Part 2: Application lifecycle, rules and requirements management".

[i.12] ETSI GS MEC 003: "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[i.13] ETSI GS MEC 002: "Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements".

[i.14] ETSI GS MEC 010-1: "Mobile Edge Computing (MEC); Mobile Edge Management; Part 1: System, host and platform management".

[i.15] ETSI White Paper No. 28: "MEC in 5G networks"; First edition - June 2018; ISBN No. 979-10-92620-22-1.

[i.16] ETSI GR NFV-EVE 012: "Network Functions Virtualisation (NFV) Release 3; Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework".

[i.17] ETSI GR NFV 001: "Network Functions Virtualisation (NFV); Use Cases".

[i.18] ETSI GR NFV-IFA 028: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on architecture options to support multiple administrative domains".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS MEC 001 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS MEC 001 [i.1] and the following apply:

3GPP	3rd Generation Partnership Project
5G	Fifth Generation
5QI	5G QoS Class Identifier
AMF	Access and Mobility Management Function
AN	Access Network
API	Application Programming Interface
CN	Core Network
CSMF	Communication Service Management Function
DN	Data Network
E2E	End-to-End
eMBB	enhanced Mobile Broadband
IoT	Internet of Things
MEAO	Multi-access Edge Application Orchestrator
MEC	Multi-access Edge Computing
MEP	Multi-access Edge Platform
MEPM	Multi-access Edge Platform Manager
MEPM-V	Multi-access Edge Platform Manager - NFV
MIoT	Massive Internet of Things
NF	Network Function
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NFVO	NFV Orchestrator
NFV-SCF	NFV-Slice Control Function
NGMN	Next Generation Mobile Networks
NRF	NF Repository Function
NS	Network Service
NSD	Network Service Descriptor

NSI	Network Slice Instance
NSMF	Network Slice Management Function
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NSSI	Network Slice Subnet Instance
NSSMF	Network Slice Subnet Management Function
NSSP	Network Slice Selection Policy
NST	Network Slice Template
ONF	Open Networking Foundation
OSS	Operations Support System
PCC	Policy & Charging Control
PCF	Policy Control Function
PDB	Packet Delay Budget
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
PNF	Physical Network Function
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RNI	Radio Network Information
RRC	Radio Resource Connection
RTT	Round Trip Time
SD	Slice Differentiator
SDN	Software Defined Networking
SDO	Standards Development Organization
SI	Service Instance
SLA	Service Level Agreement
SMF	Session Management Function
S-NSSAI	Single NSSAI
SST	Slice/Service Type
TN	Transport Network
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communications
V2X	Vehicle-to-everything
VIM	Virtualised Infrastructure Manager
VNF	Virtual Network Function
VNFFG	VNF Forwarding Graph
VNFM	VNF Manager

4 Overview

4.1 Introduction

The following clauses 4.2 to 4.5 provide an overview of network slicing concept as it has been defined in different SDOs and Fora. In particular, the following clauses refer to the most relevant external body's documents which introduce and define network slicing, and describe related specifications provided in NGMN, ONF, 3GPP and ETSI ISG NFV.

4.2 NGMN

According to NGMN "5G White Paper" [i.2], a network slice (i.e. "5G slice") supports the communication service of a particular connection type with a specific way of handling the C- and U-plane for this service. To this end, a 5G slice is composed of a collection of 5G network functions and specific Radio Access Technology (RAT) settings that are combined for the specific use case or business model while leveraging NFV and SDN concepts. Thus, a 5G slice can span all domains of the network: software modules running on cloud nodes, specific configurations of the transport network supporting flexible location of functions, a dedicated radio configuration or even a specific RAT, as well as configuration of the 5G device.

More specifically, the NGMN white paper "Description of Network Slicing Concept" [i.3] provides a detailed description of terminology and network slicing related concepts that are organized according to a three-layer architecture, as shown in Figure 4.2-1:

- **Service Instance Layer:** the end-user or business services, provided by a network operator or a 3rd party, which should be supported by the slice. Each service is represented by a Service Instance (SI).
- **Network Slice Instance Layer:** Network Slice Instances are sets of functions, each forming a complete instantiated logical network to meet certain network characteristics (e.g. ultra-low latency, ultra-reliability) required by the Service Instance(s). They are created based on Network Slice Blueprints, which provide a complete description of the network slice structure, lifecycle workflow and configuration options. A Network Slice Instance can be shared among multiple Service Instances, at least when the Service Instances are provided by network operators. Each Network Slice Instance may include one or more Sub-Network Instances to form a set of Network Functions running in physical or logical resources.
- **Resource Layer:** Resources are distinguished in "physical resources" and "logical resources". A physical resource is a physical asset for computation, storage or transport, including radio access. Logical resources are partitions of physical resources or grouping of multiple physical resources dedicated to a Network Function or shared between a group of Network Functions.

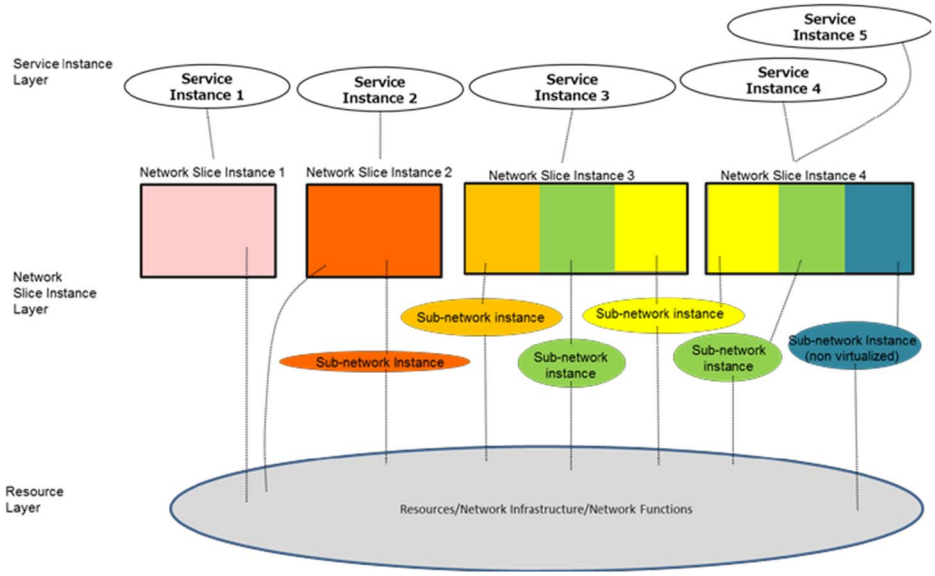

Figure 4.2-1: NGMN Network Slice Concept
(Figure 1 in NGMN White Paper "Description of Network Slicing Concept" [i.3])

The mapping between the NGMN layers and the ETSI NFV architectural framework is illustrated in Figure 4.2-2 and can be summarized as follows:

- the Service Instance layer plays the role of an OSS functional block with regards to the NFVO;
- the Network Slice Instance layer maps to the collection of Network Services handled by NFV Management & Orchestration functions. The network service can be described by a VNF Forwarding Graph (VNFFG), typically defined by a Network Service Descriptor (NSD) using a specific deployment flavour;
- the Resource layer maps to the NFVI and the VIM(s).

