ETSI GS MEC 009 V1.1.1 (2017-07)

Mobile Edge Computing (MEC);
General principles for Mobile Edge Service APIs

Disclaimer

The present document has been produced and approved by the Mobile 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-0009ApiPrinciples

Keywords
API, MEC

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Mobile 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 defines design principles for RESTful mobile edge service APIs, provides guidelines and templates for the documentation of these, and defines patterns of how mobile edge service APIs use RESTful principles.

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 at https://docbox.etsi.org/Reference.

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] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

NOTE: Available at https://tools.ietf.org/html/rfc7231.

[2] IETF RFC 7232: "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests".

NOTE: Available at https://tools.ietf.org/html/rfc72312.

[3] IETF RFC 5789: "PATCH Method for HTTP".

NOTE: Available at https://tools.ietf.org/html/rfc5789.

[4] IETF RFC 6901: "JavaScript Object Notation (JSON) Pointer".

NOTE: Available at https://tools.ietf.org/html/rfc6901.

[5] IETF RFC 7396: "JSON Merge Patch".

NOTE: Available at https://tools.ietf.org/html/rfc7396.

[6] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

NOTE: Available at https://tools.ietf.org/html/rfc6902.

[7] IETF RFC 5261: "An Extensible Markup Language (XML) Patch Operations Framework Utilizing XML Path Language (XPath) Selectors".

NOTE: Available at https://tools.ietf.org/html/rfc5261.

[8] IETF RFC 6585: "Additional HTTP Status Codes".

NOTE: Available at https://tools.ietf.org/html/rfc6585.

[9] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

NOTE: Available at https://tools.ietf.org/html/rfc63986.

[10] IETF RFC 7159: "The JavaScript Object Notation (JSON) Data Interchange Format".

NOTE: Available at https://tools.ietf.org/html/rfc7159.

[11] W3C Recommendation 16 August 2006: "Extensible Markup Language (XML) 1.1" (Second Edition).

NOTE: Available at https://www.w3.org/TR/2006/REC-xml11-20060816/.

[12] IETF RFC 5988: "Web Linking".

NOTE: Available at https://tools.ietf.org/html/rfc5988.

[13] IETF RFC 2818: "HTTP Over TLS".

NOTE: Available at https://tools.ietf.org/html/rfc2818.

[14] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

NOTE: Available at https://tools.ietf.org/html/rfc5246.

[15] IETF RFC 7807: "Problem Details for HTTP APIs".

NOTE: Available at https://tools.ietf.org/html/rfc7807.

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

NOTE: Available at https://tools.ietf.org/html/rfc6749.

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

NOTE: Available at https://tools.ietf.org/html/rfc6750.

2.2 Informative references

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

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

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

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

[i.2] "Please. Don't Patch Like An Idiot", William Durand.

NOTE: Available at http://williamdurand.fr/2014/02/14/please-do-not-patch-like-an-idiot/. Accessed 17 May 2016.

[i.3] "Richardson Maturity Model: steps toward the glory of REST", Martin Fowler, accessed 8 September 2016.

NOTE: Available at http://martinfowler.com/articles/richardsonMaturityModel.html.

[i.4] JSON Schema, Draft Specification v4, January 31, 2013.

NOTE: Available at http://json-schema.org/documentation.html. Also available as Internet Draft (work in progress) from https://tools.ietf.org/html/draft-zyp-json-schema-04.

[i.5] W3C Recommendation: "XML Schema Part 0: Primer Second Edition.".

NOTE: Available at https://www.w3.org/TR/xmlschema-0/.

[i.6] ETSI GS MEC 011: "Mobile Edge Computing (MEC); Mobile Edge Platform Application Enablement".

[i.7] ETSI GS MEC 012: "Mobile Edge Computing (MEC); Radio Network Information API".

[i.8] Hypertext Transfer Protocol (HTTP) Status Code Registry at IANA.

NOTE: Available at http://www.iana.org/assignments/http-status-codes.

[i.9] MQTT Version 3.1.1, OASIS™ Standard, 29 October 2014.

NOTE: Available at http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html.

[i.10] Apache Kafka™, https://kafka.apache.org/.

[i.11] GRPC™, http://www.grpc.io/.

[i.12] Protocol buffers, https://developers.google.com/protocol-buffers/.

[i.13] IETF RFC 7519: "JSON Web Token (JWT)".

NOTE: Available at https://tools.ietf.org/html/rfc7519.

[i.14] OpenAPI Specification.

NOTE 1: Available at https://github.com/OAI/OpenAPI-Specification.

NOTE 2: OpenAPI specification version 2.0 is recommended as it is the official release at the time of publication.

3 Definitions and abbreviations

3.1 Definitions

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

resource: object with a type, associated data, a set of methods that operate on it, and, if applicable, relationships to other resources

NOTE: A resource is a fundamental concept in a RESTful API. Resources are acted upon by the RESTful API using the Methods (e.g. POST, GET, PUT, DELETE, etc.). Operations on Resources affect the state of the corresponding managed entities.

3.2 Abbreviations

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

API	Application Programming Interface
BYOT	Bring Your Own Transport
CRUD	Create, Read, Update, Delete
DDoS	Distributed Denial of Service
GS	Group Specification
HATEOAS	Hypermedia As The Engine Of Application State
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
ISG	Industry Specification Group
JSON	Javascript Object Notation
MEC	Mobile Edge Computing
POX	Plain Old XML
REST	Representational State Transfer
RFC	Request For Comments
RPC	Remote Procedure Call
TCP	Transmission Control Protocol
TLS	Transport Layer Security

UE	User Equipment
URI	Uniform Resource Indicator
XML	eXtensible Markup Language

4 Design principles for developing RESTful mobile edge service APIs

4.1 REST implementation levels

The Richardson Maturity Model as defined in [i.3] breaks down the principal elements of a REST approach into three steps.

All RESTful mobile edge service APIs shall implement at least Level 2 of the Richardson Maturity Model explained in annex C.

It is recommended to implement Level 3 when applicable.

4.2 General principles

RESTful mobile edge service APIs are not technology implementation dependent.

RESTful mobile edge service APIs embrace all aspects of HTTP v1.1 (IETF RFC 7231 [1]) including its request methods, response codes, and HTTP headers. Support for PATCH (IETF RFC 5789 [3]) is optional.

