

ETSI MEC Overview

Standardization update on Multi-access Edge Computing

Dario Sabella

VP at xFlow Research, ETSI MEC Chair

December 2024



ETSI MEC: Enabling *Edge* through *Standardization*



Foundation for Edge Computing – Fully standardized solution to enable applications in distributed cloud created by ETSI MEC + 3GPP



Watch the new video on MEC

<https://www.youtube.com/watch?v=crnPWql-0oo>



Application Life Cycle Management

RESTful based APIs for Runtime Application Services



MEC: Multi-access Edge Computing
Cloud Computing at the Edge of the network.

ETSI: The Standards People

producing globally applicable standards for ICT-enabled systems

ETSI ISG MEC

ISG: Industry Specification Group

open to all of industry, regardless of ETSI membership and focused on all industry needs



- **Continuously growing MEC membership:** 124 (updated Dec 2022); e.g. in June 2021 it was 114
- **Diverse ecosystem:** Operators - Technology Providers - IT players - Application developers - Startups - ...



Renewed webpage: ISG MEC Leadership Team, LS officers for Vertical Industries and MEC Support Team: <https://portal.etsi.org/TB-SiteMap/MEC/MEC-Leaders-and-Support-Team>

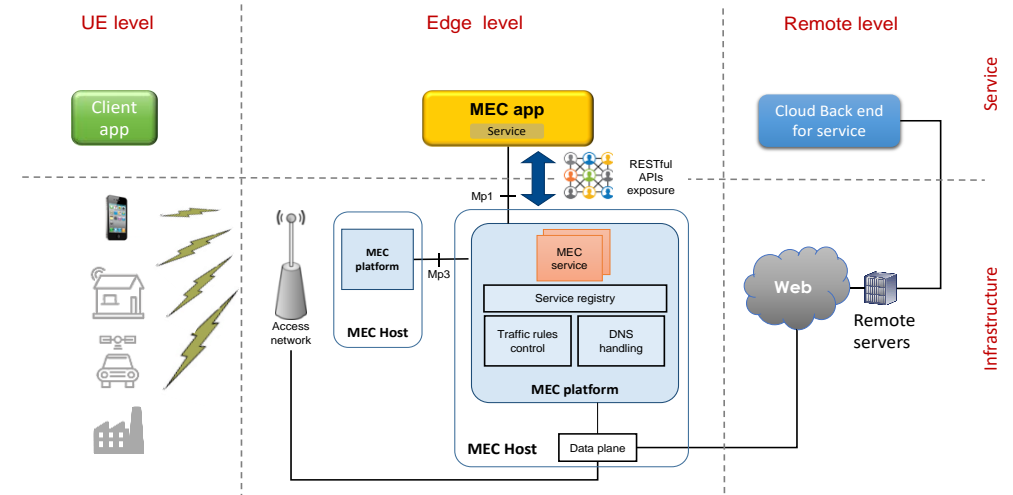
ETSI MEC – Foundation for Edge Computing



MEC offers to application developers and content providers cloud-computing capabilities and an IT service environment at the edge of the network

Basic principles:

- **Open standard** → allowing multiple implementations and ensuring interoperability
- MEC exploiting ETSI **NFV framework** and definitions → enabling MEC in NFV deployments
- Alignment with **3GPP** based on fruitful collaboration of common member companies → enabling MEC in 5G
- **Access-agnostic** nature (as per MEC acronym - Multi-access Edge Computing) → enabling other accesses
- Addressing the needs of a **wide ecosystem** → enable multiple verticals (e.g. automotive), federations



MEC is focused on *existential* questions of applications “on the edge”

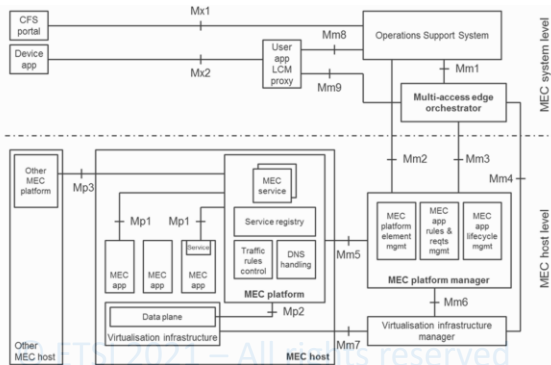
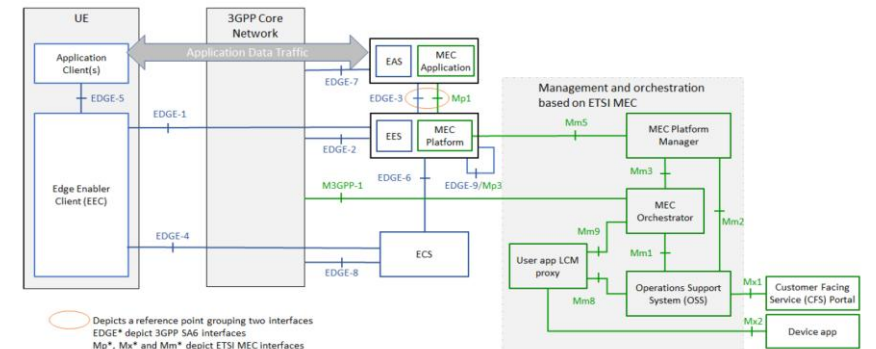
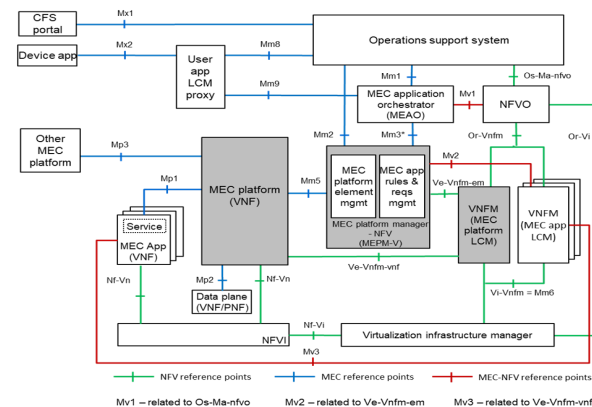
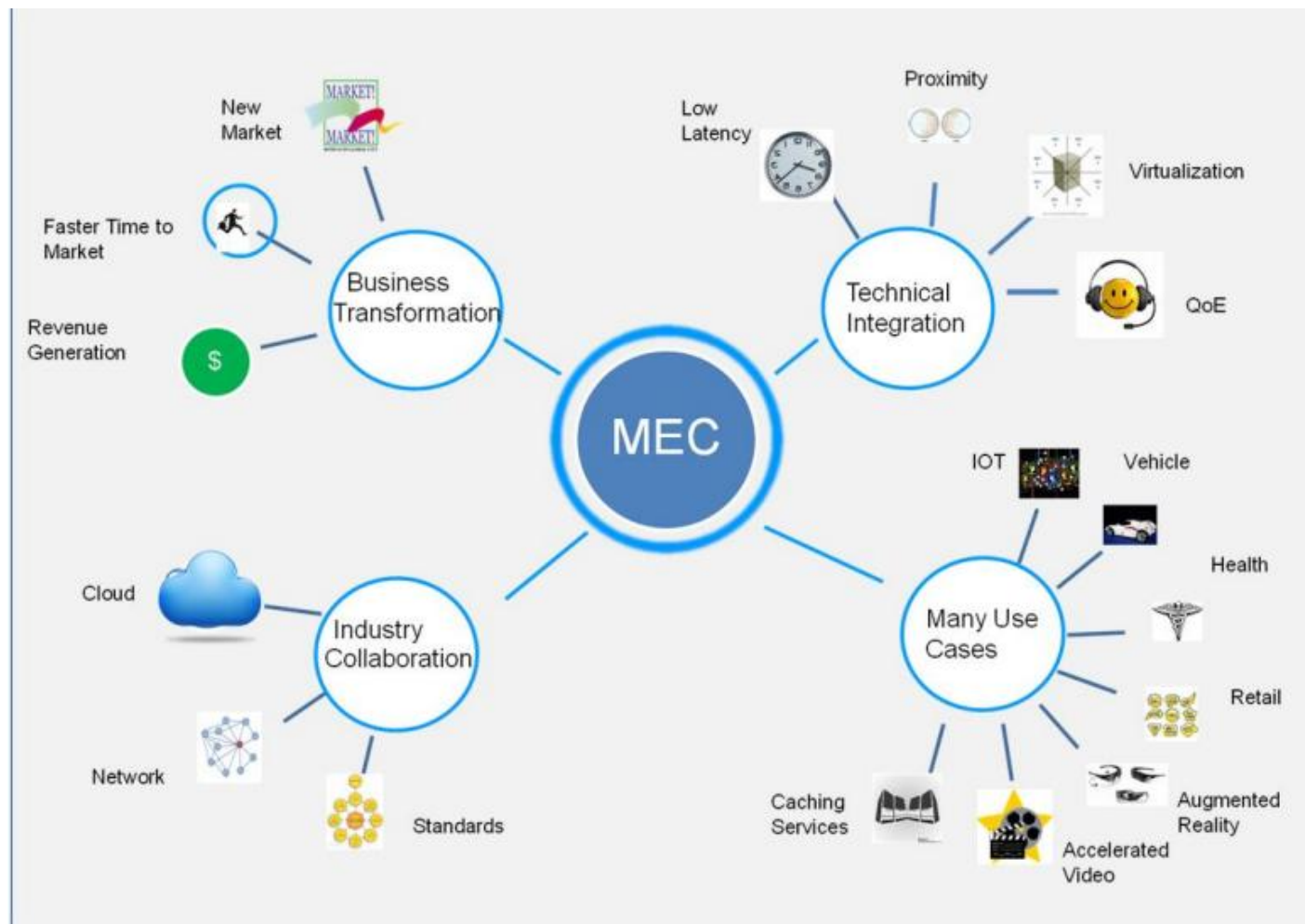


Figure 6-1: Multi-access edge system reference architecture



○ Depicts a reference point grouping two interfaces
 EDGE* depict 3GPP SAG interfaces
 Mp*, Mx* and Mm* depict ETSI MEC interfaces

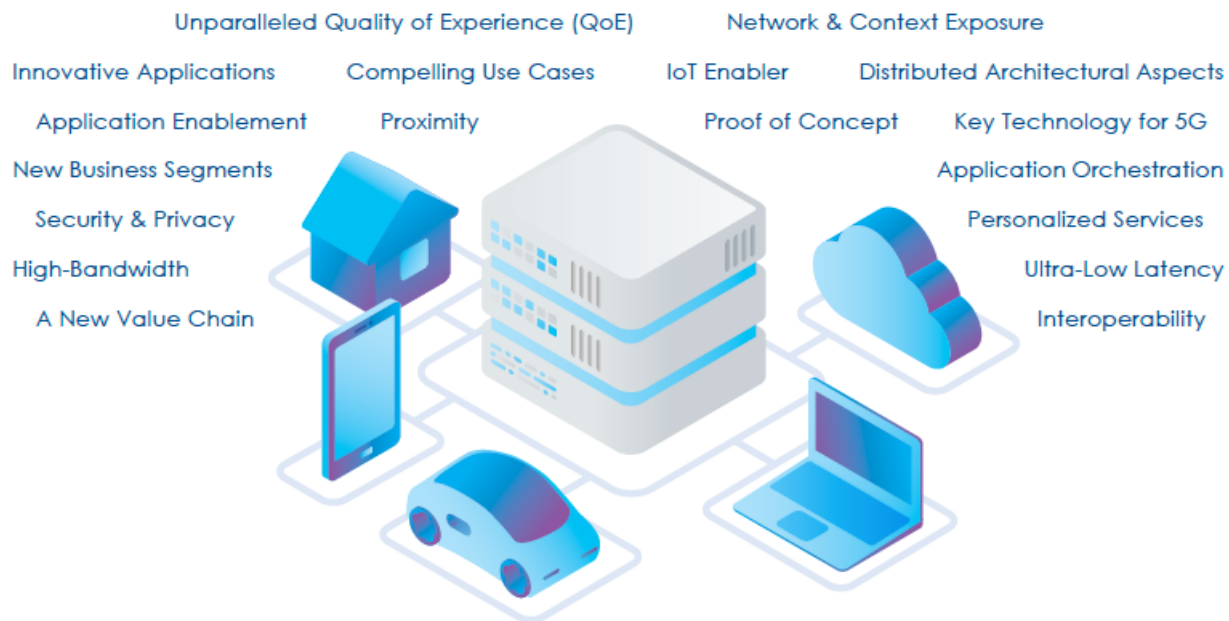
MEC supports many 5G use cases and market segments



More info at this ETSI White Paper on MEC

https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

MEC and vertical industries



MEC is a key enabler for many vertical market segments.

Several (specialized) use cases driven by different verticals:

- automotive,
- industrial automation,
- VR/AR,
- Videostreaming,
- Gaming,
- e-health,
- Smart Cities,
- Etc ...

Edge Exposure Day (Sept 18th, 2022, Kfar Saba, Israel) supported by ETSI



Edge Discovery Events



Attendance from diverse people, e.g. local companies, MEC delegates, repr from 5GAA and AECC, ...

Edge Discovery Events: meeting vertical industries

A series of live panels with relevant experts from the various vertical market segments.