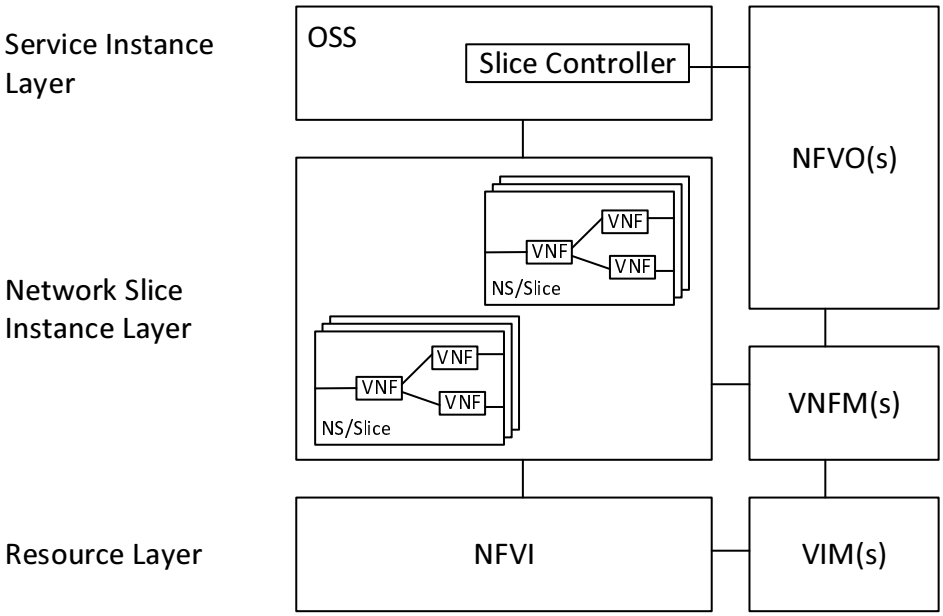

Figure 4.2-2: Mapping of the NGMN layers onto the ETSI NFV architectural framework

Based on the NGMN white papers [i.2], [i.3], the NGMN focus is mainly given to communications services and to traffic treatment into the 5G slice across both mobile and core networks while providing the network capacity when and where needed and according to the use case requirements. Moreover, although cloud nodes are considered as possible substrate to host the 5G network functions, not any reference is provided to the specific location of cloud resources used to allocate the 5G slice, whether at the edge or in the centralized cloud. Finally, although the deployment of application functions is considered as an option to address specific use cases (e.g. 5G slice for smartphone use), the on-boarding of vertical application on a cloud node is not specifically addressed except in terms of just promoting the definition of open interfaces.

4.3 ONF

The SDN architecture defined by ONF TR-526 [i.4] allows multiple client network instances to share the common underlying infrastructure in a technology-independent fashion, thus enabling the orchestration of any type of resources, such as storage, computing, and heterogeneous network resources (i.e. wired, wireless, and mobile) that may be available at any location of the network including the edge. At that end, the ONF architecture comprises three main components (see Figure 4.3-1), namely applications, SDN controller, and resources. A client-server relationship is established through the interfaces between the applications and SDN controller and between the SDN controller and the underlying resources.

The SDN controller is in charge of mapping the service requirements to the underlying resources according to policies defined by the administrator of the network and of dynamically optimizing the use of such resources. The SDN controller provides two types of resource views: one offered to the application on top, through a client context, which is specific to a given client, and a second one enabling the interaction with the underlying resources, through a server context, which is specific to a given group of underlying resources. The client context is created by the administrator after a business agreement is reached between the client organization and the serving organization. Through orchestration, the SDN controller dynamically handles the contention of multiple services for the resources of a common infrastructure and it offers a homogeneous end-to-end handling of the underlying resources, even if belonging to different technical and/or administrative domains. Through virtualisation instead, the SDN controller creates the client context by allocating (part of) the underlying resources to that client. Additionally, the client context also includes the actions by the client that are allowed over those resources. As part of the client context, resource groups determine how virtual resources are exposed to the client.

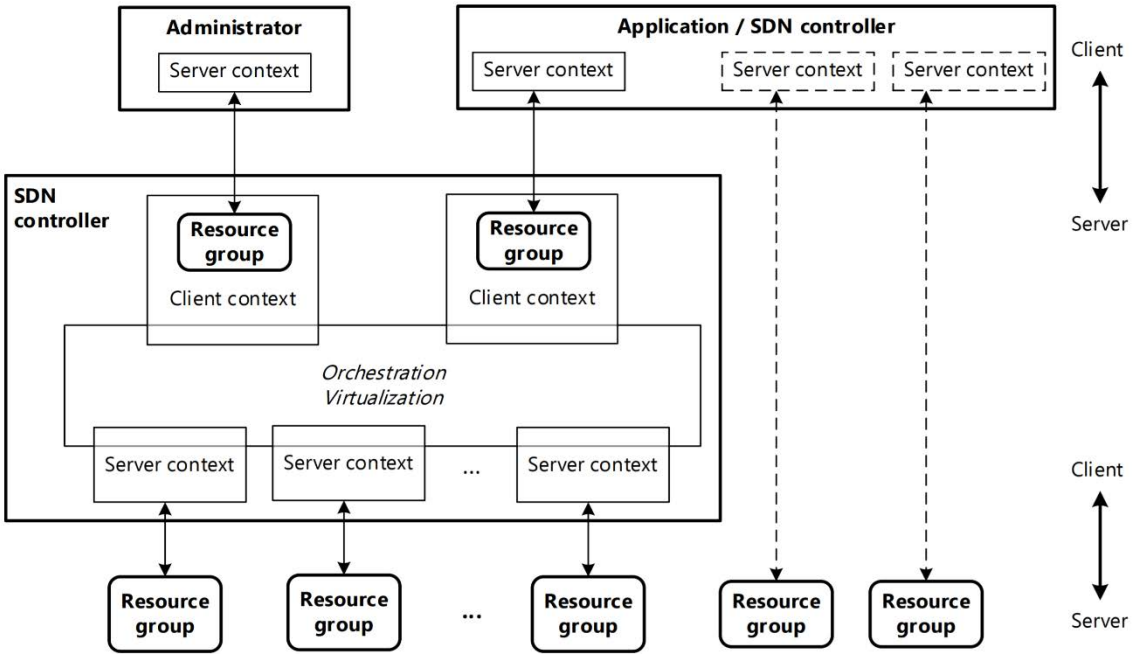

Figure 4.3-1: Core concepts of the SDN architecture (Figure 1 in ONF TR-526 [i.4])

Since resource is understood in a generic sense, the virtual resources exposed to the client may, in turn, be seen as underlying resources by that client and orchestrated and virtualised again to fulfil the service needs of the client of that client. Therefore, recursion is supported by the architecture. In general, the slicing concept is initially seen from a business perspective, in which clients request the provider to fulfil their specific service needs, including allocation of a share of the underlying resources and a set of services to operate on them. Therefore, in the SDN architecture, the client context can be directly mapped to a slice, since it offers the abstract set of resources requested by a service and the supporting control service logic. Such slices can be instantiated on demand with per-service instance granularity and tailored to the service needs, including their dynamic reconfiguration, and can span across multiple domains, including the edge.

4.4 3GPP

The 3GPP approach is based on the NGMN slicing concept. According to NGMN, a slice instance is built over physical or logical resources that are fully or partially isolated from other resources. The slice is built using the Network Function that are processing functions of the Network Slice Instance (NSI) and correspond to ETSI virtual or physical network functions (VNF and PNF, respectively). ETSI TS 123 501 [i.5] distinguishes between network slices and Network Slice Instances. A network slice is considered as *"a logical network that provides specific network capabilities and network characteristics"* [i.5]. These network capabilities and network characteristics are enabled specific through Network Functions that communicate over a Service Based Architecture and corresponding Service Based Interfaces. A Network Slice Instance is considered *"a set of Network Function instances and the required resources (…) which form a deployed Network Slice"* [i.5]. Instances of the same Network Slice provide specific features based on their associated Slice/Service Type (SST). A Slice Differentiator (SD) may be used to enable the deployment of Network Slice Instances intended for different customers. E.g. Instances of a Network Slice can be provided to different verticals with similar needs that can be satisfied with the same set of features provided by the Network Slice. Thus, a network slice is seen within the context of mobile networks, including the control and user plane functions. Network slices may support different features and network functions, but an operator is free to deploy also several network slices with the same characteristics.

When the UE registers to a network, the UE signals its Network Slice preference by providing a Slice/Service Type (SST) and possible a Slice Differentiator (SD) within a parameter referred to as Single Network Slice Selection Assistance Information (S-NSSAI). A UE may establish up to 8 PDU Sessions. A PDU Session can be served through one and only one Network Slice Instance, i.e. a PDU Session can be associated to only one S-NSSAI. However, a Network Slice can support multiple PDU Sessions. Therefore, a UE may be connected to up to eight network slices simultaneously. The set of network slices to which a UE is connected may change dynamically. The NSSAI requested by UE constitutes a vector of maximum eight S-NSSAIs, this vector is known as Requested NSSAI. The Requested NSSAI is included by UE in the Radio Resource Connection (RRC) establishment message. As described above, the S-NSSAIs are comprised of two parts:

- a **Slice/Service type (SST)**, which refers to the expected Network Slice behaviour in terms of features and services;
- a **Slice Differentiator (SD)**, which is optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.

3GPP has defined three standardized SST values so far (see ETSI TS 123 501 [i.5]) as reported in Table 4.4-1.