For each RESTful mobile edge service API specification, the following information should be included:

- Purpose of the API.
- URIs of resources including version number.
- HTTP methods (IETF RFC 7231 [1]) supported.
- Representations supported: JSON and, if applicable, XML.
- Response schema(s).
- Request schema(s) when PUT, POST, PATCH are supported.
- Links supported (Optional in Level 2 APIs).
- Response status codes supported.

4.3 Entry point of a RESTful mobile edge service API

Entry point for a RESTful mobile edge service API:

- Needs to have one and exactly one entry point. The URI of the entry point needs to be communicated to API clients so that they can find the API.
- It is common for the entry point to contain some or all of the following information:
  - Information on API version, supported features, etc.
  - A list of top-level collections.
  - A list of singleton resources.
  - Any other information that the API designer deemed useful, for example a small summary of operating status, statistics, etc.

- It can be made known via different means:
  - Client discovers automatically the entry point and meaning of the API.
  - Client developer knows about the API at time of client development.

4.4 API security and privacy considerations

To allow proactive protection of the APIs against the known security and privacy issues, e.g. DDoS, frequency attack, unintended or accidental information disclosure, etc. the design for a secure API should consider at least the following aspects:

- Ability to control the frequency of the API calls (calls/min), e.g. by supporting the definition of a validity time or expiration time for a service response.
- Anonymization of the real identities.
- Authorization of the applications based on the sensitivity of the information exposed through the API.

5 Documenting RESTful mobile edge service APIs

5.1 RESTful mobile edge service API template

Annex D defines a template for the documentation of RESTful mobile edge service APIs. Examples how to use this template can for instance be found in ETSI GS MEC 011 [i.6] and ETSI GS MEC 012 [i.7].

5.2 Conventions for names

5.2.1 Case conventions

The following case conventions for names and strings are used in the RESTful mobile edge service APIs.

1) UPPER_WITH_UNDERSCORE

   All letters of a string are capital letters. Digits are allowed but not at the first position. Word boundaries are represented by the underscore "_" character. No other characters are allowed.

EXAMPLES 1:

   a) ETSI_MEC_MANAGEMENT.

   b) MULTI_ACCESS_EDGE_COMPUTING.

2) lower_with_underscore

   All letters of a string are lowercase letters. Digits are allowed but not at the first position. Word boundaries are represented by the underscore "_" character. No other characters are allowed.

EXAMPLES 2:

   a) etsi_mec_management;

   b) multi_access_edge_computing.

3) UpperCamel

   A string is formed by concatenating words. Each word starts with an uppercase letter (this implies that the string starts with an uppercase letter). All other letters are lowercase letters. Digits are allowed but not at the first position. No other characters are allowed. Abbreviations follow the same scheme (i.e. first letter uppercase, all other letters lowercase).

EXAMPLES 3:

a) EtsiMecManagement.

b) MultiAccessEdgeComputing

4) lowerCamel

As UpperCamel, but with the following change: The first letter of a string shall be lowercase (i.e. the first word starts with a lowercase letter).

EXAMPLES 4:

a) etsiMecManagement;

b) multiAccessEdgeComputing.

5.2.2 Conventions for URI parts

5.2.2.1 Introduction

Based on IETF RFC 3986 [9], the parts of the URI syntax that are relevant in the context of the RESTful mobile edge service APIs are as follows:

- *Path*, consisting of *segments*, separated by "/" (e.g. segment1/segment2/segment3).
- *Query*, consisting of pairs of parameter name and value (e.g. ?org=etsi&isg=mec, where two pairs are presented).

5.2.2.2 Path segment naming conventions

a) The path segments of a resource URI which represent a constant string shall use lower_with_underscore.

EXAMPLE 1: tsi_mec_management

b) If a resource represents a collection of entities, the last path segment of that resource's URI shall be plural.

EXAMPLE 2: …/prefix/api/v1/user**s**

c) For resources that are not task resources, the last path segment of the resource URI should be a (composite) noun.

EXAMPLE 3: …/prefix/api/v1/users

d) For resources that are task resources, the last path segment of the resource URI should be a verb, or at least start with a verb.

EXAMPLE 4:

…/app_instances/{appInstanceId}/instantiate

…/app_instances/{appInstanceId}/do_something_else

e) The path segments of a resource URI which represent a variable name shall use lowerCamel, and shall be surrounded by curly brackets.

EXAMPLE 5: {appInstanceId}

f) Once a variable is replaced at runtime by an actual string, the string shall follow the rules for a path segment defined in IETF RFC 3986 [9]. IETF RFC 3986 [9] disallows certain characters from use in a path segment. Each actual RESTful mobile edge service API specification shall define this restriction to be followed when generating values for path segment variables, or propose a suitable encoding (such as percent-encoding according to IETF RFC 3986 [9]), to escape such characters if they can appear in input strings intended to be substituted for a path segment variable.

5.2.2.3 Query naming conventions

a) Parameter names in queries shall use lower_with_underscore.

EXAMPLE 1: ?isg_name=MEC

b) Variables that represent actual parameter values in queries shall use lowerCamel and shall be surrounded by curly brackets.

EXAMPLE 2: ?isg_name={chooseAName}

c) Once a variable is replaced at runtime by an actual string, the convention defined in clause 5.2.2.2 item f) applies to that string.

5.2.3 Conventions for names in data structures

The following syntax conventions apply when defining the names for attributes and parameters in the RESTful mobile edge service API data structures.

a) Names of attributes / parameters shall be represented using lowerCamel.

EXAMPLE 1: appName.

b) Names of arrays (i.e. those with cardinality 1..N or 0..N) shall be plural rather than singular.

EXAMPLES 2: users, mecApps.

c) The identifier of a data structure via which this data structure can be referenced externally should be named "id."

d) Each value of an enumeration types shall be represented using UPPER_WITH_UNDERSCORE.

EXAMPLE 3: NOT_INSTATIATED.

e) The names of data types shall be represented using UpperCamel.

EXAMPLES 4: ResourceHandle, AppInstance.

5.3 Provision of an OpenAPI definition

An ETSI ISG MEC GS defining a RESTful mobile edge service API should provide a supplementary description file (or supplementary description files) compliant to the OpenAPI specification [i.14], which inherently include(s) a definition of the data structures of the API in JSON schema or YAML format. A description file is machine readable facilitating content validation and autocreation of stubs for both the service client and server. This file (or files) may be attached to the GS, or a link to a repository containing the file(s) may be provided. The file (or files) shall be informative. In case of a discrepancy between supplementary description file(s) and the underlying specification, the underlying specification shall take precedence.