[https://mecwiki.etsi.org/index.php?title=Edge Discovery Events](https://mecwiki.etsi.org/index.php?title=Edge_Discovery_Events)



First event on **Drones** vertical:

- 70+ people registered
- 6 keynotes and 1 demo
- Final panel discussion

MEC meets **Spatial Computing and Gaming**

- C-level keynotes and moderated panel
- Remote: online event (bridge and material online!)
- Participation free of charge



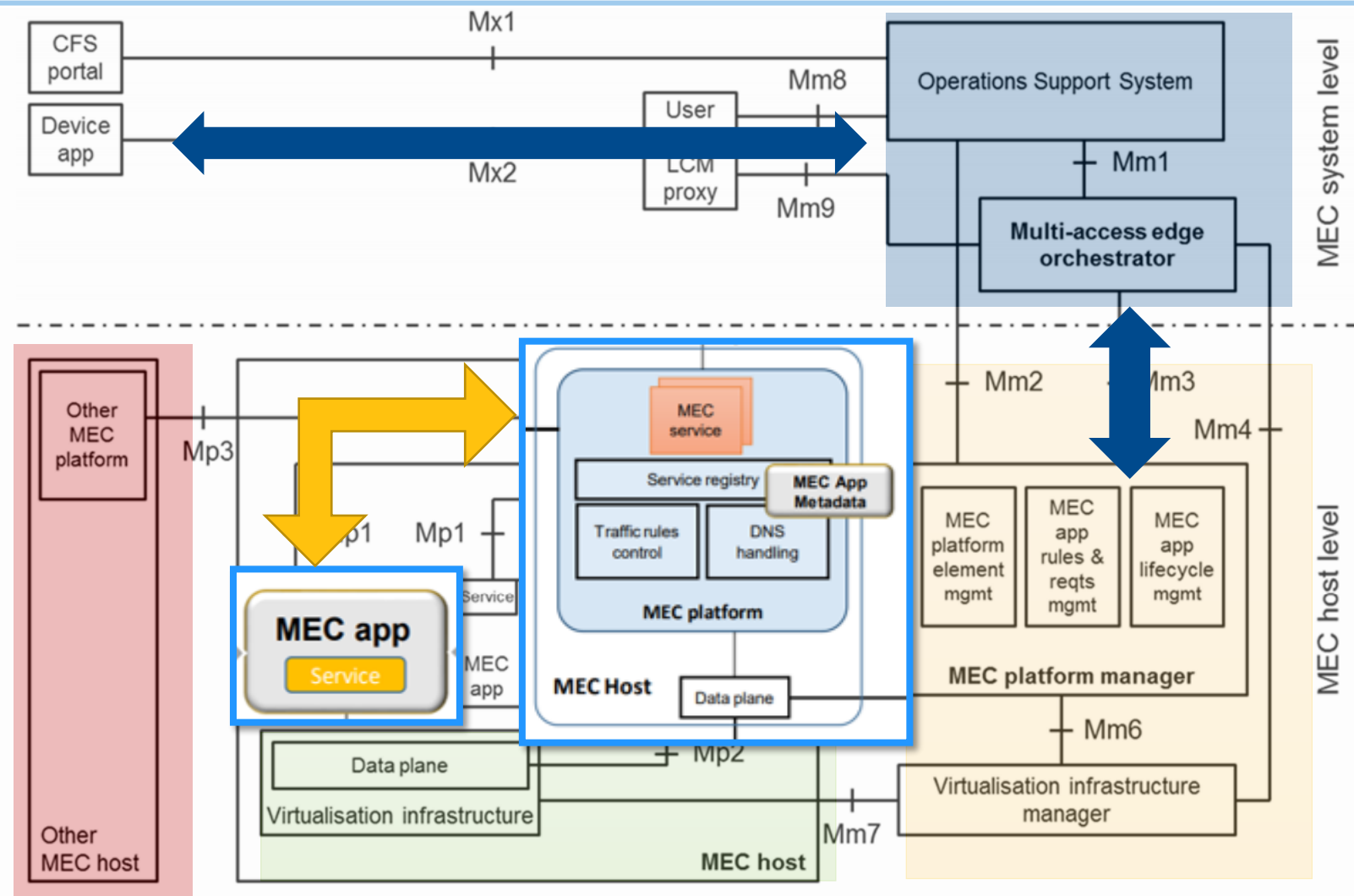
Stay tuned
for next
Edge Discovery
Events!



MEC reference architecture

- APIs
- Application Support
 - Service Management
 - Radio Network Information
 - Location
 - UE Identity
 - Bandwidth Management
 - Fixed Access Information
 - WLAN Information
 - V2X Information Service

- Application Package lifecycle and operation granting
- Device application interface

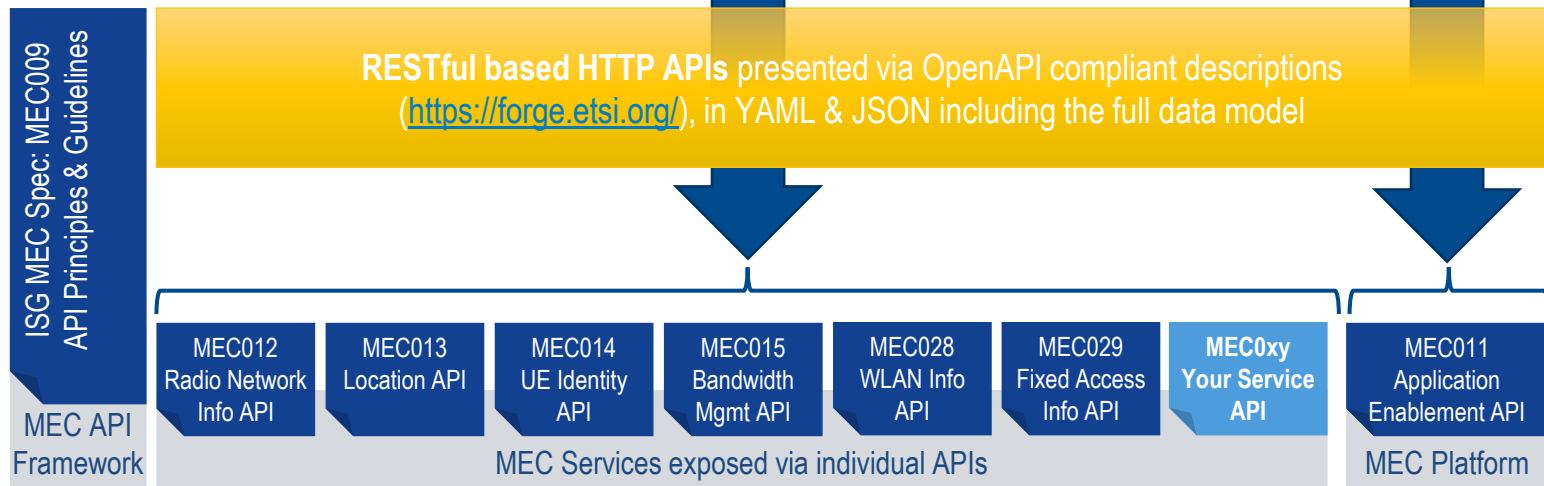


Enabling Global Application Portability



MEC Application Development Community

Interaction & Information Exposure



- ✓ Simple to use, well documented APIs, published with OpenAPI Framework
- ✓ Create innovative applications quickly and easily, reducing time-to-revenue
- ✓ New APIs (compliant with the MEC API principles) can be added
- ✓ Increase the Total Addressable Market (TAM)



MEC Standard work: from Phase 1 to Phase 4



- **Key overall specification**
 - Technical Requirements (MEC 002)
 - Framework and Ref. Archit. (MEC 003)
 - MEC PoC Process (MEC-IEG 005)
 - API Framework (MEC 009)
- **IaaS Management APIs**
 - Platform mgmt. (MEC 010-1)
 - Application mgmt. (MEC 010-2)
 - Device-triggered LCM operations (MEC 016)
- **PaaS Service Exposure**
 - Required Platform Svcs / App. Enablement (MEC 011)
 - Service APIs (MEC 012, 013, 014, 015)
- **Key Studies for Future Work**
 - Study on MEC in NFV (MEC 017)
 - Study on Mobility Support (MEC 018)
- **Evolution of Phase 1 and closing open items**
 - Application Mobility (MEC 021)
 - Lawful Intercept (MEC 026)
- **Addressing key Industry Segments**
 - V2X (MEC 022 – published; MEC 030)
 - Industrial Automation, VR/AR
- **Key use-cases and new requirement**
 - Network Slicing (MEC 024)
 - Container Support (MEC 027)
- **Normative work for integration with NFV**
 - Incorporate in v2 of existing specifications as needed
- **From “Mobile” to “Multi-Access”**
 - Wi-Fi (MEC 028)
 - Fixed Access (MEC 029)
- **MEC integration in 5G networks (MEC 031)**
- **Developer community engagement**
 - API publication through ETSI Forge (overleaf)
 - Hackathons, MEC Deployment Trials
- **Testing and Compliance (MEC-DEC 025; multipart spec MEC-DEC 032-x)**
- **Full Phase 3 work (with some pre-Phase 4).**
- **MEC as heterogeneous clouds**
 - Expanding traditional cloud and NFV LCM approaches
 - Inter-MEC systems and MEC-Cloud systems coordination: “MEC Federation” (MEC 035, MEC040)
 - Mobile/intermittently connected and resource constrained devices (MEC 036), MEC IoT API (MEC 033)
- **MEC Security (GR MEC 041)**
- **MEC deployments, e.g. in Park enterprises (MEC 038)**
- **MEC Application Slices (MEC 044)**
- **Continuing emphasis on enabling developers**
 - App Package Format and Descriptor (MEC 037)
 - API Serialization
 - MEC Sandbox development
 - Testing and compliance
- **Continue to define services that meet industry demand (e.g., Abstracted Network Info Exposure, MEC 043)**
- **Maintain and enhance existing APIs (MEC 013)**
- **Evolution of Phase 3 and closing open items, including maintenance and enhance existing APIs**
- **Addressing key Industry Segments**
 - Listen to verticals via Edge Discovery Days
 - Abstracted Network Info Exposure MEC 043
 - Distributed Edge Network MEC 047
 - Exploiting Edge Computing Resources MEC 059
- **Key use-cases, requirements & arch**
 - MEC 002, MEC 003
- **Normative work on MEC Security**
 - MEC architecture (MEC 003), (API GW for Client Apps (MEC 060), Support for Security Monitoring and Management (MEC 062)
- **Continuing emphasis on enabling developers**
 - Testing and compliance
 - API-driven MEC Sandbox and Edge Native Connector activities (STF678)
- **Collaboration with open-source communities (e.g., TeraFlowSDN, OpenCAPIF, CAMARA)**
- **STF 685 ESTIMED: Enabling Standardized IoT deployments in MEC Environments for advanced systems (OneM2M & SmartM2M)**
 - 9 GR/GS, 4 PoC, Testing
- **AI/ML in MEC (MEC 061)**

2015 ETSI MEC phase 1 (Completed)

2018 ETSI MEC phase 2 (Completed)

2021 ETSI MEC phase 3 (Completed)

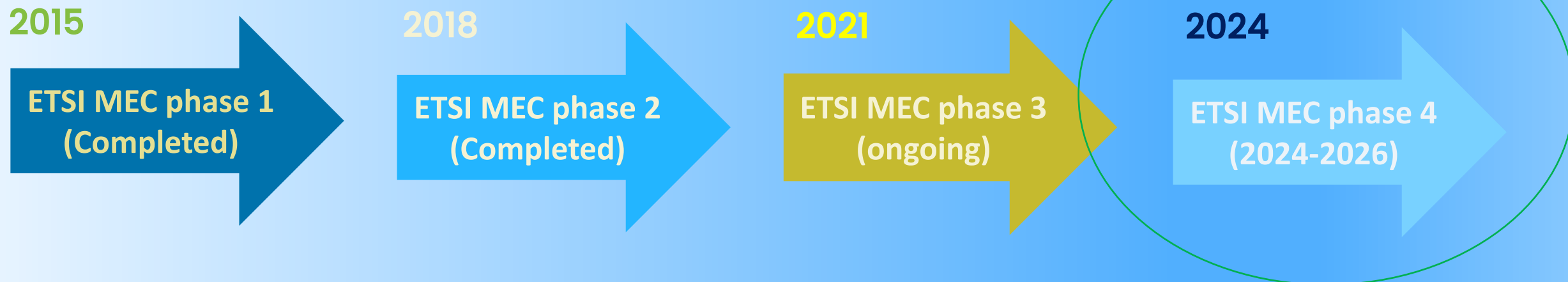
2024 ETSI MEC phase 4 (Started)

MEC – current Work Items (rapporteurs)

- MEC 002 - Use Cases and Requirements (Qin Zeng, China Telecom)
- MEC 003 - Framework and Reference Architecture (Alice Li, Huawei)
- MEC 009 - General principles, patterns and common aspects of MEC Service APIs (Uwe Rauschenbach, Nokia)
- MEC 010-2 - MEC Management; Part 2: Application lifecycle, rules and requirements management (Hongmei Zhu, China Telecom)
- MEC 011 - Edge Platform Application Enablement (Alice Li, Huawei)
- MEC0 16 - Device application interface (Jaemond Reyes, MITRE)
- MEC 036 - Constrained Device (Debashish Purkayastha, InterDigital)
- MEC 040 v3 - Federation enablement APIs (Yann Garcia, FSCOM)
- MEC 043 - Abstracted Radio Network Information for Industries (Uwe Rauschenbach, Nokia)
- MEC047 - Distributed Edge Network (Hongmei Zhu, China Telecom)
- MEC059 - Exploiting Edge Computing Resources (Shoufeng Wang, Asia Info)
- MEC060 - API Gateway for Client Applications (Michaela Vanderveen, MITRE)
- MEC061 - Artificial Intelligence / Machine Learning in MEC (Xiaohui Shi, China Mobile)
- MEC062 - Support for Security Monitoring and Management (Jaemond Reyes, MITRE)
- MEC DEC32-2 v3 - API Conformance Test Specification; Part 2: Test Purposes (TP) (Walter Featherstone, Apple) - T043
- MEC DEC32-3 v3 - API Conformance Test Specification; Part 3: Abstract Test Suite (ATS) (Walter Featherstone, Apple) - T043
- MEC DEC49 – Edge Native Connector (Walter Featherstone, Apple) – STF 678

MEC toward 6G

- CAVEAT: nobody knows yet *what 6G will be!* So, we cannot claim (still) what MEC in 6G will be, of course.
- On the other hand, MEC evolution and vision can be shaped (in a pragmatic way).
- The newly approved ToR#6 of MEC (available [here](#)) is related to the period 2025-2026.
 - Thus, it will cover entirely the scope of MEC Phase 4 (2024-2026).
- So, at least, we could draw (from the ToR#6) some differences between MEC Phase 3 (2021-2023) and **MEC Phase 4** (2024-2026).



