ETSI GS MEC 060 V4.1.1 (2026-04)

GROUP SPECIFICATION

Multi-access Edge Computing (MEC); API Gateway for Client Applications

Disclaimer

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

Reference
DGS/MEC-0060v411ClientApiGW

Keywords
authorization, gateway

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

Contents

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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.

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document specifies requirements and an information model related to the granting and revocation of client application access to MEC application client-facing endpoints via the API Gateway for client applications (AGW), and supporting the exchange of management-related information between the MEC system and the AGW.

In addition, the present document describes the access granting procedure defined by OAuth 2.0 client credentials flow when it is applied via the API Gateway. This procedure can be used to access MEC applications over the Mx3 reference point between the client application and the AGW in the MEC system.

The intended audience of the present document are the application developers for the MEC system, since it specifies requirements and an information model supporting security-related access control for client applications accessing their MEC applications via an API Gateway.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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

The following referenced documents are necessary for the application of the present document.

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

[2] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[3] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[4] IETF RFC 8705: "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens".

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

[6] ETSI GS MEC 011: "Multi-access Edge Computing (MEC); Edge Platform Application Enablement".

2.2 Informative references

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

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

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

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

[i.2] ETSI GS MEC 009: "Multi-access Edge Computing (MEC); General principles, patterns and common aspects of MEC Service APIs".

[i.3] ETSI GS MEC 003: "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[i.4] OpenAPI™ Specification.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

API gateway for client applications: system level functional element that authorizes requests from the client application to access services provided by the MEC Applications, revoking this authorization upon certain conditions

3.2 Symbols

Void.

3.3 Abbreviations

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

AA	Authentication and Authorization
AGW	API GateWay (for client applications)
SMM	Security Monitoring and Management

4 Overview

The present document addresses access control for interactions over the Mx3 reference point between client applications and the API Gateway for client applications (AGW) in the MEC system, in support of the corresponding requirements defined for the Multi-access Edge Computing in clause 6.3.17 of ETSI GS MEC 002 [1].

Clause 5 describes the access granting procedure defined by the OAuth 2.0 client credentials flow when it is applied via the API Gateway and illustrates the corresponding information flow over the Mx3 reference point.

Clauses 6 and 7 specify the normative requirements and the information model for access control related to the Mx3 reference point, including configuration and enforcement of access control by the API Gateway.

5 Description of the service (informative)

5.1 Introduction

5.1.1 Overview

Where deployed, an API gateway is an entity that serves as a single entry point for managing requests from client applications (also referred to API calls). In the context of MEC, client application interaction with a MEC application can be considered analogous to the general client interaction with an API, particularly regarding the functional role of the API gateway for client applications.

A client application interacts with a MEC application by sending request messages and receiving response messages. The API gateway authenticates the client application and ensures that only authorized requests are forwarded to the MEC application for processing them and generating a response which is then returned to the client application. This way, the API gateway enforces access control to the applications or resources it is protecting.

The involvement of the API gateway as a relay in the interaction between client application and API (i.e. MEC application) is typically transparent to the client application, except that it requires the client application to present a security token to authorize the interaction. A client application request to access a URI/server/application (i.e. MEC application) can be routed via the API gateway through appropriate network router and API gateway configuration.

The goal of the messages to be exchanged on the Mx3 interface is to specify standards-based security signalling in order to protect the MEC applications running on the MEC host. Thus, the messages specified herein are those of the "signalling" part, and will be based when possible on existing standards such as OAuth2.0 [2].

5.1.2 The functionality of API gateway for client applications

When supported, the API gateway for client applications (AGW) is part of the MEC system and it may be managed by the OSS.

An AGW authorizes access to the interface/services MEC applications provide to client applications.

The gateway interacts not only with client applications in the device (e.g. UE, laptop with internet connectivity) but also may interact with the OSS for obtaining configuration and security-related policies to apply to each MEC application.

The AGW may support the following functionality:

- Configuration by the MEC operator or MEC application provider to use an AA entity (see ETSI GS MEC 009 [i.2]) or not, subject to the access control needs of individual MEC applications (mechanism out of scope).
- Configuration by the MEC application provider for authentication and authorization of its users.
- Configuration by or via the OSS to apply one of the policies with which the AGW already has been provisioned.
- Verification - potentially using the AA entity - of access tokens (in the context of the authorization request) presented to it by client applications.
- Enabling API-related messages to flow between client application and MEC application upon authorization grant.
- Revoking authorization for a given MEC application, based for example on an instruction from the OSS to terminate connections from hosts that are identified as potential security threats (e.g. to prevent Denial of Service/flooding attacks).

