ETSI White Paper No. 49

MEC federation: deployment considerations

1st edition – June 2022

ISBN No 979109262070

Author:

Masaki Suzuki, Tetsu Joh, Hyeonsoo Lee, Walter Featherstone, Nurit Sprecher, Dario Sabella, Neal Oliver, Samar Shailendra, Fabrizio Granelli, Cristina Costa, Lijuan Chen, Henrik Nieminen, Oleg Berzin, Faraz Naim

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

About the authors

Masaki Suzuki
KDDI Corporation – ETSI ISG MEC delegate

Tetsu Joh
KDDI Corporation – ETSI ISG MEC delegate

Hyeonsoo Lee
SK Telecom – ETSI ISG MEC delegate

Walter Featherstone
Samsung – ETSI ISG MEC DECODE WG chair, ETSI ISG MEC vice-chair

Nurit Sprecher
Nokia – GSMA OPG delegate

Dario Sabella
Intel – ETSI ISG MEC chair

Neal Oliver
Intel – GSMA OPG delegate

Samar Shailendra
Intel- 3GPP SA6 delegate

Fabrizio Granelli
University of Trento

Cristina Costa
Fondazione Bruno Kessler

Lijuan Chen
ZTE – ETSI ISG MEC delegate

Henrik Nieminen
EQUINIX

Oleg Berzin
EQUINIX – LF Edge Akraino TSC co-chair

Faraz Naim
Accenture

Contents

Executive Summary

This White Paper focuses on the deployment options related to MEC federation, especially from an architectural point of view, and with a key focus on ETSI MEC implementations, but also with the aim to provide an open approach considering other standards and technologies. For this purpose, the White Paper firstly analyzes the recent publications of GSMA OPG and recent updates in ETSI MEC and 3GPP specifications, then introduces the synergized architecture supported by both standards organizations, which indicates the background information for the deployment of MEC federation.

After the architectural description, this White Paper introduces the business stories that enable readers to understand how MEC federation is beneficial for MEC system providers. Based on these business stories, corresponding deployment options are introduced. The aim is to help edge stakeholders, and all readers in general, to better understand how to choose the appropriate deployment options based on the business stories described in the document.

Additionally, this White Paper introduces some key considerations, i.e., connection between MEC systems, multi-domain orchestration and collaboration among operators and with cloud providers and third parties. An understanding of all these aspects will be beneficial for the future deployment of MEC federation and edge capability exposure in these heterogeneous environments.

1 Introduction

Multi-access edge computing (MEC) technology is increasingly recognized, alongside 5G technologies, as a key enabler of sophisticated latency-critical and quality-sensitive applications, e.g., Vehicle to Everything (V2X) applications, Augmented Reality (AR)/Virtual Reality (VR) games, as described in ETSI GS MEC 002 [1]. The MEC environment is characterized by a diverse ecosystem of market players, ranging from infrastructure owners (e.g., mobile network operators), to service providers, system integrators, and application developers. This trend makes it more complicated to organize the overall ecosystem containing several MEC systems through multiple operators, suppliers, and service providers. As described in ETSI GR MEC 035 [2], if we focus on V2X applications, MEC service providers are required to address service continuity in multi-operator operation scenarios through cooperation among MEC systems. This form of cooperation is so-called MEC federation.

MEC federation is a topic of active discussion, with related requirements and specifications being developed. In ETSI MEC activities, GR MEC 035 [2] has been published and normative work is on-going, highlighting that the MEC federation framework has reached a significant maturity level. Several related use cases and a reference architecture variant are newly added to ETSI GS MEC 002 [1] and ETSI GS MEC 003 [5] respectively. Additionally, a new dedicated work item (WI) ETSI GS MEC 040 [4] has been initiated to define the federation enablement APIs.

An important aspect of specifying the MEC federation is to align with other standards development organizations (SDOs) and industry associations. To achieve this objective, GR MEC 035 [2] and (WI) GS MEC 040 [4] are taking into account the use cases derived from the 5G Automotive Association (5GAA), as well as requirements specified by the GSMA Operator Platform Group (OPG). 5GAA targets demonstration of the use of MEC for automotive services. 5GAA recognizes an important key issue how interoperability and service continuity can be provided under multiple MNOs, automotive vendors, and infrastructure vendors situation. The goal of the GSMA initiative is to make edge computing an operator service, where customers using an edge application should have seamless MEC service experience (e.g., able to support low-latency requirements) regardless that the application is running on their operator's edge cloud, or on the edge cloud of a different operator. The work in ETSI ISG MEC is targeted at introducing a proper standard to achieve those goals.

Therefore, when developers or operators deploy a MEC system, and organize federated MEC systems, the resulting MEC federation needs to be not only compliant with ETSI MEC specifications (and 3GPP SA6) but also compatible and aligned with GSMA OPG requirements, and from other industry organizations, such as 5GAA. Building aligned and compatible standards sometimes is not sufficient, as stakeholders may need further clarity on deployment options, that often are independent from standards, and rather based on business agreements and partnerships. Consequently, it is needed to also describe deployment options related to practical implementations and instantiation of the architectural variants, to complement what is described in each specification document or publication by standard bodies. Some activities for harmonizing various specifications and collaborating among these SDOs have already started (see ETSI White Paper #36 [7]), but in terms of deployment, not so many things are well described.

This White Paper aims indeed to help developers and operators to deploy a MEC federation, which is compliant to the ETSI MEC specifications, by highlighting the potential business scenarios and deployment options.

2 Shared Operator Platform scenario in GSMA OPG

GSMA OPG has published its "Operator Platform Telco Edge Requirements" permanent reference document (PRD) [3]. Interpreting from the PRD, an Operator Platform (OP) can be considered as a facilitator of customers' seamless access to edge applications instantiated within a federation of edge networks involving multiple owners. The main objective of the document is to provide a target architecture and the associated requirements to enable an end-to-end delivery chain for different services, which covers the interactions of the entire ecosystem involved in the edge computing application delivery.

Annex C of the PRD [3] provides an overview of the deployment options of the OP, which in ETSI MEC standards can be associated to a MEC system (as indicated also in the subsequent figures in section 5). Two deployment options are introduced depending on whether each operator has its own OP instance or share a single OP instance. The first option is the case in which each operator has its own OP instance, as depicted in Figure 1. Each OP instance manages the resources of a single operator, and OP A can federate with OP B.

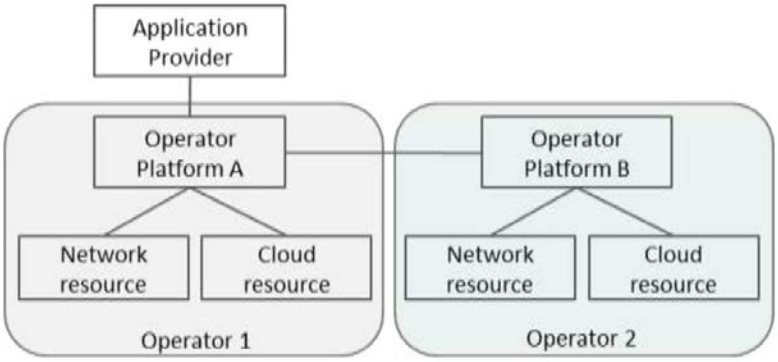

Figure 1: Each operator has its own OP (Source: Annex C.1 of GSMA OPG PRD [3])

The second option is the case in which an operator does not have its own OP as depicted in Figure 2. In this case, OP is shared by multiple operators and manages the resources of multiple operators. According to the GSMA PRD document, "*when receiving a federation request from OP B or a deployment request from an Application Provider, Operator 1 or Operator 2 is selected based on OP A's policy.*"

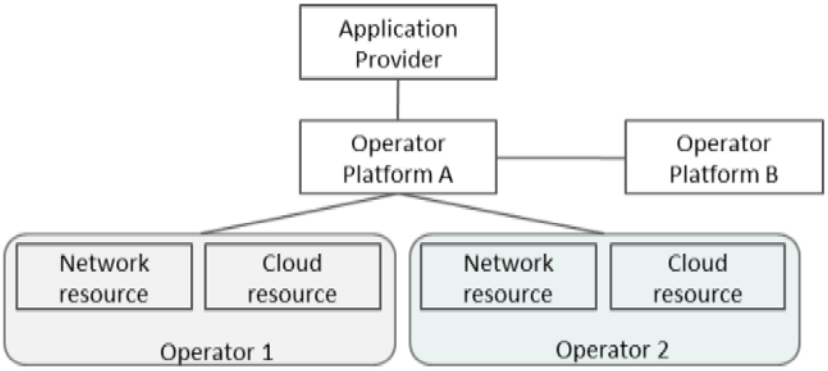

Figure 2: Multiple operators share the same OP (Source: Annex C.1 of GSMA OPG PRD [3])

While this shared OP scenario could be a starting point in the industry for example by building regional or national hubs that can be interconnected between each other fostering federation between Operator platforms, it is key to reach a global footprint and guaranteeing service capabilities such as roaming between different MNOs. The potential business case and corresponding deployment options will be introduced in Clause 6.

An important aspect is to understand how edge cloud resources are managed in an OP instance, especially when considering the above scenario with Multiple operators sharing the same OP.

As an important note, the Service Resource Manager Role is defined by GSMA PRD [3] as "*the OP role in charge of orchestrating Edge Cloud Resources and Network Resources for use by Application Providers and end-users*". This definition is not explicitly telling how the Service Resource Manager Role should be implemented. However, in other parts the same PRD clarifies that «the OP is expected to work over key industry reference infrastructures. There are various options in the industry, most based on OpenStack® or Kubernetes®, but others are also available».

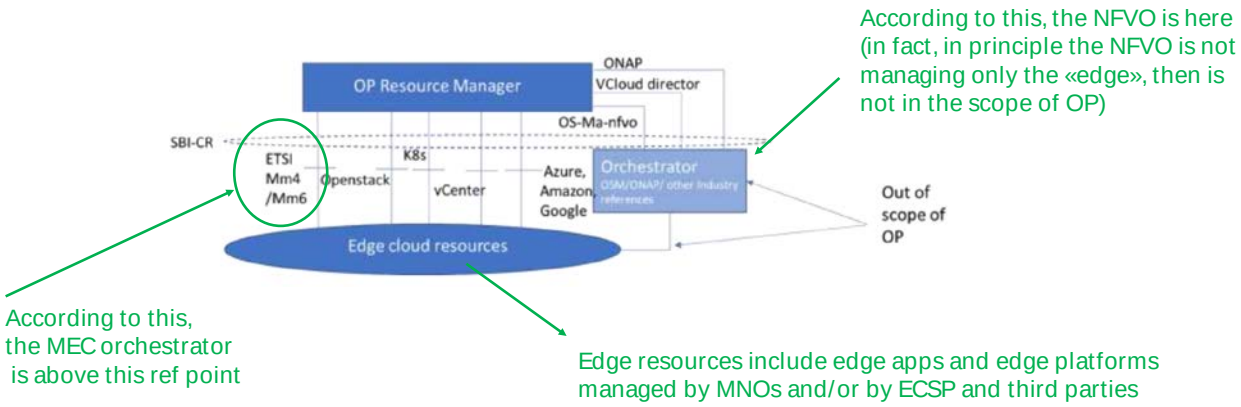

Figure 3: Overview of possible SBI-CR integrations (source Section 3.5.2.1.2 of GSMA PRD [3], updated with surrounded comments.)

In this perspective, at least it is clear that a single operator implementing an OP instance should have a MEC orchestrator (or an edge orchestrator based on other standards or technologies compliant with OPG); and moreover, this functionality can be also in need of orchestrating multiple technologies. On the other hand, it is also possible for certain operators, who do not have OP, to join Federation without their own OP implementation. In this case, OP is shared with multiple operators, e.g., via the help of an aggregator of another operator (acting as "lead" of that OP instance)[1]. Figure 4 provides a possible example of how these resources from multiple operators can be shared to form a single OP instance. However, there can be various ways of practically implementing aggregation among operators in a single OP instance (e.g., done by an edge partner, or a lead operator), and this detail is not present in the PRD.

[1] According to GSMA PRD [3] (clause 2.2.2.1): "*The OP provides edge compute resources as a virtualised service to an Application Provider or another party in the OP ecosystem (for example, an aggregator or another operator).*"

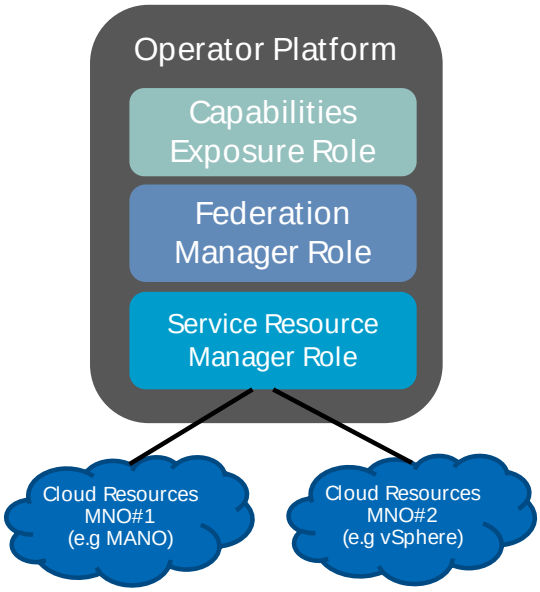

Figure 4: MNOs aggregation in a single OP instance (with a single Service Resource Manager Role)

More in general, at the time of writing this White Paper it seems clear from the GSMA definitions of OP architecture that a single OP instance should have:

- A single Service Resource Manager Role: even in case of aggregation, a single edge orchestration function should be implemented in the OP (possibly dealing with various industry standards and technologies)
- A single Federation Manager Role: this is the unique EWBI termination in the OP instance, to connect with other OP instances
- A single Capabilities Exposure Role: in fact, a single NBI termination is needed to connect with Application providers (however, the PRD also clarifies that "OP Marketplace aggregates the additional APIs offered by OPs and exposes them to Application Providers").

However, the reader should notice also that the above are considerations at OP architecture level, and the actual mapping with SDOs might not perfectly fit these considerations, simply because the standardization work is ongoing in both ETSI MEC and 3GPP. For example, the implementation of aggregation among MNOs is not clearly defined in the PRD [3], thus it is considered as optional (and left to MNOs and agreements), thus for a better reason the related standardization efforts are not necessarily covering this level of implementation within the Service Resource Manager Role.

2.1 Edge Node Sharing

The GSMA PRD [3] describes a federation scenario where two operators can share their edge nodes to improve their edge presence and coverage (see Figure 5). The operator B deploys the application in partner OP network's (Operator A) edge node while allowing the user to access the same through its own radio network. The two operators must have pre-established trust, security, and policy related agreements. The

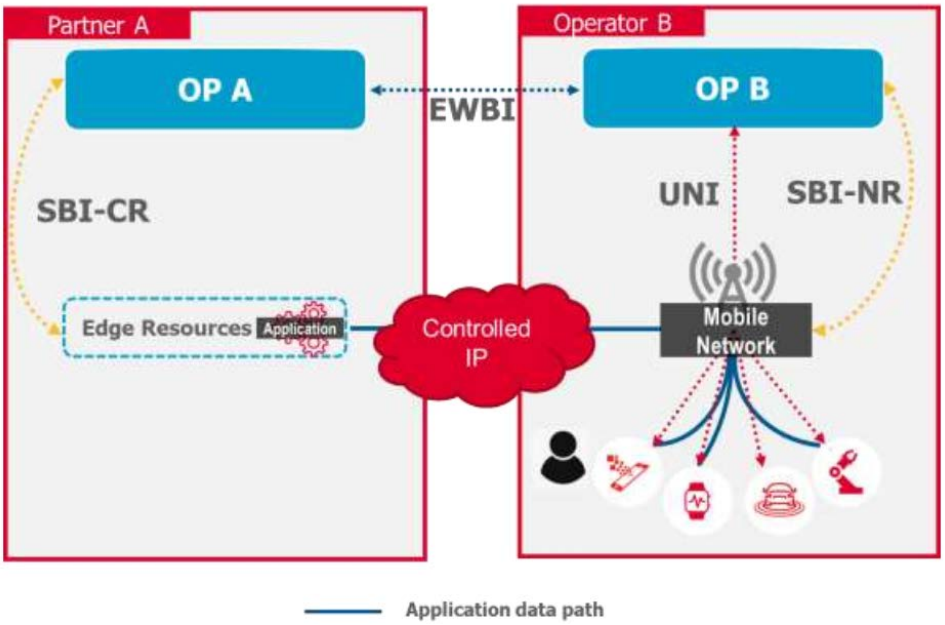

Figure 5: Edge Node Sharing (Source: Section 3.3.5 of GSMA OPG PRD [3])

two operators have connectivity over the EWBI interface. According to PRD, the network resources need to be managed by the actual service provider to the user i.e., Operator B in this case while responsibility for the management of the edge cloud resources depends on the agreement between the partners. It is also interesting to note that two operators might be using different MEC architectures (e.g., ETSI MEC and EDGEAPP). 3GPP SA6 also has contributions to study Edge Node Sharing in EDGEAPP architecture [12].