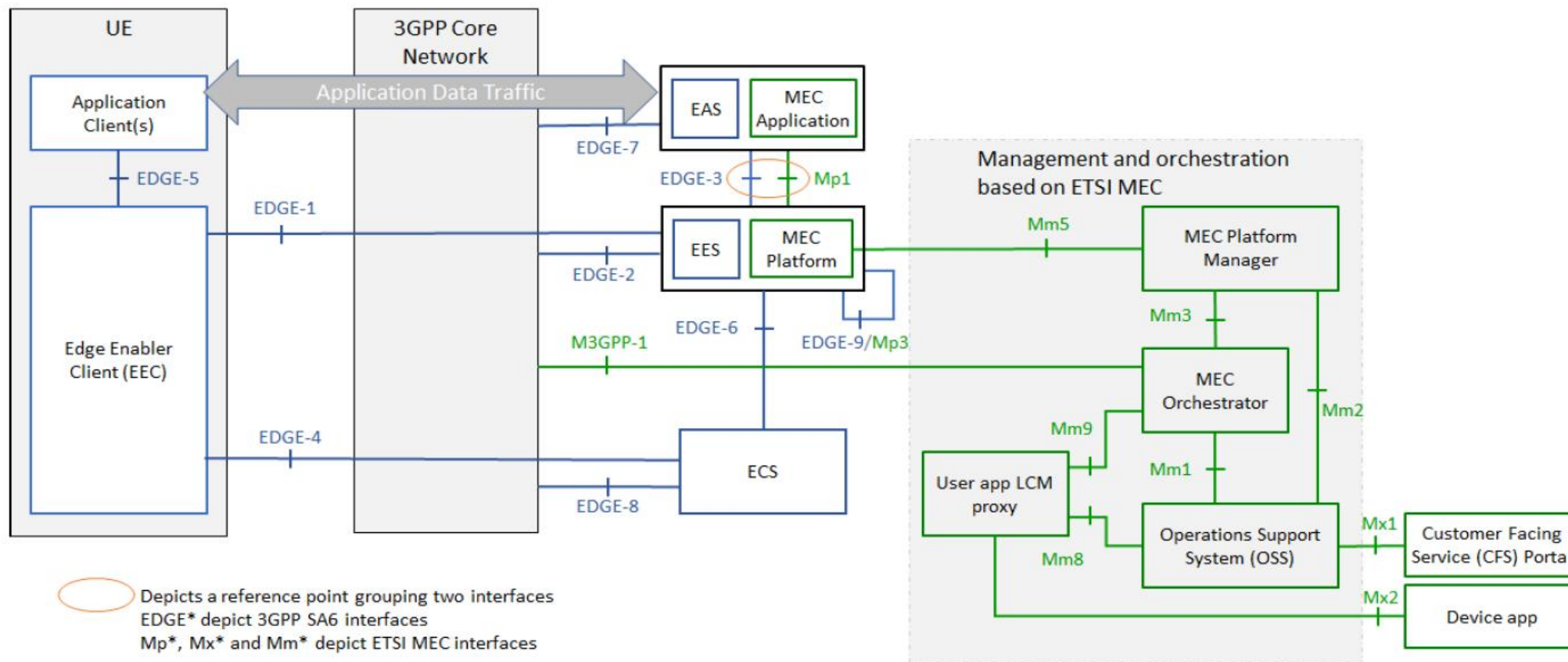
MEC *toward* 6G : running MEC Phase 4

- CAVEAT: nobody knows yet *what 6G will be!* So, we cannot claim (still) what MEC in 6G will be, of course.
- On the other hand, MEC evolution and vision can be shaped (in a pragmatic way).
- The newly approved ToR#6 of MEC (available [here](#)) is related to the period 2025-2026.
 - Thus, it will cover entirely the scope of MEC Phase 4 (2024-2026).
- So, at least, we could draw (from the ToR#6) some differences between MEC Phase 3 (2021-2023) and **MEC Phase 4** (2024-2026).

In a nutshell, a transition from MEC Phase 3 to MEC Phase 4 can lead to:

- *more consolidated work on MEC Federation, including exposure of resources managed by multiple operators, e.g. addressing multi-domain and multi-tenancy slicing and MEC support for application slicing;*
- *MEC architectural/service updates needed to support cloud native communication systems and edge native design for app developers (also with container support)*
- *introduction of proper normative work to improve security and privacy in MEC systems*
- *Further promotion of MEC as an attractive development environment for the industry by creating “developer-friendly environments” (e.g. portals, SDK) that enable convergence of key industry ecosystem, e.g. app developers and operators*
- *Further outreach efforts, e.g. Hackathons/trials in collab with open source communities, industry groups (e.g. 5GAA, etc..)*

MEC harmonized architecture with SA6 EDGEAPP



- Joint **white paper** (*) from both ETSI and 3GPP officials
- 3GPP TS **23.558** “Architecture for enabling Edge Applications; (Release 17)” v1.1.0, Oct. 2021 (informative Annex C)
- Alignment between 3GPP and ETSI MEC was in scope of eEDGEAPP in 3GPP SA6 (ref. [S6-211858](#)).

STF: Edge Native Connector

- Special Task Force (STF) under ETSI
 - <https://portal.etsi.org/xdfs/#/xTF/678/>
- Edge Native applications are designed to leverage the full potential of edge computing
- Edge service discovery is a core function of the MEC Platform, enabled via the Mp1 reference point for MEC applications, as per ETSI MEC Architecture.
- The **Edge Native Connector** STF will *extend the MEC Sandbox* by enabling the integration of APIs from various sources (e.g., CAMARA APIs, 6G-SANDBOX (SNS JU)).
 - *Provides an API-driven Sandbox for Application developers.*
 - *Supports CAPIF APIs for platform interoperability.*
 - *Supports MEC Federation APIs to enable multi-platform and multi-host interoperability*



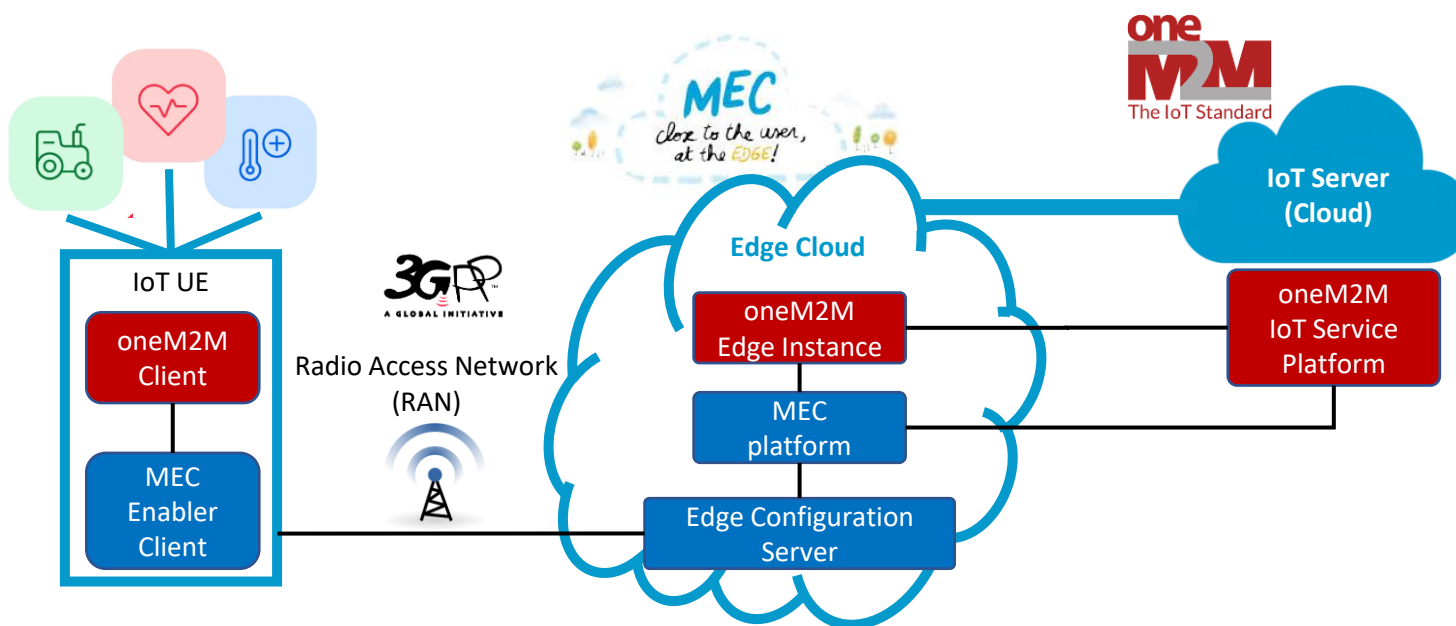
MEC Sandbox Version 1.10 includes MEC profile for CAPIF and Federation APIs



Welcome to ETSI MEC Sandbox portal

Enabling Multi-access Edge Computing in IoT: how to deploy ETSI MEC and oneM2M

- MEC interworking with oneM2M is possible (*)
- Further standardization work might be needed
- Future activities planned (e.g. EISMEDIA project in 2025)

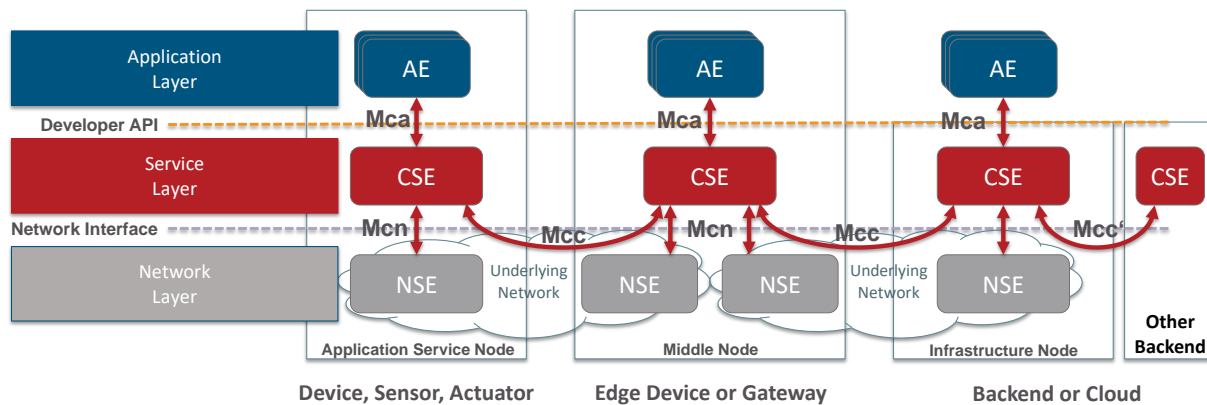


NOTE: architectural interworking between ETSI MEC and oneM2M is made possible by seeing the CSE and AE functional elements of oneM2M as particular instances of MEC services and applications from the point of ETSI MEC system



(*) <https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP59-Enabling-Multi-access-Edge-Computing-in-iot.pdf>

oneM2M architecture and MEC deployment options



- Possible mapping:**
- **CSE** in oneM2M architecture can be represented as a **MEC Service** and/or as a service-producing MEC App instance. This service would be exposed by the MEC platform to be connected to (authorized) consumer Application Entities (AE).
 - Similarly, **AE** in oneM2M architecture can be seen as a **MEC App instance** by ETSI MEC system.

