

ETSI TR 123 958 V18.2.0 (2024-07)



**LTE;
5G;
Edge Application Standards in 3GPP and
alignment with External Organizations
(3GPP TR 23.958 version 18.2.0 Release 18)**



Reference

RTR/TSGS-0623958vi20

Keywords

5G,LTE

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI [Search & Browse Standards application](#).

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#).

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under <https://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

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

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

Contents

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	4
Introduction	5
1 Scope	6
2 References	6
3 Definitions of terms, symbols and abbreviations	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Related work in other SDOs.....	8
4.1 General	8
4.2 GSMA OPG	8
4.3 ETSI ISG MEC	8
5 Alignment of EDGEAPP with ETSI MEC	10
5.1 General	10
5.2 Relationship between EDGEAPP and ETSI MEC architectures.....	10
5.3 EDGE-3 and Mp1 reference points	11
5.3.1 EASProfile and AppInfo.....	11
5.4 EDGE-9 and Mp3 reference points	13
5.5 CAPIF and MEC service API management	13
5.6 Support for Federation.....	13
5.6.1 EDGEAPP	13
5.6.2 ETSI MEC	13
6 Alignment of EDGEAPP with GSMA OP	13
6.1 General	13
6.2 Relationship between EDGEAPP architecture and GSMA OPG reference architecture	13
7 Deployment Considerations	15
7.1 General	15
7.2 Deployment option of EDGEAPP and ETSI MEC using CAPIF	16
8 Conclusions	18
AnnexA: Mapping roles between EDGEAPP architecture and GSMA OPG architecture.....	20
Annex B (informative): Change history	24
History	25

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

- shall** indicates a mandatory requirement to do something
- shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

- should** indicates a recommendation to do something
- should not** indicates a recommendation not to do something
- may** indicates permission to do something
- need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

- can** indicates that something is possible
- cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

- will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document
- will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document
- might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

This TR provides recommendations on alignment and deployment aspects of EDGEAPP with ETSI MEC and GSMA Operator Platform (OP).

1 Scope

This TR provides the recommendations for the alignment of EDGEAPP architecture with ETSI MEC reference architecture and GSMA Operator Platform (OP) for the industry stakeholders.

This document provides recommendations of using specifications from 3GPP, ETSI ISG MEC and GSMA OPG to deploy an aligned edge system.

The present document is based on 3GPP TS 23.558 [2].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 23.558: "Architecture for enabling Edge Applications".
- [3] GSMA PRD OPG.02 - "Operator Platform Telco Edge Requirements Version 5.0", <https://www.gsma.com/futurenetworks/wp-content/uploads/2023/07/OPG.02-v5.0-Operator-Platform-Requirements-and-Architecture.pdf>.
- [4] ETSI GS MEC 003 (V3.1.1), "Multi-access Edge Computing (MEC); Framework and Reference Architecture".
- [5] ETSI GS MEC 011 (V3.1.1), "Multi-access Edge Computing (MEC); Edge Platform Application Enablement".
- [6] ETSI GS MEC 040 (V3.1.1), "Multi-access Edge Computing (MEC); Federation enablement APIs".
- [7] ETSI GS MEC 021 (V2.2.1), "Multi-access Edge Computing (MEC); Application Mobility Service API".
- [8] 3GPP TS 28.538: "Management and orchestration; Edge Computing Management".
- [9] ETSI GS MEC 010-2 (V2.2.1), "Multi-access Edge Computing (MEC); MEC Management; Part 2: Application lifecycle, rules and requirements management".
- [10] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".
- [11] ETSI GR MEC 031 (V3.1.1), "Multi-access Edge Computing (MEC); MEC 5G Integration".
- [12] GSMA PRD OPG.03 - "Southbound Interface Network Resources APIs Version 3.0", <https://www.gsma.com/futurenetworks/wp-content/uploads/2023/07/OPG.03-v3.0-Southbound-Interface-Network-Resources-APIs.pdf>.
- [13] GSMA PRD OPG.04 - "East-Westbound Interface APIs Version 3.0", <https://www.gsma.com/futurenetworks/wp-content/uploads/2023/07/OPG.04-v3.0-GSMA-Operator-Platform-Group-East-Westbound-Interface-APIs-Version-3.0.pdf>.

- [14] GSMA PRD OPG.05 - "User-Network Interface APIs Version 1.0 ",
<https://www.gsma.com/futurenetworks/wp-content/uploads/2023/03/GSMA-Operator-Platform-Group-User-Network-Interface-APIs-v1.pdf>.
- [15] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".
- [16] ETSI White Paper #36 – "Harmonizing standards for edge computing - A synergized architecture leveraging ETSI ISG MEC and 3GPP specifications",
https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_wp36_Harmonizing-standards-for-edge-computing.pdf.
- [17] 3GPP TS 28.538: "Management and orchestration; Edge Computing Management".
- [18] 3GPP TS 32.257: "Telecommunication management; Charging management; Edge computing domain charging".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

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

<symbol> <Explanation>

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AC	Application Client
AEF	API Exposing Function
AF	Application Function
AMF	API Management Function
API	Application Program Interface
APF	API Publishing Function
AS	Application Server
CAPIF	Common API Framework
CCF	CAPIF Core Function
CER	Capabilities Exposure Role
EAS	Edge Application Server
ECS	Edge Configuration Server
ECSP	Edge Computing Service Provider
EDN	Edge Data Network
EEC	Edge Enabler Client
EEL	Edge Enabler layer
EES	Edge Enabler Server
ETSI	European Telecommunications Standards Institute
MEC	Multi-access Edge Computing
MEP	MEC Platform
NaaS	Network-as-a-Service

NSaaS	Network Slice-as-as-Service
OP	Operator Platform
OPG	Operator Platform Group
SBI-NR	Southbound Interface-Network Resources
SNMP	Stand-Alone Non-Public Network
SRM	Service Resource Manager
UC	User Client
UNI	User-to-Network Interface

4 Related work in other SDOs

4.1 General

This section provides an overview on the existing work in GSMA and ETSI MEC relevant to the EDGEAPP architecture describing the OP roles, existing mapping and alignment aspects provided by GSMA OP and ETSI MEC in clause 4.2 and clause 4.3 respectively.

4.2 GSMA OPG

The Operator Platform (OP) as defined by GSMA OPG in GSMA PRD OPG.02 [3], guides the industry to define a common solution for exposing network capabilities and edge compute resources to enterprise customers and developers allowing monetization of those capabilities. The technical requirements, functional blocks and interfaces characteristics of such a generic platform to facilitate access to the Edge Cloud capability of an operator or federation of operators and their partners are provided in GSMA PRD OPG.02 [3]. GSMA PRD OPG.02 [3] also provides mapping of these requirements and architectures to the specifications from certain SDOs.