3 ETSI ISG MEC reference architecture variant for MEC federation

Based on GR MEC 035 [2], ETSI ISG MEC recently updated its architecture in the GS MEC 003 [5] deliverable. In the recent update, a MEC reference architecture variant for MEC federation is introduced. This variant contains a new functional element, i.e., the MEC federator, and the corresponding reference points, i.e., Mfm and Mff. The MEC federator contains MEC federation manager and (optionally) MEC federation broker roles, and enables a MEC federation between MEC systems by supporting the following functionalities:

- registration of MEC system information by a MEC orchestrator
- MEC system discovery

- (optionally) broker capability acting as a one-to-many intermediary between MEC federators
- information exchange
- application lifecycle management across different MEC systems
- application monitoring across different MEC systems.

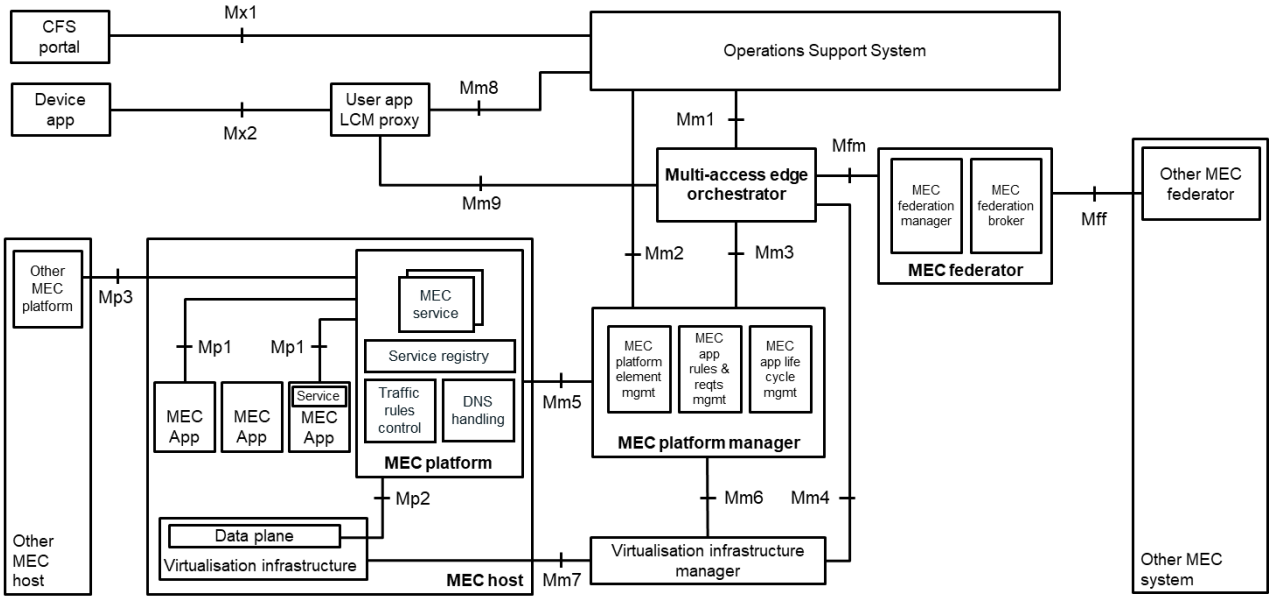

Figure 6: Multi-access edge system reference architecture variant for MEC federation. (Source: ETSI GS MEC 003 [5])

4 Synergized architectures among GSMA OPG, ETSI MEC and 3GPP

As described in the previous section, the starting point for the definition of MEC Federation is the recently added MEC reference architecture variant. This is in fact very relevant for a cross-SDO mapping of the OP architecture, where the Annex C of ETSI GS MEC 003 [5] provides a first tentative mapping between interfaces in GSMA OP architecture with reference points of the MEC Federation architecture variant. For example, OP North bound interface (OP:NBI) is considered to have correspondence with Mx1 and Mp1; OP South Bound Interface Network Resources (OP:SBI-NR) with Mp2; OP South Bound Interface Cloud Resources (OP:SBI-CR) with Mm6 and Mm4; and OP East and West Bound Interface (OP:E/WBI) with Mff. From the viewpoint of MEC federation, interaction between federated MEC systems would be conducted through the OP:E/WBI.[2] However, the reader should notice that currently this complex SDO mapping is ongoing and still there are discussions on the exact relevance of Mx2 for OP:NBI, for example. Moreover, the standardization work is still ongoing both in ETSI MEC and 3GPP, and this will further need to be aligned

[2] Note: relevant standard bodies are using in different documents use these reference points in different ways (e.g., 3GPP NBI vs OPG NBI). In this context, we insert a suffix "OP" to the various reference points, to avoid confusion.

with the work in OPG and open-source implementations (e.g. CNCF project CAMARA [9]). As a consequence, White Paper 36 [7] should be considered as the current view from ETSI MEC relevance of OP interfaces.

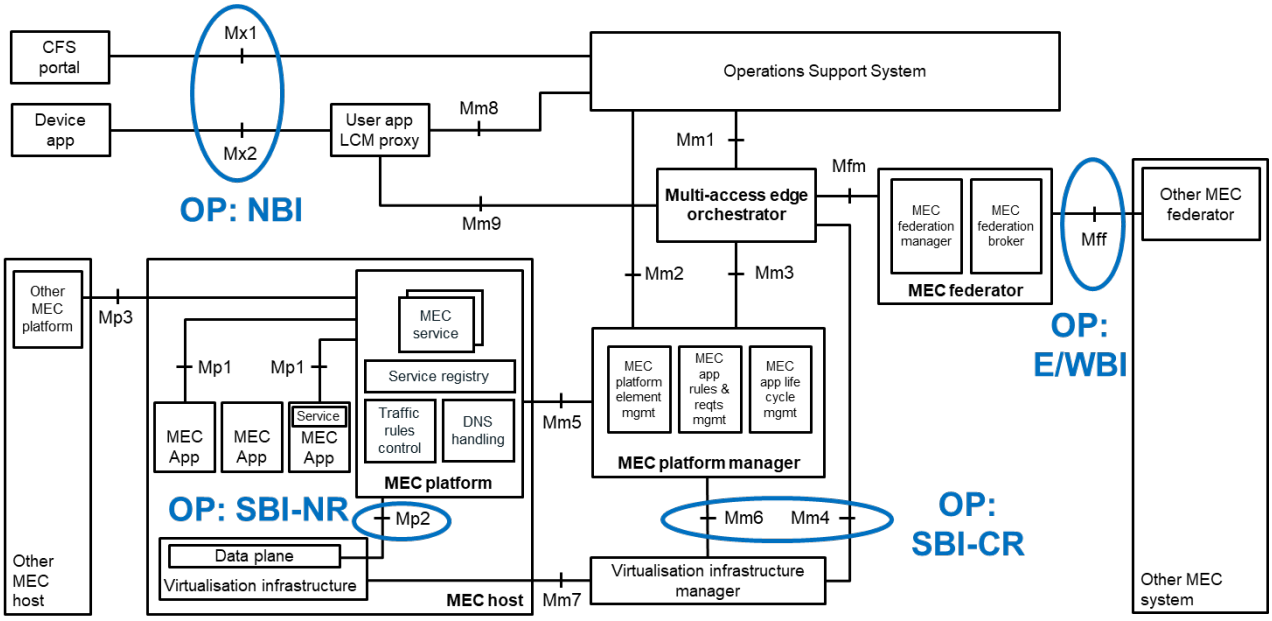

Figure 7: Mapping between the E/WBI, NBI and SBI interfaces of the GSMA OP architecture to reference points of the reference architecture variant for MEC federation (Source: ETSI GS MEC 003 [5])

A more complete (and recent) view of a cross-SDO mapping of the OP architecture is depicted in Figure 8 (presented in the joint workshop organized by GSMA OPG with ETSI MEC and 3GPP [8]), which is in fact showing both ETSI MEC and 3GPP EDGEAPP architecture elements, with some more accurate indication of the relevance of the various reference points for the OP architecture interfaces.

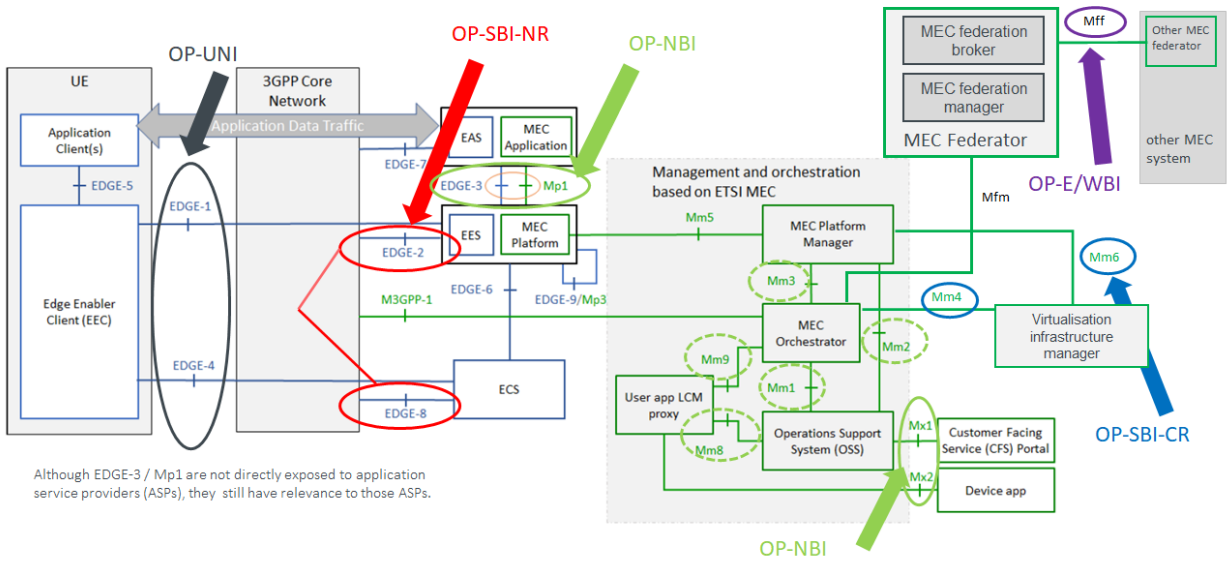

Figure 8: Cross-SDO mapping of the OP architecture (top-down approach).

In this figure, 3GPP SA6 (EDGEAPP) architecture and ETSI MEC architecture can complement each other, as described in Annex B of GS MEC 003 [5]. In 3GPP Rel-17, EDGEAPP activities may not provide coverage for the OP:E/WBI or Mff reference point. However, current standardization work in both SDOs is targeting not only a complete coverage of GSMA OPG requirements but also a better alignment between ETSI MEC (Phase 3) and 3GPP (Release 18). For these reasons, the synergized architecture (supported by both ETSI MEC and 3GPP EDGEAPP) is a suitable starting point for a cross-SDO mapping of the OP architecture (although at the time of writing this White Paper the mapping is still not finalized).

More in general, the reader should notice also that a final view will also need to take into account the progresses in open-source project CAMARA [9] (in alignment with GSMA OPG and its API subgroup called OPAG), as this work will likely complement the work in the scope of SDOs. At the end, the overall efforts from the various entities are intended to avoid duplication of work, with the aim to provide full coverage of federation requirement, with an open approach taking into account both standards, open source and of course also proprietary implementations and technologies.

5 Business cases for MEC federation

5.1 Federation cases within one operator

The business case for MEC federation rests on the ability to deploy MEC systems at various scales. This is achieved both by federating individual MEC systems together, and by enabling systems to be integrated by new incremental users. GR MEC 035 [2] describes business stories pertaining to sharing and aggregation requirements. In this section, new business stories related to shared deployments will be described.

For the integrated MEC system business case, consider the base case in which a MEC system is deployed at a single facility, e.g., factory, hospital, airport. This MEC system is integrated into the facility owner's

internal operations, possibly to perform a specific task. Visiting users needing to operate in the facility can also access the MEC system in this deployment, as shown in Figure 9.

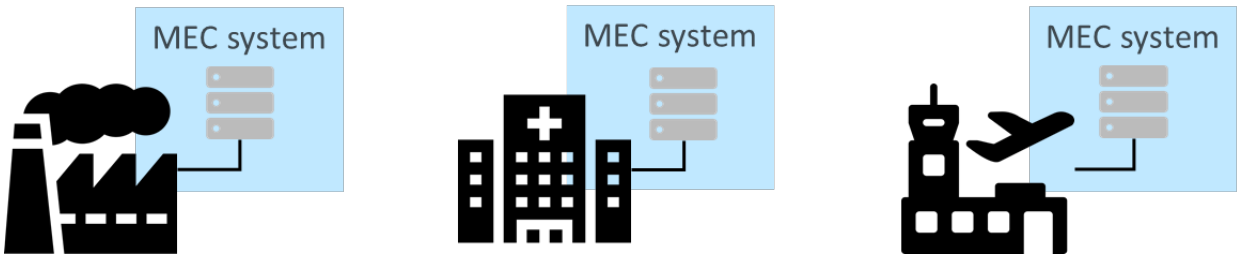

Figure 9: MEC system deployed at a specific facility, e.g., factory, hospital, and airport.

This single-facility deployment can be scaled to support geographically distributed users using, e.g., V2X services, or AR/VR gaming, as depicted in Figure 10.

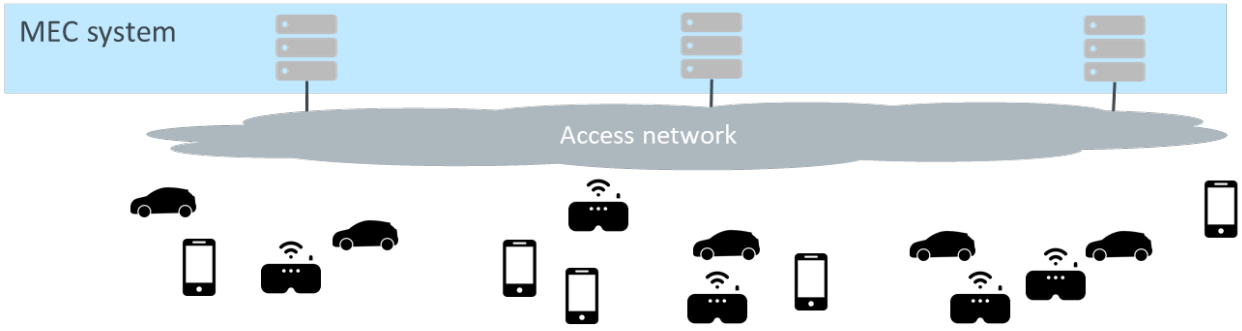

Figure 10: MEC system deployment for geographically distributed users.

Based on the concept of MEC federation, MEC systems of the two aforementioned deployment options can be integrated. According to the functionality of MEC federator, which was a recently added entity to the ETSI MEC reference architecture variant for MEC federation, individual MEC systems are connected to each other via the MEC federator.

If all MEC federators only have a MEC federation manager role, then all MEC systems are required to establish peer-to-peer connections, i.e., full-mesh network as illustrated in Figure 11.