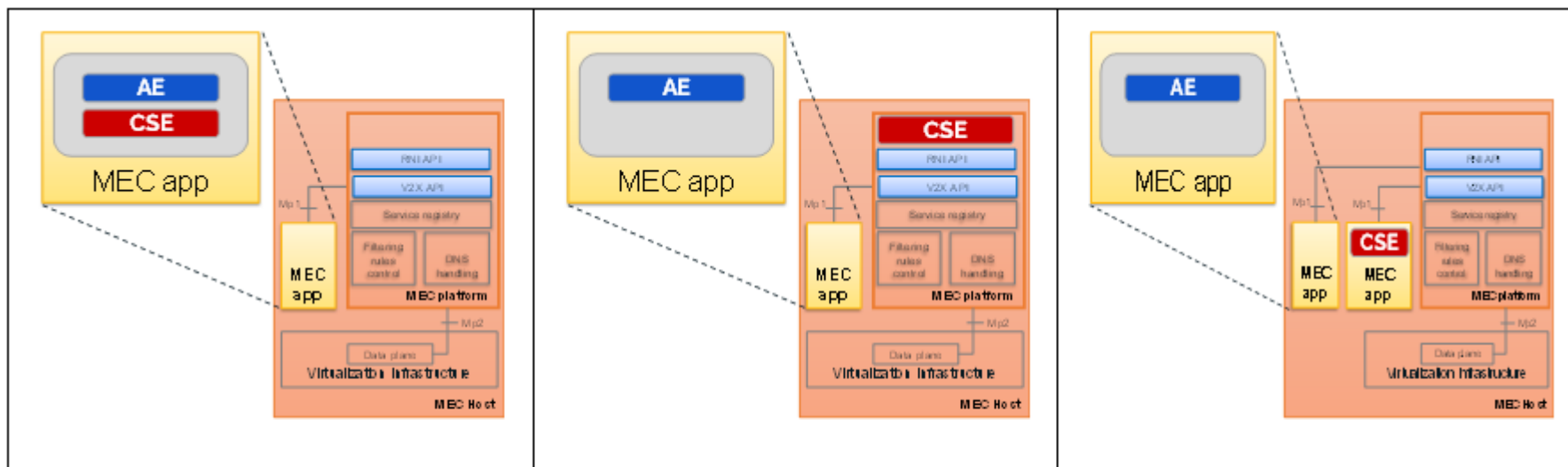
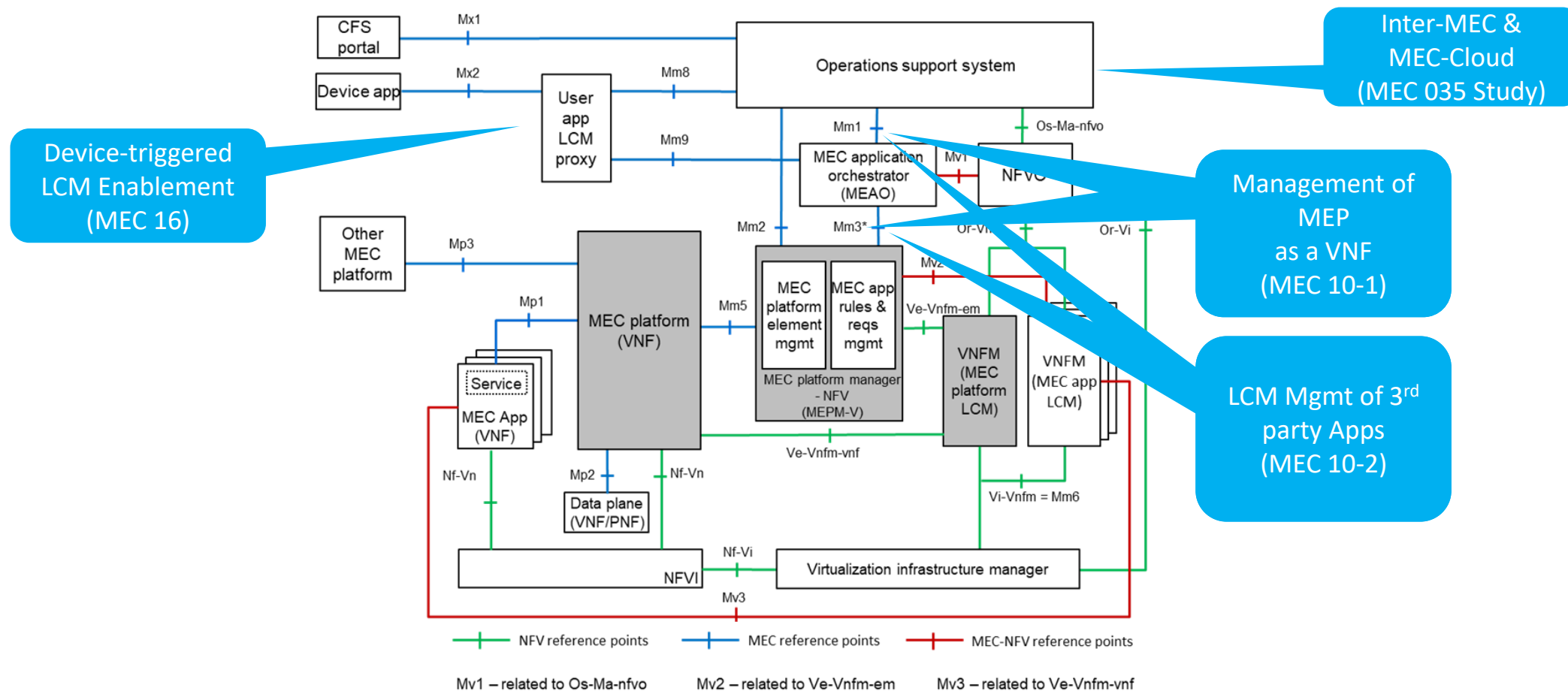


Figure 4-2: deployment options of CSE and AE in MEC systems:
 (left) both AE and CSE as a single MEC App instance; (center) CSE as a service in the MEC platform;
 (right) CSE implemented as a service-producing MEC App instance (CSFs)

A key part of ETSI Network Automation Standards



MEC White Papers: A view of a whole picture

Standards are necessarily tools, not solutions

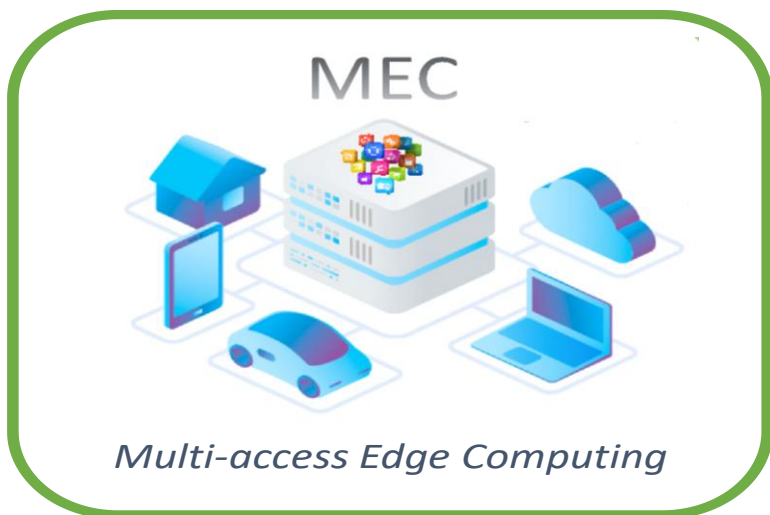
- ✓ Enable interoperability
- ✓ Support a broad range of use cases and system architecture
- ✓ Address only a specific part of the whole picture

MEC White Papers: how we help industry see the whole picture

- ✓ Harmonizing Standards for Edge Computing: a synergized architecture leveraging ETSI MEC and 3GPP
https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_wp36_Harmonizing-standards-for-edge-computing.pdf
- ✓ MEC in an Enterprise Setting
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp30_MEC_Enterprise_FINAL.pdf
- ✓ MEC in 5G Networks: http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf
- ✓ MEC deployment in 4G and towards 5G:
http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf
- ✓ CRAN and MEC: A Perfect Pairing:
http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp23_MEC_and_CRAN_ed1_FINAL.pdf
- ✓ Developing SW for MEC (2nd Ed.)
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp20ed2_MEC_SoftwareDevelopment.pdf
- ✓ ETSI White Paper 49 – MEC Federation: deployment considerations, 1st edition, June 2022
https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_WP_49_MEC-Federation-Deployment-considerations.pdf



ETSI White paper on MEC Federation: deployment considerations



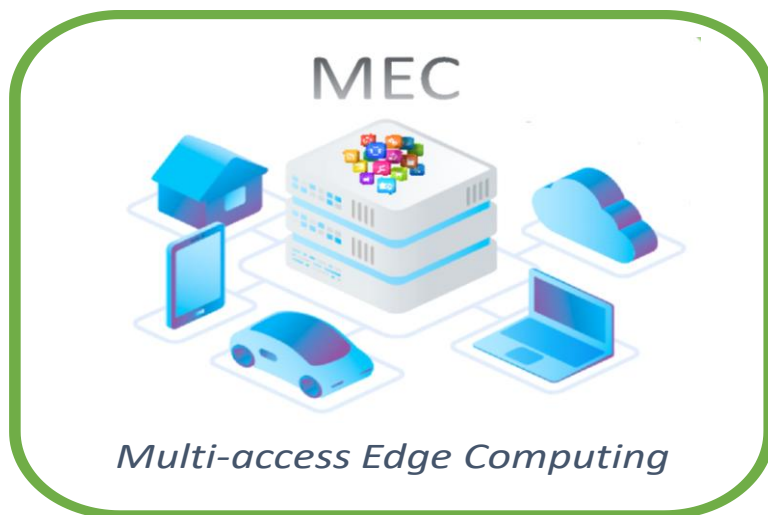
- This White Paper focuses on the deployment options related to MEC federation, especially from an architectural point of view, and with a key focus on ETSI MEC implementations, but also with the aim to provide an open approach considering other standards and technologies.
- For this purpose, the White 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.

Key considerations in the 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.
- Provide insights for edge stakeholders, and all readers in general, to better understand how to choose the appropriate deployment options



MEC security: status of standards support and future evolutions



- MEC scenarios are characterized by a complex multi-vendor, multi-supplier, multi-set of equipment including both HW and SW devices. Given this overall level of **system heterogeneity**, areas of security, trust, and privacy are key topics for the edge environments.
- In that perspective, MEC stakeholders should pay attention to the vulnerability and integrity of any third-party elements, and a truly **end-to-end approach to MEC security** needs to consider not only the current standards in ETSI ISG MEC, but also the other available standards that can be applicable to the MEC environment.

- ETSI white paper, authored by many experts (in the domain of edge computing, security and involved in various standard bodies), provides an overview of **ETSI MEC standards** and current support for security, which is also complemented by a description of other relevant standards in the domain (e.g. ETSI TC CYBER, ETSI ISG NFV, 3GPP SA3) and **cybersecurity regulation** potentially applicable to edge computing.

- <https://www.etsi.org/newsroom/press-releases/2123-2022-09-etsi-publishes-a-new-white-paper-on-multi-access-edge-computing-security>

© ETSI 2021 – All rights reserved



**Second edition
published Sept 2022**

MEC Support for Edge Native Design: an application developer perspective



- This White Paper provides an overview and vision about the Edge Native approach, as a natural evolution of Cloud Native. Edge Native was first introduced in 2020 by the Linux Foundation's Open Glossary of Edge Computing
- It explains in detail the concept of “Edge Native”, describes what Edge Native means for edge developers to build their applications and introduces how ETSI ISG MEC and other organizations support this Edge Native design paradigm. In particular, the White Paper guides developers in the principles and specific requirements of edge computing and how they can combine them with the modern architectural approach introduced by Cloud Native. It also gives insight into the general technical community interested in ETSI MEC solutions or Edge Native application design concepts.
- The authors of the White Paper conclude that the ETSI MEC standard (synergized with 3GPP specifications) can offer a footprint for interoperability, API basic design principles to ensure universal adoption, and possibly also some guidelines for API abstraction, complementing the work of open-source projects. Therefore, to fully exploit edge capabilities and for the adoption of edge native design principles from application development communities, joint efforts from open source and standards will be needed.
- https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP55-MEC_support_towards_Edge_native.pdf

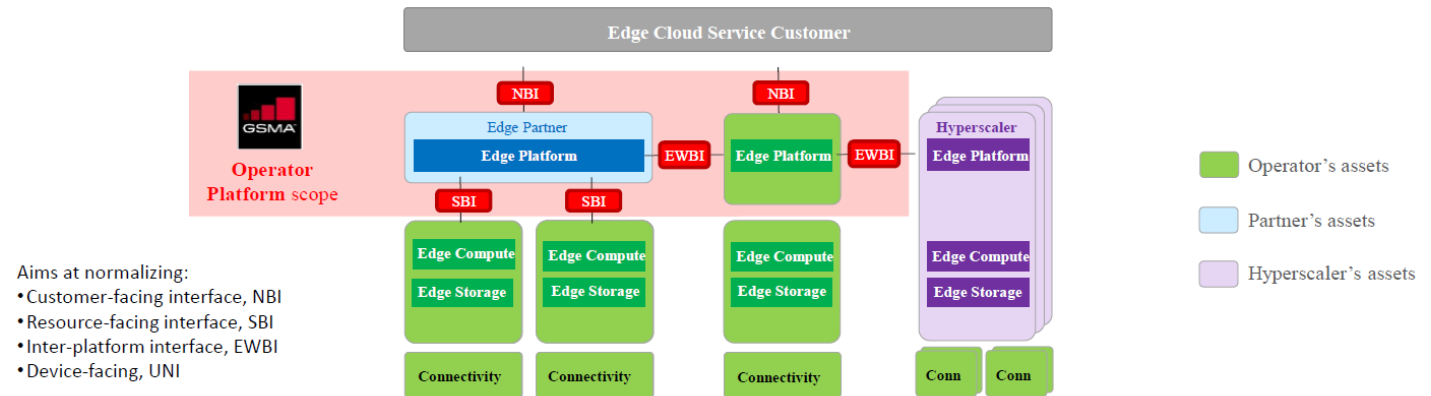


Suggested reading:
ETSI White Paper on
“MEC support towards
Edge Native Design”



MEC Phase 3 expanded the scope to MEC Federation

Starting from Industry requirements ...