Table 4.4-1: Standardized SST values [i.5]

Slice/Service type	SST value	Characteristics
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband.
URLLC	2	Slice suitable for the handling of ultra- reliable low latency communications.
MIoT	3	Slice suitable for the handling of massive IoT.

Within the 5G-network, Network Slice Instances are identified by their Network Slice Instance Identifier (NSI ID). The NSI ID is used for bookkeeping which of the parts of the 5G network is used for which network slice. An operator does not have to support all SSTs, also a Network Slice can be deployed in a part of a network only. The supported slices can differ among tracking areas, however, when a UE registers to the network, the network provides the UE, within a vector referred to as Allowed NSSAI, with a set of S-NSSAIs (i.e. a set of Network Slice Instances) that the UE is allowed to use within a Registration Area. All S-NSSAIs within the Allowed NSSAI should be supported in all TAs within the Registration Area the UE registers to. The initial selection of Network Slices for a UE takes place during the Registration procedure. The selection of Network Slices the UE is allowed to use can be made either by the Access and Mobility Management Function (AMF) or with the support of the Network Slice Selection Function (NSSF). These are C-plane function. Additional functions, which may provide different functionalities for different Network Slices are:

- Session Management Function (SMF);
- User Plane Function (UPF).

The AMF instance serving a UE logically belongs to each Network Slice Instance. I.e. this AMF instance is common to all NSIs (Network Slice Instance) serving the UE. The NF Repository Function (NRF) may be deployed on PLMN level, shared-slice level, and slice-specific level. In each of the cases the NRF is configured with information for the specific level. The operator may provision the UE with Network Slice Selection Policy (NSSP). The NSSP is a set of rules, which associate application to a S-NSSAI. Default rule may exist that associate all applications to one S-NSSAI. In contrast to the architectural aspects of network slicing in ETSI TS 123 501 [i.5], 3GPP TR 28.801 [i.6] and ETSI TS 128 530 [i.7] focus on operational and management aspects of network slicing. According to clause 4.2.1 of 3GPP TR 28.801 [i.6], the Network Slice concept includes the following aspects:

- **completeness of an NSI:** an NSI is complete in the sense that it includes all functionalities and resources necessary to support certain set of communication services thus serving certain business purpose;
- **components of an NSI:** an NSI contains NFs belonging to AN, Transport Network (TN), and CN. If the NFs are interconnected, the 3GPP management system contains the information relevant to the connections between these NFs such as topology of connections, individual link requirements (e.g. QoS attributes), etc. For supporting connectivity between the NFs in the TN, the 3GPP management system provides link requirements (e.g. topology, QoS attributes) to the management system that handles the part of the TN supporting connectivity between the NFs;
- **resources used by the NSI:** the NSI is realized via the required physical and logical resources;

- **Network Slice Template:** the Network Slice is described by a Network Slice Template (NST). The NSI is created using the NST and instance-specific information;
- **NSI policies and configurations:** instance-specific policies and configurations are required when creating an NSI. Network characteristics examples are ultra-low-latency, ultra-reliability, etc. NSI contains a Core Network part and an Access Network part;
- **isolation of NSIs:** a NSI may be fully or partly, logically and/or physically, isolated from another NSI.

3GPP TR 28.801 [i.6] describes an information model where a Network Slice contains one or more Network Slice subnets, each of which in turn contains one or more network functions and can also contain other Network Slice subnets. A Network Slice Subnet Instance (NSSI) can be shared by multiple NSIs. 3GPP TR 28.801 [i.6] identifies 3 management functions related to network slicing management:

- **Communication Service Management Function (CSMF):** this function is responsible for translating the communication service related requirement to Network Slice related requirements. The CSMF communicates with the Network Slice Management Function (NSMF);
- **Network Slice Management Function (NSMF):** this function is responsible for the management (including lifecycle) of NSIs. It derives Network Slice subnet related requirements from the Network Slice related requirements. NSMF communicates with the NSSMF and the CSMF;
- **Network Slice Subnet Management Function (NSSMF):** this function is responsible for the management (including lifecycle) of NSSIs. The NSSMF communicates with the NSMF. These management functionalities and the interfaces among them are still under definition in 3GPP SA5.

3GPP TR 28.801 [i.6] describes the lifecycle of Network Slice Instances, which is comprised of the four following phases:

- preparation;
- instantiation, configuration and activation;
- run-time;
- decommissioning.

The preparation phase includes the creation and verification of NST(s). From a MEC perspective, a critical functionality is to control traffic redirection in UPFs to the MEC applications.

4.5 ETSI NFV

ETSI NFV (Network Function Virtualisation) presents in ETSI GR NFV 001 [i.17] a use case for network slicing. In ETSI GR NFV-EVE 012 [i.16], ETSI NFV presents the notion of network slicing used by different SDOs. Moreover, ETSI GR NFV-EVE 012 [i.16] describes how SDN and NFV concepts can be used to achieve isolation among Network Slices in a multi-tenant and multi-domain environment and how a Network Slice Instance can be created. Based upon these use cases, ETSI GR NFV-EVE 012 [i.16] analyses how to support network slicing in the ETSI NFV framework.

In general, ETSI GR NFV-EVE 012 [i.16] considers network slicing as means to run multiple logical networks on a common infrastructure. Virtualisation technologies are considered as key enablers for network slicing, especially Network Function Virtualisation (NFV), Software Defined Networks (SDN), and Software Defined Radios (SDR). These virtualisation technologies provide the flexibility for sharing resources among Network Slices and deploying and scaling Network Slices automatically. Virtualisation may be provided both via hypervisors or via containers; Network Slices may as well include physical network functions. Finally, ETSI NFV considers that network functions (e.g. VNFs) may be shared across Network Slices.

ETSI GR NFV-EVE 012 [i.16] covers both functional and management aspects of Network Slices. Network slices establish connectivity between endpoints and may include functions to process traffic being exchanged between endpoints. Additionally, each Network Slice is required to support network and service management as well as business administration. After creation of a Network Slice, several operations are therefore foreseen: monitoring, performance management, update, upgrade, snapshot, testing, scaling, migration, and termination. The management functionalities may be provided both by the end-to-end service provider(s) or by the customer(s) or end-user(s) of the Network Slices. Several Network Slices in one administrative domain may be orchestrated jointly. Some of the management functions may be deployed also as virtual functions within a Network Slice to reduce reaction times for operations such as scaling or healing. Each Network Slice is managed by a Network Slice manager. Whether there is a dedicated Network Slice manager for each slice or whether several slices are managed by a common one is left for further study in ETSI GR NFV-EVE 012 [i.16].

The deployment of a new Network Slice subsuming a limited set of resources requires the configuration of a new set of policies, access control rules, monitoring and service level agreement rules, and usage and charging consolidation rules. Additionally, a new management or orchestration entity may be created. If additional resources are needed, further steps need to be undertaken, such as on-boarding of the virtual network functions, testing and certification, instantiation and configuration, etc.

Based on the procedures above, ETSI GR NFV-EVE 012 [i.16] describes a use case for a single-operator domain Network Slice. Defining a new Network Slices is therefore seen as the definition of a new set of policies and lifecycle processes. Although this is a single-operator domain use case, a Network Slice may span multiple NFV sites. The NFV sites may have their own NFVO (NFV Orchestrator), OSS/BSS (Operating/Business Support System), VIM (Virtual Infrastructure Manager), VNFM (Virtual Network Function Manager), etc. functionality. Additionally, NFVO and OSS/BSS functionality may span several NFV sites.

Each Network Slice may have its own Network Slice manager for automation, closed-loop monitoring, and self-healing of services deployed in it. Security and reliability of the Network Slice are considered to be relevant also at the reference points between the Network Slice management functions and the NFV framework itself. A Network Slice manager may consolidate the definition of policies by translating the requirements of the applications and services into the requirements of the Network Slices. Moreover, a Network Slice manager is responsible of the maintenance of the Network Slice blueprints, catalogues and the lifecycles.

In case of multi-tenant and multi-domain environments, ETSI GR NFV-EVE 012 [i.16] focuses on the isolation among distinct Network Slices. Besides isolation regarding performance, resiliency, security and privacy, ETSI GR NFV-EVE 012 [i.16] considers also isolation regarding management. Figure 4.5-1 shows an example of several infrastructure providers (InP1, InP2 and InP3) and several tenants using such infrastructure to create multiple Network Slices.