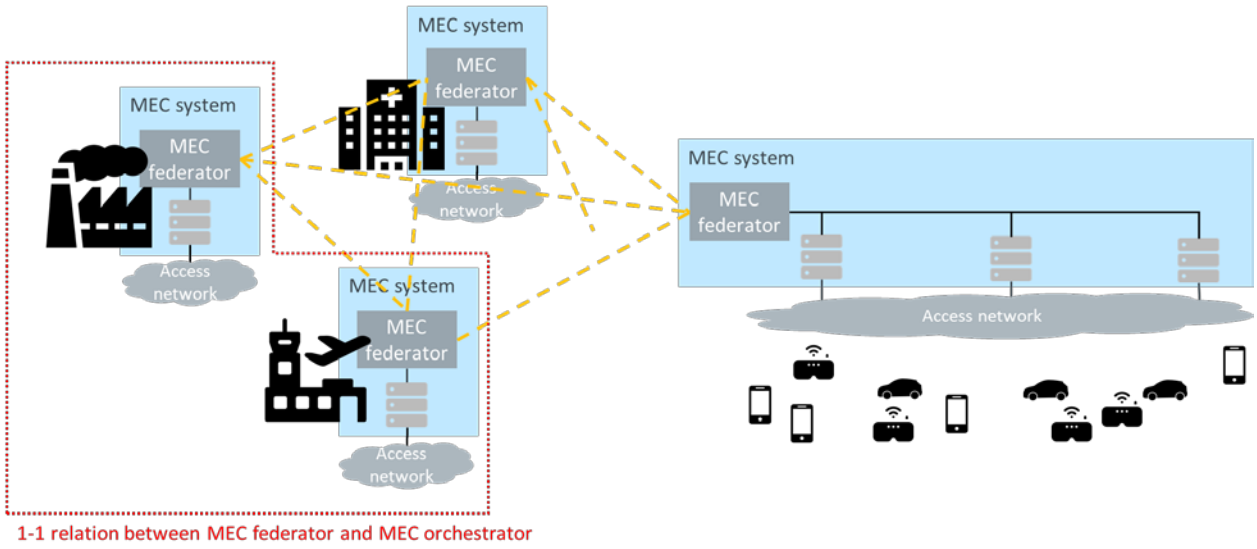

Figure 11: MEC federation deployment via MEC federator (peer-to-peer connection).

A MEC federator may also support a MEC federation broker role, which allows it to act as a hub for a hub-and-spoke topology. Figure 12 depicts a MEC network with this topology. Note that even in this case, individual MEC systems may support direct connectivity as illustrated in Figure 11. Furthermore, more than one MEC federator may support the MEC federation broker role (this is the case of more complex hierarchies, e.g., encompassing different regions / continents / areas).

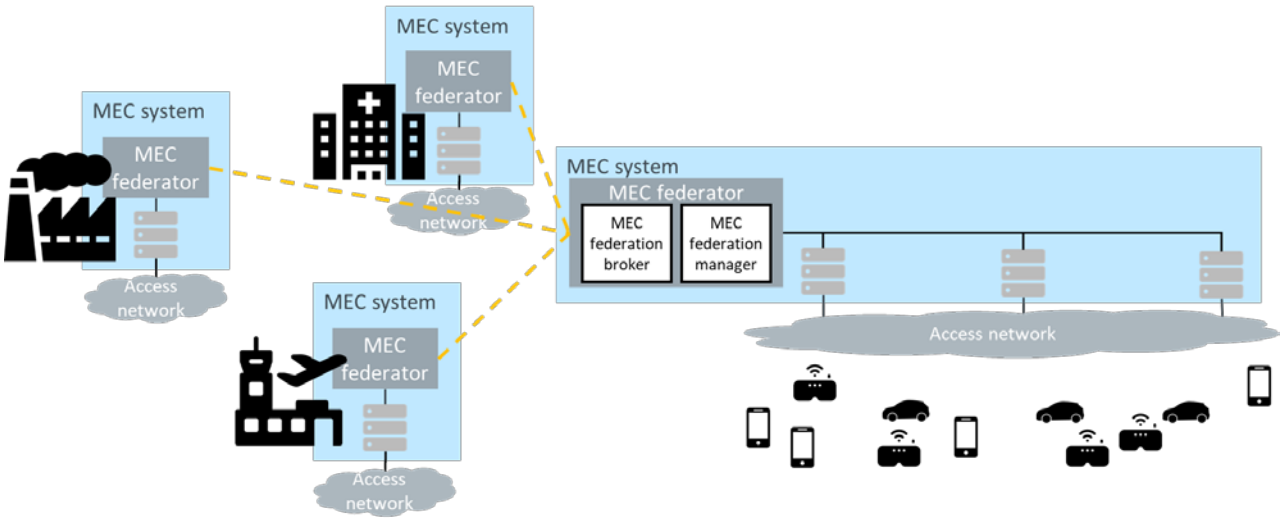

Figure 12: MEC federation deployment via MEC federator (hub-and-spoke topology).

In all the options above, all MEC systems are required to have a MEC federator. In addition, the shared OP option allows a MEC system to join a MEC federation without its own MEC federator, which means an additional MEC system can be integrated with lower overheads. This scenario is considered particularly

relevant to supporting integration of smaller MEC systems, e.g., standalone individual facility deployments as highlighted in Figure 9, into a larger region federated deployment.

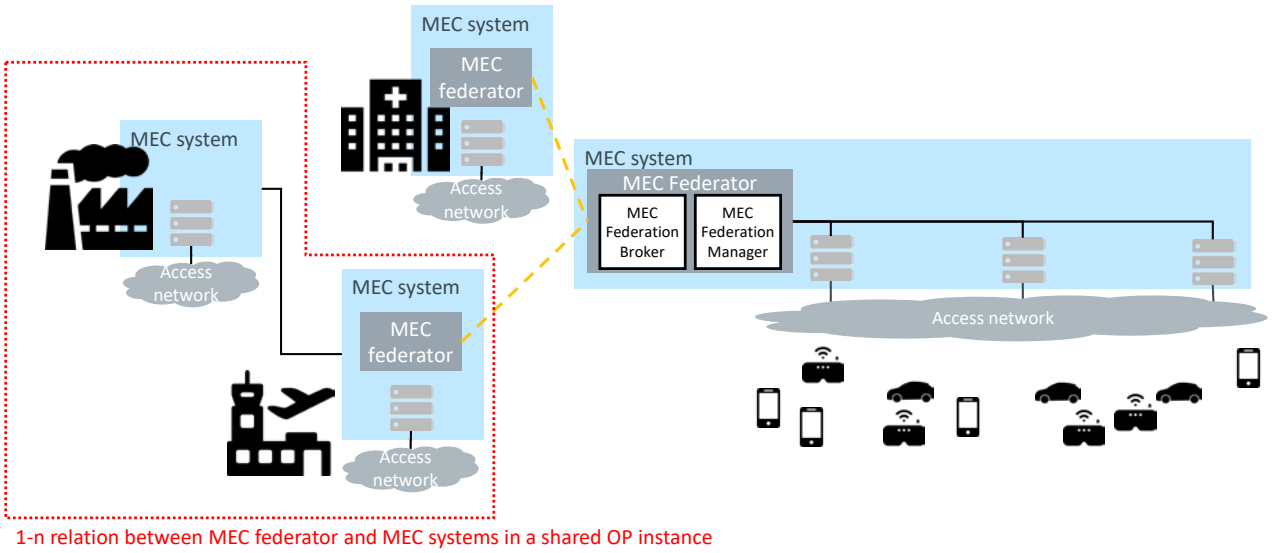

Figure 13: MEC federation deployment using shared OP.

Another possible story of federation deployment is integration of different MEC pieces in different regions of an operator. For an operator who has several subsidiaries, every subsidiary might have deployed MEC systems in their service regions. These deployments, e.g., MEC systems providing IoT service deployed in different regions, might have their own specific features because they were deployed at difference levels of functionalities. It was progressing with a different pace not only according to maturity of standardization but also to requirements, business models and other reasons in different regions.

The MEC federator can be considered as an enabler that provides compatibility with each other for MEC systems of subsidiaries when the operator plans to group the MEC systems providing the same service in different regions as a grouped MEC system. The grouped MEC system could be used for management purposes from the group company's point view at the beginning stage. So just a sub-set of capability, like information exchange or/and application monitoring across different MEC systems, of federator might be used at this stage. The other capabilities, like application lifecycle management across different MEC systems or/and new functionalities defined by SDOs, could be adopted with the growth of the grouped MEC system and the individual MEC system in each region. Whether or not to deploy a specific federator in each region can be decided by subsidiaries respectively. Figure 14 illustrates one possibility of the federator deployment in grouped MEC system. The other federator deployment possibilities showed in Figure 15 apply to this story.

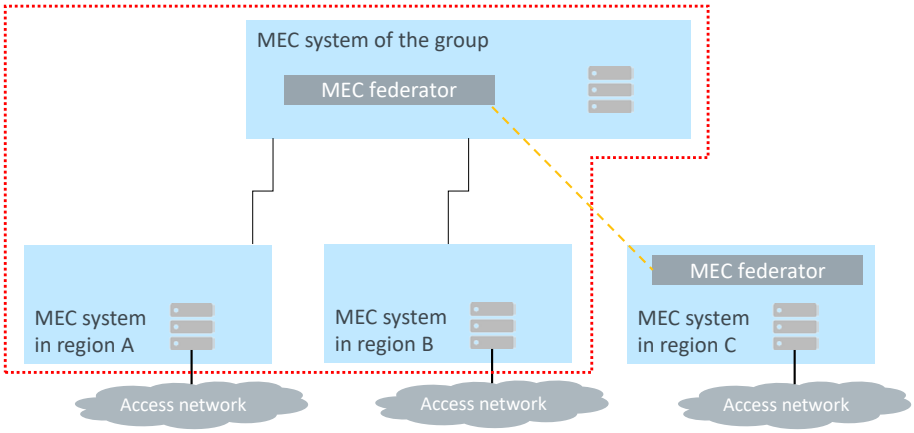

Figure 14: MEC federation deployment in grouped MEC system

5.2 Federation cases among multiple operators

As extracted from GSMA OP PRD [4], the main benefit of MEC federation is to obtain the global access to the MEC systems across different regions or different access networks as illustrated in Figure 15. MEC federation enables application providers to deliver their own application service to consumers who connect with any access networks that link with the federated MEC systems. Even if the consumer moves across the different access networks, the application service is expected to seamlessly continue as the consumer connects to the visited networks.

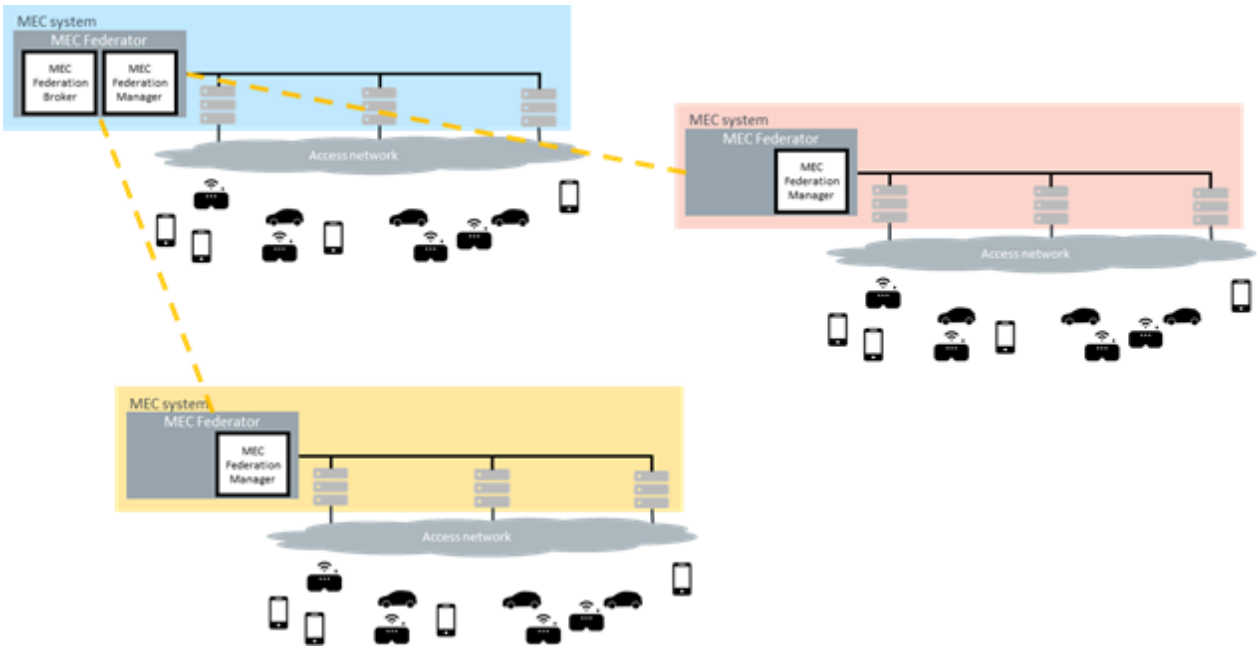

Figure 15: MEC federation deployment across different regions or different access networks

On the other hand, similarly to Clause 5.1, "small start" approach can be applicable also to multiple operator cases.

According to Figure 12, all MEC systems are not necessarily owned by the same operator, as shown in the example of Figure 16. In a MEC federation deployment, Operator 1 in this example could allow Operator 2 to use Operator 1's MEC system. The federation scenario can potentially resolve technical complexities. For example, if Operator 1 deploys a private 5G network (also known as Local 5G), a federated MEC system between the operators may lead to difficulties in maintaining the interconnected networks. Sharing Operator 1's network may sidestep this problem.

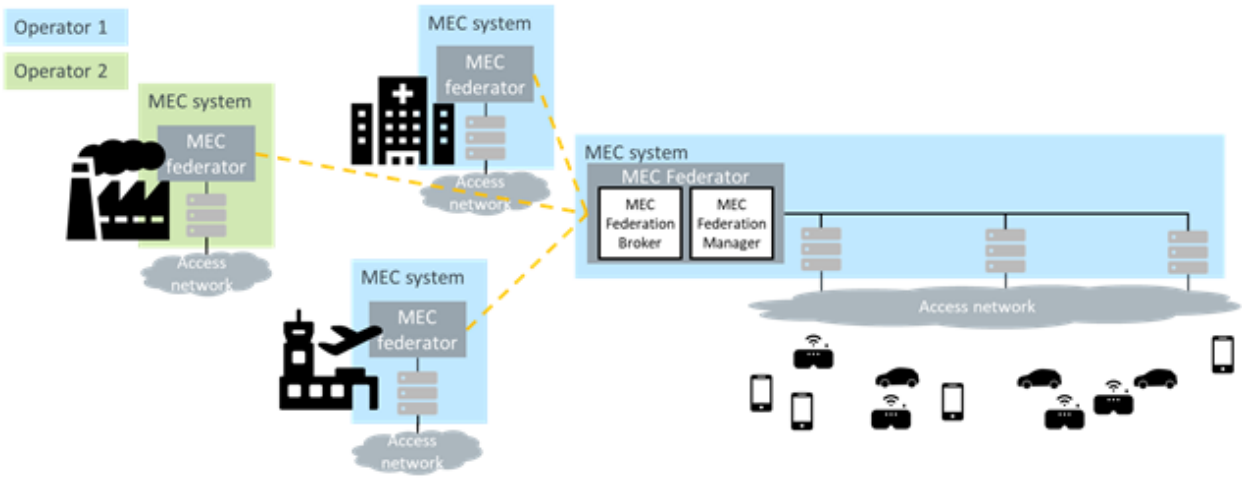

Figure 16: MEC federation deployment within multiple MEC system operators.

In Figure 13, the aggregated MEC systems via MEC federator can lead to the following business case. A small operator, which cannot afford the operational expense (OPEX) of maintaining a full MEC system with a MEC Federator and network, could be invited to federate with a MEC system owned by a larger operator which already supports such a system. The smaller operator can avoid the OPEX of the MEC Federator and still be part of a federated network.