The integration of OP with the mobile network takes place using the Southbound Interface-Network Resources (SBI-NR) through the set of APIs specified in GSMA PRD OPG.03 [12] which is linked to the corresponding 3GPP-defined APIs. GSMA PRD OPG.04 [13] specifies the set of APIs for the interactions/operations over the East/West Bound Interface (E/WBI), which enables an OP to share network and edge capabilities with other OP(s). The E/WBI interactions enable the management of a federation (i.e. creation/update/removal), management of the application onboarding in the federation, edge node discovery, etc. The APIs for the interactions between OP and the User Client (UC) are provided in GSMA PRD OPG.05 [14]. The interactions between OP and the User Client (UC) are supported by the User-to-Network Interface (UNI), allowing the UC to discover the existence of an Edge Cloud service, to register to the OP's Service Resource Manager (SRM), to trigger the selection of a cloudlet (a point of presence for the Edge Cloud offering a set of resources at a particular location as specified in GSMA PRD OPG.02 [3]) by the OP, to trigger the instantiation of an application instance on the selected cloudlet.

4.3 ETSI ISG MEC

Figure 4.3-1 shows the MEC reference architecture as specified by ETSI ISG MEC. This reference architecture describes the functional elements that comprise the multi-access edge system and the reference points between them. It consists of MEC host and MEC management system necessary to run MEC Applications within an operator network or a subset of an operator network.

The MEC platform is the collection of essential functionalities required to run MEC applications on a particular Virtualisation infrastructure and enable them to provide and consume MEC services.

MEC applications are instantiated on the Virtualisation infrastructure of the MEC host based on configuration or requests validated by the MEC management. An already instantiated MEC application can optionally register with MEC platform. The application registration procedure allows an authorized MEC application instance to provide its information to the MEC platform [5].

The Mp1 reference point between the MEC platform and the MEC applications provides service registration, service discovery, and communication support for services. It also provides other functionality such as application availability, session state relocation support procedures, traffic rules and DNS rules activation, access to persistent storage and time of day information, etc.

The Mp3 reference point between MEC platforms is used for control communication between MEC platforms.

ETSI ISG MEC also provides Multi-access system reference architecture variants for the deployment in an NFV environment and for MEC federation [4] as shown in Figure 4.3-2. In [6], ETSI ISG MEC specifies "Federation enablement APIs" that enable the shared usage of MEC services and applications across different systems (e.g., MEC system, Cloud system).

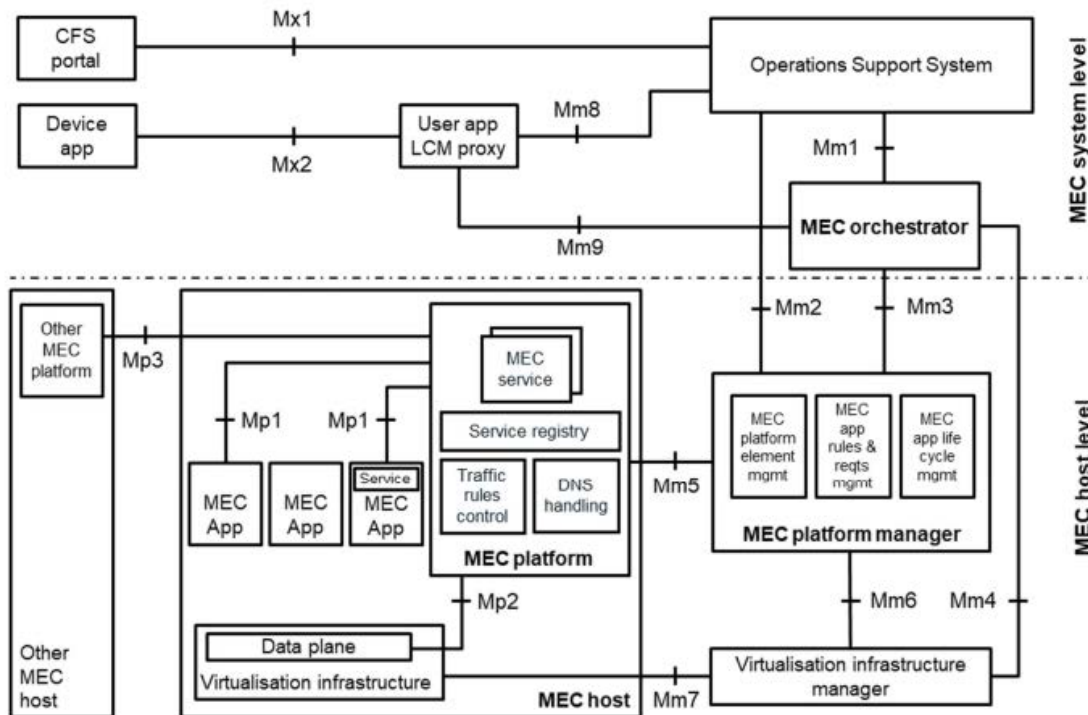


Figure 4.3-1: Multi-access Edge System reference architecture

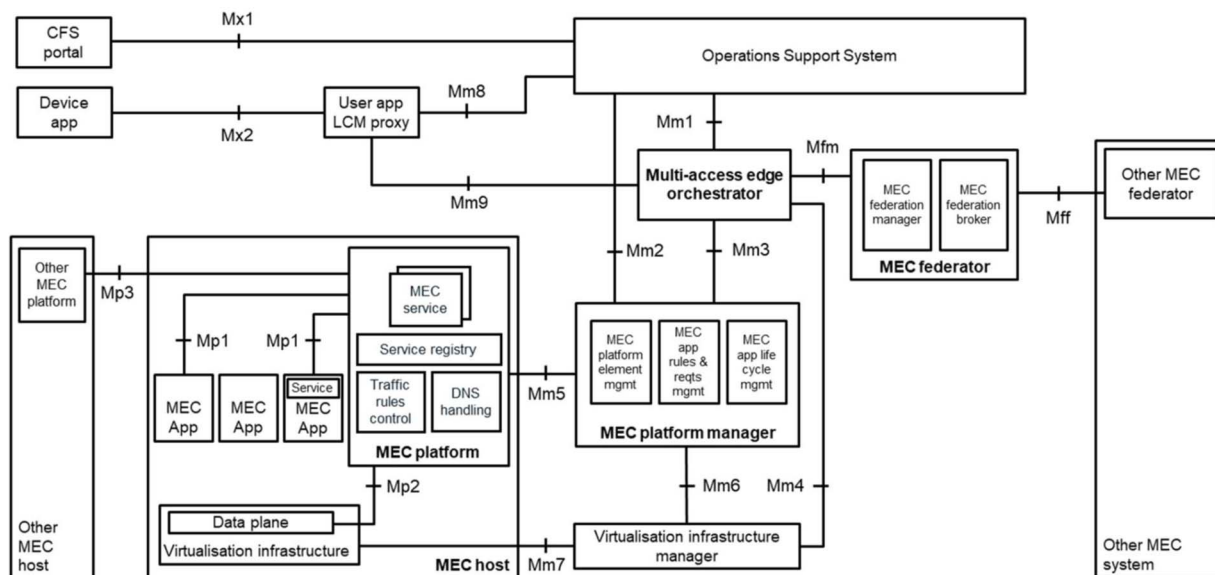


Figure 4.3-2: Multi-access Edge System reference architecture variant for MEC federation

5 Alignment of EDGEAPP with ETSI MEC

5.1 General

An early effort on alignment between 3GPP EDGEAPP and ETSI MEC was initiated during Rel-17, and a summary is available in a white paper published by ETSI - "Harmonizing standards for edge computing - A synergized architecture leveraging ETSI ISG MEC and 3GPP specifications" [16].