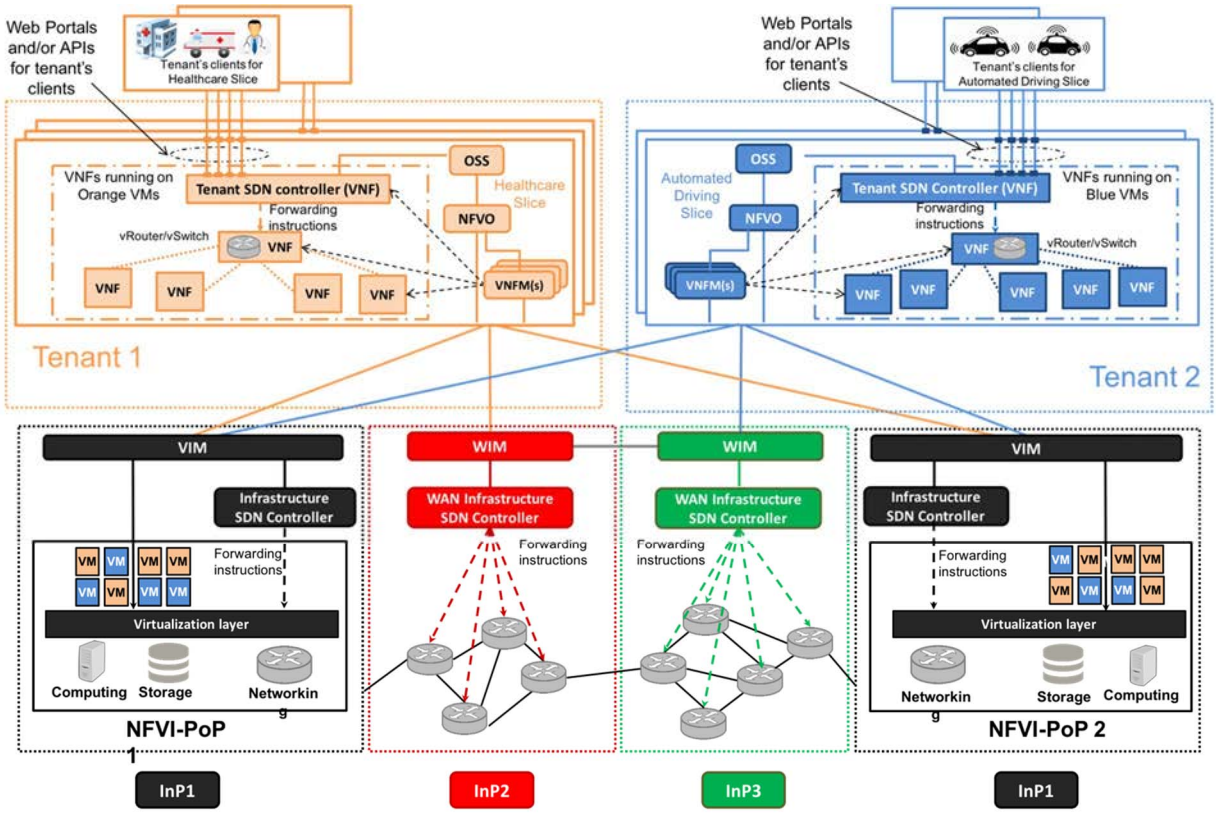

Figure 4.5-1: Network slicing deployment applying NFV concepts to achieve isolation (Figure 4.3-1 in ETSI GR NFV-EVE 012 [i.16])

To achieve management isolation, each Network Slice includes a tenant SDN controller for the configuration of the VNF chains in the tenant domain. The infrastructure SDN controllers are responsible for configuring the connectivity required for the tenant VNFs in the infrastructure domain. Furthermore, to achieve a full management isolation, each Network Slice contains a dedicated OSS, NFVO and VNFM(s). Nevertheless, ETSI GR NFV-EVE 012 [i.16] allows other combinations of NFVO/VNFM such as one NFVO being responsible for multiple Network Slices of one tenant, following the different models in ETSI GR NFV-IFA 028 [i.18].

5 Use cases

5.1 Introduction

This clause discusses six use cases on network slicing in the context of Multi-access Edge Computing (MEC) and based on the concepts described in clause 4.

5.2 Creation and termination of a Network Slice

5.2.1 Description

This use case describes the instantiation and termination of a Network Slice Instance (NSI) including a MEC platform. The use case "Provisioning of a Network Slice Instance", ETSI TS 128 530 [i.7], clause 5.4.2, is extended with Step 2mec (inserted between Step 2 and Step 3 as shown in Table 5.2.1-1).

Table 5.2.1-1: Additional 3GPP step for Network Slice instantiation

Use case stage	Evolution/Specification	<<Uses>> Related use
Step 2mec (O)	If there is information indicating whether an existing MEP can be used, then this step is complete, and the use case continues with step 3. Otherwise, the NSMF requests the NSSMF to request a Network Slice subnet instance for a new MEP. This NSSI contains the MEP and may be distributed across several multi-access edge hosts.	

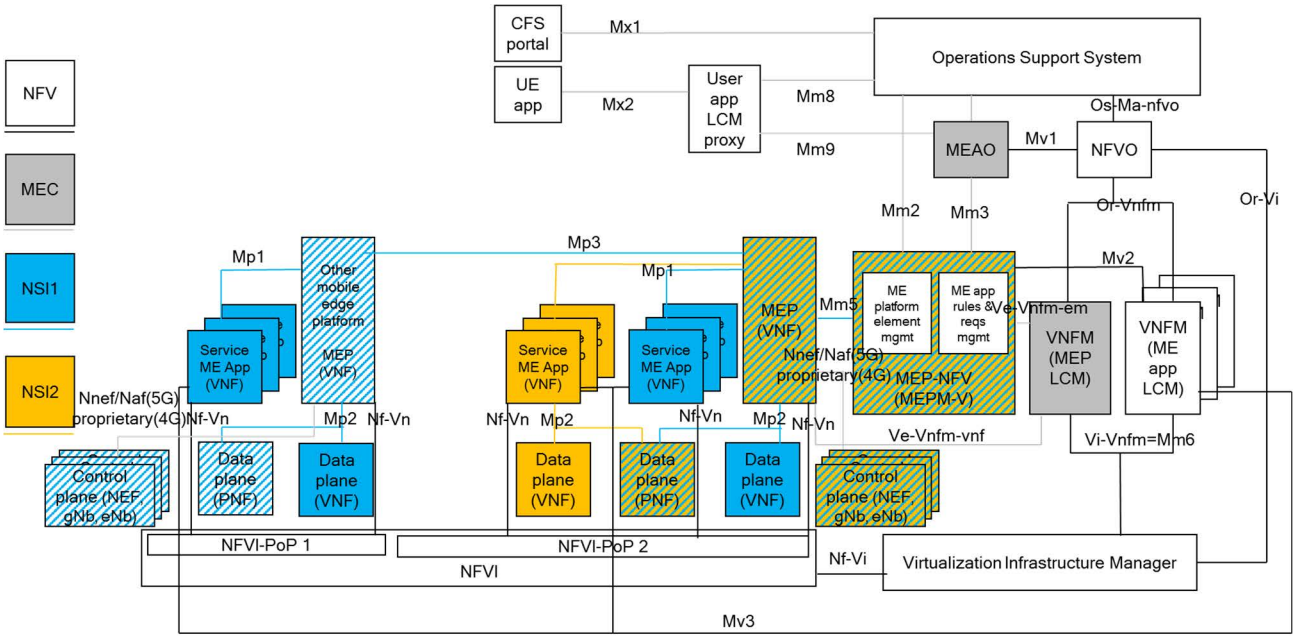

Figure 5.2.1-1: Example of MEC in NFV supporting network slicing

In case one MEC host is shared among several NSIs, MEAO and MEP need to be made slice aware. Eventually, MEC applications associated to a NSI may access information or traffic of UEs only, which may access this NSI. The VNFs requesting services from the MEP and the MEP itself needs to share an authentication/authorization infrastructure that allows to accept/reject procedures on the granularity of NSIs. E.g. a C-plane function may issue commands on a MEP for traffic redirection. Vice versa, a MEP has to authenticate itself towards a C-plane function, e.g. to retrieve radio information of a UE. In case a MEP is dedicated to an NSI, no such additional authentication/authorization mechanisms are needed. Those mechanisms already in place for a 4G/5G network without network slicing but with MEC should be used within an NSI nevertheless. In general, one NSI is connected to at most one MEP. When a MEP is shared among several NSIs, it should be terminated only when all the NSIs using it have been terminated. As part of creating an NSI using MEC, MEC applications may be started in this MEC host. Vice versa, when the NSI is terminated, the corresponding MEC applications should be terminated as well. An example of MEC in NFV supporting several NSIs is shown in Figure 5.2.1-1. Here, two NSIs with MEC support are shown.