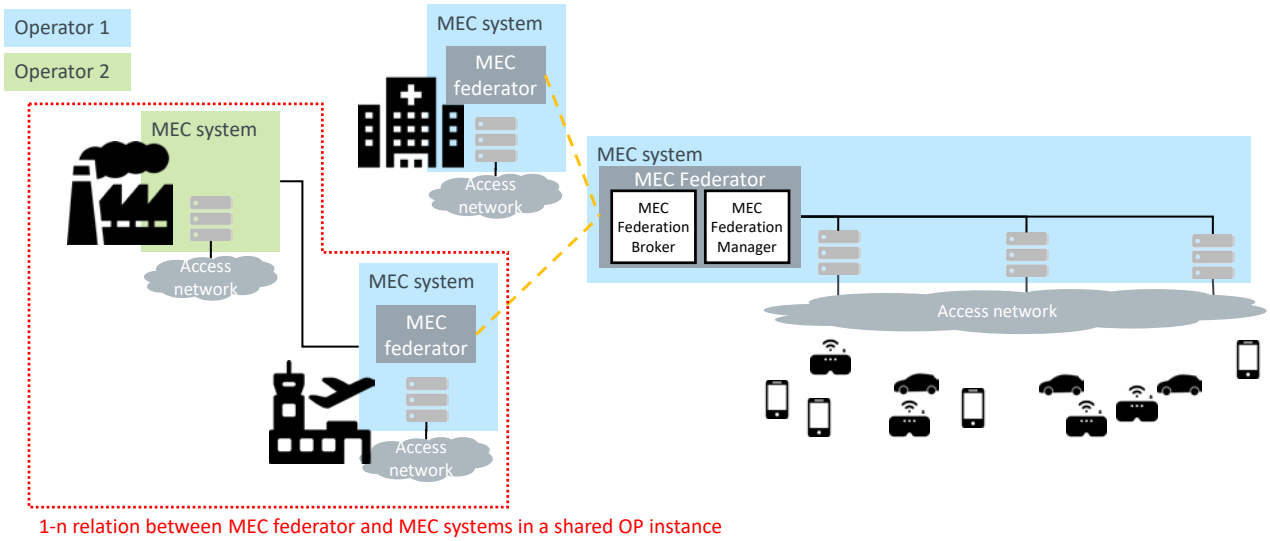

Figure 17: MEC federation deployment with different MEC operators via shared OP.

In the extreme case, a single MEC Federator could organize multiple MEC systems in a federated system, as shown in Figure 18.

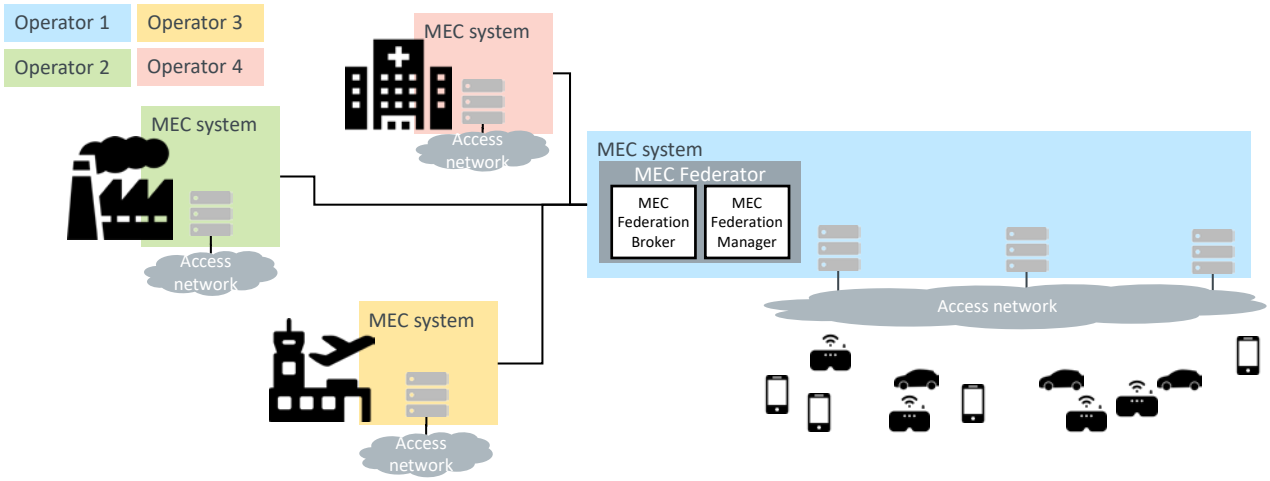

Figure 18: MEC federation deployment via one MEC federator using shared OP.

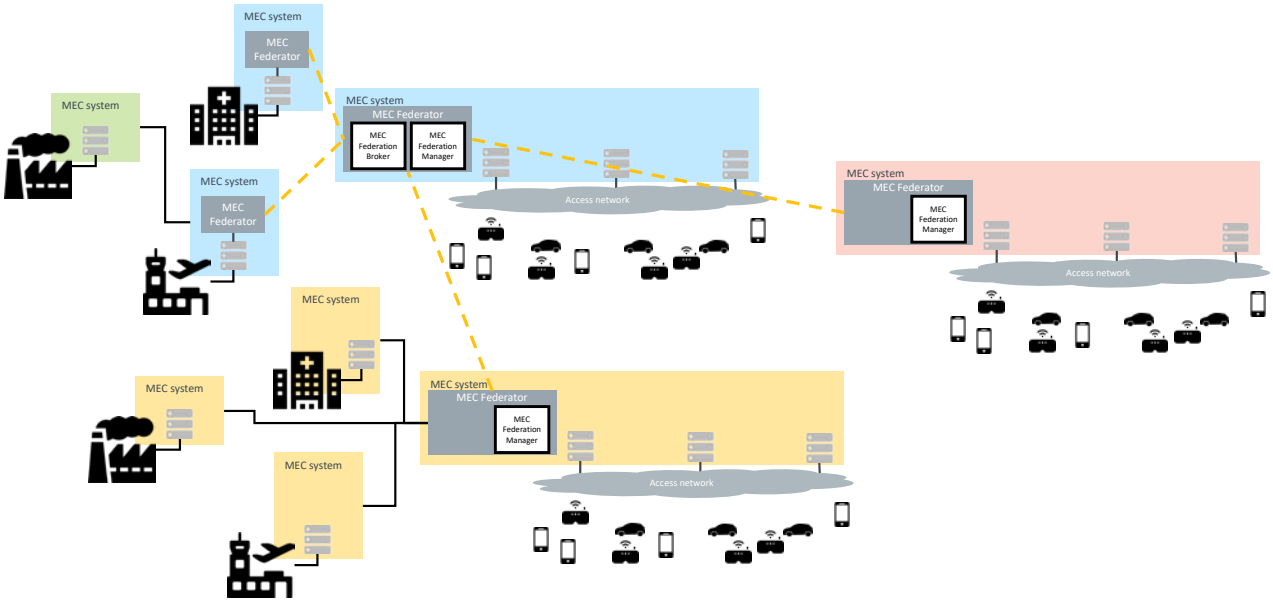

Figure 19: A whole picture of federated MEC systems.

5.3 Potential scenario with public cloud service providers

Collaboration with public cloud providers will be considered for MEC business as essential. There are two types of cloud environment: Cloud edge and Cloud Core, through which public cloud providers as well as operators provide various cloud services accordingly. Currently, the common collaboration model is for operators to manage multiple cloud services as shown in Figure 20. For example, an application provider can choose the appropriate cloud services, check usage data, and manage LCM (Lifecycle Management) process easily according to its needs through an integrated customer portal. Also, Platform Manager and

Cloud orchestration can manage cloud resources in accordance with requests of application providers. Federation entity works only for the other MEC systems in MEC federation not for Cloud services.

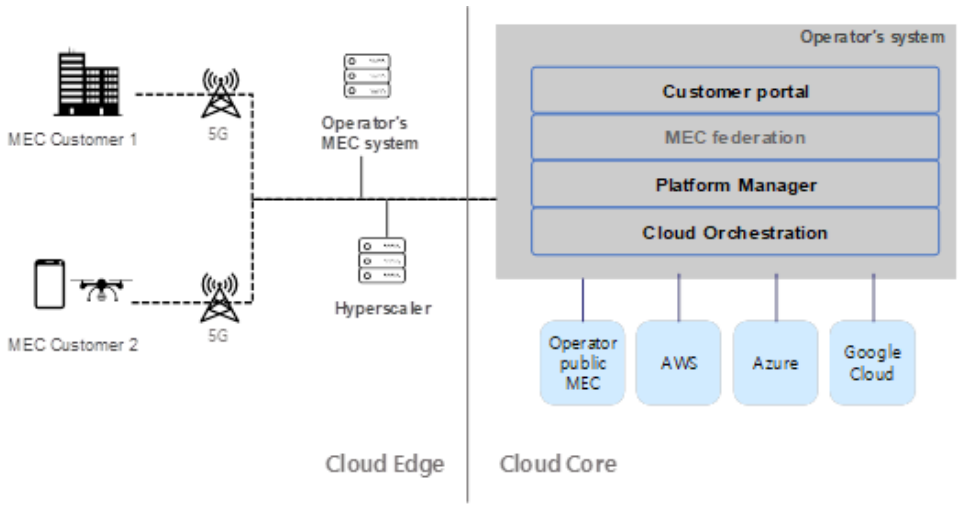

Figure 20: Current collaboration model with cloud service providers

When MEC federation becomes popular in the market, additional approaches can be expected. GSMA also describes two collaboration models in the annex C2 of PRD [3]. As illustrated in Figure 21, first, Operator platform simply manages the Hyperscaler's cloud resources, the same as in the current collaboration model. The second is for the Hyperscaler to join the MEC federation's ecosystem by supporting OP in order to connect with other MEC systems of MEC federation via E/WBI. In this second case, various business cases described in section 5 are also applicable. In addition, since public cloud service providers are providing their cloud services with their own APIs, conversion between public cloud service providers' APIs and E/WBI APIs defined in ETSI may be considered rather than implementing new APIs for E/WBI.

As a summary of this clause, by combining the options listed above, a MEC federator can flexibly support many deployment conditions (i.e., one for specific facilities vs. one for distributed users, supporting big operators and small operators, and the collaboration with Hyperscalers) to maximize the sharing and exploitation of the MEC systems.

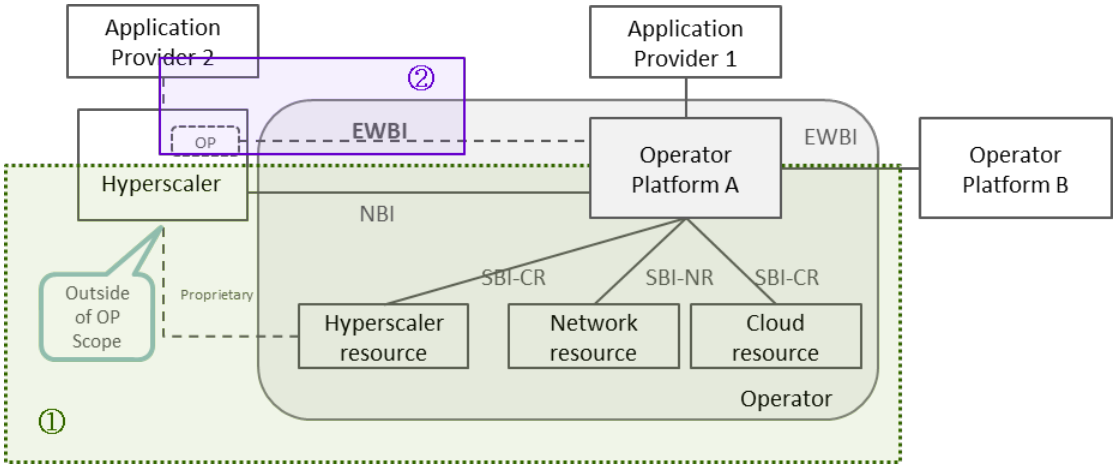

Figure 21: Relationship with Hyperscalers (Source: Annex C.2 of GSMA OPG PRD [3], updated with green and purple squares.)

6 Potential deployment options

6.1 Introduction

Various forms of deployment appear in the business cases. For the wider compatibility, it is important to align with both ETSI MEC architecture and GSMA OP architecture. This section attempts to describe various forms of deployments based on the ETSI MEC architecture while also mapping the deployment options to the GSMA OP architecture.

6.2 1:1 relation between MEC federator and MEC orchestrator

In the case where each operator has its own OP instance (see GSMA PRD [3], Annex C.1), the federated MEC systems are linked via their individual MEC federators through the Mff reference point. The relationship between the MEC orchestrator and the MEC federator in each MEC system is 1:1. In this case, the potential deployment option is depicted in Figure 22. Each OP instance contains one MEC federator and one MEC orchestrator. Application Provider (AP) has a sole connection to OP A and if AP wants to deploy its application package to OP B and to provide its MEC services in Operator 2, it can be performed through E/WBI between OP A and OP B. OP A performs “Aggregator Role”, “Resource Manager Role” and OP B performs only Resource Manager role as defined in the GSMA Whitepaper, “Operator Platform Concept” [6].

As described in Figure 7, interfaces defined in GSMA OP (fonts in blue) corresponds with reference points defined in ETSI MEC (fonts in green). This option corresponds to the business case presented in Figure 11 and this case is regarded as the simplest option.

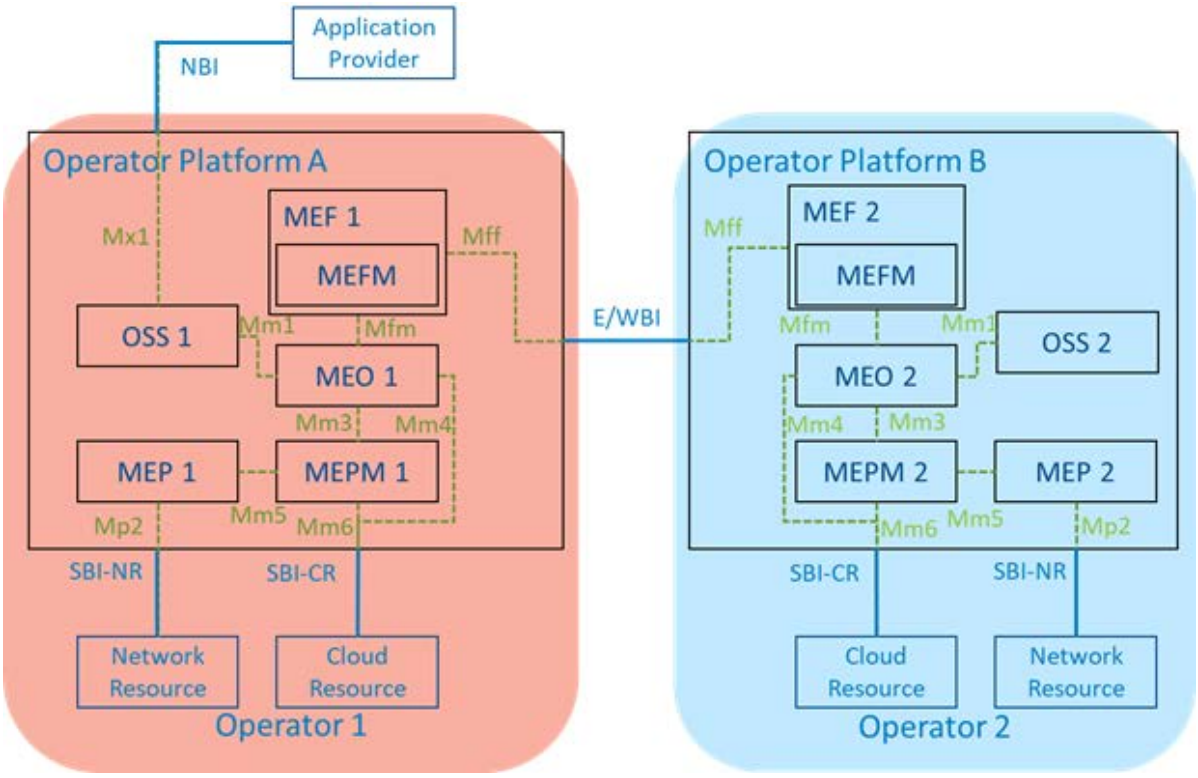

Figure 22: Deployment option of MEC federation in case of 1:1 relation between MEO and MEF.

6.3 1:N relation between MEC federator and MEC orchestrator

If the shared OP case is considered (i.e., GSMA PRD [3], Annex C.2), one OP instance links to multiple Operators. In this context, single MEC federation manager role associates with multiple MEC orchestrators, as depicted in Figure 23. MEF supports linking with multiple MEC orchestrators through the Mfm reference point. Therefore, this option is compliant with the ETSI MEC specifications.

Note that the coverage of operator's resources is still under discussion. In Figure 23, we have tried to draw OP boundary separately from the boundary of operator's resources. We also newly defined the extended scope of OP in order to populate multiple functions (e.g., OSS/MEO/MEPM/MEP) and to remain consistent with SBI-CR/NR. In the figures, MEO/OSS/MEP/MEPM are in the extended scope of OP A and in the coverage of each operators' resources at the same time. However, the coverages of OP instance and Operator domain should not be overlapped because they are separate as described in Figure 2. For the time being, there exists no way to describe a deployment option that aligns with all descriptions.