6 Patterns of RESTful mobile edge service APIs

6.1 Introduction

This clause describes patterns to be used to model common operations and data types in the RESTful mobile edge service APIs. The defined patterns are used consistently throughout different RESTful mobile edge service APIs as defined by ETSI ISG MEC.

For RESTful APIs exposed by mobile edge services designed by third parties, it is recommended to use these patterns if and where applicable.

6.2 Pattern: Name syntax

6.2.1 Description

This clause defines the syntax for strings used as names in the RESTful mobile edge service APIs.

In the following clauses, "lower camel case" is used, defined as follows: the first character of the string is lowercase, every word boundary in the string is represented by an uppercase character, and all remaining characters are lowercase. Only letters and digits are allowed, whereas the first character is always a letter. An abbreviation is treated like any other word.

EXAMPLES: mobileEdgeComputing, mecHost, etsiMec.

6.2.2 Names in payload bodies

The following rules are recommended for names in payload bodies used in RESTful mobile edge service APIs to encourage coherence. For JSON-encoded payload bodies, the provisions defined by IETF RFC 7159 [10] shall be followed. For XML-encoded payload bodies, the provisions defined by the XML specification [11] shall be followed.

Enumerations: A name that represents an enumeration value should be all-uppercase, with underscore "_" separating words if needed.

Attribute/Element names (XML): The names of attributes/elements in payload bodies should be in "lower camel case".

Object/Array names (JSON): The names of objects/arrays in payload bodies should be in "lower camel case".

6.2.3 Names in URIs

The following rules are recommended for names in URIs used in RESTful mobile edge service APIs to encourage coherence. The provisions for URI syntax defined by IETF RFC 3986 [9] shall be followed.

URI constants: A name that is a URI path segment constant (i.e. not a URI variable) should be in all-lowercase, with underscore "_" separating words if needed. Only letters, digits and underscore "_" are allowed.

EXAMPLE 1: mobile_edge_computing, mec_host, etsi_mec

URI variable names: A name that represents a URI path segment in the documentation but serves as a placeholder for an actual value created at runtime shall be represented in "lower camel case", and enclosed in curly brackets.

EXAMPLE 2: {mecHostAddress}, {id}

URI variable values: A string that is part of a URI and that is generated at runtime or provided as input to a process shall not render the overall URI non-compliant with IETF RFC 3986 [9]. That document puts restrictions on the character set that can be freely used at any place in the URI. Implementations shall obey this restriction when generating URI variable values, and deploy suitable transformations such as percent-encoding (see IETF RFC 3986 [9]) on strings that they include in URIs, but whose structure they do not control.

6.3 Pattern: Resource identification

6.3.1 Description

Every resource is identified by at least one resource URI. A resource URI identifies at most one resource.

6.3.2 Resource definition(s) and HTTP methods

The syntax of each resource URI shall follow IETF RFC 3986 [9]. In the RESTful mobile edge service APIs, the resource URI structure shall be as follows:

{apiRoot}/{apiName}/{apiVersion}/{apiSpecificSuffixes}

"apiRoot" consists of the scheme ("https"), host and optional port, and an optional prefix string. "apiName" defines the name of the API. The "apiVersion" represents the version of the API. "apiSpecificSuffixes" define the tree of resource URIs in a particular API. The combination of "apiRoot", "apiName" and "apiVersion" is called the root URI. "apiRoot" is under control of the deployment, whereas the remaining parts of the URI are under control of the API specification.

All RESTful mobile edge service APIs shall support HTTP over TLS (also known as HTTPS) (see IETF RFC 2818 [13]). TLS version 1.2 as defined by IETF RFC 5246 [14] shall be supported. HTTP without TLS is not recommended to use on a production system.

With every HTTP method, exactly one resource URI is passed in the request to address one particular resource.

6.4 Pattern: Resource representations and content format negotiation

6.4.1 Description

Resource representations are an important concept in REST. Actually, a resource representation is a serialization of the resource state in a particular content format. A resource representation is included in the payload body of an HTTP request or response. It depends on the HTTP method whether a representation is required or not allowed in a request, as defined in IETF RFC 7231 [1] (see table 6.4.1-1). If no representation is provided in a response, this shall be signalled by the "204 No Content" response code.

Table 6.4.1-1: Payload bodies requirements in HTTP requests for the different HTTP methods

HTTP method	Payload body is…
GET	unspecified; not recommended
PUT	required
POST	required
PATCH	required
DELETE	unspecified; not recommended

HTTP (IETF RFC 7231 [1]) provides a mechanism to negotiate the content format of a representation. Each ETSI MEC API specification defines the content formats that are mandatory or optional by the server to support for that API; the client may use any of these. Examples of content types are JSON (IETF RFC 7159 [10]) and XML [11]. In HTTP requests and responses, the "Content-Type" HTTP header is used to signal the format of the actual representation included in the payload body. If the format of the representation in an HTTP request is not supported by the server, it responds with a "415 Unsupported Media Type" response code. The content formats that a client supports in a HTTP response are signalled by the "Accept" HTTP header of the HTTP request. If the server cannot provide any of the accepted formats, it returns the "406 Not Acceptable" response code.

6.4.2 Resource definition(s) and HTTP methods

This pattern is applicable to any resource and any HTTP method.

6.4.3 Resource representation(s)

This pattern is applicable to any resource representation.

6.4.4 HTTP headers

The client uses the "Accept" HTTP header to signal to the server the content formats it supports. It is also possible to provide priorities. The HTTP specification can be found in IETF RFC 7231 [1].

As defined in the HTTP specification, both client and server use the "Content-Type" HTTP header to signal the content format of the payload included in the payload body of the request or response, if an payload body is present.

For the RESTful mobile edge service APIs, the following applies: In the "Accept" and "Content-Type" HTTP headers, the string "application/json" shall be used to signal the use of the JSON format (IETF RFC 7159 [10]) and "application/xml" shall be used to signal the use of the XML format [11].

6.4.5 Response codes and error handling

Servers that do not support the content format of the representation received in the payload body of a request return the "415 Unsupported Media Type" response code.

A server returns "406 Not Acceptable" in a HTTP response if it cannot provide any of the formats signalled by the client in the "Accept" HTTP header of the associated HTTP request.