Clause 5.2 provides the relationship between EDGEAPP and ETSI MEC architectures. Clause 5.3 provides the mapping of EAS Profile and AppInfo to allow application registration across the platforms. Clause 5.4 provides description for EDGE-9 and Mp3 reference points. Clause 5.5 provides the description for CAPIF and MEC service API management.

5.2 Relationship between EDGEAPP and ETSI MEC architectures

Figure 5.2-1 provides the relationship of ETSI ISG MEC architecture with EDGEAPP architecture.

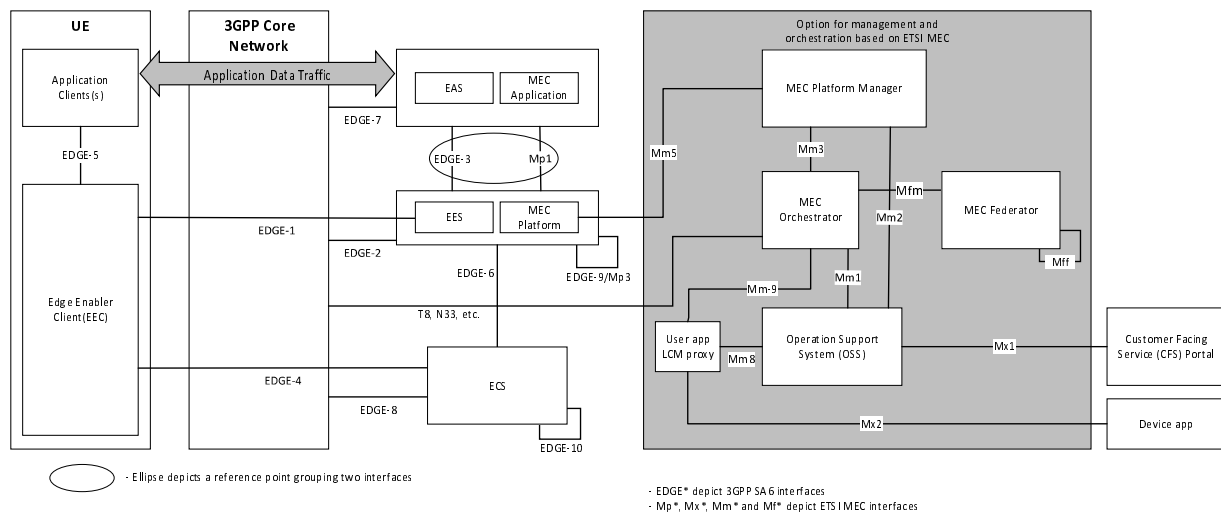


Figure 5.2-1: Relationship between EDGEAPP and ETSI MEC architectures

Details about MEC entities (MEC Platform, MEC Application, MEC Platform Manager, MEC Orchestrator, MEC Federator, OSS and CFS) can be found in ETSI GS MEC 003 [4].

In ETSI MEC, MEC Applications and MEC Platform can expose services which can include network services, subject to their availability at the core or access network level.

Both EAS and MEC application are application servers and can provide similar application specific functionalities. EAS utilizes the services of EES as specified in 3GPP TS 23.558 [2] whereas MEC application utilizes the services provided by MEC platform as specified in ETSI GS MEC 003 [4]. The EAS and MEC application can be aligned in an implementation.

NOTE 1: The details of the functionalities of application servers are implementation specific.

Both EES and MEC platform provide application support capabilities towards the application servers. The EES and MEC platform and their interfaces can be aligned in an implementation.

The orchestration and management aspects of architecture for enabling edge applications are specified in 3GPP TS 28.538 [8].

5.3 EDGE-3 and Mp1 reference points

5.3.1 EASProfile and AppInfo

Both EDGEAPP and ETSI MEC supports registration of EAS and MEC application instance with EES and MEC platform respectively. In order to support MEC application instance registration on EES, it is required that registration request includes at least the mandatory IEs that are required for EAS registration, i.e. EAS ID and EAS endpoint. On the other hand, according to ETSI GS MEC 011 [5] the application registration request must include appName.

AppInfo is the data type describing the information exchanged by a MEC application instance at registration to a MEC platform. It is defined in clause 7.1.2.6 of ETSI GS MEC 011 [5] and includes appName as a mandatory IE and endpoint as an optional IE. However, endpoint is mandatory when the AppInfo IE isInsByMec is FALSE and, as stated above, would have to be provided for MEC application instance registration to an EES. The isInsByMec IE of the AppInfo, with type Boolean, indicates whether the application instance is instantiated by a MEC management system. The IE appName can be considered equivalent to EAS ID. Furthermore endpoint can be directly mapped to EAS endpoint and that mapping is explicitly stated in note 2 of Table 7.1.2.6-1 of ETSI GS MEC 011 [5].

Table 5.3.1-1 provides a mapping of MEC attributes to those in the EAS Profile for MEC application registration with EES.

Table 5.3.1-1: Mapping with EASProfile for MEC application registration with EES

Information element	Status/ Cardinality	Description	Mapped with
EASID	M	The identifier of the EAS	AppInfo >appName
EAS Endpoint	M	Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the EAS. This information maybe discovered by EEC and exposed to ACs so that ACs can establish contact with the EAS.	AppInfo >endpoint
ACID(s)	O	Identifies the AC(s) that can be served by the EAS	Not available in case of MEC application registration
EAS Provider Identifier	O	The identifier of the ASP that provides the EAS.	AppInfo >appProvider
EAS Type	O	The category or type of EAS (e.g. V2X)	AppInfo >appCategory
EAS description	O	Human-readable description of the EAS	AppD >appDescriptor
EAS Schedule	O	The availability schedule of the EAS (e.g. time windows)	Not available in case of MEC application registration
EAS Geographical Service Area	O	The geographical service area that the EAS serves. ACs in UEs that are located outside that area shall not be served.	Not available in case of MEC application registration
EAS Topological Service Area	O	The EAS serves UEs that are connected to the Core Network from one of the cells included in this service area. ACs in UEs that are located outside this area shall	Not available in case of MEC application registration