Ref: GSMA White paper: "Telco Edge Cloud: Edge Service Description and Commercial Principles", Oct 2020

... ETSI MEC published a very first work on **MEC federation**

ETSI GR **MEC 035** v3.1.1: "Multi-access Edge Computing (MEC); Study on Inter-MEC systems and MEC-Cloud systems coordination", June 2021,

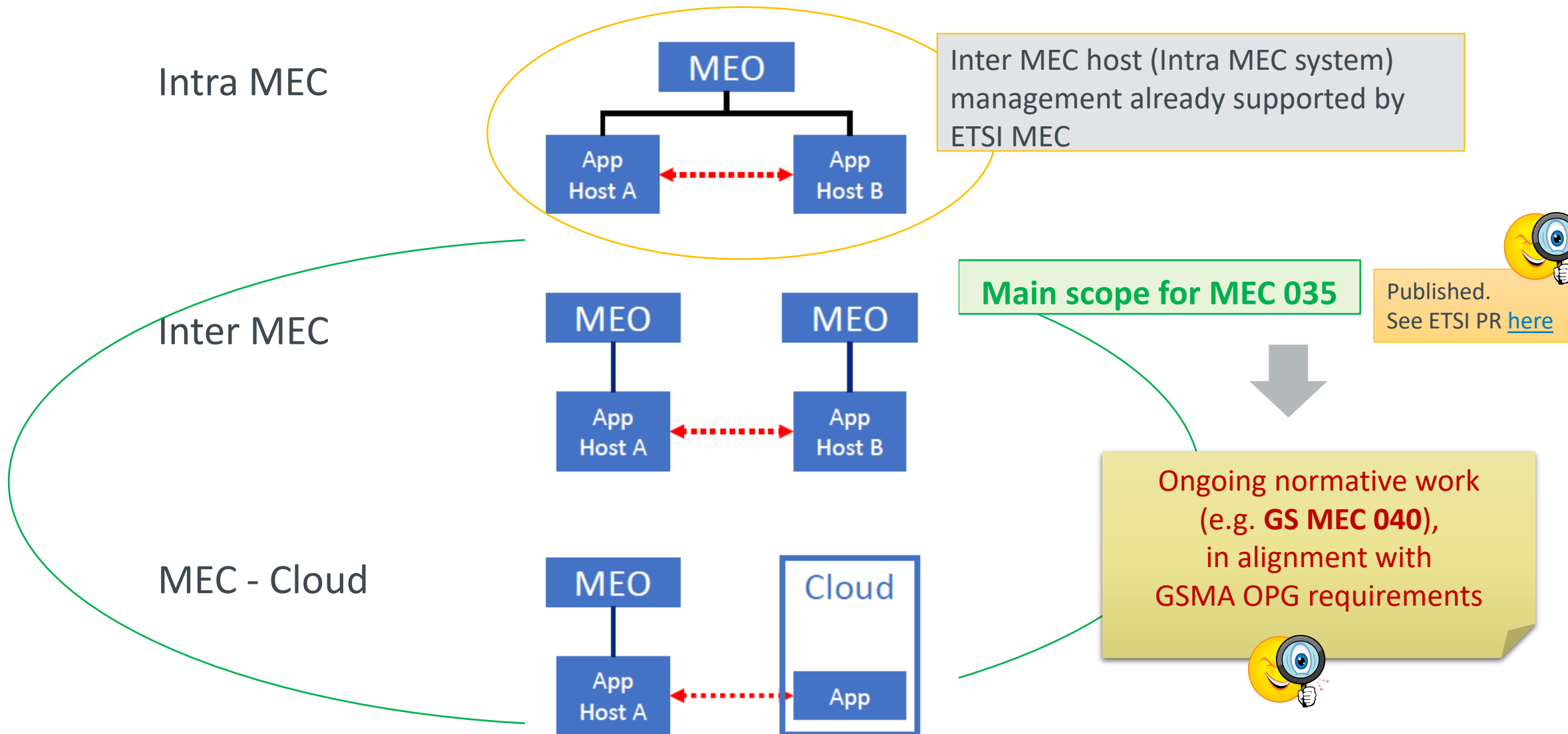
https://www.etsi.org/deliver/etsi_gr/MEC/001_099/035/03.01.01_60/gr_mec035v030101p.pdf



MEC Federation:

"federated model of MEC systems enabling shared usage of MEC services and applications"

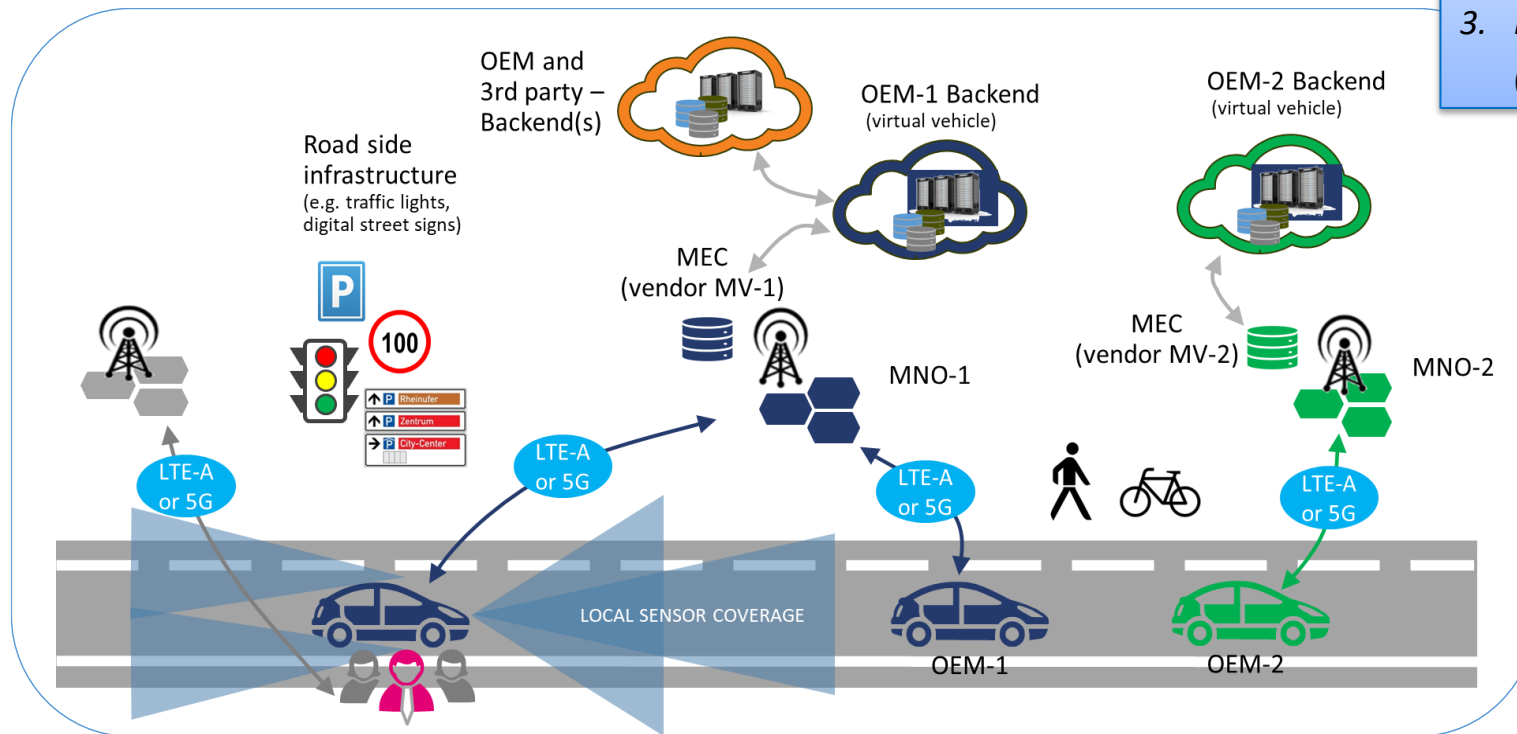
Phase 3 expanded the scope to MEC Federation



MEC Study on Inter-MEC systems and MEC-Cloud systems coordination (MEC 035)

Many Use cases

#1: MEC federation scenario of V2X services



1. Interop. between MNOs
2. Interop. between MEC vendors/suppliers
3. Interop between OEMs (applications)

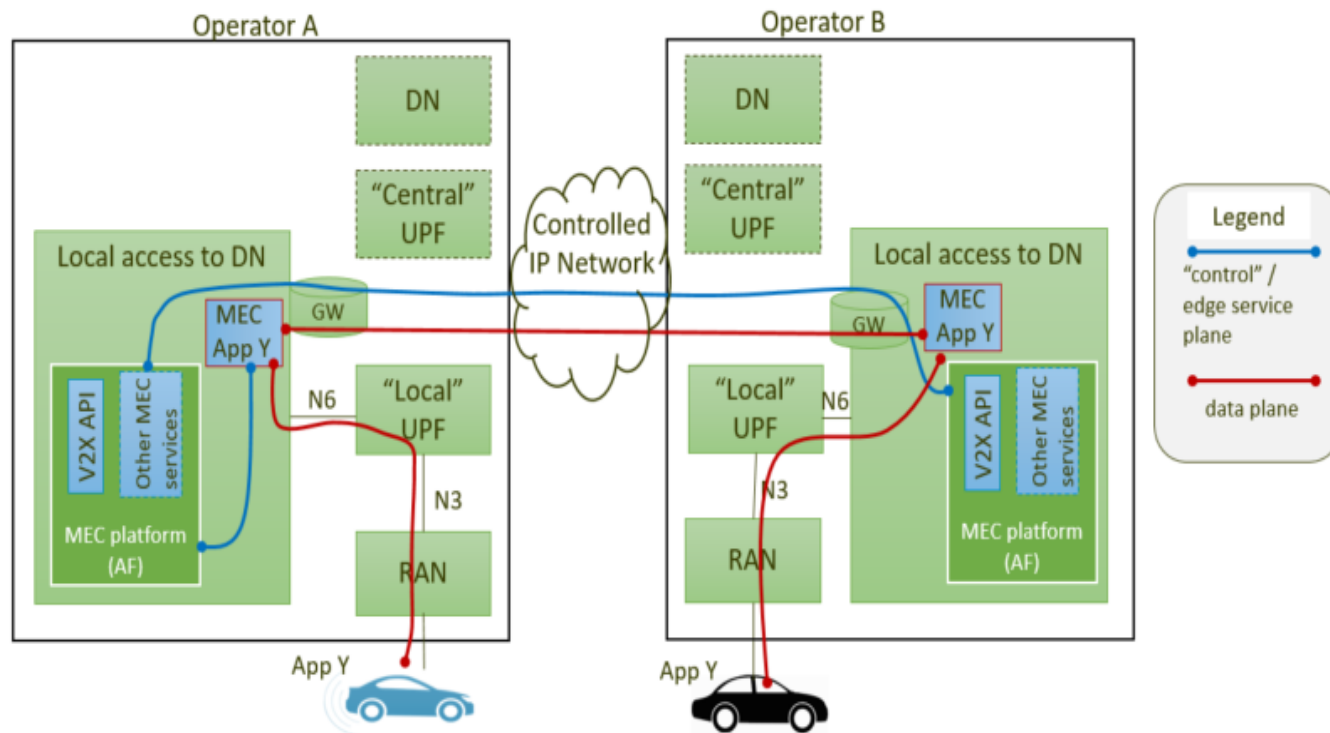
Inspired by 5GAA use cases including multi-MNO, multi-OEM, multi-MEC

Requirements for MEC:

- MEC system discovery
- MEC platform discovery
- MEC platform level information exchange

Study (MEC 035) on inter-MEC system and Cloud-MEC system coordination

Multi-operator agreements enabling MEC Federation for V2X services

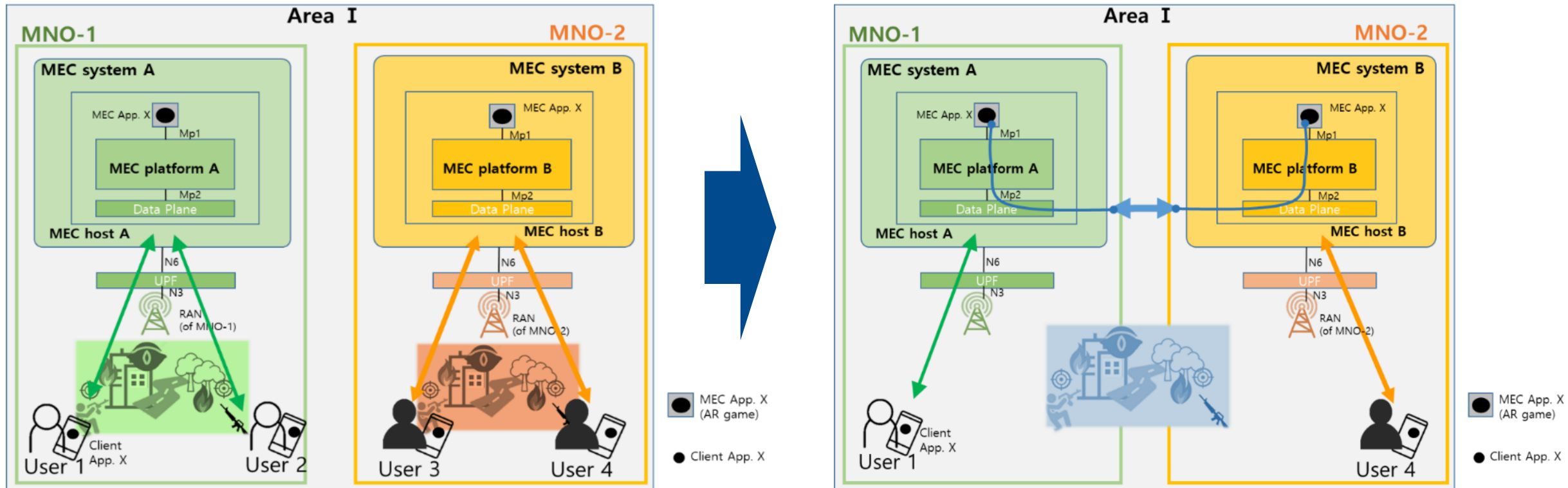


- Type-1 use case - national roaming like scenario: customers of operator A could access the edge infrastructure of operator B to ensure the best possible service.
- Type-2 use case: An app developer has a commercial relationship with operator A. Federation agreements could allow the app developer to deploy its App in operator B's MEC system.
- Type-3 use case - federation broker: a federation broker has a set of agreements with several MNOs.