A server that wishes to omit the payload body in a successful response returns "204 No Content" instead of "200 OK". This can make sense for DELETE, PUT and PATCH, but makes no sense for GET, and makes rarely sense for POST.

6.5 Pattern: Resource creation

6.5.1 Description

New resources are created on the origin server as children of a parent resource. In order to request resource creation, the client sends a POST request to the parent resource and includes a representation of the resource to be created. The server generates a name for the new resource that is unique for all child resources in the scope of the parent resource, and concatenates this with the resource URI of the parent resource to form the resource URI of the child resource. The server creates the new resource, and returns in a "201 Created" response a representation of the created resource along with a "Location" HTTP header that contains the resource URI of this resource.

Figure 6.5.1-1 illustrates creating a resource.

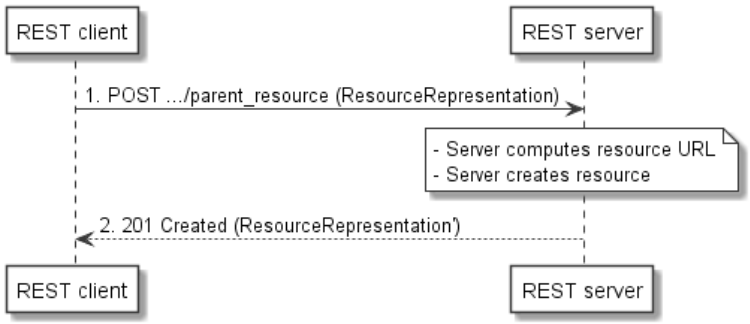


Figure 6.5.1-1: Resource creation flow

6.5.2 Resource definition(s) and HTTP methods

The following resources are involved:

1) parent resource: A container that can hold zero or more child resources;

2) created resource: A child resource of a container resource that is created as part of the operation. The resource URI of the child resource is a concatenation of the resource URI of the parent resource with a string that is chosen by the server, and that is unique in the scope of the parent resource URI.

The HTTP method shall be POST.

6.5.3 Resource representation(s)

The payload body of the request shall contain a representation of the resource to be created. The payload body of the response shall contain a representation of the created resource.

NOTE: Compared to the payload body passed in the request, the payload body in the response may be different, as the resource creation process may have modified the information that has been passed as input.

6.5.4 HTTP headers

On success, the "Location" HTTP header shall be returned, and shall contain the URI of the newly created resource.

6.5.5 Response codes and error handling

On success, "201 Created" shall be returned. On failure, the appropriate error code (see annex B) shall be returned.

Resource creation can also be asynchronous in which case "202 Accepted" shall be returned instead of "201 Created". See clause 6.13 for more details about asynchronous operations.

6.6 Pattern: Reading a resource

6.6.1 Description

This pattern obtains a representation of the resource, i.e. reads a resource, by using the HTTP GET method. For most resources, the GET method should be supported. An exception is task resources (see clause 6.11); these cannot be read.

Figure 6.6.1-1 illustrates reading a resource.

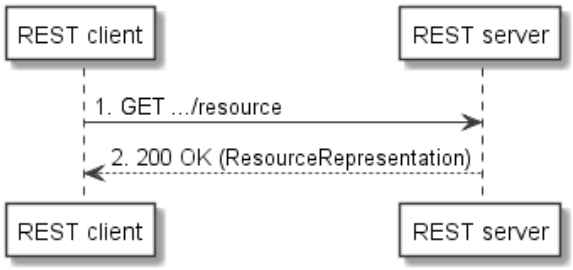


Figure 6.6.1-1: Reading a resource

6.6.2 Resource definition(s) and HTTP methods

This pattern is applicable to any resource that can be read. The HTTP method shall be GET.

6.6.3 Resource representation(s)

The payload body of the request shall be empty; the payload body of the response shall contain a representation of the resource that was read, if successful.

6.6.4 HTTP headers

No specific provisions for HTTP headers for this pattern.

6.6.5 Response codes and error handling

On success, "200 OK" shall be returned. On failure, the appropriate error code (see annex B) shall be returned.

6.7 Pattern: Queries on a resource

6.7.1 Description

This pattern influences the response of the GET method by passing resource URI parameters in the query part of the resource URI. The syntax of the query part is specified by IETF RFC 3986 [9].

Typically, query parameters are used for:

- restricting a set of objects to a subset, based on filtering criteria;
- controlling the content of the result;
- reducing the content of the result (such as suppressing optional attributes).

EXAMPLES:

GET …/foo_list?vendor=MEC&ue_ids=ab1,cd2

→ would return a foo_list representation that includes only those entries where vendor is "MEC" and the UE IDs are "ab1" or "cd2".

GET …/foo_list?group=group1

→ would return a foo_list representation that includes only those entries that belong to "group1".

GET …/foo_list/123?format=reduced_content

→ would return a representation of the resource …/foo_list/123 with content tailored according to the application-specific "reduced_content" scope.

GET …/foo_list?fields=name,address,key

→ would return a representation of the resource …/foo_list where the entries are reduced to the attributes "name", "address" and "key".

Query values that are not compatible with URI syntax shall be escaped properly using percent encoding as defined in IETF RFC 3986 [9].

6.7.2 Resource definition(s) and HTTP methods

This pattern is applicable to any resource that can be read. The HTTP method shall be GET.

6.7.3 Resource representation(s)

The payload body of the request shall be empty; the payload body of the response shall contain a representation of the resource that was read, adjusted according to the parameters that were passed.

6.7.4 HTTP headers

No specific provisions for HTTP headers for this pattern.

6.7.5 Response codes and error handling

On success, "200 OK" shall be returned. On failure, the appropriate error code (see annex B) shall be returned.

6.8 Pattern: Updating a resource (PUT)

6.8.1 Description

When a resource is updated using the PUT HTTP method, this operation has "replace" semantics. That is, the new state of the resource is determined by the representation in the payload body of PUT, previous resource state is discarded by the REST server when executing the PUT request.

If the client intends to use the current state of the resource as the baseline for the modification, it is required to obtain a representation of the resource by reading it, to modify that representation, and to place that modified representation in the payload body of the PUT. If, on the other hand, the client intends to overwrite the resource without considering the existing state, the PUT can be executed with a resource representation that is created from scratch.