		not be served. See possible formats in Table 8.2.7-1.	
EAS Service KPIs	O	Service characteristics provided by EAS, detailed in Table 8.2.5-1	Not available in case of MEC application registration
EAS service permission level	O	Level of service permissions e.g. trial, gold-class supported by the EAS	Not available in case of MEC application registration
EAS Feature(s)	O	Service features e.g. single vs. multi-player gaming service supported by the EAS	Not available in case of MEC application registration
EAS Service continuity support	O	Indicates if the EAS supports service continuity or not. This IE also indicates which ACR scenarios are supported by the EAS.	Not available in case of MEC application registration
General context holding time duration	O	The time duration that the EAS holds the context before the AC connects to the EAS in case of ACR for service continuity planning. It is an indication of the time the EAS holds the application context for a UE to move to its service area after receiving an ACR notification from the EES following an ACR request from the EEC.	Not available in case of MEC application registration
List of EAS DNAI(s)	O	DNAI(s) associated with the EAS. This IE is used as Potential Locations of Applications in clause 5.6.7 of 3GPP TS 23.501 [15]. It is a subset of the DNAI(s) associated with the EDN where the EAS resides.	Not available in case of MEC application registration
List of N6 Traffic Routing requirements	O	The N6 traffic routing information and/or routing profile ID corresponding to each EAS DNAI.	Not available in case of MEC application registration
EAS Availability Reporting Period	O	The availability reporting period (i.e. heartbeat period) that indicates to the EES how often it needs to check the EAS's availability after a successful registration.	Not available in case of MEC application registration
EAS Status	O	The status of the EAS (e.g. enabled, disabled, etc.)	Not available in case of MEC application registration

5.4 EDGE-9 and Mp3 reference points

EDGE-9 reference point in EDGEAPP architecture is used to provide target EAS discovery to support ACR in case of mobility of user from one EES to another EES. On the other hand, Mp3 reference point between MEC platforms is used for control communication between MEC platforms [4] with a separate application mobility service [7] being provided in support of mobility of users between MEC hosts within a MEC system. Currently, ETSI MEC has not specified APIs over Mp3.

5.5 CAPIF and MEC service API management

CAPIF is the Common API Framework for northbound APIs specified in 3GPP TS 23.222 [10]. The Edge Enabler Layer supports CAPIF for northbound API exposure of edge service APIs as specified in 3GPP TS 23.558 [2]. The MEC platform supports CAPIF in the form of MEC service management API as specified in ETSI GS MEC 011 [5]. The CAPIF APIs are similar to the MEC service management APIs and the mapping is described in ETSI GS MEC 011 [5].

5.6 Support for Federation

5.6.1 EDGEAPP

EDGE-9 and EDGE-10 reference points are used to support federation functionalities as per clause 8.17 and clause 8.18 of 3GPP TS 23.558 [2]. EDGE-9 reference point in EDGEAPP architecture is used to discover EAS from the EES of the partner ECSP for edge node sharing. EDGE-10 reference point in EDGEAPP architecture is used for ECS registration, ECS discovery via ECS-ER and Service provisioning information retrieval from ECS-ER in order to provide support for roaming, federation and edge node sharing. EDN information is exchanged between ECSs/ECS-ERs using EDGE-10 reference point.

Further, application life cycle management for federation is specified in 3GPP TS 28.538 [17]. Once application server is instantiated, it registers with EES, which in turn registers with ECS. The EDN information contains EDN connection information, list of EES along with EASIDs, provider's ID, endpoint information and other required details.

5.6.2 ETSI MEC

The MEC federator (MEF) as described in clause 7.1.9 of ETSI GS MEC 003 [4] enables a MEC federation between MEC systems. Mff reference point is defined between MEFs within the MEC federation for sharing information, such as MEC system information that includes MEC system ID, MEC system name, MEC system provider and MEF endpoint information. The federation enablement service is summarised in clause 5.2.1 of ETSI GS MEC 040 [6] and enables the shared usage of MEC services and applications across different systems.

6 Alignment of EDGEAPP with GSMA OP

6.1 General

Clause 6 describes the alignment between 3GPP EDGEAPP and GSMA OP by illustrating the mapping relationship between 3GPP EDGEAPP architecture and GSMA OP architecture (which includes ECS, EES and Edge management system) as described in clause 6.2.

6.2 Relationship between EDGEAPP architecture and GSMA OPG reference architecture

Figure 6.2-1 and Figure 6.2-2 illustrates the relationship between EDGEAPP architecture and GSMA OPG reference architecture [3].

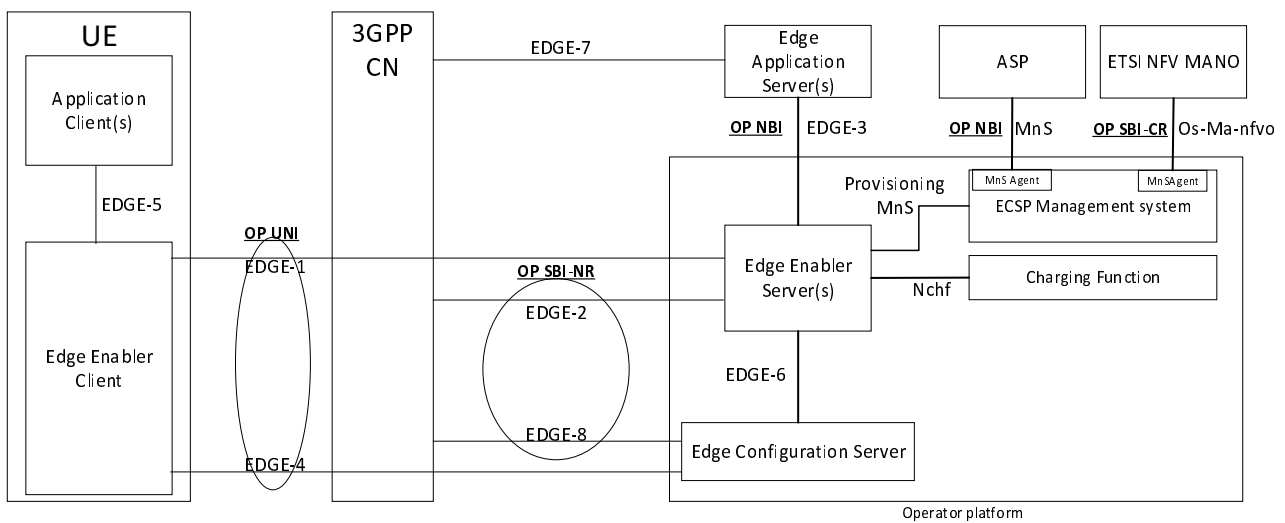


Figure 6.2-1: Relationship between EDGEAPP architecture and GSMA OPG reference architecture without Federation