5.2.2 Use case recommendations

- The MEAO should be made slice aware:
  - In case of MEP shared among NSIs, the MEAO has to ensure that a MEP is available as long as it is used in at least one NSI.
  - The MEAO has to be available as long as there is an NSI supporting MEC.
- The MEP should be made slice aware, to support the case of sharing MEPs among NSIs:
  - Services registered from different NSIs are distinguished. An announced service can be discovered within its NSI only.

- Different sets of features may be provided to different NSIs using the same MEP.
- The MEP and MEPM-V should allow configuring per-NSI traffic rules.
- An entity in one NSI should not be able to configure traffic rules in another NSI.
- The DNS support should be slice aware, i.e. the same FQDN could be mapped to different IP addresses in different NSIs.
- The time of day accuracy may differ among NSIs.
- The support of UserApps may differ among NSIs.
- The support of RNIS may differ among NSIs. RadioNetworkInformation should be available in those NSIs, to which the UE is associated, and which support the feature called RadioNetworkInformation.
- The support of LocationService may differ among NSIs. Location information should be provided only for UEs associated with an NSI supporting the feature Location Service.
- The MEP should support per-NSI policies in the BandwidthManager.
- The support of UEIdentify may be different among NSIs. Different tokens may be used for the same UE in different NSIs.
- Performance data should be collected per NSI. Charging should be applied per NSI.

5.2.3 Evaluation

The proposed solution is technically feasible, on condition of making MEAO and MEP slice aware as described above.

5.3 Instantiation of a Network Slice integrating MEC applications and using 3GPP elements

5.3.1 Description

This use case assumes a Network Slice that requests the deployment of MEC applications along with other VNFs. The MEC applications need both access to a MEC service, such as RNIS, and to one or more 5G UPFs (i.e. they require traffic redirection).

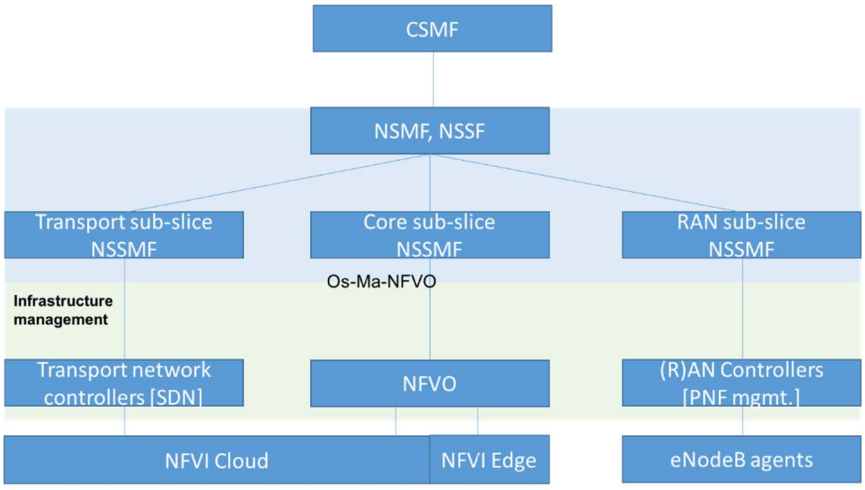

Figure 5.3.1-1: Network Slice architecture including MEC

The CSMF, via a Network Slice Template (NST) requests the creation of an end-to-end Network Slice composed by several sub-slices that spans over (R)AN, Core Network and transport network. The NSMF translates the request and redirects it to each NSSMF, as illustrated in Figure 5.3.1-1. The (R)AN NSSMF is in charge of updating the configuration of the (R)AN, via a RAN controller that interacts with the involved eNBs (PNF) indicated in the NS template using a southbound protocol. The NSSMF in charge of Core Network instantiation translates the NS template information into a Network Service Descriptor (NSD) (see ETSI GS NFV-MAN 001 [i.8]) and requests the instantiation of this NSD to the NFVO using the Os-Ma-Nfvo reference point (see ETSI GS NFV-IFA 013 [i.9]). Note that this use case considers the case of MEC in NFV (see ETSI GR MEC 017 [i.10]), i.e. the NFVO is also in charge of the deployment of VNFs that are MEC applications, and the MEP runs as a VNF. The last network slice subnets is about the transport part, where the NSSMF managing the transport part is assumed to interact with SDN controllers to isolate and forward NS traffic to the Internet. Once each network slice subnet is created, the NSMF is in charge of stitching together the network slice subnets to build the end-to-end slice.

Regarding MEC deployment, after the reception of the NSI creation request from the core NSSMF, the NFVO requests the deployment of the VNFs for the MEC application instances by either using an extended VNFD (which includes the AppD fields), or the AppD included in the NSD (extended to include AppD). The AppD includes the *appTrafficRule* and *appServiceRequired* fields, which indicate the type of traffic to offload and the MEC service to consume. The NSD should also reference VNFs implementing the Core Network elements (such as AMF, SMF, UPF, etc.) and the list of involved (R)AN PNFs. The MEAO communicates the traffic offloading requirements to the MEPM-V which in turn are communicated to the MEP.

When deployed in a 5G network, the MEP may play the role of a 5G Application Function (AF) towards the 5G core network. In this role, the MEP transmits the traffic offloading requirements to Core Network elements (such as NEF or PCF) and the specific application traffic that could be offloaded by UPFs.

5.3.2 Use case recommendations

- the NSD or the VNFD/VNF package should be extended to include AppD;
- the UPF should be deployed at the edge cloud to ensure traffic redirection.

5.3.3 Evaluation

The proposed solution is technically feasible, on condition of the NSD is capable to reference MEC applications, e.g. via VNFDs/VNF packages containing the AppD of the MEC application.

5.4 MEC enables the network latency assurance for network slicing

5.4.1 Description

This use case describes the Multi-Access Edge Computing can support to realize the end-to-end network latency assurance of a Network Slice Instance.

The 5G network slicing is consisted of access network, core network and transport network, and each network domain has its own resource and operation management. Therefore, the network latency requirement should be included in the NSD, and be distributed to the access network, core network and transport network.

Although the network slicing design includes the three network domains, it is hard to realize end-to-end network latency assurance:

- First reason is that the end-to-end network latency assurance means the latency requirement from UE to application, and the application which is deployed in the internet network is out of scope of network slicing. Therefore, the MEC platform should be included in a Network Slice Instance, in order to introduce application deployed from internet network to MEC platform.
- The second reason is the uncertainty of latency estimation for transport network. The longer transmission distance and the larger traffic data aggregation will result in worse network quality once a traffic burst happens. And the MEC platform located in the edge of mobile network can help to reduce the uncertainty of transport network latency.

As the Figure 5.4.1-1 shows, the end-to-end latency of a NSI with MEC includes: access network latency, core network latency, transport network latency and internet network latency. The following 5 steps can be used to realize the NSI latency assurance.