The AA entity and related interactions are out of scope of the present document.

5.2 Sequence diagrams

5.2.1 Introduction

The following clauses describe how the client application interacts with the AGW over the Mx3 reference point, and how the AGW interacts with the OSS over the Mm10 reference points. The sequence diagrams that are relevant for the APIs are presented.

For access control, the client application presents an access token to the AGW with every request in order to assert that it is allowed to access the service provided by a given MEC Application. The access token is included in the "Authorization" request header field as a bearer token according to IETF RFC 6750 [3], or another type of token such as a certificate-bound access token as per IETF RFC 8705 [4].

5.2.2 Access token-based authorization

The client application access is the procedure to request access to APIs/services provided by MEC applications to client applications. The endpoint with which the client communicates is referred to as the API Producer (another name could be API endpoint). The client application access procedure based on OAuth 2.0 client credentials grant type is illustrated in figure 5.2.2-1.

NOTE 1: The application of other OAuth 2.0 flows, besides the client credentials flow, are not considered in the present document.

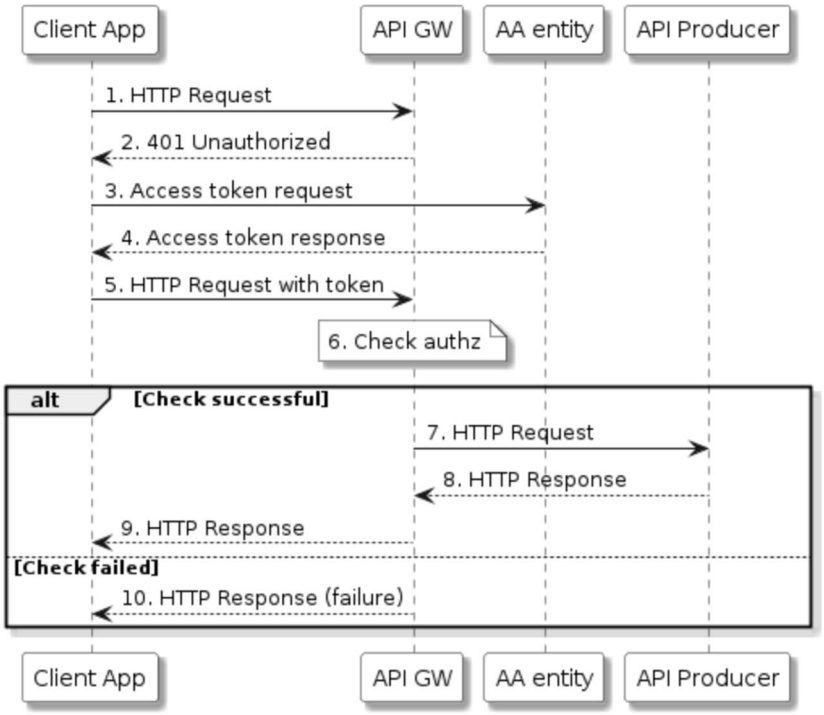

Figure 5.2.2-1: Client Application authorization

1) The client application sends an HTTP request to the AGW to access the client-facing services of a MEC application, i.e. the API Producer.

2) The AGW responds with "401 Unauthorized" which indicates to the client application that it has to obtain an access token for access to the resource.

3) The client application sends an access token request to the token endpoint provided by the AA entity as specified by IETF RFC 6749 [2], and authenticates towards the AA entity with its client credentials.

4) The AA entity sends an access token response and provides the access token and additional configuration information to the client application, as specified by IETF RFC 6749 [2].

5) The client application repeats the request from step (1) with the access token included as a bearer token (e.g. in an HTTP "Authorization" request header field), according to IETF RFC 6750 [3].

6) The AGW checks the token for validity, optionally with assistance from the AA entity (details out of scope) and determines whether the client application is authorized to access the API Producer identified in the token. For malformed access tokens, step 10) follows.

In case the client application is authorized:

7) The AGW forwards the HTTP request to the API Producer.

8) The API Producer executes the HTTP request and returns an appropriate HTTP response.

9) The AGW forwards the HTTP response to the client application.

In case the client application is not authorized:

10) The AGW sends an HTTP response (indication of authorization error) to the client application. For this access, the AGW prohibits the client application to access the client-facing services of that MEC application.

NOTE 2: In general, whenever the AGW receives a request, it may use an HTTP response 429 if the client sends too many requests. This response may include a "Retry-After" header, to inform the client how long to wait before retrying

NOTE 3: The AA entity may not be the same one as that referred to by ETSI MEC 009; it may be deployed for client application credential provisioning purposes and may be co-located with the AGW.