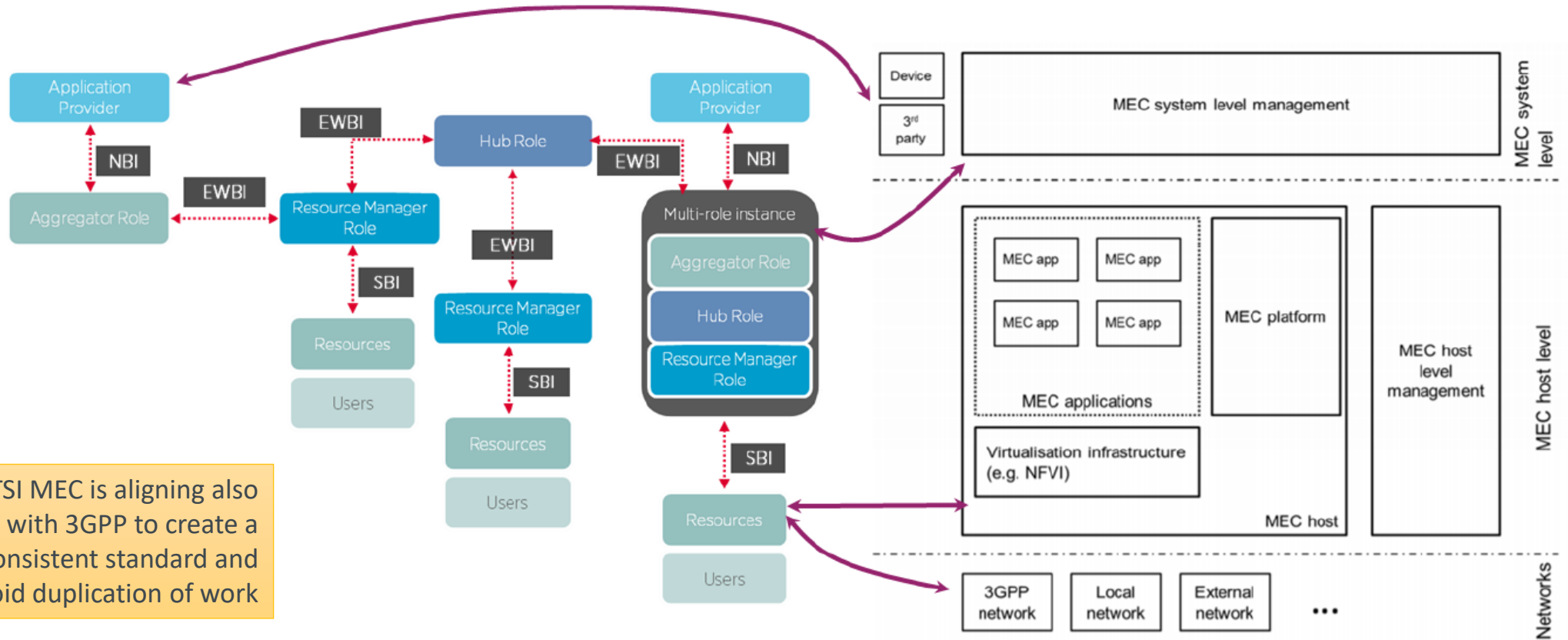
MEC Study on Inter-MEC systems and MEC-Cloud systems coordination (MEC 035)

Many Use cases

#6: MEC federation scenario for immersive AR game



GSMA OPG (Operator Platform Group) mapping with ETSI MEC



ETSI MEC is aligning also with 3GPP to create a consistent standard and avoid duplication of work

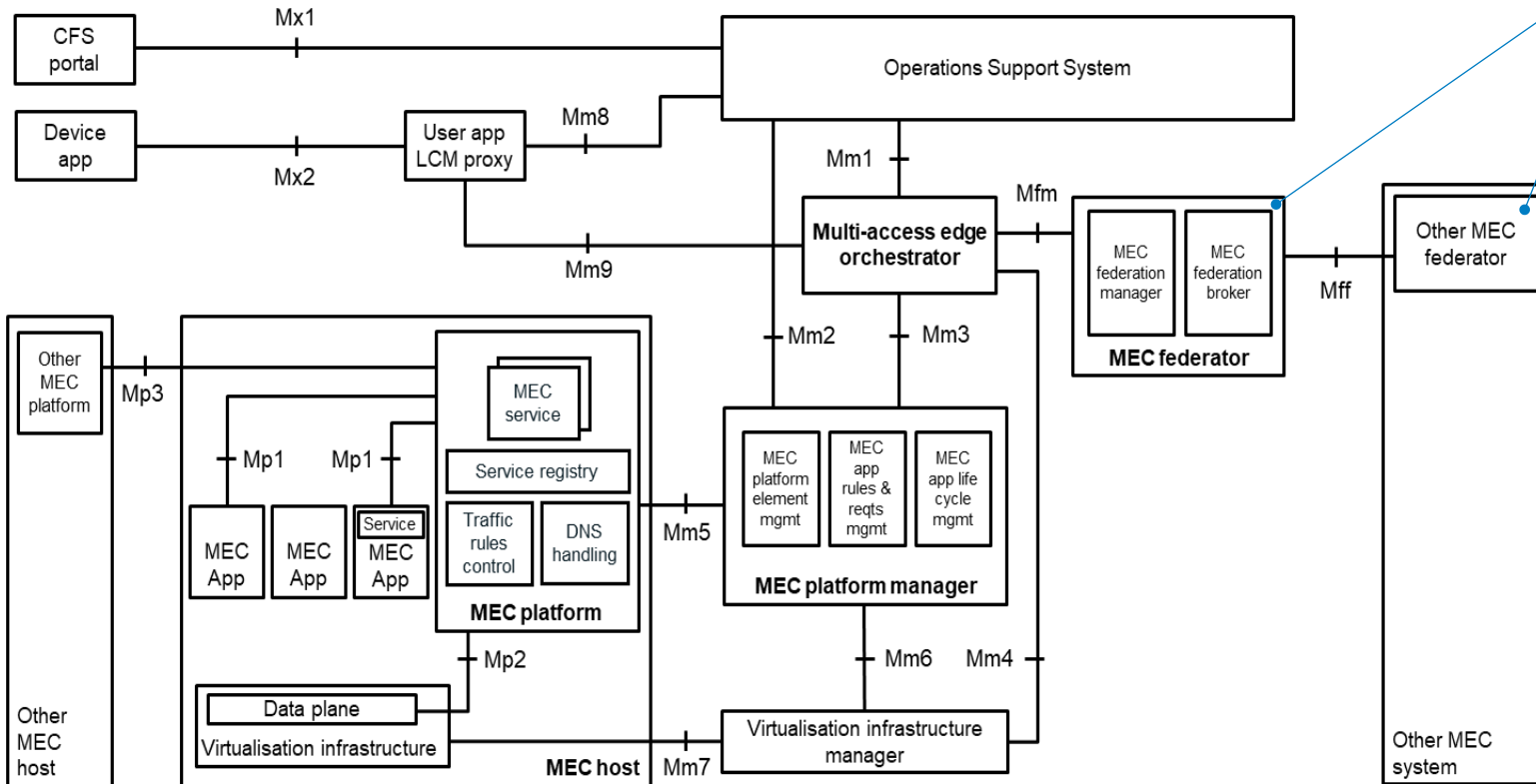
Note: GSMA is listed as a MEC Participant, can submit contributions to ISG MEC for Discussion or Decision, and not only for Information. Dually, ETSI MEC nominated 2 observers, to represent the ISG in GSMA OPG.

Ref: GSMA Permanent Reference Document, "Operator Platform Telco Edge Requirements", v2.0, April 2022.

Link: <https://www.gsma.com/futurenetworks/wp-content/uploads/2022/04/GSMA-Operator-Platform-Telco-Edge-Requirements-2022-v2.0.pdf>

MEC 003 – introducing Architecture variant for MEC federation

Phase 3 deliverable published in March 2022



MEC federator (MEF): enables a MEC federation between MEC systems

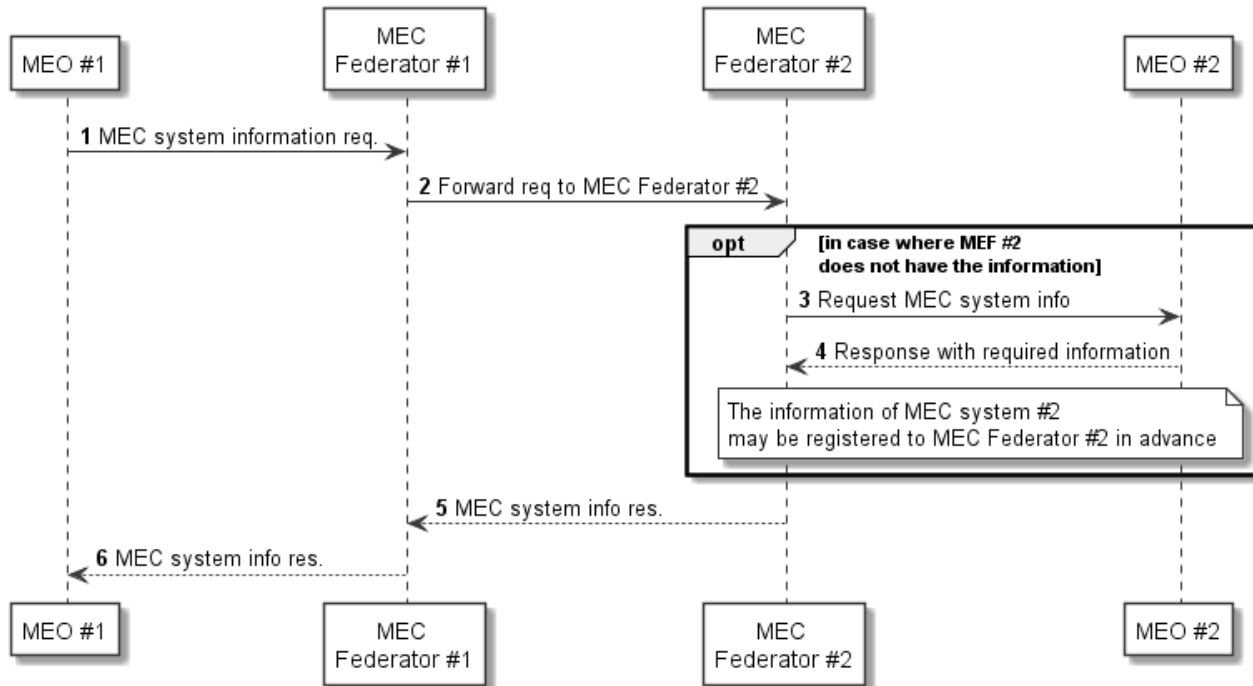
- A MEF interfaces to at least one MEO
- Each MEF enables information exchange with at least one other MEF
- A MEF may serve as a single point of contact for multiple MEFs in the MEC federation

MEF may support the following functionality:

- registration of MEC system information by a MEO;
- MEC system discovery;
- broker capability acting as a one to many intermediary between MEFs;
- information (e.g. MEC system information) exchange;
- application lifecycle management (e.g. on-boarding/instantiation/termination) across different MEC systems;
- application monitoring across different MEC systems.

MEC 040 – introducing MEC Federation Enablement APIs

Phase 3 deliverable v311 ongoing (stable draft @Oct 2022)



Federation Enablement APIs offer services such as discovery, information exchange and application life cycle management to enable the inter-work of one MEC system with another MEC system:

- Registration/Update/Deregistration of MEC system(s) to the federation
- MEC system discovery
- MEC application instance discovery
- MEC service discovery
- Application package mgmt and App instance LCM
- Providing/updating MEC system-wide MEC App instance information updates to MEF

Example (MEC System Discovery) :

- Information flow used for enabling MEO to be aware of another MEC system
- The MEC system discovery is the primitive and essential procedure for enabling the other functionalities relating to the Feature MEC Federation

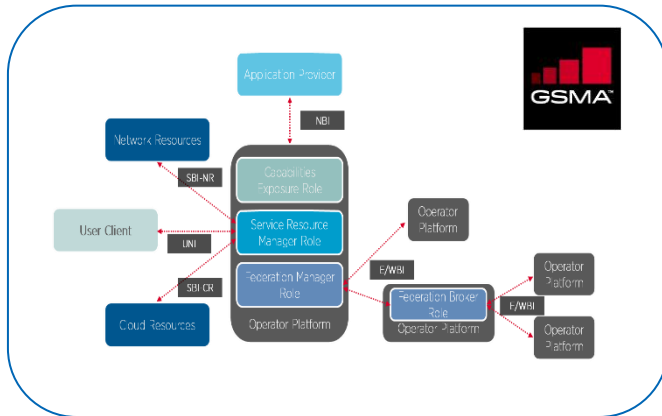
Alignment between GSMA OPG, ETSI MEC and 3GPP SA6



A possible relationship could consist in the following high-level steps:

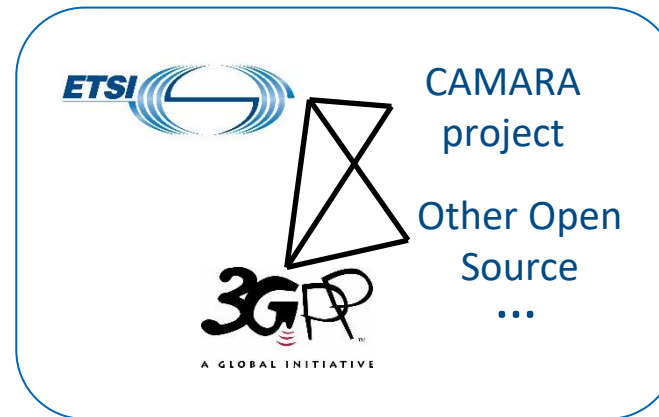
1. GSMA asks SDOs to cover standards for the OP architecture (and OSCs to complement with open source)
2. Worksplitted (ETSI, 3GPP, OSCs,..) and consequent std work, publication of standards etc..
3. Finally, GSMA will certify OP compliance

1.