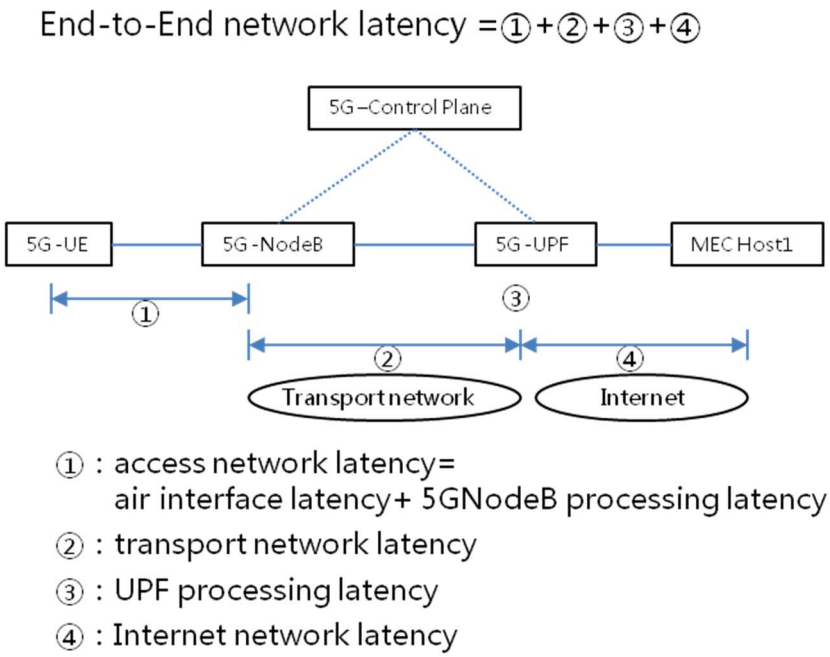

Figure 5.4.1-1: End-to-end latency of a Network Slice Instance with MEC

Step 1: Latency requirement distribution. The NSD will include the network latency requirement. And the requirement will be distributed to access network, core network, transport network and internet network.

Step 2: UPF deployment. The transport network and core network will coordinate to determine the UPF deployment location to meet the transport network latency requirement.

Step 3: MEC platform deployment. The MEC platform should be deployed with synthesizing MEC application requirement, virtualisation resource requirement and internet latency.

Step 4: Calculating the end-to-end network latency. The MEC (e.g. application) may support latency calculation. A testing data packet with timestamp can be transmitted between the UE and MEC. Therefore, the network latency can be obtained in real network environment.

Step 5: Accessing the end-to-end network latency. If the network latency obtained from step4 cannot satisfy the requirement, the work needs to go back to start from step 2.

Finally, the network latency of a Network Slice Instance with MEC can be obtained. The vertical application deployed on the MEC platform can be offered with assured network latency in running time.

5.4.2 Use case recommendations

- the NSD should be extended to include MEC;
- the latency calculation between UE and MEC should be supported;
- the UPF and MEC can be deployed rapidly in the virtualised environment.

5.4.3 Evaluation

The proposed solution is technically feasible, on condition of NSD includes MEC platform and the latency calculation between UE and MEC platform can be supported.

5.5 Dedicated instances of MEC components in a Network Slice

5.5.1 Description

This use case describes the integration of MEC components within a Network Slice deployed in an NFV environment. The Network Slice comprises in form of VNF one or more MEC applications and a MEC platform. A dedicated MEPM-V exists for the Network Slice. The MEAO and the VNFM for the MEP lifecycle management are instead shared across multiple Network Slices. An example of MEC in NFV supporting several NSIs with dedicated MEC instances is shown in Figure 5.5.1-1. Here, two NSIs with dedicated MEC instances are shown in green and blue, respectively. The MEC components shown in grey are instead shared across the two NSIs.

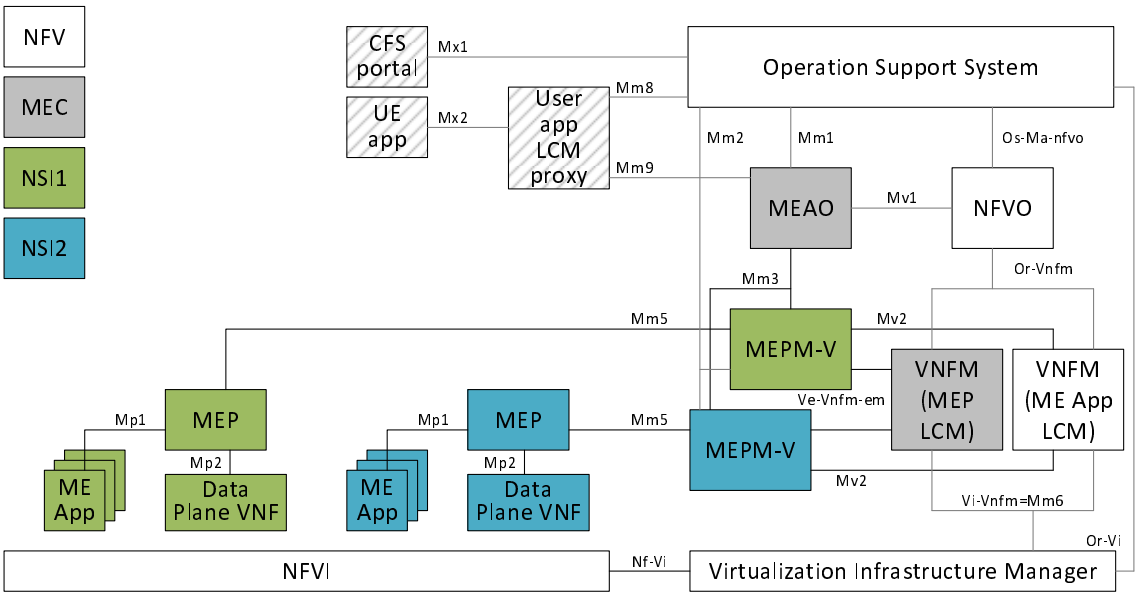

Figure 5.5.1-1: Example of MEC in NFV with dedicated instances of MEC components in distinct NSIs

5.5.2 Use case recommendations

- The MEAO should be made slice aware:
  - the MEAO has to be available as long as there is an NSI supporting MEC.

5.5.3 Evaluation

The proposed solution is technically feasible, on condition of making MEAO slice aware as described above.

5.6 Multiple tenants in a single Network Slice

5.6.1 Description

According to ETSI White Paper No. 28: "MEC in 5G networks" [i.15], network slicing allows the allocation of the required features and resources from the available network functions to different services or to tenants that are using the services. This use case presents the scenario where several MEC applications belonging to multiple tenants are deployed in a single NSI. In case of MEC in NFV (see ETSI GR MEC 017 [i.10]), these MEC applications may also reside on the same NFVI-PoP. Figure 5.6.1-1 shows an exemplary scenario with two tenants whose MEC applications are deployed in a single NSI. The tenants are shown in red and yellow while the NSI is shown in blue. The MEC components shown in blue are shared among the multiple tenants while the MEC components shown in grey are shared across multiple NSIs. For instance, the MEP in the NSI expose services to the MEC applications of both tenants.

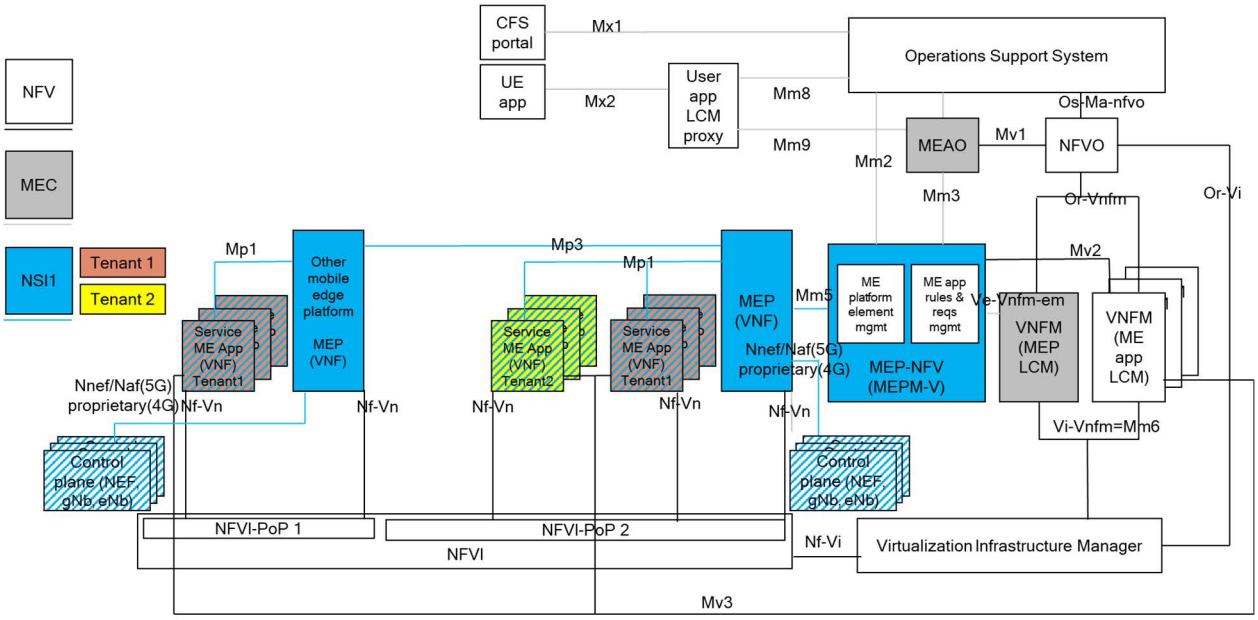

Figure 5.6.1-1: Example of multiple MEC applications belonging to different tenants deployed in a single NSI

5.6.2 Use case recommendations

- the MEAO should be made slice and tenant aware:
  - the MEAO should be able to perform distinct orchestration operations depending on the slice and on the tenant.
- the MEPM-V should be made tenant aware:
  - the MEPM-V should be able to perform distinct management operations depending on the tenants.
- the MEP should be made tenant aware:
  - different sets of features may be provided to different tenants using the same MEP.