Figure 6.8.1-1 illustrates this flow.

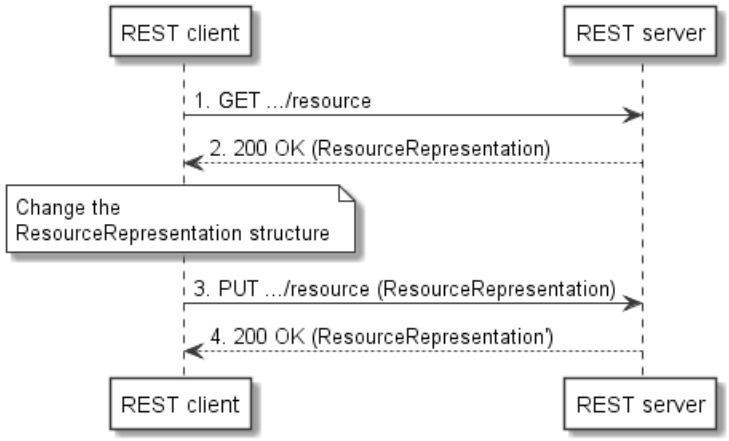


Figure 6.8.1-1: Basic resource update flow with PUT

The approach illustrated above can suffer from race conditions. If another client modifies the resource after receiving the response to the GET request and before sending the PUT request, that modification gets lost (which is known as the lost update phenomenon in concurrent systems). HTTP (see IETF RFC 7232 [2]) supports conditional requests to detect such a situation and to give the client the opportunity to deal with it. For that purpose, each version of a resource gets assigned an "entity-tag" (ETag) that is modified by the server each time the resource is changed. This information is delivered to the client in the "ETag" HTTP header in HTTP responses. If the client wishes that the server executes the PUT only if the ETag has not changed since the time the GET response was generated, the client adds to the PUT request the HTTP header "If-Match" with the ETag value obtained from the GET request. The server executes the PUT request only if the ETag in the "If-Match" HTTP header matches the current ETag of the resource, and responds with "412 Precondition Failed" otherwise. In that conflict case, the client needs to repeat the GET-PUT sequence. This is illustrated in figure 6.8.1-2.

Figure 6.8.1-2: Resource update flow with PUT, considering concurrent updates

In a particular API, it is recommended to stick to one update pattern - either PUT or PATCH.

6.8.2 Resource definition(s) and HTTP methods

This pattern is applicable to any resource that allows update by PUT.

6.8.3 Resource representation(s)

This pattern has no specific provisions for resource representations, other than the following note.

NOTE: Compared to the payload body passed in the request, the payload body in the response may be different, as the resource update process may have modified the information that has been passed as input.

6.8.4 HTTP headers

If multiple clients can update the same resource, the client should pass in the "If-Match" HTTP header of the PUT request the value of the "ETag" HTTP header received in the response to the GET request.

NOTE: This prevents the "lost update" phenomenon.

6.8.5 Response codes and error handling

On success, either "200 OK" or "204 No Content" shall be returned. If the ETag value in the "If-Match" HTTP header of the PUT request does not match the current ETag value of the resource, "412 Precondition Failed" shall be returned. Otherwise, on failure, the appropriate error code (see annex B) shall be returned.

Resource update can also be asynchronous in which case "202 Accepted" shall be returned instead of "200 OK". See clause 6.13 for more details about asynchronous operations.

6.9 Pattern: Updating a resource (PATCH)

6.9.1 Description

The PATCH HTTP method (see IETF RFC 5789 [3]) is used to update a resource on top of the existing resource state with the changes described by the client (unlike resource update using PUT which overwrites a resource (see clause 6.8)). The "Update by PATCH" pattern can be used in all places where "Update by PUT" can be used, but is typically more efficient for partially updating a large resource.

As opposed to PUT, PATCH does not carry a representation of the resource in the payload body, but a document that instructs the server how to modify the resource representation. For JSON, JSON Patch (see IETF RFC 6902 [6]) and JSON Merge Patch (IETF RFC 7396 [5]) are defined for that purpose. Whereas JSON Patch declares commands that transform a JSON document, JSON Merge Patch defines fragments that are merged into the target JSON document. For XML, a patch framework is specified in IETF RFC 5261 [7] which defines operations to modify the target document as well.

Figure 6.9.1-1 illustrates updating a resource by PATCH.

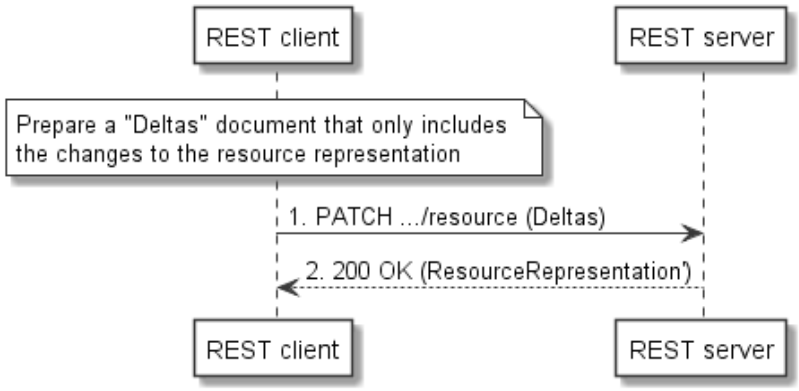


Figure 6.9.1-1: Basic resource update flow with PATCH

Careful design of the PATCH payload can make the method idempotent, i.e. the order in which particular PATCH operations are executed does not matter. If this can be achieved, the "lost update" phenomenon cannot occur. However, if conflicts are possible, the If-Match HTTP header should be used in the same way as with PUT, as illustrated by figure 6.9.1-2.

NOTE: Like in the PUT case, the ETag refers to the whole resource representation, not only to the portion modified by the PATCH.