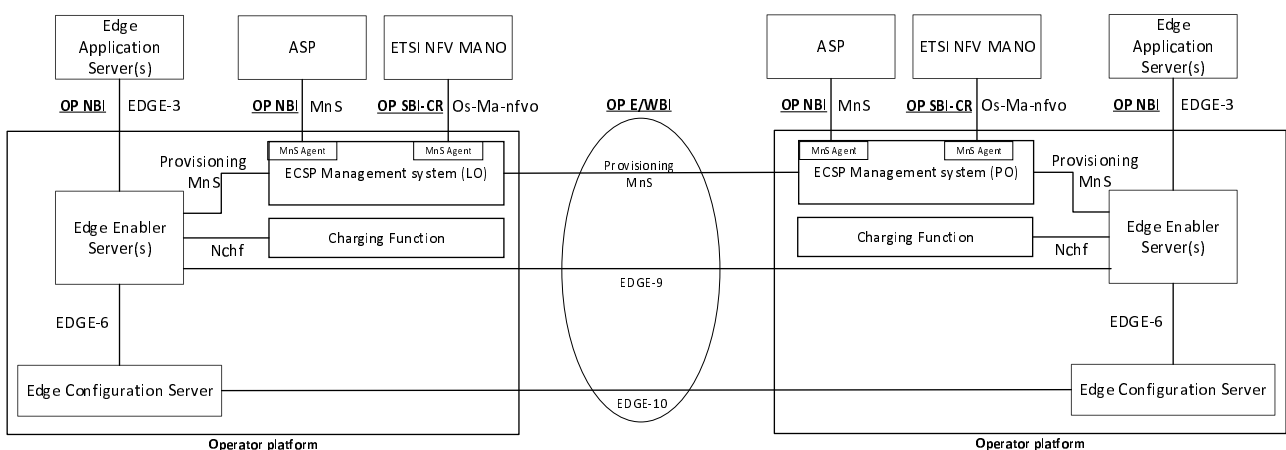


Figure 6.2-2: Relationship between EDGEAPP architecture and GSMA OPG reference architecture with Federation

EDGE-1 and EDGE-4 reference points can support similar function(s) as OP's User-Network interface (UNI), providing the Edge Enabler Client (corresponding to Edge/User Client in OP) with the information required to access the edge services. EDGE-1/EDGE-4 neither impact nor overlap with other existing 3GPP interfaces between the UE and the network, catering to the OP's requirements on UNI.

EDGE-2 and EDGE-8 reference points can support similar function(s) as OP's Southbound interface (SBI), through which the edge enabler layer (corresponding to the operator platform) access the 3GPP network capabilities and services (e.g. SCEF/NEF). Specifically, EDGE-2 and EDGE-8 cater to the requirements of the SBI-NetworkResource interface. ECSP management system utilizes ETSI NFV MANO as specified in 3GPP TS 28.538 [8] and caters to the requirements of OP's SBI-CloudResource interface over Os-Ma-nfvo reference point. The charging function is specified in 3GPP TS 32.257 [18].

EDGE-3 reference point can support similar function(s) as OP's Northbound interface (NBI), exposing the capabilities of Edge Enabler Server to the Edge Application Servers (EAS) hosted on the edge. OP's NBI also expands capabilities exposure to ASPs, for example to on-board applications to be deployed as EASs based on specific criteria.

EDGE-9 and EDGE-10 reference point can support similar function(s) as OP's East/Westbound interface (E/WBI), allowing the edge enabler layer to interact within and beyond its domains e.g., between operator platforms. OP's E/WBI focuses on use cases like user and application roaming or resource sharing across domains. The ECSP management system as specified in 3GPP TS 28.538 [8] caters to the requirements of OP's EWBI enabling the interactions between

ECSP management systems of a Leading Operator (LO) and a Partner Operator (PO) to support use cases for Federation relationship management and Federation Management.

7 Deployment Considerations

7.1 General

Figure 7.1-1 shows the EDGEAPP and ETSI MEC aligned Application Server and platform deployment. The depicted Edge platform consists of functionalities provided by both EES and MEC platform. The EES and MEC platform are functionally aligned in the implementation of the Edge platform. The depicted Application Server implements the functionalities of an Edge Application Server or MEC application instance or both.

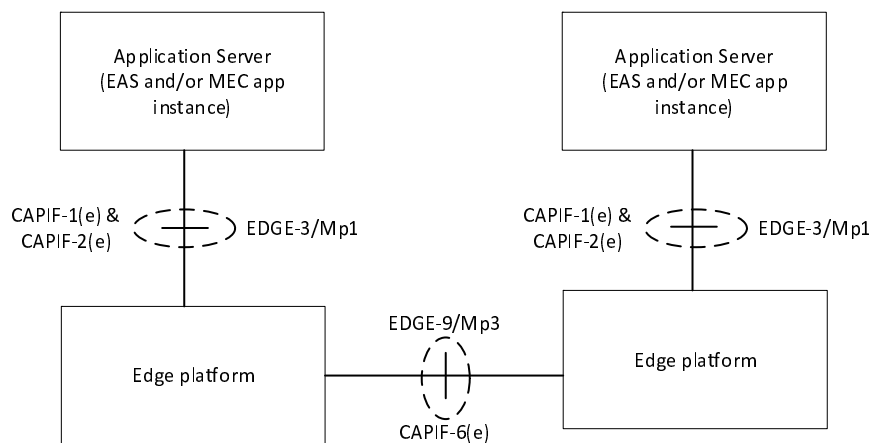


Figure 7.1-1: EDGEAPP and ETSI MEC aligned Application Server and platform deployment.

EDGE-3 is provided to Application Servers presenting themselves to the Edge platform as Edge Application Servers. Mp1 is provided for Application Servers presenting themselves to the Edge platform as MEC application instances.

An Edge platform adopting the CAPIF framework could provide the capabilities offered by EDGE-3 and Mp1 through utilisation of CAPIF-1 (/CAPIF-1e) and CAPIF-2 (/CAPIF-2e) to provide a unified service. For instance, a mapping of the MEC service management API to the 3GPP CAPIF API is presented in Annex B of ETSI GS MEC 011 [5].

EDGE-9 and Mp3 provide services required for interconnectivity between Edge platforms. EDGE-9 provides the interconnectivity required by Edge Enabler Servers, whilst Mp3 provides the interconnectivity required by MEC platforms.

An Edge platform adopting the CAPIF framework could provide the capabilities offered by EDGE-9 and Mp3 through utilisation of CAPIF-6 (/CAPIF-6e) to provide a unified service.

NOTE: APIs supported over Mp3 have not currently been specified by ETSI MEC.

Management aspects relating to application server and platform management are captured in 3GPP TS 28.538 [8] (EDGEAPP entity specific) and ETSI GS MEC 010-2 [9] (MEC entity specific), where the commonality is that both specify ETSI NFV MANO for performing lifecycle management functions. Management related interfaces are not depicted in Figure 7.1-1.