NOTE 4: In step 9, the forwarded response from the API producer can itself contain an HTTP error code to which the client application can react, which can result in additional retries to access APIs/services of a MEC application.

6 Specification level requirements

6.1 Requirements for reference point Mm10

The following requirements apply when the feature "APP-GW" is supported (see ETSI GS MEC 002 [1]):

REQ-MM10-1: The Mm10 reference point shall support a capability allowing the OSS to configure the AGW whether to use Authentication and Authorization to control access, per client-facing MEC application endpoint.

REQ-MM10-2: The Mm10 reference point shall support a capability allowing the OSS to instruct the AGW regarding which authorization policies to be used for a given client-facing MEC application endpoint.

REQ-MM10-3: The Mm10 reference point shall support a capability allowing the OSS to ask AGW to block one or more devices running client applications from accessing all the client-facing endpoints of a given MEC application.

7 Information model

7.1 Type: SecConfig

This information object class represents the type of information that the OSS sends to the AGW in order to enable the AGW to make correct access control decisions for client applications seeking access to a given MEC application client-facing endpoint.

Table 7.1-1 provides definitions for the attributes of SecConfig.

Table 7.1-1: SecConfig Attributes

Attribute name	Data type	Cardinality	Description
appName	String	1	Human readable name of the MEC application, the same as the attribute appName of the AppD information element (table 6.2.1.2.2-1 in ETSI GS MEC 010-2 [5]).
endPoints	EndPointInfo	1..N	Client-facing service endpoints, the same as the attribute endpoint (table 7.1.2.6-1 in ETSI GS MEC011 [6]) See note.
useAA	Boolean	1	Whether or not the AGW is to use authentication/authorization for the corresponding MEC application client-facing endpoint. Permitted values: • TRUE: AGW is to use authentication/authorization • FALSE: AGW is not to use authentication/authorization See note.
authzPolicies	String	0..N	List of selectors indicating which policies are to be used by the AGW to determine authorization of the client (per MEC application client-facing endpoint), or none. (Implementation dependent)
blockClientIps	IpAddr	0..N	List of IP addresses of devices (running client application) to be blocked from accessing any of the client-facing endpoints of the MEC application.
NOTE: A MEC application may make available multiple API service endpoints to the client application. Authentication and authorization by the AGW may be applied for each endpoint; therefore the endPoints and useAA attributes have the same multiplicity and are ordered to have a 1-1 mapping for the use of authentication and authorization for each endpoint in the endPoints list.			

Annex A (informative): Aspects related to API Gateways

A.1 Background information

In contemporary cloud infrastructures, an API Gateway represents a functional component that supports the reliable, secure, and scalable interaction between clients and distributed services. Functioning as an intermediary middleware layer, in general an API Gateway may serve as a centralized point of entry for all API calls, performing certain operational tasks such as request routing, load balancing, user authentication, request and response logging, and the enforcement of security and compliance policies. An API Gateway not only streamlines the way clients interface with backend services but also provides a common mechanism for applying governance across increasingly complex and distributed systems.

An API Gateway can act as a protocol mediator. By translating messages between differing communication protocols (e.g. HTTP, gRPC, WebSockets), the gateway enables seamless interoperability among heterogeneous services.

The importance of API Gateways has grown substantially in recent years due to the proliferation of microservices architectures, Internet of Things (IoT) deployments, and AI-driven applications. These environments typically involve a vast number of loosely coupled components that need to interact efficiently, securely, and at scale. In such contexts, API Gateways can offer visibility, governance, and security controls necessary to orchestrate complex interactions across a dynamic ecosystem of services.

A.2 API Gateways in Multi-access Edge Computing

The Multi-access Edge Computing (MEC) environment offers extremely low latency and high data throughput, along with immediate access to contextual radio network data that applications can utilize to improve responsiveness and efficiency. Within the MEC ecosystem, API Gateways can streamline access to distributed edge resources by, e.g. handling message routing, enforcing security policies and managing traffic load. Additionally, decentralized deployments of API Gateways based on the ETSI MEC architecture (see ETSI GS MEC 003 [i.3]) are well suited to the need to manage local edge service exposure.

In the context of Multi-access Edge Computing (MEC), the API Gateway (AGW) can enable secure and policy-driven access to MEC services by serving as a control point through which client applications interact with MEC applications hosted on edge hosts, as defined in the present document.

When deployed, the AGW may be co-located with the MEC platform and supports the following essential functionalities:

1) **Stable service connection endpoints:**

   - The API Gateway enables client applications to access the MEC system via consistent and stable service connection endpoints. Even in the event of IP address changes (e.g. due to MEC application scaling or relocation), client applications are not required to update their endpoint configurations. This simplifies connectivity and ensures robust service continuity across dynamic network environments.