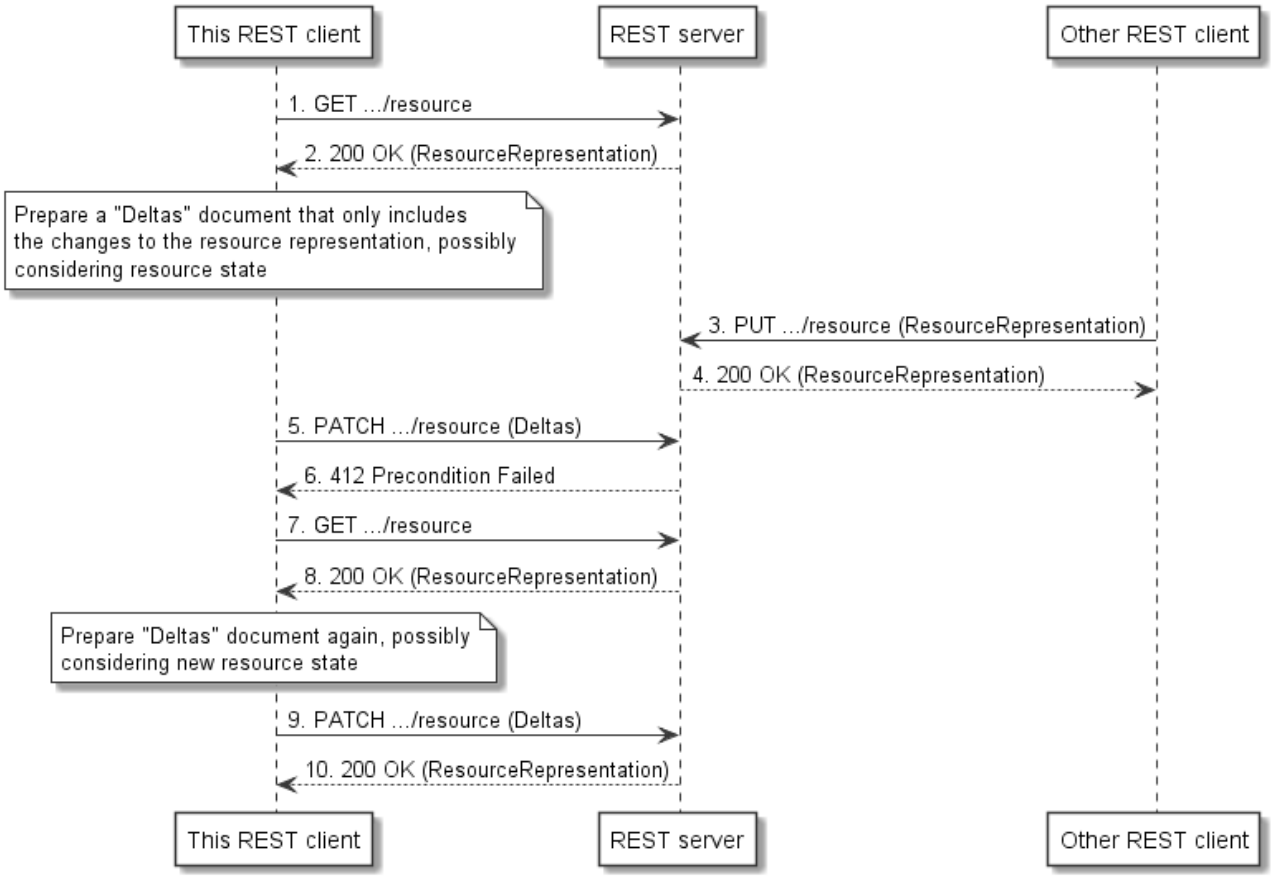


Figure 6.9.1-2: Resource update flow with PATCH, considering concurrent updates

In a particular API, it is recommended to stick to one update pattern - either PUT or PATCH.

6.9.2 Resource definition(s) and HTTP methods

This pattern is applicable to any resource that allows update by PATCH.

6.9.3 Resource representation(s)

The payload body of the PATCH request does not carry a representation of the resource, but a description of the changes in one of the formats defined by IETF RFC 6902 [6], IETF RFC 7396 [5] and IETF RFC 5261 [7].

The APIs defined as part of the ETSI MEC specifications will use IETF RFC 7396 [5] when using PATCH with JSON.

The payload body of the PATCH response may either be empty, or may carry a representation of the updated resource.

6.9.4 HTTP headers

In the request, the "Content-type" HTTP header needs to be set to the content type registered for the format used to describe the changes, according to IETF RFC 6902 [6], IETF RFC 7396 [5] or IETF RFC 5261 [7].

If conflicts and data inconsistencies are foreseen when multiple clients update the same resource, the client should pass in the "If-Match" HTTP header of the PUT request the value of the "ETag" HTTP header received in the response to the GET request.

6.9.5 Response codes and error handling

On success, either "200 OK" or "204 No Content" shall be returned. If the ETag value in the "If-Match" HTTP header of the PATCH request does not match the current ETag value of the resource, "412 Precondition Failed" shall be returned. Otherwise, on failure, the appropriate error code (see annex B) shall be returned.

Resource update can also be asynchronous in which case "202 Accepted" shall be returned instead of "200 OK". See clause 6.13 for more details about asynchronous operations.

6.10 Pattern: Deleting a resource

6.10.1 Description

The Delete pattern deletes a resource by invoking the HTTP DELETE method on that resource. After successful completion, the client shall not assume that the resource is available any longer.

The response of the DELETE request is typically empty, but it is also possible to return the final representation of the resource prior to deletion.

When a deleted resource is accessed subsequently by any HTTP method, typically the server responds with "404 Resource Not Found", or, if the server maintains knowledge about the URIs of formerly-existing resources, "410 Gone".

Figure 6.10.1-1 illustrates deleting a resource.

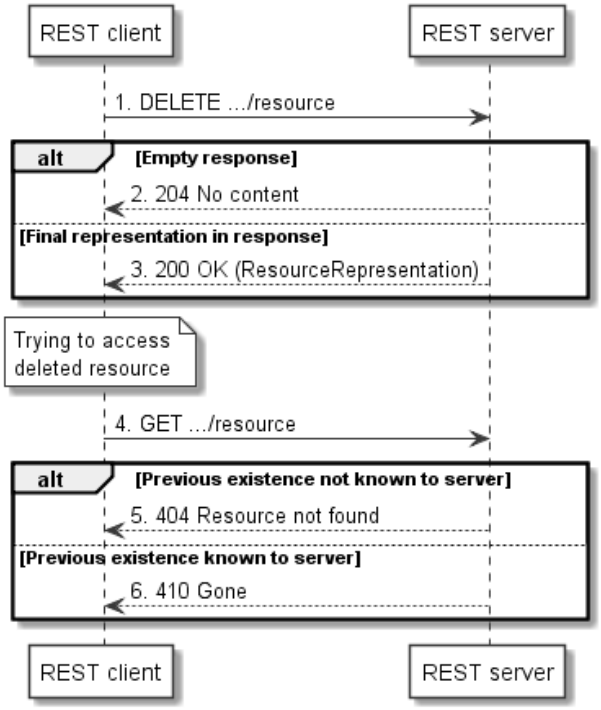


Figure 6.10.1-1: Resource deletion flow

6.10.2 Resource definition(s) and HTTP methods

This pattern is applicable to any resource that can be deleted. The HTTP method shall be DELETE.