7.2 Deployment option of EDGEAPP and ETSI MEC using CAPIF

3GPP provides a framework for supporting common capabilities for northbound APIs (e.g., onboarding, authentication, authorization, discovery, auditing, etc.) through the common API framework (CAPIF) as specified in 3GPP TS 23.222 [10]. The functional model of CAPIF enables an API invoker to access (and invoke) service APIs and supports API exposing functions in publishing the API towards the API invokers. To enable the common supporting capabilities among API invokers and API providers, the CCF is introduced as the functional entity in charge of, among other tasks, authenticating an API invoker, providing authorization for the API invoker prior to accessing the service API, publishing, storing, and supporting the discovery of service APIs information, etc.

As from Annex A in TS 23.558 [2], an EAS may assume the role of:

- API invoker: for accessing northbound APIs exposed by SCEF/NEF or consuming service APIs offered by other EASs or EES, or
- API provider: exposing its service APIs for consumption by other API invokers,

whereas the EES may act like AEF and CCF (the latter being dispensable if, e.g., a centralized instance of CCF is available, see Clause A.5.3 in 3GPP TS 23.558 [2]).

Additionally, as from Annex B in ETSI GR MEC 031 [11], a MEC App may assume the role of:

- API invoker: for accessing northbound APIs exposed by SCEF/NEF or consuming MEC services advertised by the MEP, or
- API provider: registering (publishing) its service APIs and exposing them for consumption by other API invokers,

whereas the MEP may assume the role of API provider, CCF, and API invoker. A MEC service produced by a MEC App or MEP can be mapped into the API provider domain in CAPIF.

Since the different functional entities of both EDGEAPP and ETSI MEC may assume several roles, the number of scenario combinations is high. Therefore, rather than providing an exhaustive study of possible CAPIF-based deployments, some generic scenarios are presented in Figure 7.2-1.

In Figure 7.2-1, it is assumed that:

- Edge Platforms (e.g., complying with MEC platform and/or EDGEAPP) can co-exist in the network within the same PLMN trust domain,
- API invokers want to access MEC services, or API invokers want to consume EDGEAPP services,
- Extensible transport for service invocations (Different protocol and data formats including REST-HTTP are supported) is used.

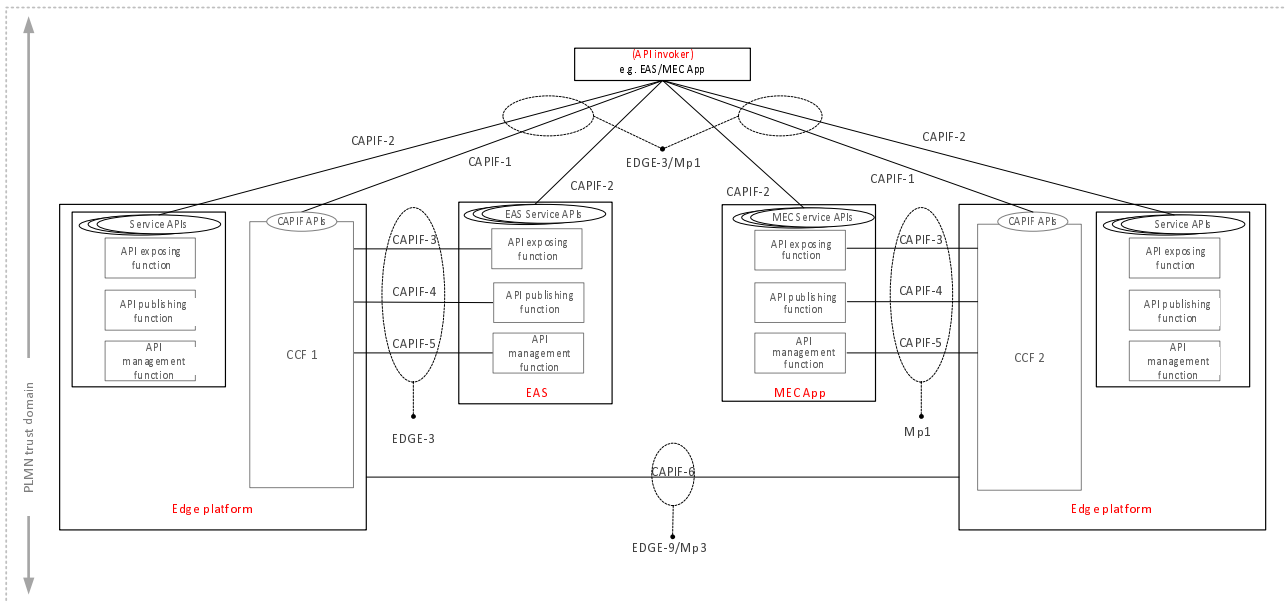


Figure 7.2-1: Illustration of deployment option using CAPIF

On the left-hand side of Figure 7.2-1, the Edge Platform implements CCF 1 to manage the Service APIs exposed by EAS and EES, EAS implements the API Provider domain functions to expose EAS Service APIs to EASs (and ETSI MEC Applications acting as API invokers). The Edge Platform implements API Provider domain functions to expose EES Service APIs (e.g., UE location API, AC information exposure API, etc.) to API invokers (e.g., EASs, ETSI MEC Applications).

On the right-hand side of Figure 7.2-1, the Edge Platform implements an instance of CCF (i.e., CCF 2) to manage the MEC Services exposed by MEP and MEC App. Both MEP and MEC App implement API Provider domain functions to expose MEC Services via CAPIF-2.

CCF 1 and CCF 2 interact via CAPIF-6 reference point, which supports publishing the service APIs information and discovering the service APIs information on both platforms. The CCF 1 and the CCF 2 publish the service API provided by its connected API exposing function(s) and obtains the service API information provided by other CCF.

An API invoker (e.g., EAS or MEC App) connected to the any of the CCF can discover and invoke service APIs provided by the API exposing function connected to the other CCF.

In Figure 7.2-2, another possible deployment scenario (out-of-many) is illustrated in which:

- Two ECSPs are present with different trust domains,
- A PLMN operator (or SNPN provider) deploys API provider functions via the NEF to expose northbound APIs, as illustrated in Section B.2.2.3 in 3GPP TS 23.222 [10],
- An API invoker wants to access MEC services or EES services or wants to consume network capabilities,

Extensible for service invocations (Different protocol and data formats including REST-HTTP are supported) transport is used.