5.6.3 Evaluation

The proposed solution is technically feasible on condition of MEAO, MEPM-V, and MEP to be able to distinguish operations depending on the tenants.

5.7 Efficient E2E multi-slice support for MEC-enabled 5G deployments

5.7.1 Description

This use case focuses on the deployment of a MEC system in a (fully virtualised) 5G system with multiple slices, and consists in optimizing the allocation of MEC applications (VNFs) to the edge cloud, according to a slice-aware strategy, in order to meet the End-to-End (E2E) performance requirements of the slice, which are assumed to be part of a Service Level Agreement (SLA), between the network operator and a vertical industry. The starting point is the consideration that:

i) For a given Network Slice, the E2E performance of a (virtualised) 5G system, integrating a MEC system deployment, cannot be fully described only by 5G QoS Class Identifier (5QI) characteristics (e.g. packet Delay Budget (PDB), as defined by 3GPP, i.e. terminated at the UPF), but also depends on MEC system performance, since user traffic is terminated at the MEC application instance.

ii) Optimal MEC deployment is also Network Slice-dependent, as MEC architectural entities need to be connected both to the UE and to the 5G VNFs, in order for the E2E system performance to comply with each slice's needs.

NOTE 1: While the text in the following focuses on a fully virtualised 5G system, the present use case is not conditioned on the full virtualisation of the 5G system. The proposed use case recommendations and evaluation (see clauses 5.7.2 and 5.7.3) also apply in the case of a non-fully virtualised 5G system.

As observed in Figure 5.7.1-1, in addition to the typical latency given by the 3GPP Network Slice (UE-UPF), one should consider the delay between the UPF and the local Data Network (DN) and also the time needed for the MEC application to gather/consume information from the MEP (preferably instantiated at a local DN, thus in proximity to the MEC application, and providing output through the Mp1 interface).

NOTE 2: Examples of this information refer to e.g. Radio Network Information (RNI), location information, or any other slice-specific information (e.g. a packet carrying information on PC5 configuration parameters stored in the MEC host available via a V2X API relevant to a vehicular application, or a packet carrying information on IoT-related parameters available via an IoT API).

Hence, in general the Round Trip Time (RTT) for a traffic flow associated to a specific Network Slice, will be expressed as follows:

$$RTT = d_{3GPP} + d_{MEC},$$

where, the first term refers to the RTT components relevant to the 3GPP network and the second term denotes the RTT components originating from the MEC system.

NOTE 3: To model and evaluate E2E performance, measurement data (e.g. time instants appearing in Figure 5.7.1-1) need to be properly produced, exposed and consumed for management purposes. Such data can be then used for various procedures, e.g. mobility, scaling, reconfiguration, etc. Data could be related to the infrastructure, the MEP, and/or the MEC application. There may be multiple system entities consuming data that can react depending on the current measurement. For example, a 5G orchestrator may trigger a relocation, while scaling could be triggered by a UE application. The OSS could also consume such measurement data and react according to a set of predefined SLAs. The measurement production/ consumption framework is not in the scope of the present document.

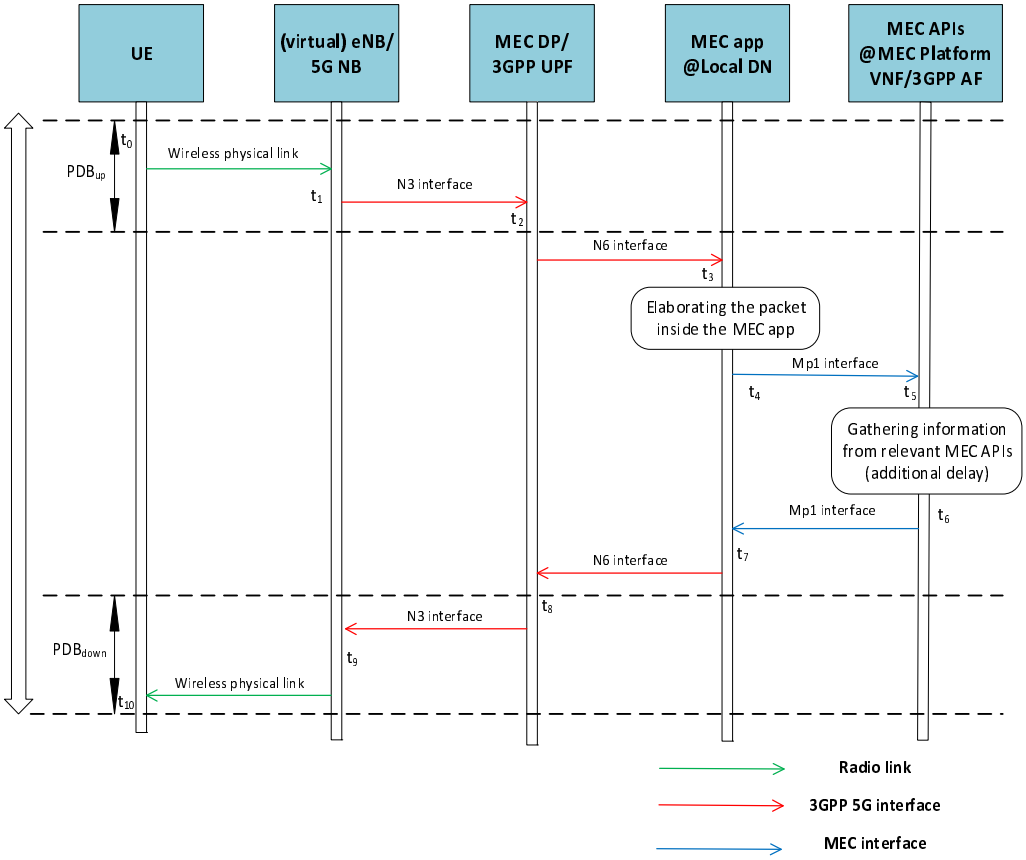

Figure 5.7.1-1: Message sequence chart illustrating the various latency components during the direct communication between a client app (at the UE) and a MEC application (at the edge), which consumes in its turn some MEC services running on the MEP

Consequently, having modelled and evaluated the different components of the slice's E2E performance, e.g. in terms of latency, as depicted in Figure 5.7.1-1, the management entities of the 3GPP 5G system (i.e. the OSS) and the MEC system (i.e. the MEAO and the NFVO), need to interact, in order to instantiate the MEC application.

5.7.2 Use case recommendations

- The contribution of each (virtualised) MEC and 3GPP 5G system entity to the total E2E slice performance, i.e. between the UE and the current Local DN, should be evaluated by the respective management entity (OSS, MEAO). E2E performance evaluation can be performed by means of properly producing, exposing and consuming measurement data at the involved management functional entities.
- The management entities of the 3GPP 5G system (i.e. the OSS) and the MEC system (i.e. the MEAO and the NFVO), need to interact.
- The MEAO and NFVO need to be made aware of the slice characteristics and attributes to be able to implement the slice-aware MEC application allocation policy.

5.7.3 Evaluation

The proposed solution is technically feasible, on condition of establishing a signalling framework among the 3GPP 5G system's OSS, the MEC system's MEAO and the NFVO, applicable to multiple Network Slices and QoS flows.

6 Key issues and solutions

6.1 Key issue 1: Slice-awareness of the MEAO

6.1.1 Description

The MEAO may orchestrate MEC applications that belong to different NSIs. This may require the MEAO to adapt the orchestration operations based on the available NSIs and their different requirements (e.g. bandwidth, latency, security, etc.). To that end, the MEAO needs to be slice-aware for enabling per-NSI operations.