6.10.3 Resource representation(s)

The payload body of the request shall be empty. The payload body of the response is typically empty, but may also include the final representation of the resource prior to deletion.

6.10.4 HTTP headers

No specific provisions for HTTP headers for this pattern.

6.10.5 Response codes and error handling

On success, "204 No content" should be returned, unless it is the intent to provide the final representation of the resource, in which case "200 OK" should be returned. On failure, the appropriate error code (see annex B) shall be returned.

If a deleted resource is accessed subsequently by any HTTP method, the server shall respond with "410 Gone" in case it has information about the deleted resource available, or shall respond with "404 Resource Not Found" in case it has no such information.

Resource deletion can also be asynchronous in which case "202 Accepted" shall be returned instead of "204 No content" or "200 OK". See clause 6.13 for more details about asynchronous operations.

6.11 Pattern: Task resources

6.11.1 Description

In REST interfaces, the goal is to use only four operations on resources: Create, Read, Update, Delete (the so-called CRUD principle). However, in a number of cases, actual operations needed in a system design are difficult to model as CRUD operations, be it because they involve multiple resources, or that they are processes that modify a resource and that take a number of input parameters that do not appear in the resource representation. Such operations are modelled as "task resources".

A task resource is a child resource of a primary resource which is intended as an endpoint for the purpose of invoking a non-CRUD operation. That non-CRUD operation executes a procedure that modifies the state of that actual resource in a specific way, or performs a computation and returns the result. Task resources are an escape means that allows to incorporate aspects of a service-oriented architecture into a RESTful interface.

The only HTTP method that is supported for a task resource is POST, with an payload body that provides input parameters to the process which is triggered by the request. Different responses to a POST request to a task resource are possible, such as "202 Accepted" (for asynchronous invocation), "200 OK" (to provide a result of a computation based on the state of the resource and additional parameters), "204 No Content" (to signal success but not return a result), or "303 See Other" to indicate the target resource that was modified. The actual code used depends greatly on the actual system design.

6.11.2 Resource definition(s) and HTTP methods

A task resource that models an operation on a particular primary resource is often defined as a child resource of that primary resource. The name of the resource should be a verb that indicates which operation is executed when sending a POST request to the resource.

EXAMPLE: …/call_sessions/{sessionId}/call_participants/{participantId}/transfer.

The HTTP method shall be POST.

6.11.3 Resource representation(s)

The payload body of the POST request does not carry a resource representation, but contains input parameters to the process that is triggered by the POST request.

6.11.4 HTTP headers

In case the task resource represents an operation that is asynchronous, the provisions in clause 6.13 shall apply.

In case the operation modifies a primary resource and the response contains the "303 See Other" response code, the "Location" HTTP header shall point to the primary resource.

6.11.5 Response codes and error handling

The response code returned depends greatly on the actual operation that is represented as a task resource, and may include the following:

- For long-running operations, "202 Accepted" is returned. See clause 6.13 for more details about asynchronous operations.
- If the operation modifies another resource, "303 See Other" is returned.
- If the operation returns a computation result, "200 OK" is returned.
- If the operation returns no result, "204 No Content" is returned.

On failure, the appropriate error code (see annex B) shall be returned.

6.12 Pattern: REST-based subscribe/notify

6.12.1 Description

A common task in distributed system is to keep all involved components informed of changes that appear in a particular component at a particular time. A common approach to spread information about a change is to distribute notifications about the change to those components that have indicated interest earlier on. Such pattern is known as Subscribe/Notify. In REST which is request-response by design, meaning that every request is initiated by the client, specific mechanisms needs to be put into place to support the server-initiated delivery of notifications. The basic principle is that the REST client exposes a lightweight HTTP server towards the REST server. The lightweight HTTP server only needs to support a small subset of the HTTP functionality - namely the POST method, the 204 success response code plus the relevant error response codes, and, if applicable, authentication/authorization. The REST client exposes the lightweight HTTP server in a way that it is reachable via TCP by the REST server.

NOTE: This clause describes REST-based subscribe/notify. Notifications can also be subscribed to and delivered by an alternative transport mechanism, such as a message bus. There is a separate pattern for this, see clause 7.

To manage subscriptions, the REST server needs to expose a container resource under which the REST client can request the creation/deletion of subscription resources. Those resources typically define criteria of the subscription. See clauses 6.5 and 6.10 for the patterns of creating and deleting resources which apply to subscription resources as well.

To receive notifications, the client exposes one or more HTTP endpoints on which it can receive POST requests. When creating a subscription, the client shall inform the server of the endpoint to which the server will later deliver notifications related to that particular subscription.

To deliver notifications, the server includes the actual notification payload in the payload body of a POST request, and sends that request to the endpoint it knows from the subscription. The client acknowledges the receipt of the notification with "204 No Content".

Figure 6.12.1-1 illustrates the creation of subscriptions and the delivery of a notification.