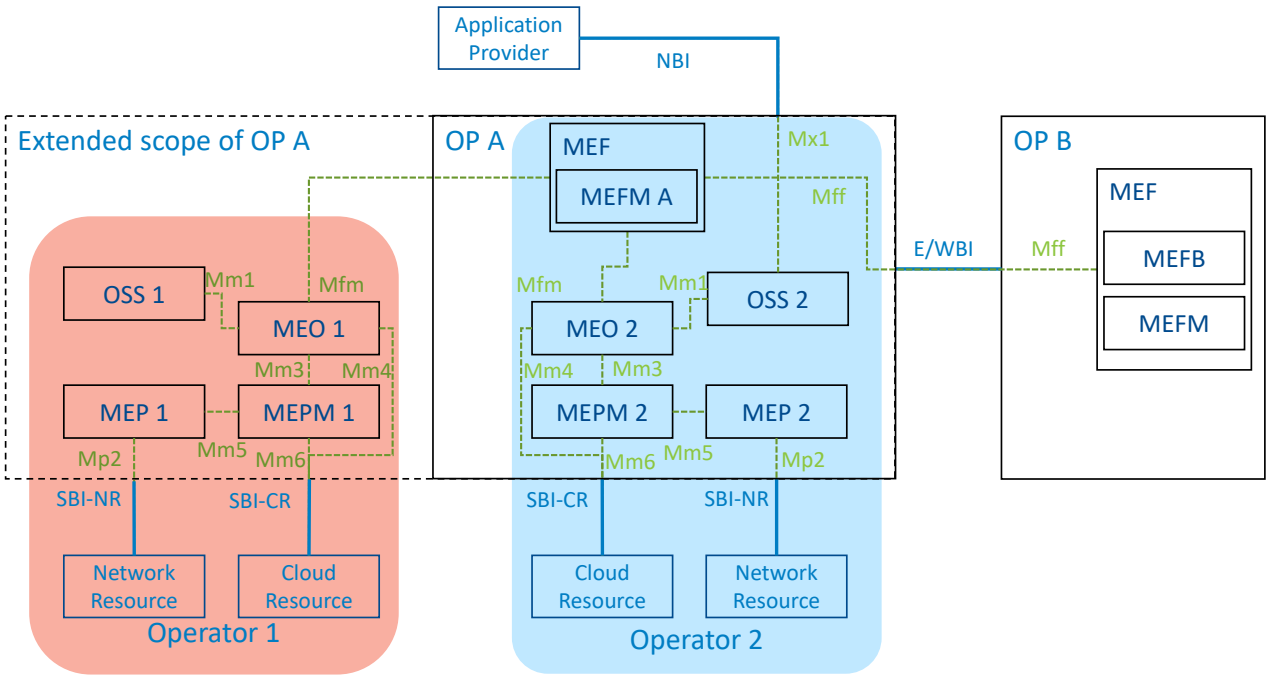

Figure 23: Deployment option of MEC federation in case of 1:N relation between MEF and MEO with a single MEFM role.

6.4 1:N relation between MEC federator and MEC orchestrator owned by a single operator

As mentioned in Clause 5, multiple MEC systems are not necessarily owned by different operators. In this context, two cases can be considered. In the first case, (a) there are two different MEC systems inside a single operator, but there is one MEC orchestrator which links with multiple MEC platform managers/Operation support systems (OSSs), as illustrated in Figure 24. In the second case, (b) two different MEC systems exist, share OSS, but have each MEC orchestrator that linked to a single MEC federator as illustrated in Figure 25 Figure 24. In both cases, MEF is responsible for federating with the other OP (OP B).

As for (a), the MEC orchestrator is required to connect with multiple MEC platform managers and multiple OSSs respectively. However, this is the typical case of deployment with multiple MEC systems (belonging to a single operator or multiple operators), thus a single MEC orchestrator is generally not sufficient to orchestrate multiple systems. As for (b), MEC federator needs to connect with multiple MEC orchestrators and multiple MEC orchestrators need to connect with a single OSS. The OSS is supposed to be a singleton in an operator's MEC systems. Note that even for the federated MEC systems of the same operator, MEO to MEO direct communication is not supported by ETSI MEC specifications.

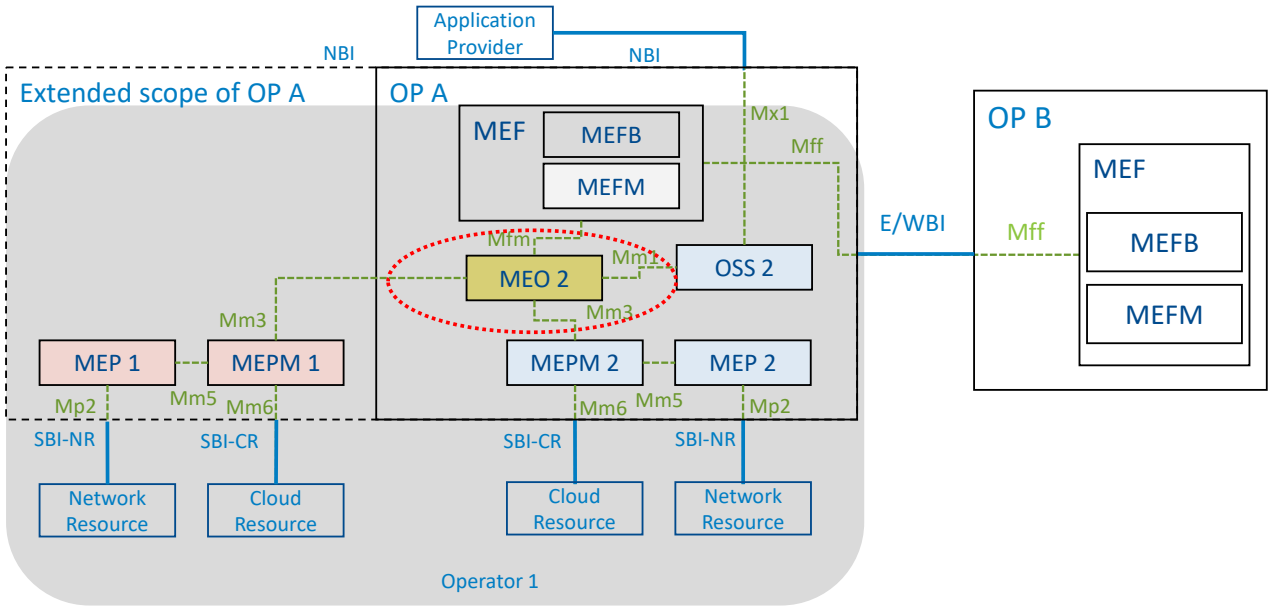

Figure 24: Deployment option of MEC federation in case of 1:N relation between MEO and MEPM.

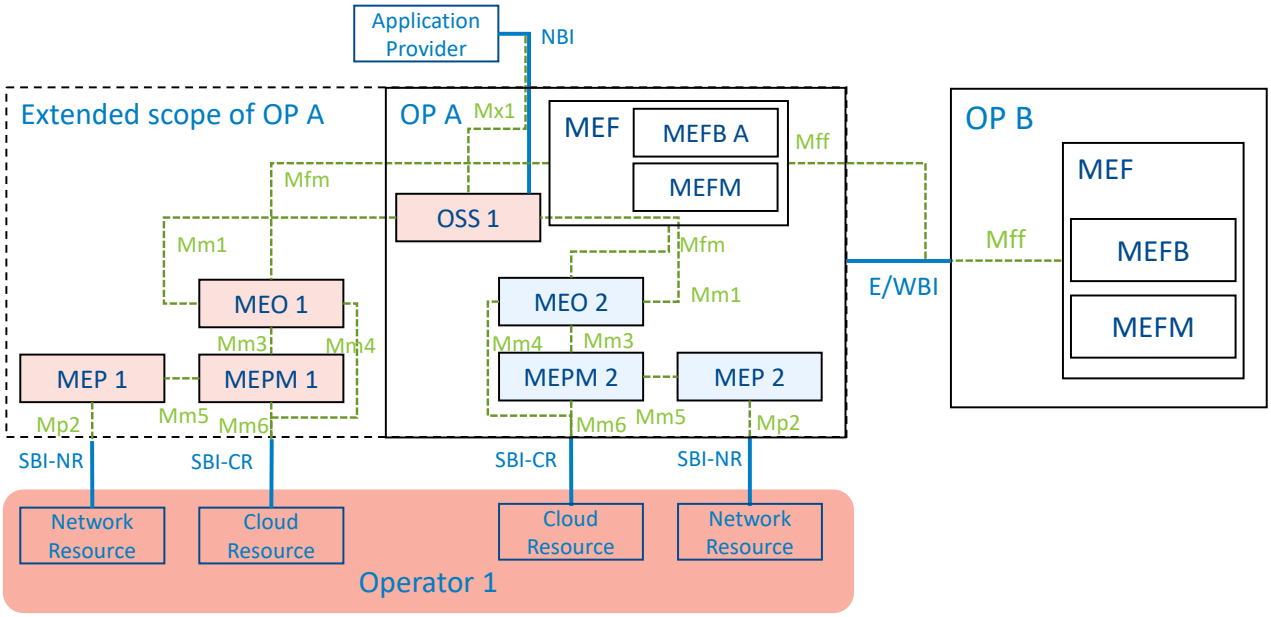

Figure 25: Deployment option of MEC federation in case of 1:N relation between MEF and MEO, corresponding resource is owned by a single operator.

7 Additional key considerations

7.1 Connection between MEC systems

7.1.1 Introduction

To enable connectivity between different operator platforms in a deterministic and secure way the Internet may not be optimal. To realize the interconnection between operators and systems, a similar approach to GRX/IPX or private connections to cloud providers should be considered. In a peering solution like GRX/IPX a dedicated switching platform in a carrier neutral facility (CNF) would be a good option as it provides a similar environment as the industry is used to today. Private connectivity over an interconnection platform at a carrier neutral provider would be another option which would enable API driven connectivity models on demand. Depending on the specific use case a combination of the two options could be an alternative where the switching platform is used for signaling and discovery and the private connectivity platform to set up dedicated data-plane connections on demand.

Requirements set in document, ETSI GR MEC 035 [2], V3.1.1 (2021-06) - Inter MEC systems and MEC-cloud system coordination, would be met by the interconnection options described above.

1. A MEC platform should be able to ***discover*** other MEC platforms that may belong to ***different*** MEC systems.
2. A MEC platform should be able to ***exchange*** information in ***secure*** manner with other MEC platforms that may belong to ***different*** MEC systems.
3. A MEC platform should be able to ***exchange*** information in a ***secure*** manner with other MEC ***applications*** that may belong to ***different*** MEC system.

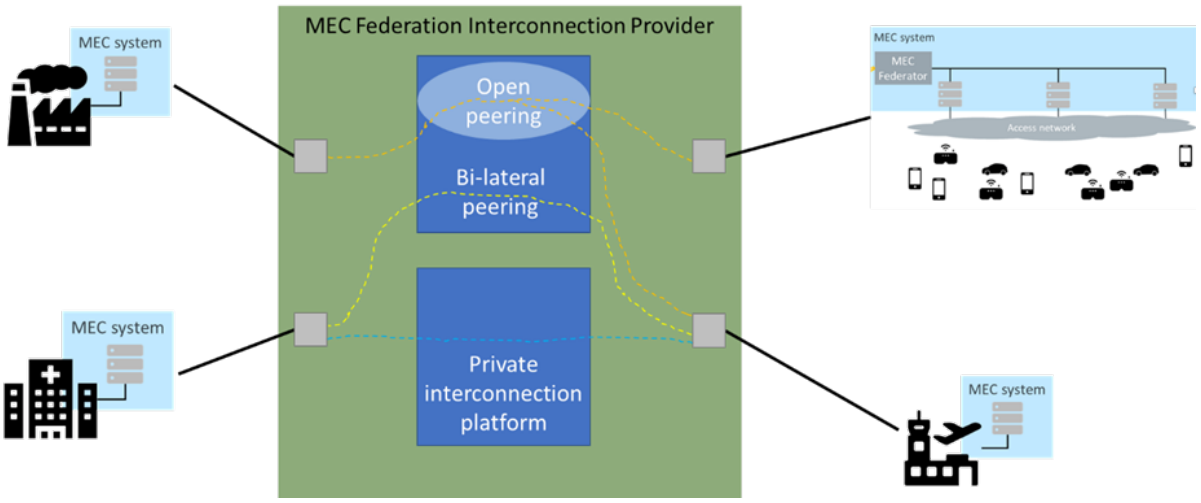

Figure 26: Peering and private connectivity options

Deployments at a carrier neutral facility generally host most local and many regional and global operators. These CNFs also have the connectivity to public cloud providers and host rich eco-systems from various

industry vertical, public sectors, etc. which would enable efficient and secure connections to application providers utilizing the MEC platforms.

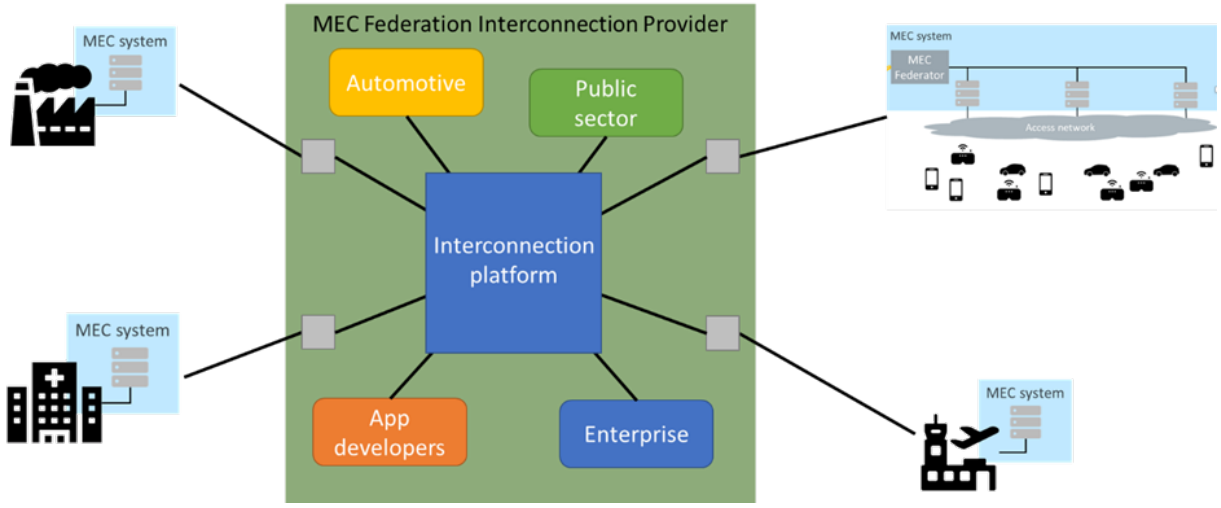

Figure 27: MEC Federation Interconnection Provider facilitating secure and performant deployment, interconnection MEC Federation.

In addition to the connectivity options and rich eco-systems a CNF would be the optimal place to deploy a neutral MEC federation manager and broker as this is where the different autonomous systems converge.

7.1.2 Business stories for MEC Federation

All practical deployments of the discussed examples of business stories, will greatly benefit and may even require an interconnection provider to achieve scalability, security and efficiency of information and data exchange among the federated MEC systems. The role of interconnection provider in the context of MEC Federation may be referred to as MEC Federation Interconnection Provider (MFIP). The role of MFIP is to enable fundamental data plane connectivity (e.g., L0/L1/L2/L3) among the MEC systems, as this connectivity is required to facilitate control information exchange for the higher levels of MEC Federation functions to operate (e.g., registration, discovery, life cycle management, monitoring) as well as the application data transfers between MEC Platforms. MEC Systems may have a business relationship with MFIP as shown in figure 28.