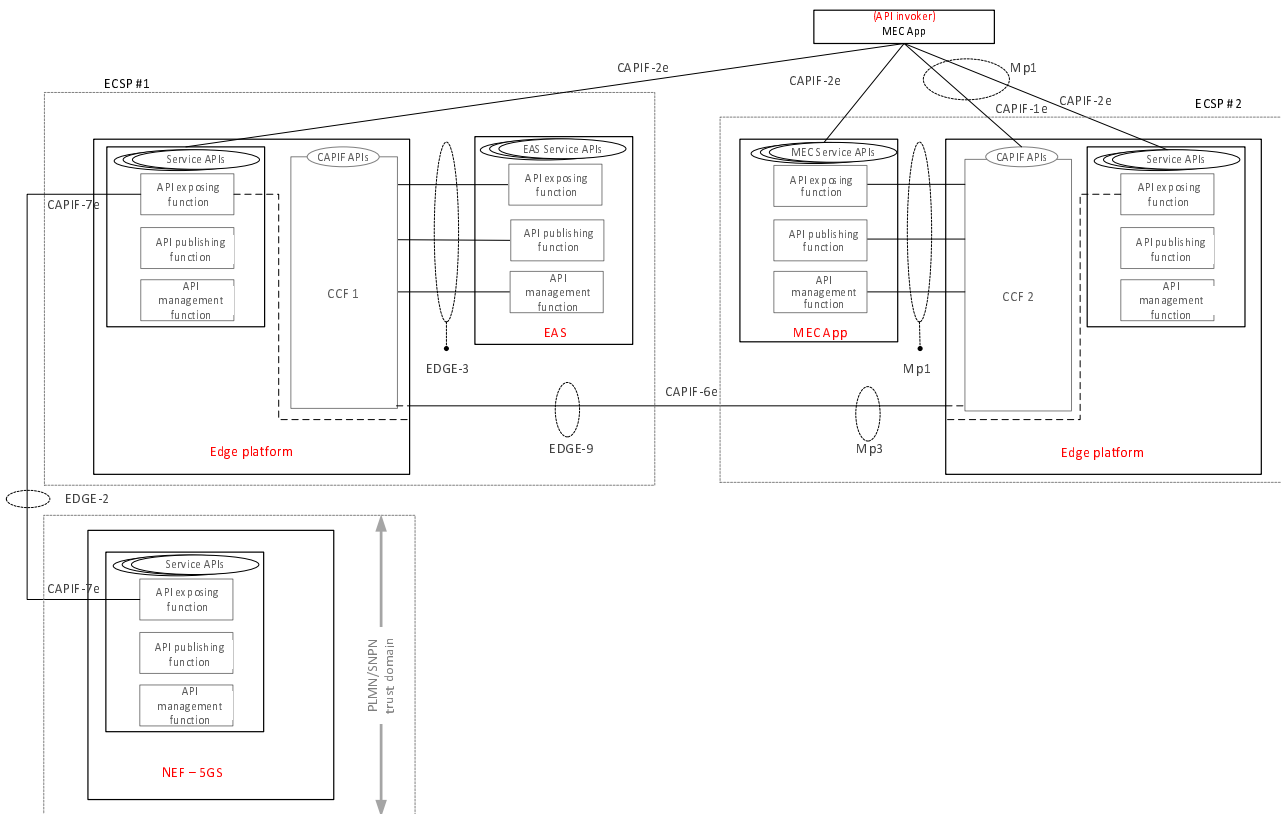


Figure 7.2-2: Illustration of deployment MEC using CAPIF across several trust domains

In this scenario, Edge platform deployed by ECSP#1 acts as a proxy for accessing 5GS capabilities, enabling in that manner topology hiding for the API invoker accessing the service APIs from outside the PLMN/SNPN trust domain.

NOTE: The details about CAPIF-related reference points within the same trust domains have been removed for the sake of readability.

ECSP#1 applies topology hiding and provides the AEF details of the Edge platform for invocation of NEF services to ECSP#2. The API invoker onboarded on ECSP#2 is able to discover the NEF services offered by ECSP#1 (supported by CAPIF-1 and CAPIF-6e). The API invoker performs API invocation on the AEF in ECSP#1’s Edge platform which further forwards or routes the API invocation to the NEF.

8 Conclusions

The following is the conclusion on the alignment of 3GPP Edge Enabler Layer, ETSI MEC and GSMA OP architectures:

1. CAPIF framework is aligned between 3GPP EDGEAPP and ETSI MEC architectures. An Edge application acting as a CAPIF API invoker can discover and invoke Edge platform services from 3GPP EDGEAPP, and ETSI MEC.
2. For Alignment of 3GPP EDGEAPP with ETSI MEC:
 - a) EASProfile and AppInfo are mapped for mandatory information elements. The mapping between EASProfile and AppInfo can be used for aligning EES and MEC platform and their interfaces in an implementation.
 - b) Using mapping between EASProfile and AppInfo, MEC application instance can register to EES by providing mandatory IEs.
 - c) 3GPP EDGEAPP architecture and ETSI MEC architecture are functionally aligned.
3. For Alignment of 3GPP EDGEAPP with GSMA OP:

- a) GSMA OPG specified edge computing related use cases, requirements (e.g. roaming, federation and edge node sharing) for Operator Platform can be realized by 3GPP EDGEAPP.

AnnexA: Mapping roles between EDGEAPP architecture and GSMA OPG architecture

GSMA Operator Platform Group has published their edge requirements in Operator Platform Telco Edge Requirements [3].

Clause 3 of Operator Platform Telco Edge Requirements [3] provides the OP Roles and Interfaces Reference Architecture. Clause 3.2 of Operator Platform Telco Edge Requirements [3] defines roles along with their key functions.

The three main roles in the GSMA OP architecture and their mapping with EDGEAPP architecture entity is as follows:

- 1) Capabilities Exposure Role: It enables an Application Provider to operate their applications. Table A-1 shows the scenarios enabled by Capabilities exposure role as indicated in Operator Platform Telco Edge Requirements [3] and their mapping with 3GPP EDGEAPP architecture.

Table A-1: Capabilities exposure role

Interface	Scenario	Description	Mapping to 3GPP EDGEAPP
NBI	Edge Cloud Infrastructure Endpoint Exposure	The Application Provider uses an authenticated and authorized endpoint to carry out scenarios involving application instances on edge clouds;	ASP interacts with 3GPP Management system using Management Service for Edge Computing, as defined in Clause 8 of 3GPP TS 28.538, to carry out scenarios involving application instances on Edge Data Network.
	Application Onboarding	The Application Provider uses the NBI to provide application images and metadata to the OP Federation Broker/Manager Role	Application instances are managed by 3GPP Management System as VNFs. VNF on boarding is defined in ETSI GS NFV IFA-013. This may require additional functionality to be defined between ASP and ECSP Management System.
	Application Metadata/Manifest Submission	The Application Provider uses the NBI and the metadata model to submit application metadata to the OP and follows defined procedures to extend the metadata model specification	
	Application CI/CD Management DevOps	The Application Provider integrates the CI/CD framework used to create an application with the OP via NBI APIs (which implies an integration between a CI/CD framework and Application Onboarding and Lifecycle Management)	
	Application Lifecycle Management	The Application Provider observes and changes the operational state of application instances, including the geographical/network extent of the OP on which application instances may run;	Clause "7.1 Lifecycle management" of 3GPP TS 28.538.
	Application Resource Consumption Monitoring	The Application Provider observes resource consumption of application instances, using the resource data model	Defined in clause "8.2.1 EAS performance assurance" of 3GPP TS 28.538. The virtual resource usage can be monitored by collecting the respective performance measurements as defined in clause 8.2.1.2 of 3GPP TS 28.538.
	Edge Cloud Resource Catalogue exposure	The Application Provider inventories edge cloud resources nominally available to application instances	
	Network Capabilities exposure	The Application Provider inventories network capabilities, like Network Analytics, nominally available to application instances	EES (as per clause 8.7.3)

- 2) Service Resource Manager Role: The Service Resource Manager role in the OP is responsible for managing Cloud and Network resources from the Edge Cloud(s) via the SBI and UNI interfaces. Table A-2 shows typical scenarios enabled by the Service Resource Manager role towards the different interfaces as indicated in Operator Platform Telco Edge Requirements [3] and their mapping with 3GPP EDGEAPP architecture.