6.1.2 Solution

- The Mv1 reference point between MEAO and NFVO needs to be extended to include information to enable a distinction between multiple Network Slices.
- The Mm1 reference point between the OSS/NSSMF and the MEAO needs to distinguish between multiple Network Slices.
- The Mm3 reference point between MEAO and MEPM-V needs to be extended to support the necessary Network Slice related information.
- The Mm9 reference point between User App LCM Proxy and MEAO needs to be extended to support the necessary Network Slice related information.

6.1.3 Gap analysis

- according to ETSI GR MEC 017 [i.10], the Mv1 reference point is based on the Os-Ma-Nfvo reference point (see ETSI GS NFV-IFA 013 [i.9]) which already allows to distinguish network services and thus allows also to distinguish Network Slices. Therefore, no additional actions are needed for the Mv1 reference point;
- no reference to Network Slices support is specified in ETSI GS MEC 010-2 [i.11], clause 4.1.1 for the reference point Mm1. A requirement for enabling the distinction of Network Slices should be added to ETSI GS MEC 010-2 [i.11], clause 4.1.1 Requirements for reference point Mm1;
- no reference to Network Slices support is specified in ETSI GS MEC 010-2 [i.11], clause 4.1.2 for the reference point Mm3. A requirement for enabling the distinction of Network Slices should be added to ETSI GS MEC 010-2 [i.11], clause 4.1.2 Requirements for reference point Mm3;
- Mm9 reference point is not further specified as stated in ETSI GS MEC 003 [i.12]. Therefore, no further actions are required for the Mm9 reference point.

As a result, extending the reference points Mm1 and Mm3 by including a reference to the NSIs would allow the MEAO to distinguish operations on different NSIs.

6.2 Key issue 2: Slice-awareness of a shared MEP

6.2.1 Description

A MEP may be shared across several NSIs. In this case, the MEP has to ensure the isolation of the services and information available in a given NSI (or in a set of NSIs) from other Network Slices. For example, a ME App may access only the information of the UEs connected to the same NSI.

6.2.2 Solution

- The Mm5 reference point between MEP and MEPM-V needs to distinguish between multiple NSIs.

Distinct NSIs may use different sets of services. The MEP has to support separate sets of services according to their availability on different NSIs. This would cover both the ME services provided by the MEP itself and by the ME Apps.

6.2.3 Gap analysis

- According to ETSI GR MEC 017 [i.10], the Mm5 is an unspecified reference point. Therefore, no further actions are required for the Mm5 reference point.
- Differentiating sets of services per NSI would allow to share the same MEP across several NSIs. To that end, the technical requirements in ETSI GS MEC 002 [i.13] should be extended to support service separation across distinct NSIs (or a set of NSIs):
  - The MEP should be able to provide different sets of features in distinct NSIs.
  - The MEP should be able to provide the same feature differently in distinct NSIs.
  - The MEP should be able to provide different sets of services in distinct NSIs.
  - The MEP should be able to provide the same service differently in distinct NSIs.
  - The MEP should collect performance data per NSI, charging should be applied per NSI.

6.3 Key issue 3: Slice-awareness of a MEPM-V

6.3.1 Description

A MEPM-V provides element management functionality to a MEP and it manages application rules and requirements including service authorizations, traffic rules, DNS, etc. In the case of deploying MEC in an NFV environment (see ETSI GR MEC 017 [i.10]) the life cycle management of applications is delegated to VNFMs. In case of MEC not being deployed in an NFV environment, the MEPM manages also the lifecycle. Similar to the MEP (see clause 6.2), the MEPM-V needs to be slice aware.

6.3.2 Solution

- The Mm2 reference point between MEPM-V and OSS needs to distinguish between multiple Network Slices.
- The Mm3 reference point between MEAO and MEPM-V needs to include a reference to the Network Slices.
- The Mv2 reference point between the VNFM and MEPM-V needs to include a reference to the Network Slices.

6.3.3 Gap analysis

- No reference to Network Slices support is specified in ETSI GS MEC 010-1 [i.14], clause 5.1.1 for the reference point Mm2. A requirement for enabling the distinction of Network Slices should be added to ETSI GS MEC 010-1 [i.14], clause 5.1.1 Requirements for reference point Mm2.
- No reference to Network Slices support is specified in MEC 010-2 [i.13], clause 4.1.2 for the reference point Mm3. A requirement for enabling the distinction of Network Slices should be added to ETSI GS MEC 010-2 [i.11], clause 4.1.2 Requirements for reference point Mm3.
- According to ETSI GR MEC 017 [i.10], the Mv2 reference point is based on Ve-Vnfm-em. The Ve-Vnfm-em reference point already operates on specific VNFs. Therefore, no additional actions are needed for the Mv2 reference point.

Extending the reference points with a reference to Network Slices would allow the MEPM-V to distinguish operations on different NSIs.

7 Conclusions and recommendations

7.1 Prioritized concepts of network slicing

There are four network slicing concepts that have been described in clause 4; and two of them have been considered and analysed in the use cases described in clause 5:

- **3GPP:** a Network Slice Instance (NSI) is considered as a set of Network Function (NF) instances and of the required resources. A Network Slice Subnet Instance (NSSI) can be shared by multiple NSIs and may contain a Multi-access Edge Platform (MEP) playing the role of a 5G Application Function (AF) towards the 5G Core network;
- **ETSI NFV:** an NFV Network Service (NS) can be regarded as a resource-centric view of a 3GPP Network Slice, for the cases where an NSI would contain at least one Virtualised Network Function (VNF). In MEC-in-NFV context, it is assumed that ME apps and MEP can be realized as VNFs and managed according to ETSI NFV procedures.

Therefore, priority is given to the above two network slicing concepts representing the functionalities that need to be supported in this phase.

7.2 Consolidated recommendations

There are several recommendations that are common to the considered five use cases (see clause 5) and the three key issues on MEC components (see clause 6). Taking into account the evaluations made for each recommendation, the overall consolidated recommendations are summarized below:

[CR-1] It is recommended that the MEAO supports the capability to distinguish operations based on the available NSIs and their different requirements (e.g. bandwidth, latency, security, etc.). To that end, the Mm3 reference point needs to support per-NSI operations.

[**CR-2**] It is recommended that a MEP supports the capability to serve a single NSI.

[**CR-3**] It is recommended that a MEP supports the capability to serve multiple NSIs.

[**CR-4**] It is recommended that a MEC application may be associated to a specific NSI.

[**CR-5**] It is recommended that a MEC application may also be associated to multiple NSIs.

NOTE 1: In this case a MEP supports the application enablement for the MEC application.

[CR-6] It is recommended that the MEC system supports the capability to collect and expose usage and performance data per NSI. This allows to verify the fulfilment of the Service-Level Agreement (SLA) requirements per NSI and react accordingly (e.g. charging-related procedures, etc.).

NOTE 2: The term "usage" is seen as a superset of all possible usage types (e.g. resource usage, application data usage, etc.). The specific usage types to be included will be decided during the normative phase of this work.

7.3 Recommendations for future work

Three key issues are identified and discussed with potential solutions (see clause 6), which are related to the key recommendations on network slicing support. Taking into account of the gap analysis provided in clause 6, it is therefore recommended:

- to capture the consolidated recommendations as normative requirements in ETSI GS MEC 002 [i.13], ETSI GS MEC 010-1 [i.14], and ETSI GS MEC 010-2 [i.11];

- to collaborate with ETSI ISG NFV for identifying which NFV procedures may require extension when MEC is deployed in an NFV environment and the network slicing concept is adopted. This may include the scenarios where the MEC components (e.g. MEP and MEPM-V) are either shared across multiple Network Slices or dedicated to a single Network Slice;

- to collaborate with 3GPP for identifying which 3GPP procedures may require extension when MEC is deployed in a 5G network. This may include the scenario where the MEP plays the role of a 5G Application Function (AF) towards the 5G core network and a 3GPP NSI is created or terminated;

- to collaborate with ETSI ISG NFV and 3GPP all together for identifying the necessary extensions when MEC is deployed in an NFV environment within a 5G network. This scenario considers both network slicing concepts (i.e. 3GPP and ETSI NFV) being applied simultaneously.

History

Document history		
V2.1.1	November 2019	Publication