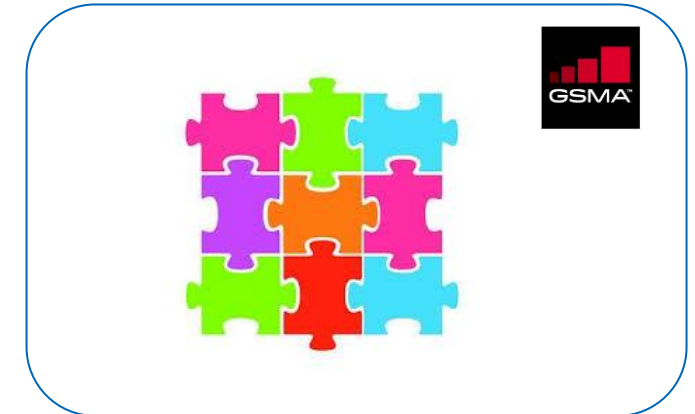
GSMA PRD document
(requirements)

2.



Work from SDOs and OSCs
(under the GSMA guidance)

3.



GSMA compliance & OP
certification

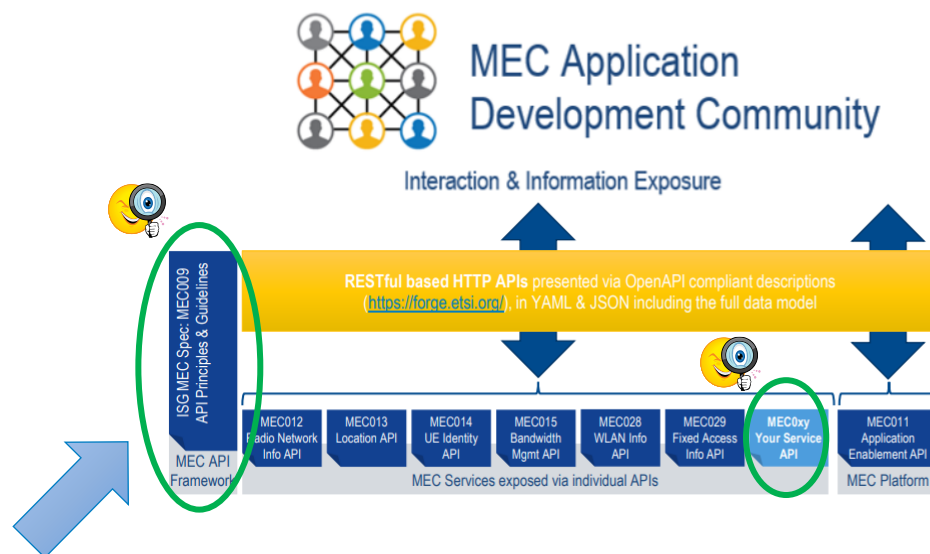
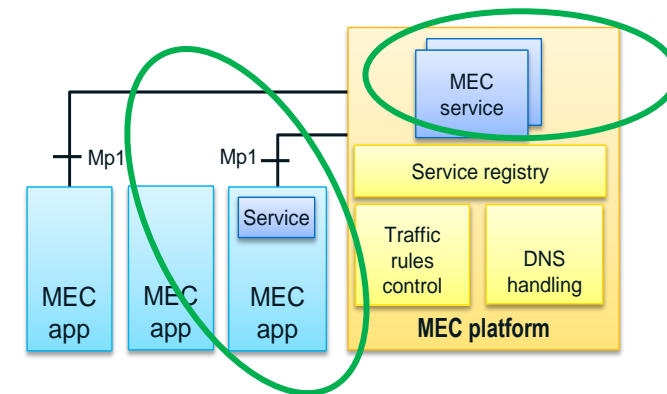


ETSI MEC APIs, external APIs and API exposure

Extending MEC with new MEC Service APIs

MEC Services: value-added capabilities to enable MEC applications

- "Built-in" MEC standardized services provided via the MEC Platform.
- **MEC applications can offer new MEC Services APIs, extending the MEC system**



- ✓ Simple to use, well documented APIs, published with OpenAPI Framework
- ✓ Create innovative applications quickly and easily, reducing time-to-revenue
- ✓ New APIs (compliant with the MEC API principles) can be added
- ✓ Increase the Total Addressable Market (TAM)



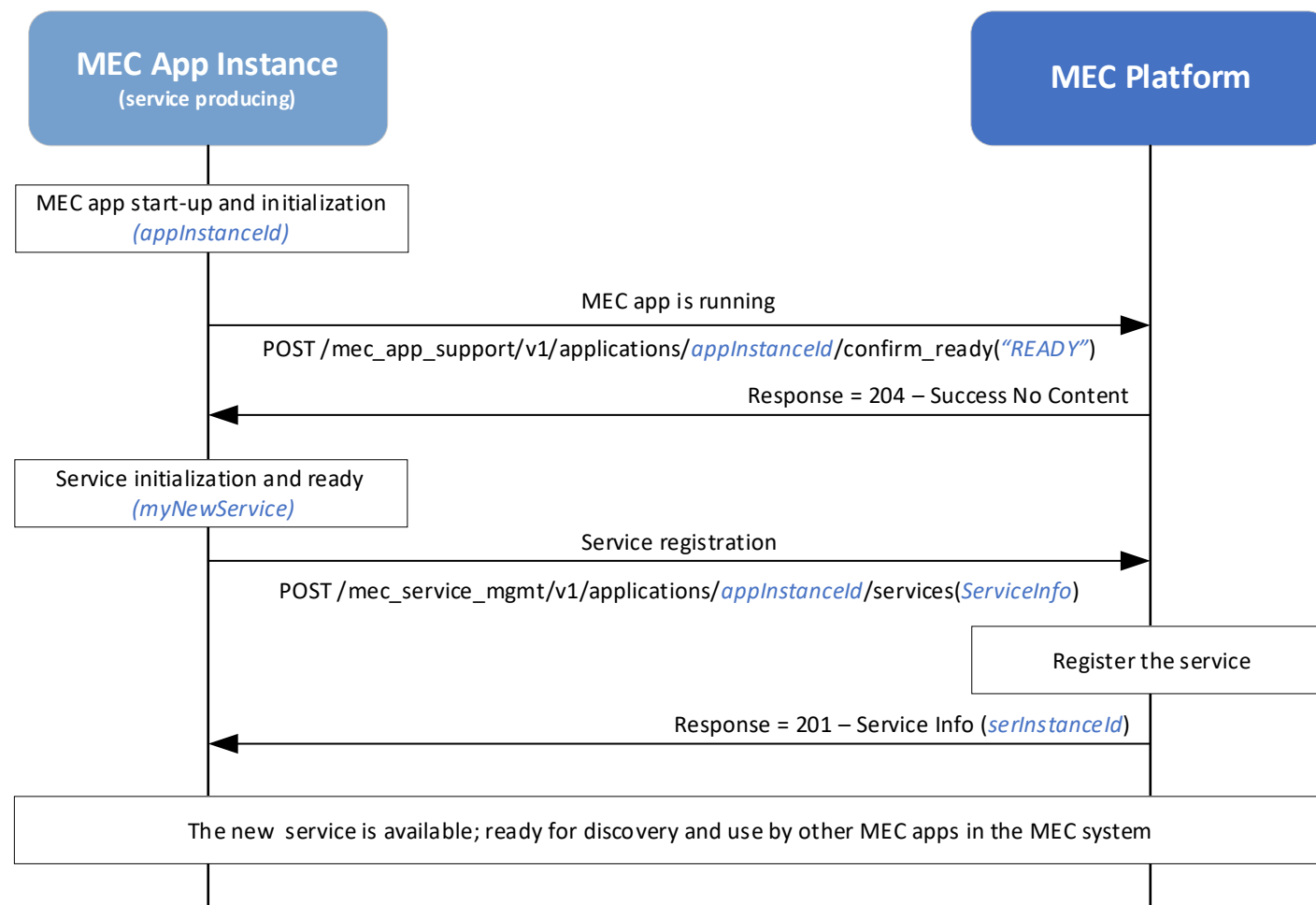
NOTE: ETSI GS MEC 009 is defining General principles, patterns and common aspects of MEC Service APIs

NOTE: also the MEC Sandbox includes capabilities to advertise, discover, and consume New MEC Services

2 – MEC App exposing a New MEC Service

New Service Registration:

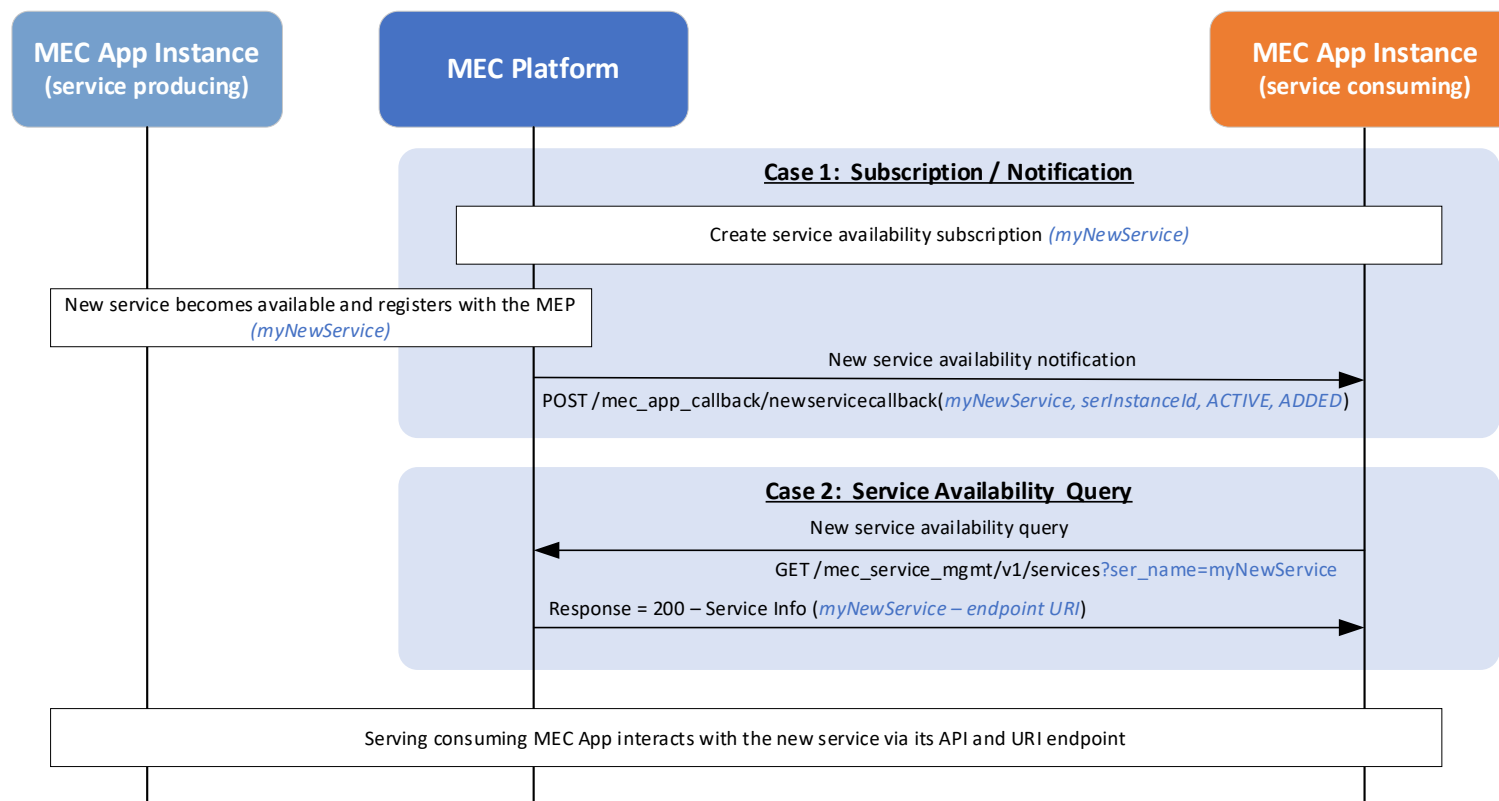
- MEC application initializes and confirms it is ready to the MEC Platform (MEP)
- MEC app prepares its new service API
- MEC app registers the new service with the MEP, providing Service Information
- MEP registers the service and allocates a service instance
- The New MEC Service is now available for other MEC Apps in the MEC system