Table A-2: Service Resource Manager Role

Interface	Scenario	Mapping to 3GPP EDGEAPP
SBI	Inventory, Allocation and Monitoring of Compute resources from Edge Cloud Infrastructure via the Southbound Interface – Cloud Resources (SBI-CR);	Application instances are managed by 3GPP Management System as VNFs. VNF resource orchestration, including reservation, is defined in ETSI NFV IFA013
	Orchestration of Application instances on the Edge Cloud Infrastructure via the SBI-CR interface	
	Cloud resource reservation managed by the OP	
	Configuring UE traffic management policies to accomplish the application's requirements, or the UE's IP address shall be maintained	
	Exposure of usage and monitoring information to operator's charging engine via the Southbound Interface – Charging functions (SBI-CHF) to enable operators to charge for the OP's services.	The charging for edge is defined in 3GPP TS 32.257.
Southbound Interface – Network Resources (SBI-NR)	Fetch Cloudlet locations based on the mobile network data-plane breakout location	
	Subscribe and receive notifications on UE Mobility events from the network to assist applications	UE mobility events are exposed by NEF (TS 23.502) and EES and ECS subscribes to receive UE mobility notification to assist applications for ACR
	Configure traffic steering in the Mobile Network towards Applications orchestrated in Edge Clouds	NEF exposes TrafficInfluence service (TS 23.502), EES uses the TrafficInfluence service to steer the traffic (related to traffic influence)
	Receive statistics/analytics, e.g. to influence Application placement or mobility decisions	
	Receive information related to the network capabilities, such as QoS, policy, network information, etc	NEF exposes events related to network capabilities, EES and ECS subscribes to receive network capability related information.
UNI	Application Instantiation/Termination, e.g. based on triggers from the UNI	
	Application Endpoint exposure towards User Clients (UC) via the UNI	EES (clause 8.4.2 and clause 8.5)
	Application Placement decisions, e.g. based on measurements/triggers from the UNI	

3) Federation Broker and Federation Manager Roles: The Federation Broker and Manager Roles in the OP are responsible for interfacing with other OPs via the East-West Bound Interface. Table A-3 shows typical scenarios enabled by the Federation Broker and Federation Manager Roles as indicated in Operator Platform Telco Edge Requirements [3] and their mapping with 3GPP EDGEAPP architecture.

Table A-3: Federation Broker and Federation Manager Roles

Interface	Scenario	Mapping to 3GPP EDGEAPP
EWBI	Federation Interconnection Management	Clause "7.5.2 Edge Federation Establishment" of 3GPP TS 28.538.
	Edge Cloud Resource Exposure and Monitoring towards partner OPs	
	Network and Analytics Capabilities Exposure towards partner OPs	
	Application Images and Application metadata transfer towards partner OPs	Application instances are managed by 3GPP Management System as VNFs. Application Image and metadata management is considered part of VNF onboarding. VNF onboarding is defined in ETSI NFV IFA013.
	Application Instantiation/Termination towards partner OPs	Clause "7.5.3 Edge Federation Establishment" of 3GPP TS 28.538.
	Application Monitoring towards partner OPs	
	Edge Cloud Resource Catalogue exposure	EES (Exposing EAS profile) (See NOTE 1)
	Service Availability in visited networks	ECS (Table 8.3.3.3.3-2 and clause 8.17.2.4 of TS 23.558) (See NOTE 2)
NOTE 1: Edge Cloud Resource Catalogue may contain information other than EAS profile which is within scope of SA5.		
NOTE 2: EASIDs are considered as available services in partner ECSP and are exchanged between ECSs of home ECSP and partner ECSP.		

Based on the mapping tables in this clause, EES and ECS of 3GPP EDGEAPP architecture can be mapped to take responsibilities of the some roles as defined in GSMA OPG reference architecture.

Editor's note: Alignment of EDGEAPP and GSMA OP for ECSP Management System is FFS and requires inputs from SA5.

Annex B (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2022-08	SA6#50-e					TR Initial Version	0.0.0
2022-09	SA6#50-e					TR Skeleton (as per TR template)	0.0.1
2022-09	SA6#50-e					Implementation of the following pCRs approved by SA6: S6-222591, S6-222592	0.1.0
2022-10	SA6#51-e					Added Introduction through pCR: S6-222662	0.2.0
2023-03	SA6#53					Added background and updated index through pCR: S6-231043 and S6-231078	0.3.0
2023-03	SA6#53					Corrected the mistake in implementing S6-231043	0.3.1
2023-04	SA6#54-e					Implemented pCR: S6-231508	0.4.0
2023-08	SA6#56					Implemented pCRs: S6-232648, S6-232370, S6-232651, S6- 232649, S6-232471, S6-232664, S6-232473	0.6.0
2023-09	SA#101	SP-230986				Submitted to SA#101 for information	1.0.0
2023-10	SA6#57					Implemented pCRs: S6-233419, S6-233341, S6-233404, S6- 233343, S6-233344	1.1.0
2023-10	SA6#57					Editorial correction to add missing version v1.0.0 in the present history table	1.1.1
2023-11	SA6#58					Implemented pCRs: S6-233988, S6-233960, S6-233990, S6- 233991, S6-233490, S6-234032, S6-234099, S6-233997, S6- 23998, S6-233698, S6-234066, S6-234070	1.2.0
2023-12	SA#102	SP-231538				Submitted to SA#102 for approval	2.0.0
2023-12	SA#102	SP-231538				MCC Editorial update for publication after TSG SA approval (SA#102)	18.0.0
2024-03	SA#103	SP-240301	0001	2	F	Updates to role mapping between EDGEAPP and GSMA	18.1.0
2024-06	SA#104	SP-240752	0002	2	F	Update on Alignment of EDGEAPP and GSMA OP for ECSP Management System	18.2.0

History

Document history		
V18.1.0	April 2024	Publication
V18.2.0	July 2024	Publication