2) **Load balancing across MEC service instances:**

   - The AGW can distribute client applications requests across multiple MEC application instances. This ensures efficient utilization of resources, minimizes latency, and enhances fault tolerance. Load balancing policies may be customized by the MEC operator depending on performance requirements and service-level objectives.

3) **Request throttling for controlled throughput:**

   - To safeguard system performance and fairness among clients, the API Gateway may support throttling of API requests. For example, as outlined in the present document (clause 5.2.2), the AGW may issue HTTP 429 (Too Many Requests) responses and optionally include a Retry-After header. This mechanism prevents overload conditions and enables request rate adaptation in accordance with operator-defined policies.

4) **Monitoring and observability:**

   - The AGW may enable the collection of metrics on access requests to the MEC system, which can be used for service usage monitoring, performance analysis, and statistical reporting, also from a security perspective. For example, AGW may interact with SMM for data analytic purposes related to access requests to the MEC system.

These capabilities enable managing secure access to MEC applications and ensuring consistent quality of service. Additionally, through its integration with the OSS as described in ETSI GS MEC 003 [i.3], the AGW can be dynamically configured to apply specific authentication and authorization policies per client-facing endpoint.

Annex B (informative): AGW authorization policy examples

B.1 Introduction

This annex provides examples of authorization policies an AGW can enforce in checking client app access to APIs/services provided by MEC applications.

B.2 Examples

This clause provides authorization policy examples as described in table B.2-1.

Table B.2-1: Authorization policy examples

AGW policy for a given MEC application	Description
RestrictByIpAddressRange	Only allow requests from clients with an IP address from a given range (which can, e.g. be used for geofencing)
RestrictByHours	Only allow requests from clients during certain (local) hours (e.g. business hours)
RestrictByHoursAndIpAddressRange	Only allow requests from clients during certain (local) hours and from IP addresses within a given range (which can, e.g. be used for restricting access to business hours and for geofencing)
RestrictByClientCredentials	Limit client application access based on their credentials (e.g. only allow requests if certificates are issued by a trusted certificate authority)
RestrictByLocation	Limit client application access based on their location

Annex C (informative): Complementary material for data model utilization

To complement the definitions for each method and resource defined in the interface clauses of the present document, ETSI MEC ISG is providing for the AGW data model a supplementary description file compliant to the OpenAPI Specification [i.4].

In case of discrepancies between the supplementary description file and the related data structure definitions in the present document, the data structure definitions take precedence.

The supplementary files, relating to the present document, are located at https://forge.etsi.org/rep/mec/gs060-clientapigw-api.

Annex D (informative): Change history

Date	Version	Information about changes
September 2024	V4.0.1	Publication of first draft.
October 2024	V4.0.2	Incorporates MEC(24)000346r3 (clause 5.1.1), MEC(24)000349r2 (clause 5.2).
November 2024	V4.0.3	Incorporates MEC(24)000347r2 (clause 5.1.2), and previously missed reference [i.2].
March 2025	V4.0.4	Incorporates MEC(24)00473r3, MEC(24)00447r7, MEC(25)0059r2.
April 2025	V4.0.5	Incorporates MEC(25)000078r1, MEC(25)000079r1, MEC(25)000133, removes [i.2] as it is already in [1].
July 2025	V4.0.6	Incorporates MEC(25)000288r3.
October 2025	V4.0.7	Incorporates MEC(25)000342r1, MEC(25)000357r3, MEC(25)000362r2, MEC(25)000368, MEC(25)000364r4. For MEC(25) 000364r4 Editor replaced Annex A with Annex B since Annex A was already in use, and also reformatted title in order to match existing Annex A.
October 2025	V4.0.8	Minor editorial changes suggested via email Oct 22 2025.
October 2025	V4.0.9	Stable draft version based on V4.0.8.
December 2025	V4.0.10	Incorporates MEC(25)000400r1 and makes minor editorial changes to clauses 7.1.1 and 7.2.
December 2025	V4.0.11	Final draft similar to Stable draft V4.0.10 and ready to go to MEC RC for review.
January 2026	V4.0.12	Addresses comment received during RC about combining the two tables, editorials including adding to references.
February 2026	V4.0.12	Addresses comments received during RC for MEC060 approval, e.g. add SMM term and add informative annex about complementary material. Updates accepted at MEC Tech call#387 as per contribution MEC(26)000026r1.
March 2026	V1.1.1	First published version.

History

Version	Date	Status
V4.1.1	April 2026	Publication