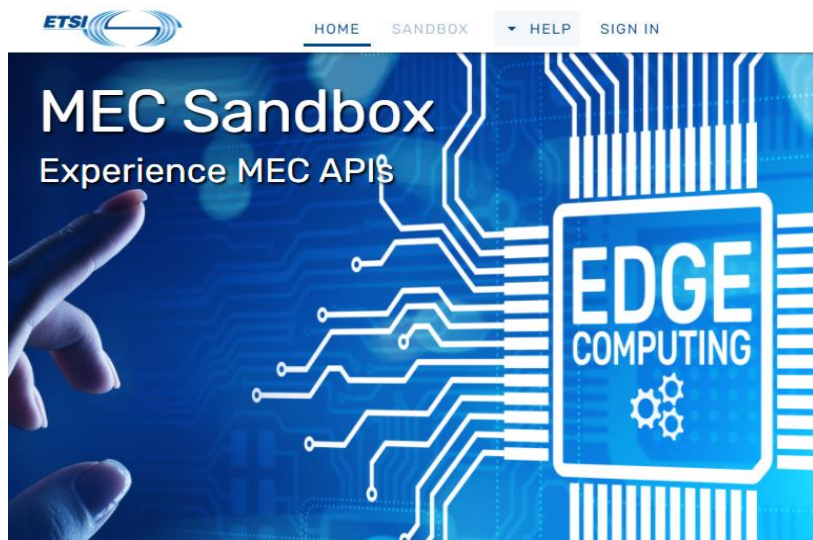
3 – MEC App discovering a new MEC Service

New MEC Service Discovery:

- Case 1: Subscription / Notification
 - Service consuming MEC App creates a Service Availability Subscription
 - When the new service registers and becomes available, the MEP issues a Service Availability Notification, indicating the New Service is available
- Case 2: Service Availability Query
 - Service consuming MEC App issues a service availability query to the MEP
 - MEP responds with the new service's information, including it's URI endpoint.
- MEC app utilises the New MEC Service via it's API and endpoint



MEC Sandbox – try new MEC Service APIs



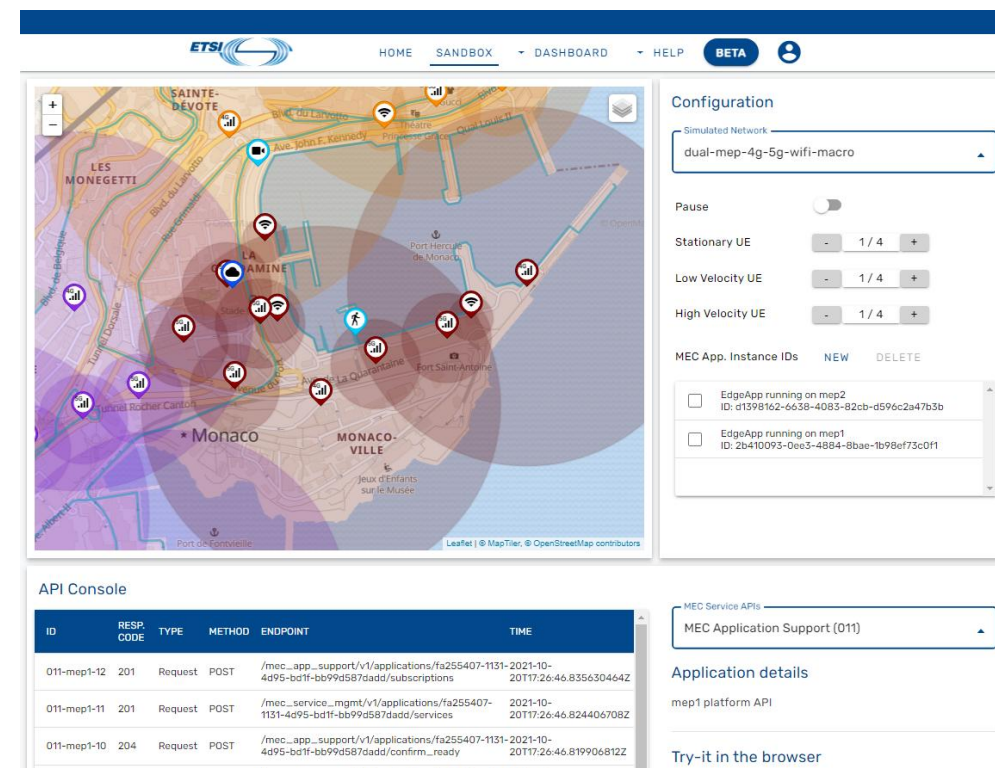
try-mec.etsi.org



The ETSI MEC Sandbox is an interactive environment that enables developers to learn & experiment with “live” ETSI MEC Service APIs from anywhere in the world

Available MEC Services:

- MEC Platform Application Enablement & Service Management APIs (MEC 011)
- Radio Network Information (MEC 012)
- Location Service (MEC 013)
- **New** Bandwidth Management and Traffic Steering (MEC 015)
- **New** Device Application Interface (MEC 016)
- Application Mobility Service (MEC 021)
- WLAN Access Information (MEC 028)
- V2X Information Service (MEC 030)



The screenshot shows the ETSI MEC Sandbox interface. At the top, there's a navigation bar with 'HOME', 'SANDBOX', 'DASHBOARD', 'HELP', and a 'BETA' badge. The main area is divided into three sections:

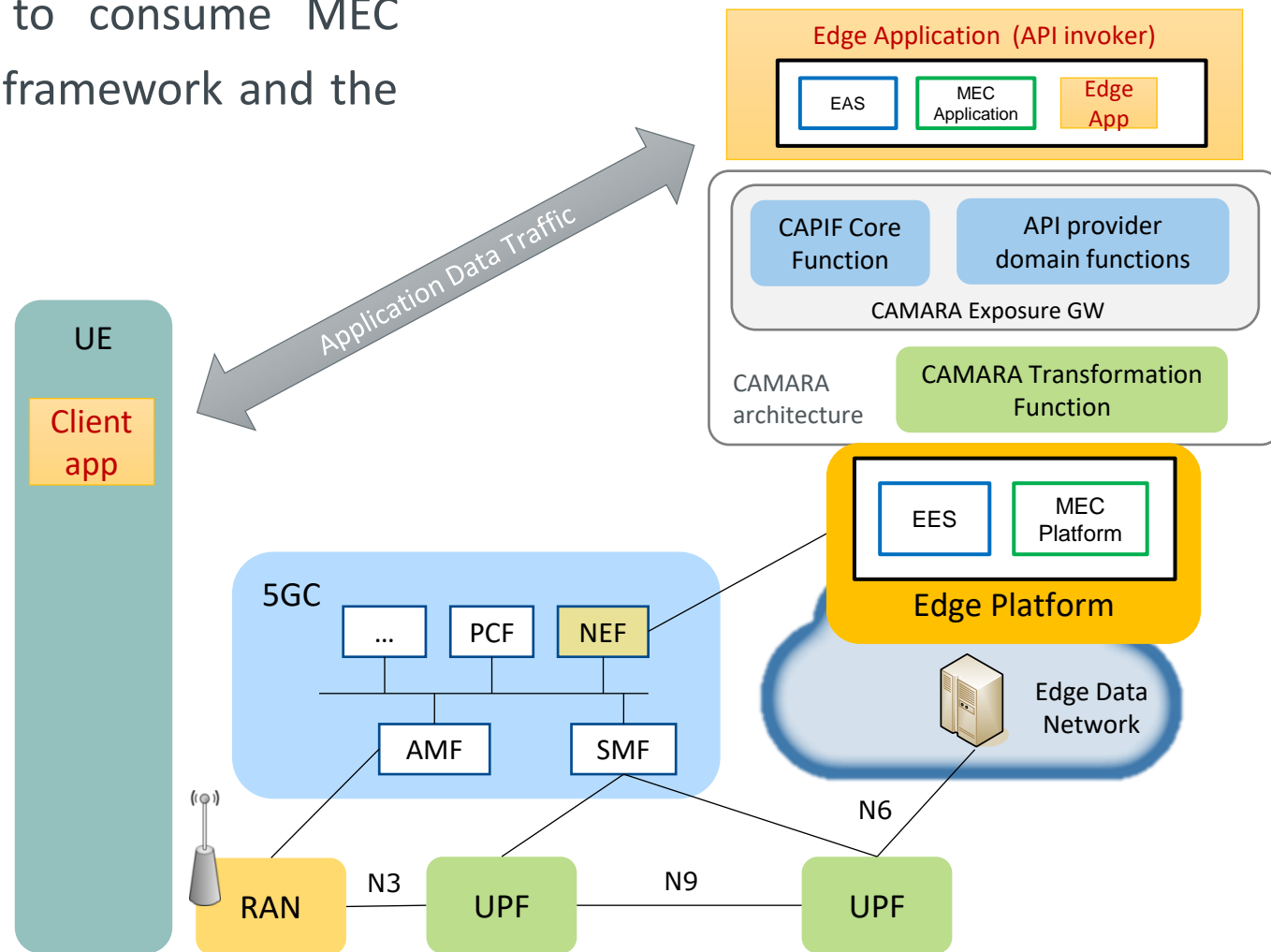
- Map:** A map of Monaco with various MEC service coverage areas and icons.
- Configuration:** A sidebar on the right with a dropdown for 'Simulated Network' (set to 'dual-mep-4g-5g-wifi-macro'), a 'Pause' toggle, and three UE type sliders: 'Stationary UE' (1/4), 'Low Velocity UE' (1/4), and 'High Velocity UE' (1/4). Below these are 'MEC App. Instance IDs' with 'NEW' and 'DELETE' buttons, and a list of running applications with checkboxes.
- API Console:** A table at the bottom showing API request logs.

ID	RESP. CODE	TYPE	METHOD	ENDPOINT	TIME
011-mep1-12	201	Request	POST	/mec_app_support/v1/applications/fa255407-1131-2021-10-4d95-bd1f-bb99d587dadd/subscriptions	2017:26:46.835630464Z
011-mep1-11	201	Request	POST	/mec_service_mgmt/v1/applications/fa255407-1131-4d95-bd1f-bb99d587dadd/services	2021-10-20T17:26:46.824406708Z
011-mep1-10	204	Request	POST	/mec_app_support/v1/applications/fa255407-1131-2021-10-4d95-bd1f-bb99d587dadd/confirm_ready	2017:26:46.819906812Z

API Exposure and cross-consumption in a MEC Federation

- Option for Edge Native applications to consume MEC services in a MEC federation (via CAPIF framework and the CAMARA architecture)

NOTE: this option also facilitates the synergies with ETSI MEC and GSMA OPG architecture, as API exposure can be exploited also in the MEC federation for edge native application development.

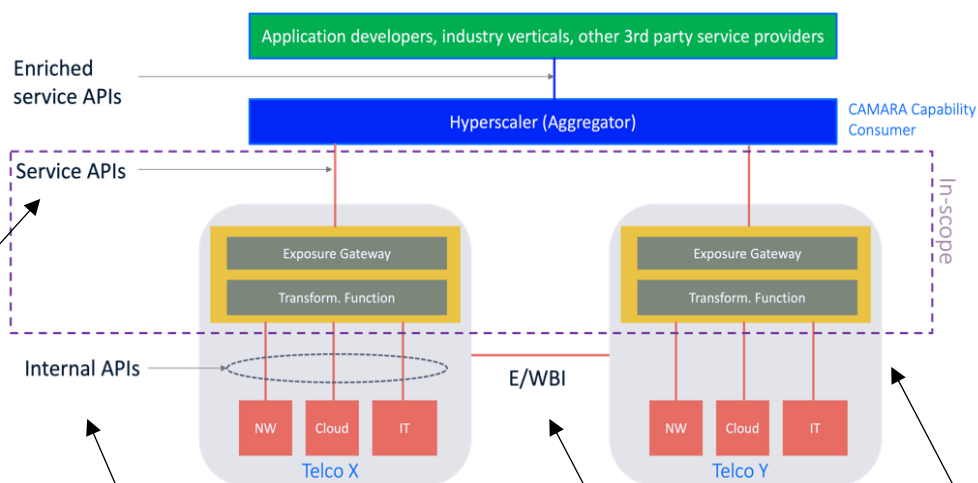


(*) ETSI White Paper “MEC Support for Edge Native Design”, https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP55-MEC_support_towards_Edge_native.pdf

ETSI MEC & CAMARA: topics for collaboration

Technical highlights

- CAMARA is focused on NBI “Service APIs”, as abstractions from “Internal APIs”
 - Since CAMARA’s focus is “application developers” interface APIs, the assumption is for them to have limited or zero knowledge of the network and edge infrastructure.
- According to the figure below, ETSI MEC is standardizing some “Internal APIs”



REMARKS:

- ETSI MEC standardized APIs are “relevant for NBI”, i.e. can be abstracted in CAMARA, for the actual NBI exposure to app devs
- Also new APIs (i.e. not in need to be standardized in ETSI MEC) can be added, recognized by the MEC Platform, and exposed to authorized Applications
- CAPIF is a well recognized (and standard) reference for universal API exposure



ETSI MEC & CAMARA: collaboration establishment

MoU in place
between ETSI and LF

Topics of the collaboration:

- Technical work northbound interface and support for ubiquitous API exposure
 - ensuring complementary work on standards / API definitions (CAMARA NBI, SBI by ETSI MEC and cloud federation) and open-source implementations / tests
 - guidelines for API exposure and interwork (e.g., joint white papers)
 - Join forces to engage application development communities (e.g., to better attract application developers, increase the awareness on edge application and help creating API market demand)
- Other areas of collaboration (to be further elaborated) may include the work item MEC 043 on Abstracted API for Industries



The identified MEC observers are volunteering delegates that can practically facilitate the joint work and collaboration with CAMARA.



Thank you!



dario.sabella@xflowresearch.com