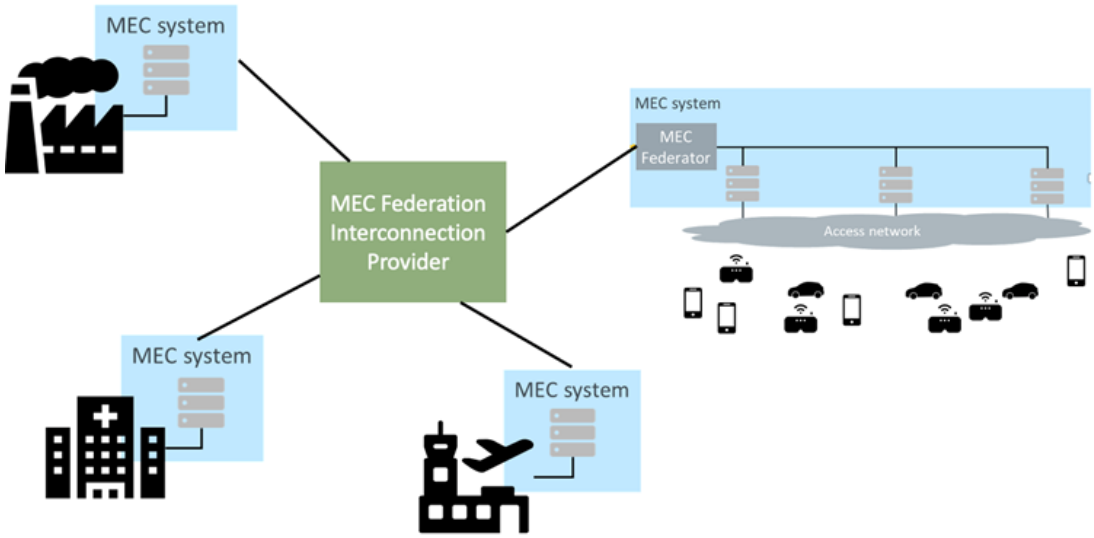

Figure 28: MEC Federation Interconnection Provider enabling connectivity among federated MEC Systems.

The MFIP may be providing other services in addition to interconnection, such as co-location and bare metal resources, and therefore one of the possible deployment scenarios is when a MEC System can be physically located on the premises of the MFIP as shown in figure 29 below.

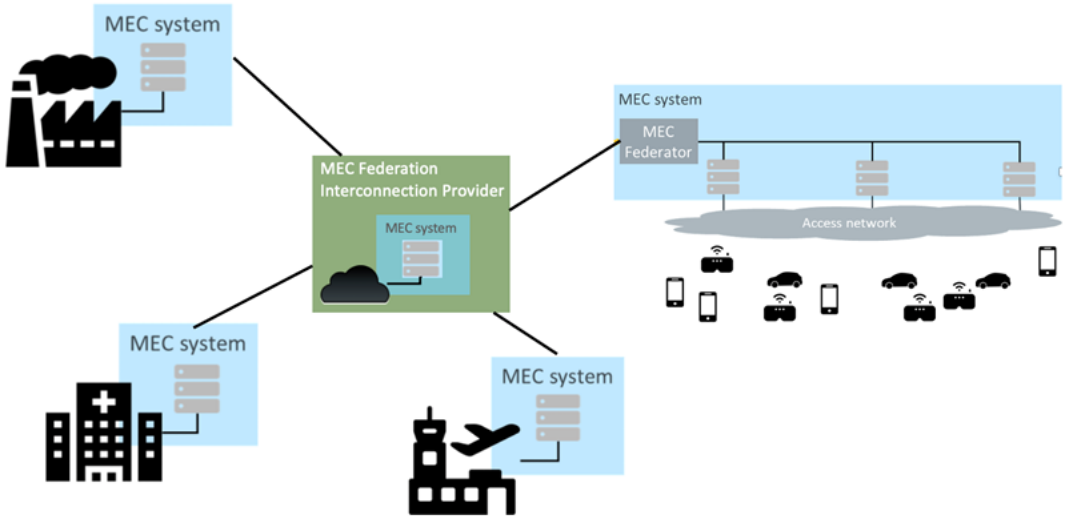

Figure 29: MEC Federation Interconnection Provider enabling co-location of MEC System.

In many cases MEC Systems may also be deployed in Public Clouds. A MFIP may provide connectivity between the MEC Systems in Public Clouds and other federated MEC Systems as shown in figure 30 below:

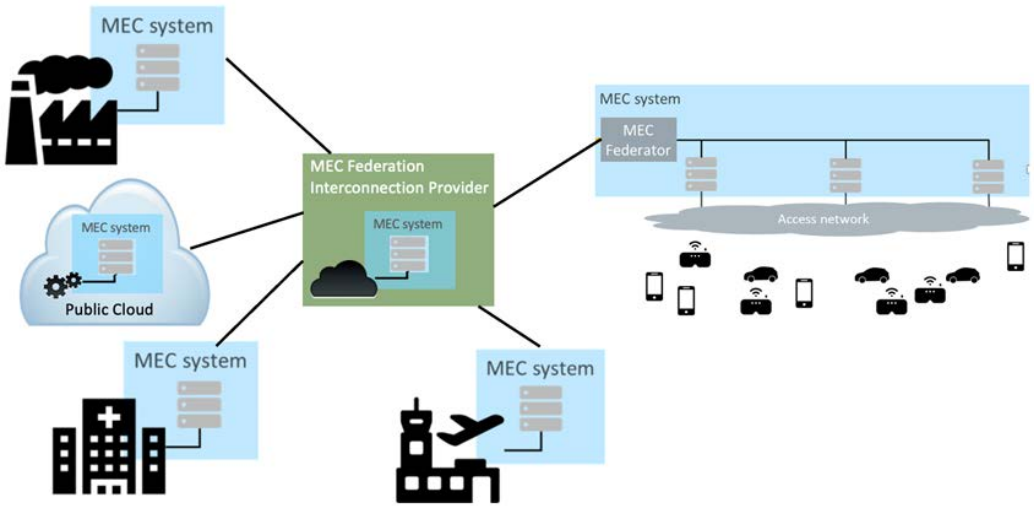

Figure 30: MEC Federation Interconnection Provider enabling interconnection to MEC System in Public Cloud.

All connectivity scenarios for MEC Federation, such as peer-to-peer and hub-and-spoke, across MEC Systems of the same Operator or of multiple Operators along with the ability to include MEC Systems in co-location facilities as well as in the Public Clouds can be facilitated by the MEC Federation Interconnection Provider. This connectivity may leverage virtual connections (e.g., VLAN/VxLAN) over a common physical interconnection infrastructure for further efficiency and cost savings as shown in figure 31 below.

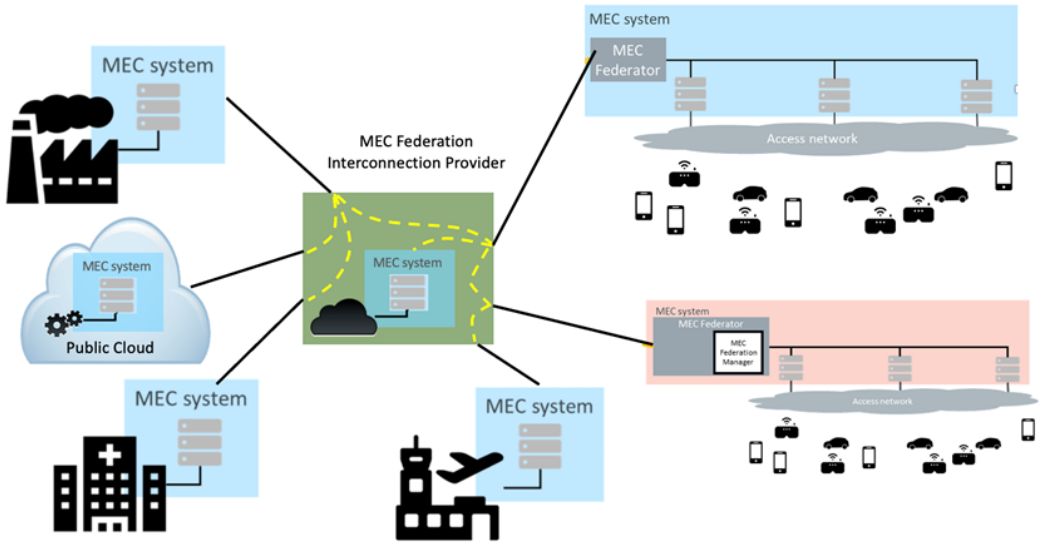

Figure 31: Multiple connectivity patterns enabled by MFIP among various MEC System deployments and across multiple Operators.

An additional benefit from utilizing the MFIP for enabling connectivity for MEC Federation is the fact that the MFIP facilities can be local to given geographic areas (e.g., Metropolitan Areas) and that the MFIP facilities in different geographic areas are interconnected together over private and secure links. This can allow for *geo-aware MEC Federation* where MEC Systems that require low latency for federated applications can be linked in a proximal manner in a desired geographical area, while other entities such as MEC Federator may be located some distance away, as shown in figure 32 below.

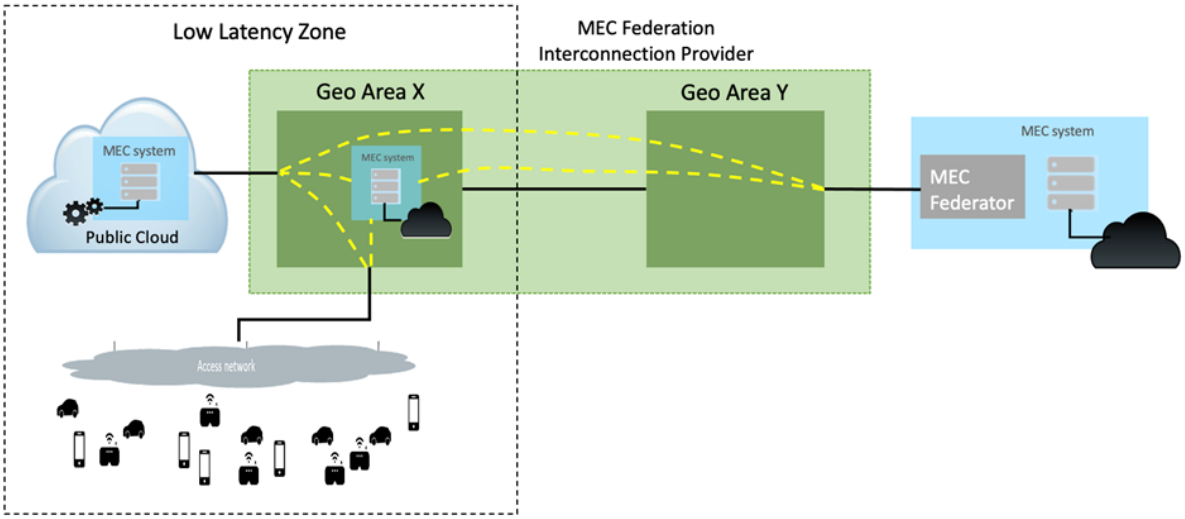

Figure 32: Enabling low latency MEC Federation zones with MFIP

The concept of proximal connectivity and geo-awareness can be extended to supporting MEC slices. For example, multiple slices can be extended from the access networks (e.g., 5G) to form low latency MEC slice and general access MEC slice in the MEC Federation, as shown in figure 33 below.

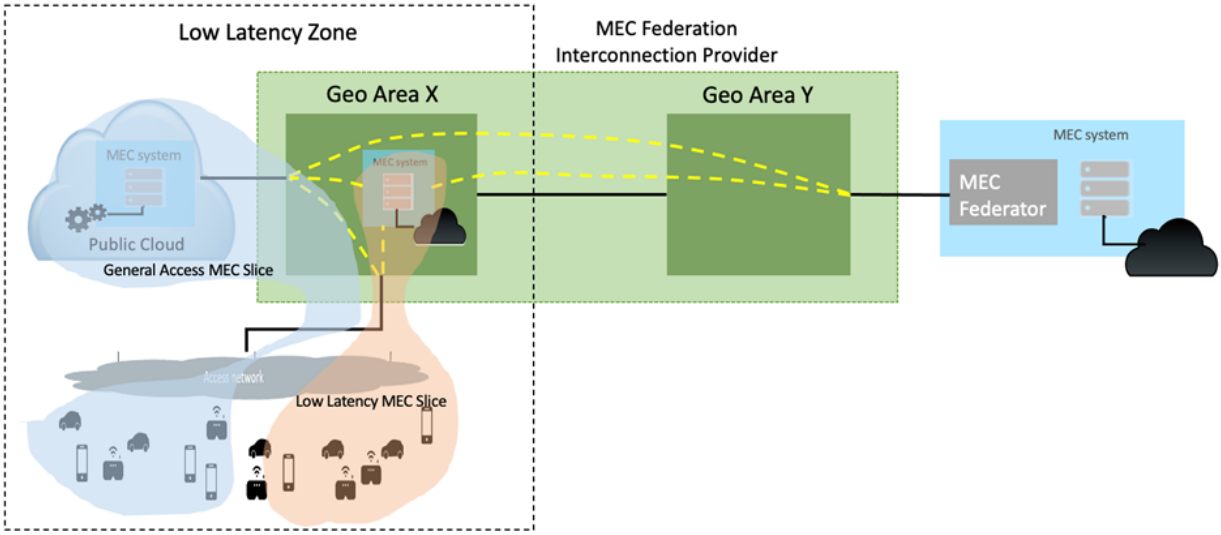

Figure 33: Enabling MEC slices under MEC Federation.

7.1.3 Potential deployment options

In many production scenarios operators rely on interconnection providers to enable connectivity to other operators, public clouds, and enterprises in carrier neutral facilities (CNF). In this case the interconnection provider acting as a MEC Federation Interconnection Provider (MFIP) may provide Network Resources (NR) as well as access to Cloud Resources (CR) as shown below.

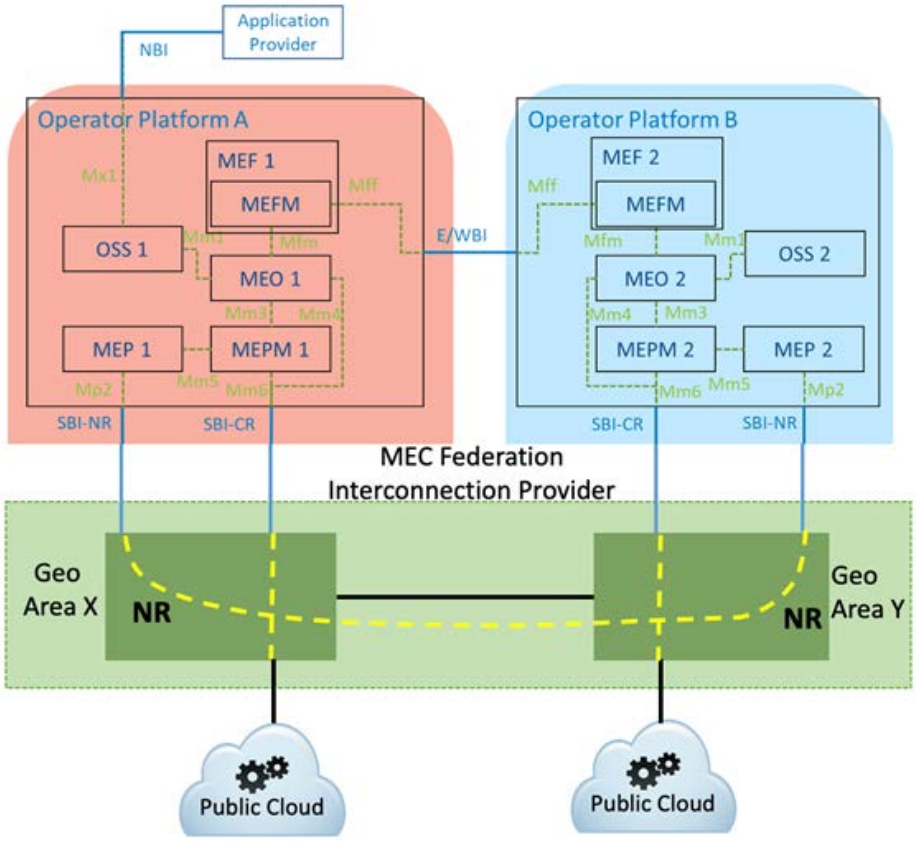

Figure 34: MEC Federation Interconnection Provider enabling Network Resources and access to Cloud Resources to Operator Platforms in MEC Federation.

In addition, MEC Platforms (MEP) may also be deployed in a CNF and interconnected by the MFIP as shown in figure 35.

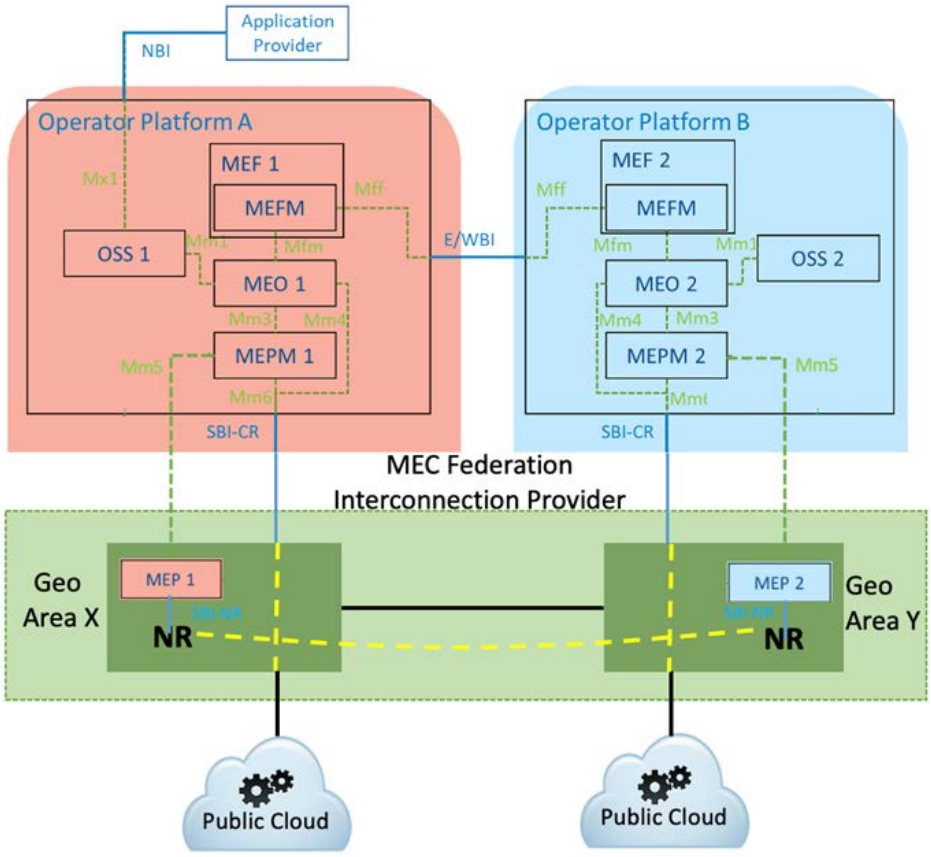

Figure 35: MEC Federation Interconnection Provider hosting MEC Platforms, enabling Network Resources and access to Cloud Resources to Operator Platforms in MEC Federation.

7.2 Aspects of Multi-Domain Orchestration relevant to MEC Federation

7.2.1 Introduction

The infrastructure required to support MEC Federation is expected to be comprised of resources that exist in multiple domains, including Operators (mobile and fixed), Public Clouds, as well various 3rd parties including co-location, interconnection, and bare metal providers. It is also expected that MEC Platforms may be built on diverse infrastructure. Some of the considerations that may impact MEC Federation approaches to orchestrating the underlying infrastructure are described below:

- **Public Cloud Driven Edge Computing**. Edge computing infrastructure and resources are increasingly provided by public clouds (e.g., AWS Outposts, IBM Cloud Satellite, Google Anthos). The Public Cloud based edge computing resources are also expected to be used in building the MEC Systems (e.g., MEC Platform) that are part of MEC Federation.

- **Hybrid infrastructure.** Most practical deployments of edge infrastructure and applications are hybrid in nature, where an application deployed at the edge needs services residing in the core cloud to function (coupled model). In addition, an application deployed at the edge, may need to communicate, and consume resources from multiple public cloud environments. MEC Federation solution supporting these applications would then be expected to enable federation of the hybrid infrastructure.
- **Multi-Domain.** Individual infrastructure domains (e.g., edge, cloud, network fabric) present their own APIs and/or other provisioning methods, thus making end-to-end orchestration challenging both in complexity and in time. A MEC Federation solution should be able to perform multi-domain orchestration in a uniform and consistent manner.
- **Interconnection and Federation.** The data plane (L0/L1/L2/L3) interconnection between edge clouds and core clouds as well as between the edges is a fundamental requirement for MEC Federation. It is often assumed that this connectivity exists, however it may not be the case in all scenarios. Therefore, in general, a MEC Federation solution should support orchestration of data plane connectivity between the domains that are being federated.
- **Bare Metal orchestration**. As with the interconnection, many orchestration solutions assume that the bare metal compute/storage hardware and basic operating system resources are available in edge cloud locations for the deployment of virtualization and application/services layers. In many scenarios this is not the case, and it would be desirable for a MEC Federation solution to support orchestration of bare metal resources for federated MEC Platforms.
- **Developer-centric capabilities.** Capabilities such Infrastructure-as-Code are becoming critical for activation and configuration of public cloud and edge cloud infrastructure components, interconnection as well as the end-to-end application deployment, integrated with CI/CD environments.

One of the biggest challenges with federated infrastructure orchestration across multiple domains is finding a common and uniform method of describing the required resources and parameters in different domains, especially in public clouds. Every public cloud provides many service categories with a variety of different services, with each service having several different components, and each component having multiple features with different parameters as shown in Figure 36.

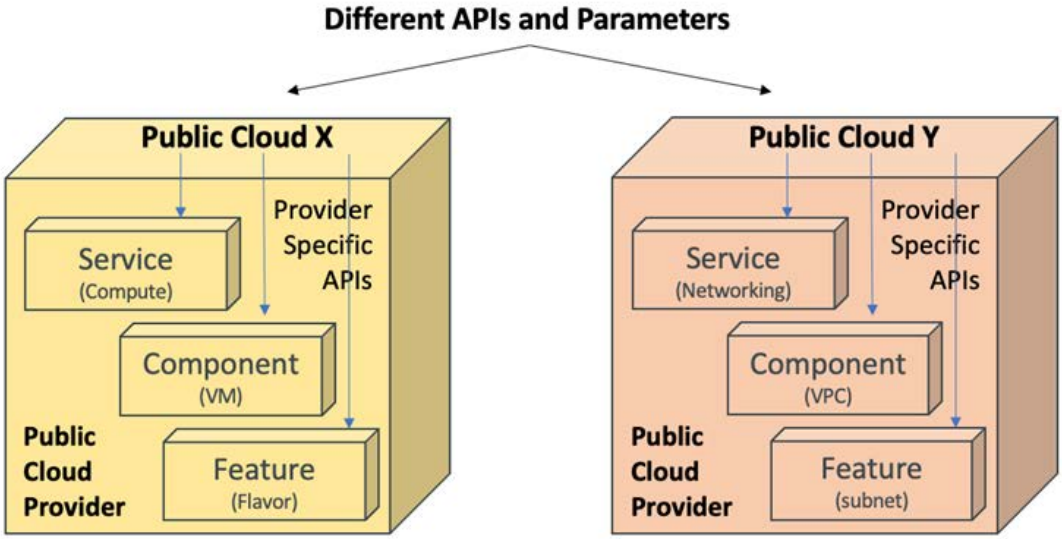

Figure 36 Challenges with uniform representation of Cloud Resources in different public clouds.

7.2.2 Infrastructure-as-Code as a uniform method of orchestrating infrastructure for MEC Federation

Infrastructure-as-Code emerged as a common tool that allows to abstract diverse provisioning methods (API, CLI, etc.) used in the individual domains and activate infrastructure components using a high-level language.

One notable point relevant to the orchestration of federated MEC infrastructure is that it is possible to integrate Infrastructure-as-Code tools as a microservice, within an orchestrator (e.g., in the MEO role). This enables important orchestration properties:

- Uniformity - use of the same infrastructure orchestration methods across public clouds, edge clouds and interconnection domains.
- Model-free – the orchestrator does not need to understand the details of the individual infrastructure domains (i.e., implement their models). It only needs to know where to retrieve the Infrastructure-as-Code programs for the domain in question and execute the code using the specified data and parameters.
- DevOps driven – the Infrastructure-as-Code programs can be developed and evolved using DevOps tools and processes.

Consider a scenario where MEC Federation must enable infrastructure, network, and cloud resources in three domains: a public cloud, an edge cloud provider, and an interconnection provider (to link compute at the edge to public cloud) for the subsequent deployment of a MEC application. An Infrastructure-as-Code based orchestrator may enable this federation as shown in figure 37 below.

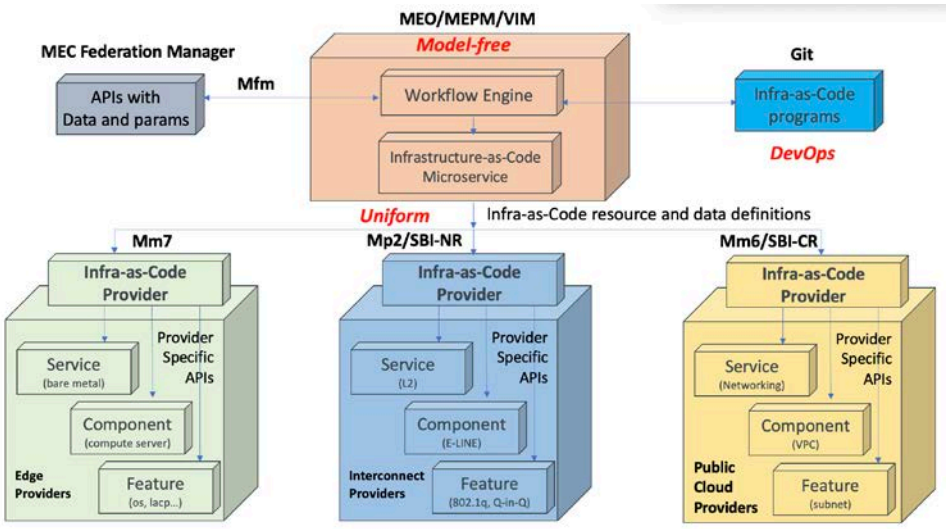

Figure 37: Utilizing Infrastructure-as-Code as a common orchestration tool for federated infrastructure across multiple domains.

7.2.3 Open-source example of implementation of combined MEO/MEPM/VIM with Infrastructure-as-Code based multi-domain orchestration relevant to MEC Federation

One relevant example of an implementation of a combined MEO/MEPM/VIM Infrastructure-as-Code based orchestrator relevant to MEC Federation deployments is the Linux Foundation Edge (LFE) Akraino Public Cloud Edge Interface (PCEI) blueprint. PCEI demonstrated a multi-domain orchestrator with functions mapping to ETSI MEC architecture elements like MEO, MEPM and VIM (Kubernetes, Openstack and Public Cloud IaaS/SaaS). It allows for infrastructure orchestration across multiple public clouds, edge clouds and interconnection providers, as well as the end-to-end edge application deployments including select ETSI MEC services (e.g., MEC 013 Location API). The PCEI architecture and relevant ETSI MEC as well as GSMA OP interfaces are shown in Figure 38 below.

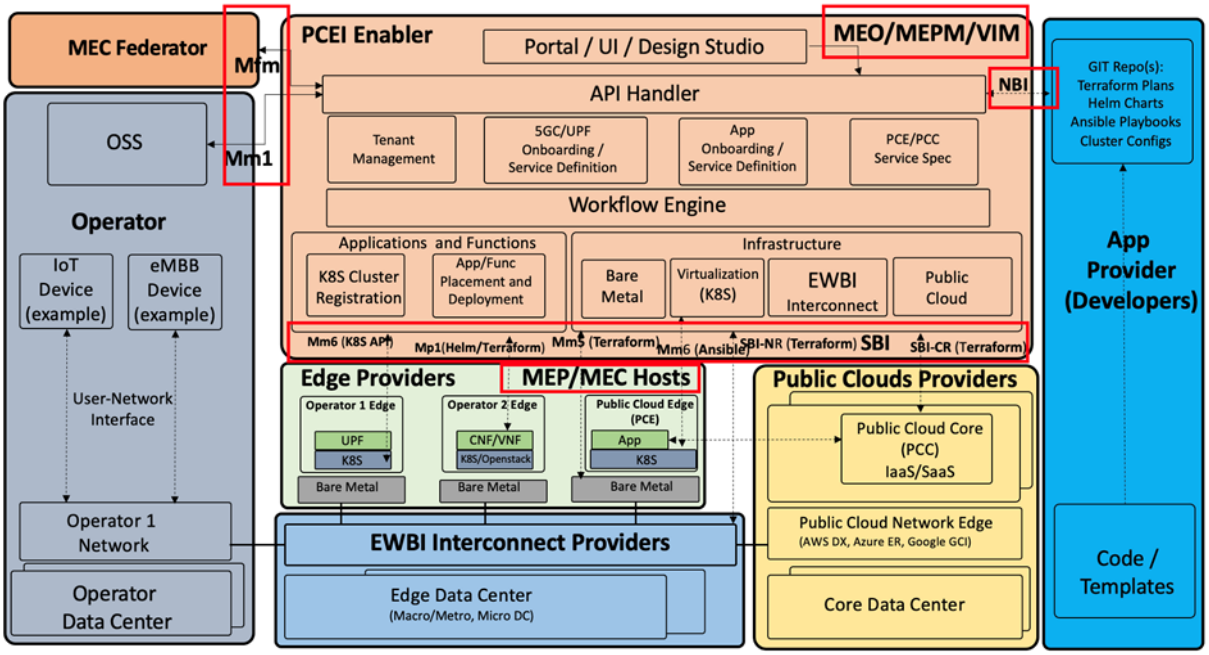

Figure 38: Open-source implementation of Infrastructure-as-Code based MEO/MEPM/VIM orchestrator relevant to MEC Federation.

7.3 Security considerations for MEC federation deployments

The establishment of a uniform level of security policies for all MEC federation deployment elements to minimize the risks is extremely important as mentioned in the ENISA-5G supplement – Guidelines on Security Measures under EECC [15], ETSI White Paper #46 [12], MEC security: Status of standards support and future evolutions, ETSI GS MEC 040 [4], and the GSMA Permanent Reference Document, “Operator Platform Telco Edge Requirements [3].

There are many challenges related to security that need to be considered in future standardization work: Infrastructure security and protection from physical to virtual and application levels, Data protection and User security which includes data encryption - at rest, in transit and in motion.

ETSI MEC is working on MEC security with a study item (to be GR MEC 041) that would define recommendations for future normative work in that perspective of security.

8 Conclusions

This White Paper has focused on the deployment options related to MEC federation, especially from an architectural point of view, and with a key focus on ETSI MEC implementations. We also describe the synergized architecture, as showing a comprehensive cross-SDO mapping with the OP architecture defined by GSMA OPG, and correspondence among different standards related to MEC federation. However, the authors of this White Paper acknowledge that a final mapping will necessarily need to take into account further development in each SDO, including the progress made in the open-source project CAMARA (in alignment with OPAG).

This White Paper has introduced a number of business cases and a consequent list of deployment options, with each option corresponding to a specific business story. The aim was in fact to help edge stakeholders, and all readers in general, to better understand how to choose the appropriate deployment options based on the business stories described in the document.

Finally, this White Paper has introduced some key considerations, i.e., interconnection between MEC systems, multi-domain orchestration and collaboration among operators and with cloud providers and third parties, and security for MEC federation deployments. An understanding of all these aspects will be beneficial for the future deployment of MEC federation and edge capability exposure in these heterogeneous environments.

Annex A: Northbound APIs in the MEC Federation and relation with standards, fora and open source: focus on CAMARA APIs

Talking about OP:NBI, the recent open-source project established under LF CNCF with the name of CAMARA [9] is in charge of defining the **Service APIs**, which enable the network operators to make their network capabilities available for consumption from the end-customers (e.g. application developers, vertical market segments, 3rd parties, ..). The project CAMARA is also working in alignment with OPAG (the API subgroup within GSMA OPG).

In this context, **Internal APIs** are typically defined in SDOs or industry fora, and quietly tied to the underlying technology. Examples of these APIs include the ones defined by 3GPP, ETSI, TMF and CNCF, among others. In this context, the CAMARA project defines an **Exposure Gateway**, which provides a set of capabilities to policy the interaction between the API provider and consumer, when they both belong to different administrative domains. The **Transformation function** keeps the information on correspondences (mappings) between service APIs & internal APIs and executes the workflows to enforce these mappings.

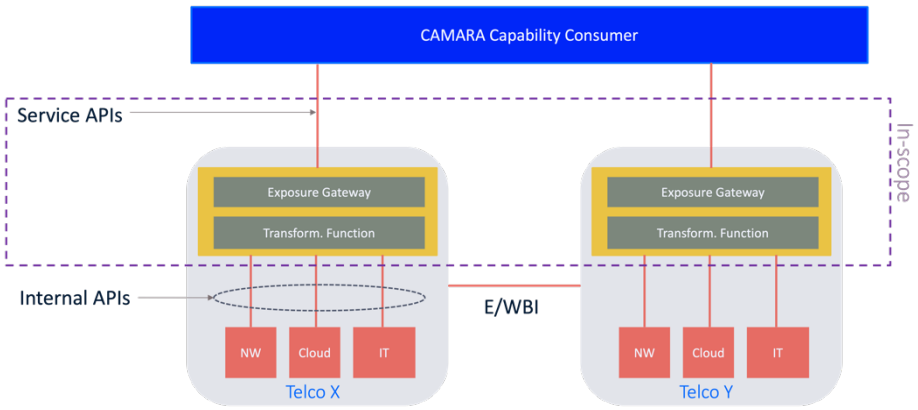

Figure A.1: CAMARA reference architecture

In this perspective, while the CAMARA project scope is more on the definition of Service APIs and related Transformation Function, the so-called "Internal APIs" are instead supposed to be provided by the various SDOs and fora, whose work can be enabled by the *Exposure Gateway*. The Internal APIs (lower part of the CAMARA reference architecture) can come from various domains, thus not only limited to expose capabilities from the core network:

- **Other network domains**: fixed access, access network, transport network (IP/MPLS, optical/DWDM and microwave backhauling) and data network (hosting value-added functions and services).
- **Cloud domain**, with IaaS/CaaS to host virtualized and cloud-native workloads, respectively. This domain is typically distributed across an operator's infrastructure footprint, following the edge-to-cloud continuum. For the exposure of capabilities from this domain, APIs such as those being

defined in ETSI NFV, ETSI MEC, EDGEAPP, Linux Foundation's CNCF or other de-facto solutions (e.g., Openstack, k8s) might be used.

- **IT domain**, covering tools used in OSS/BSS and NOC systems, taking care of network and service management aspects (FCAPS management, orchestration, topology & inventory management, etc.). For the exposure of capabilities from this domain, APIs such as those being defined in 3GPP, ETSI and TMF might be used.

All APIs (corresponding to internal APIs in CAMARA initiative) need to be abstracted into service APIs that are suitable for 3rd party consumption. For this purpose, CAMARA considers the **CAPIF framework** as a convenient reference for the implementation of the *Exposure Gateway*, as it is a standard solution, with wide acceptance at industry, and it is not tied only to 3GPP APIs (in fact, CAPIF can be used as *Exposure Gateway* solution for any API independent of their semantics).

In this perspective, many of API frameworks (including MEC service APIs available via Mp1 reference point) can be considered as OP:NBI enablers (or as "internal API", using the terminology from the CAMARA reference architecture). Figure A.2 below shows the principle of consuming any API framework from an API invoker (that can be an EAS, a MEC App or a generic edge application).

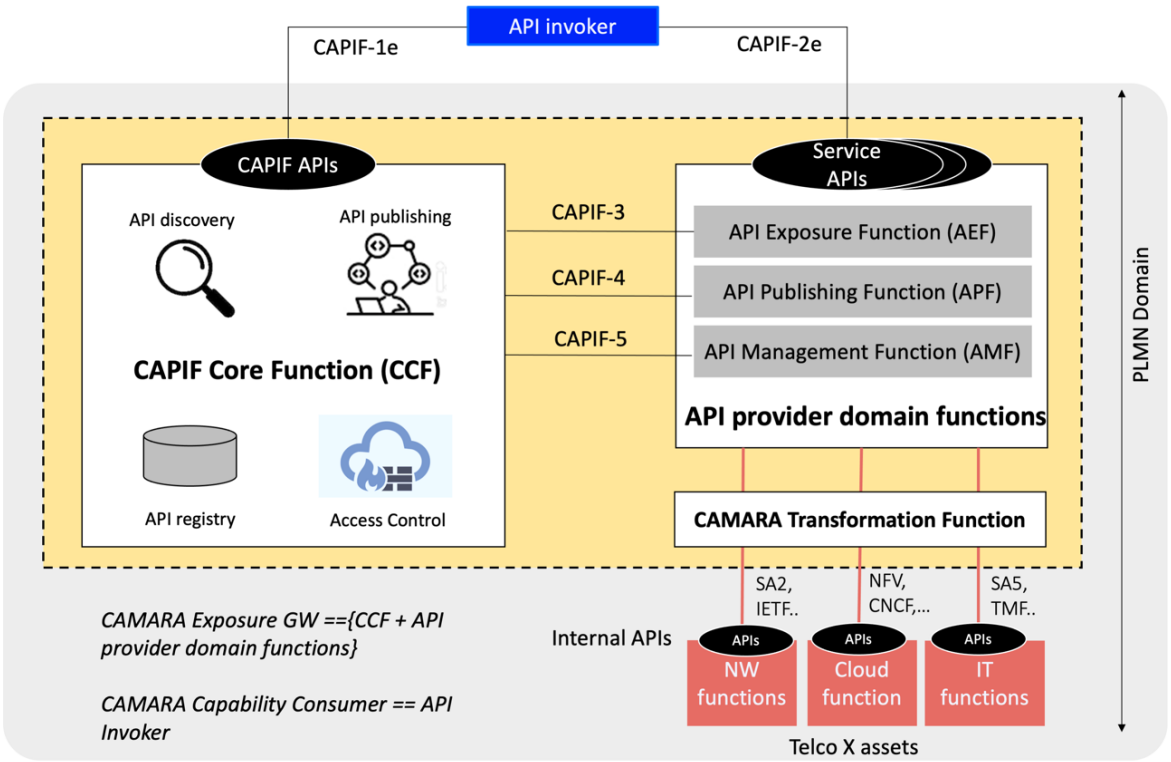

Figure A.2: Example of *Exposure Gateway* (Ref. CAMARA project [9])

It should also be noticed that other platforms (external to the PLMN domain) can be exploited, as they may offer API frameworks as well. For this purpose, CAPIF supports this kind of API exposure, i.e., where the API provider domain functions are running outside the PLMN domain. In these cases, the CAPIF framework can support EDGEAPP and other edge computing platforms even when they are outside of the PLMN trust

domain (e.g., ECSP domain). The figure A.3 below (in accordance with ETSI TS 123.558 [14], annex A, clause A.5) shows an implementation example of distributed CAPIF functions, where and EES (or also alternatively a MEC platform supporting CCF) can expose its APIs to 3rd party applications in various EDNs (Edge Data Networks) even outside that ECSP trust domain. So, in the most general case, the figure A.3 below appears to be considered as a very general case for CAPIF usage as a reference for the *Exposure Gateway* defined by CAMARA.

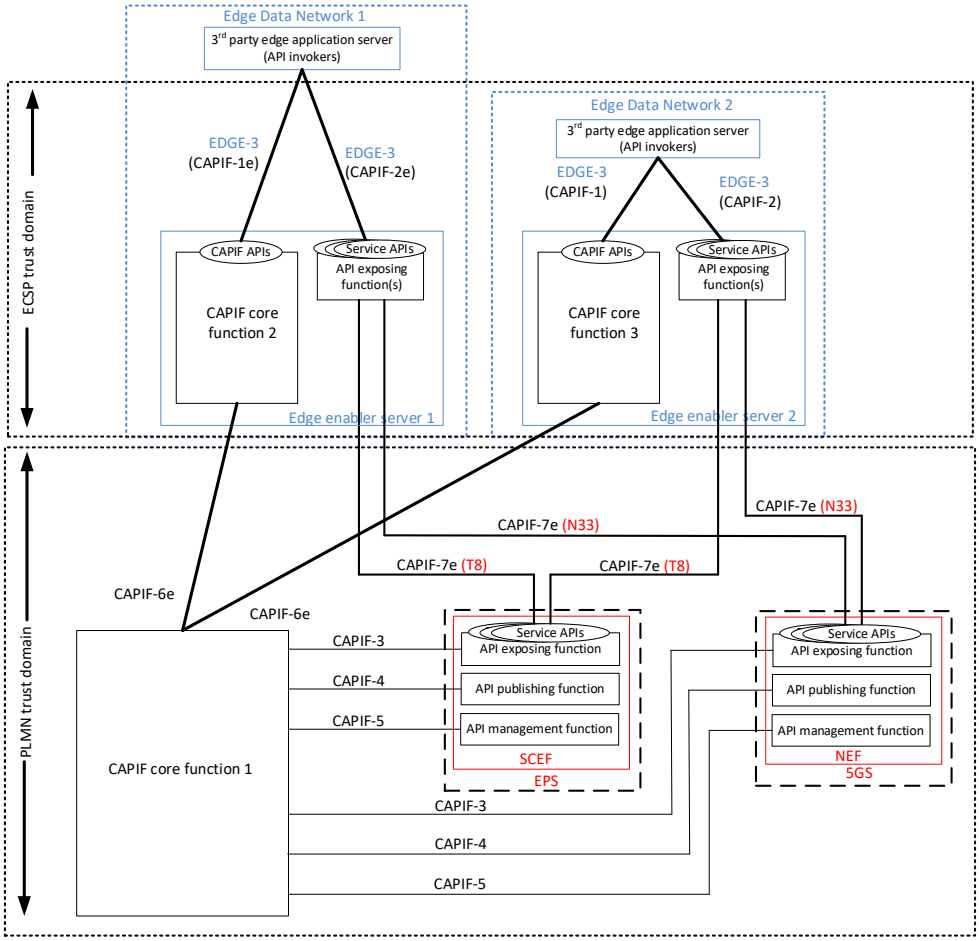

Figure A.3: Example of CAPIF as *Exposure Gateway* connected to external API frameworks (TS 23.558 [14])

It is important to note that the actual OP-NBI implementation will result from a joint effort between SDOs and open-source projects. The exposure of the API framework defined by ETSI MEC between MEC applications and MEC platforms (via Mp1 reference point) will be enabled by an *Exposure Gateway*. This is usually implemented by CAPIF, as widely accepted by the industry, and considered as good reference by CAMARA for integrating the Internal APIs to the upper layers toward the end customers (CAMARA API consumers [11]). On the ETSI MEC side, it was already clarified how CAPIF can be used for MEC 5G integration (ref. to GR MEC 031 [10]).

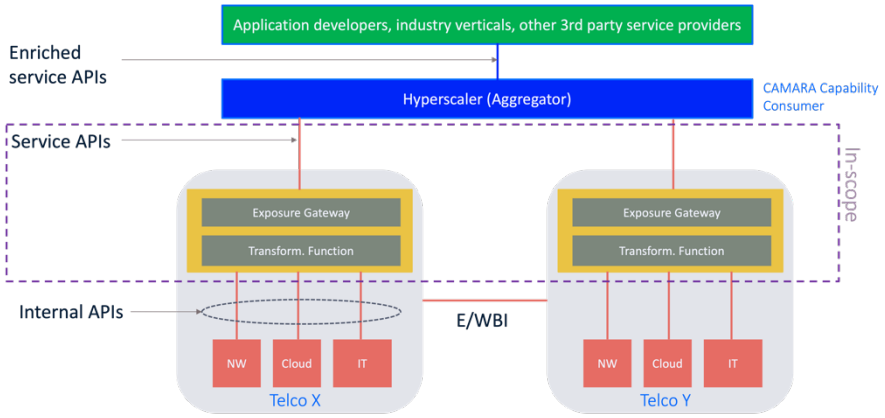

Figure A.4: Example of CAMARA deployment model

As an additional remark, the industry can also consume some "Enriched Service APIs" (see Figure A.4 just as an example of many possible deployment models) as a further level of abstraction on top of the Service APIs produced by CAMARA. This will address the need to further aggregate multiple marketplaces and connect to application developers and multiple customers and verticals. Thus, the definition of NBI in many environments may change and truly depends on the consumer that is considered in each case. Moreover, currently common companies in CAMARA and 3GPP SA5 are discussing about the separation of duties between SDOs and open source (ref. 3GPP S5-222286 [12]).

Lastly, in the context of MEC Federation, it appears clear that the endpoint for OP:NBI could not be terminated just by SDOs, rather needs to leverage the work done by open-source projects e.g. the CAMARA project and other stakeholders. In fact, the ultimate goal is to expose a set of APIs and functionalities to end-customers.

Annex B: References

[1] ETSI GS MEC 002 V2.2.1 (2022-01): "Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements", www.etsi.org/deliver/etsi_gs/MEC/001_099/002/02.02.01_60/gs_MEC002v020201p.pdf

[2] ETSI GR MEC 035 V3.1.1 (2021-06): "Multi-access Edge Computing (MEC); Study on Inter-MEC systems and MEC-Cloud systems coordination", https://www.etsi.org/deliver/etsi_gr/MEC/001_099/035/03.01.01_60/gr_mec035v030101p.pdf

[3] GSMA Permanent Reference Document, "Operator Platform Telco Edge Requirements", v2.0, Apr. 2022.
Online: https://www.gsma.com/futurenetworks/wp-content/uploads/2022/04/GSMA-Operator-Platform-Telco-Edge-Requirements-2022-v2.0.pdf

[4] ETSI GS MEC 040: "Multi-access Edge Computing (MEC); Federation Enablement APIs", Drafts available at MEC Open Area: https://docbox.etsi.org/isg/mec/open (Retrieved May 2022)

[5] ETSI GS MEC 003 V3.1.1 (2022-03): "Multi-access Edge Computing (MEC); Framework and Reference Architecture"
www.etsi.org/deliver/etsi_gs/MEC/001_099/003/03.01.01_60/gs_MEC003v030101p.pdf

[6] GSMA Whitepaper, "Operator Platform Concept", v1.0, Jan. 2020.
Online: https://www.gsma.com/futurenetworks/resources/operator-platform-concept-whitepaper/

[7] ETSI White paper #36 "Harmonizing standards for edge computing", July 2020.
https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_wp36_Harmonizing-standards-for-edge-computing.pdf

[8] GSMA OPAG joint workshop with ETSI MEC and 3GPP, online meeting, 21/01/2022, workshop recording: https://www.gsma.com/futurenetworks/resources/operator-platform-api-group-with-3gpp-etsi-workshop-recording/

[9] CNFC project CAMARA,
Online: https://github.com/camaraproject (Retrieved May 2020.)

[10] ETSI GR MEC 031 V2.1.1 (2020-10), Multi-access Edge Computing (MEC), "MEC 5G Integration", www.etsi.org/deliver/etsi_gr/MEC/001_099/031/02.01.01_60/gr_MEC031v020101p.pdf

[11] LF CNCF, CAMARA project: "API Exposure Reference Solution",
Online:
https://github.com/camaraproject/WorkingGroups/blob/main/Commonalities/documentation/Deliverables/API-exposure-reference-solution.docx (Retrieved April 2020)

[12] S6-220894 EAS discovery in Edge Node sharing scenario, March 2020, Online:
https://www.3gpp.org/ftp/tsg_sa/WG6_MissionCritical/TSGS6_048-e/docs/S6-220894.zip

[13] MEC Security: Status of standards support and future evolutions, 1st edition, May 2021

https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_WP_46-_MEC_security.pdf

[14] ETSI TS 123.558 V17.3.0 (2022-05), “5G; Architecture for enabling Edge Applications”, https://www.etsi.org/deliver/etsi_ts/123500_123599/123558/17.03.00_60/ts_123558v170300p.pdf

[15] ENISA-5G supplement – Guidelines on Security Measures under EECC

[16] GSMA White Paper - Telco Edge Cloud: Edge Service Description and Commercial Principles, October 2020 https://www.gsma.com/futurenetworks/wp-content/uploads/2020/10/GSMA-Telco-Edge-Service-Description-Commercial-Principles-Oct-2020.pdf

Annex C: Abbreviations

3GPP	3rd generation partnership project
5GAA	5G automotive association
AP	Application provider
API	Application programming interface
AR	Augmented reality
CI/CD	Continuous integration/ Continuous delivery
CLI	Command line interface
CNF	Carrier neutral facility
CR	Cloud resources
E/WBI	East and west bound interface
GR	Group report
GRX	GPRS roaming exchange
GS	Group specification
GSMA	Global system for mobile communications association
IoT	Internet of things
IPX	IP exchange
LCM	Lifecycle management
LFE	Linux foundation edge
MEC	Multi-access edge computing
MEF	MEC federator
MEFB	MEC federation broker
MEFM	MEC federation manager
MEO	MEC orchestrator
MEP	MEC platform
MEPM	MEC platform manager
MFIP	MEC federation interconnection provider
NBI	North bound interface
NR	Network resources
OPEX	Operational expense
OPG	Operator platform group
OSS	Operation support system
PCEI	Public cloud edge interface
PRD	Permanent reference document
SA	Service and system aspects
SBI	South bound interface
SDO	Standards development organization
V2X	Vehicle to everything
VIM	Virtualization infrastructure manager
VLAN	Virtual local area network
VR	Virtual reality
VxLAN	Virtual extensible local area network

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