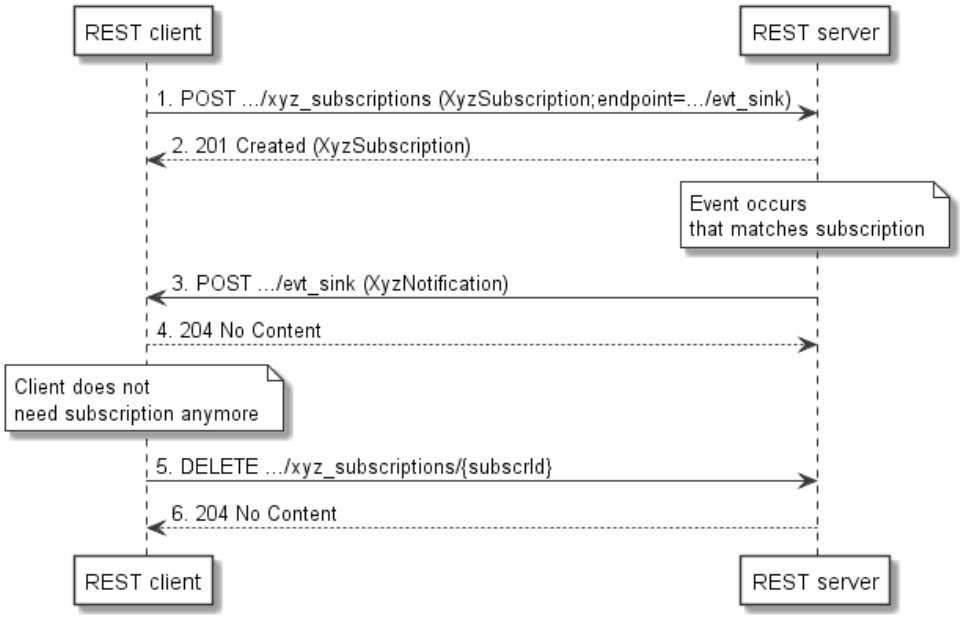


Figure 6.12.1-1: Creation of subscriptions and delivery of a notification

Beyond this very basic scheme described above, the server may also allow the client to update subscriptions, and subscriptions may carry an expiry deadline. Update shall be performed using PUT. In particular, when applying the update operation, the REST client can modify the expiry deadline to refresh a subscription. If the server expires a subscription, it sends an ExpiryNotification to the client's HTTP endpoint defined in the subscription. See clause 6.8 for the pattern of updating a resource using PUT, which applies to the update of subscription resources as well.

Once a subscription is expired, the subscription resource is not available anymore.

Figure 6.12.1-2 illustrates a realization with update and expiry of subscriptions.

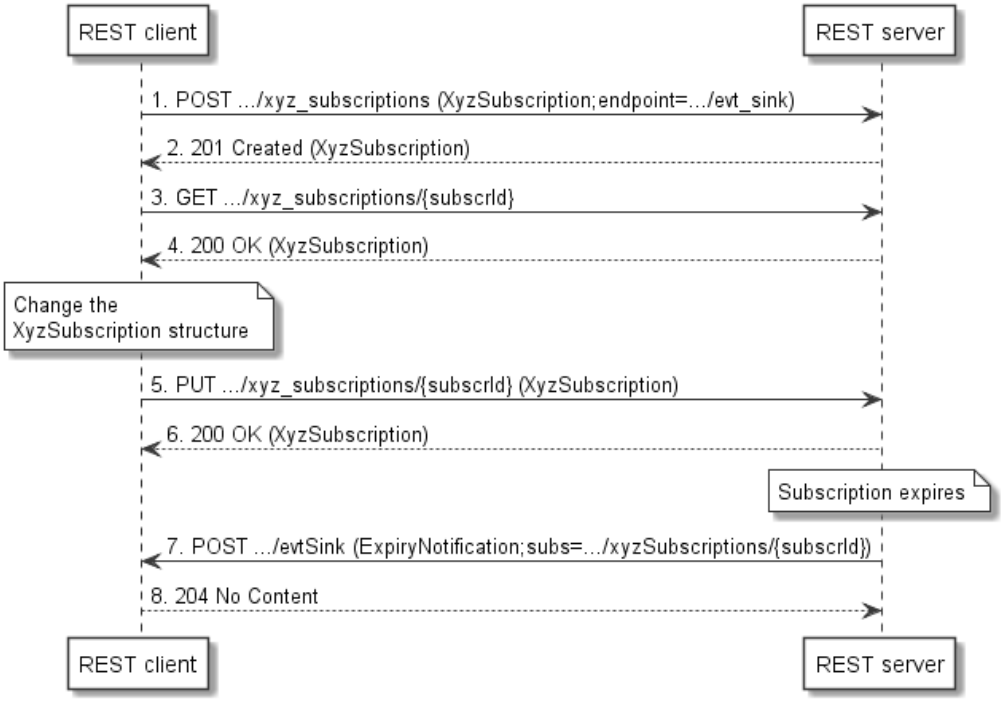


Figure 6.12.1-2: Management of subscriptions with expiry

6.12.2 Resource definition(s) and HTTP methods

The following resources are involved:

1) Subscriptions container resource: A resource that can hold zero or more subscription resources as child resources.

2) Subscription resource: A resource that represents a subscription.

3) An HTTP endpoint that is exposed by the REST client to receive the notifications.

The HTTP method to create a subscription resource inside the subscription container resource shall be POST. The HTTP method to terminate a subscription by removing a subscription resource shall be DELETE. The HTTP method used by the server to deliver the notification shall be POST.

If update of subscriptions is supported, the HTTP method to perform the update shall be PUT.

If expiry of subscriptions is supported, the delivery of an expiryNotification to the subscribed clients, and the update of subscription resources should be supported to allow extension of the lifespan of a resource.

6.12.3 Resource representation(s)

The following provisions are applicable to the representation of a subscription resource:

- It shall contain an HTTP endpoint that the REST client exposes to receive notifications.
- It should contain criteria that allow the server to determine the events about which the client wishes to be notified.
- If expiry of subscriptions is supported, it shall contain an expiry time after which the subscription is no longer valid, and no notifications will be generated for it.

If subscription expiry is supported, the following provisions are applicable to the representation of an expiryNotification:

- It shall contain a reference to the subscription that has expired.
- It may contain information about the reason of the expiry.

The following provisions are applicable to the representation of any other notification:

- It should contain a reference to the related subscription.
- It shall contain information about the event.

6.12.4 HTTP headers

No specific provisions are applicable here.

6.12.5 Response codes and error handling

The response codes for subscription creation, subscription deletion, subscription read and subscription update are the same as for the general resource creation, resource deletion, resource read and resource update.

On success of notification delivery, "204 No Content" shall be returned.

On failure, the appropriate error code (see annex B) shall be returned.

If expiry of subscriptions is supported: Once an expiry notification has been delivered to the client, any HTTP request to the expired subscription resource shall fail. For a timespan determined by policy or implementation, "410 Gone" is recommended to be used as the response code in that case, and "404 Not Found" shall be used afterwards.

NOTE: In order to be able to respond with "410 Gone", the server needs to keep information about the expired subscription.

6.13 Pattern: Asynchronous operations

6.13.1 Description

Certain operations, which are invoked via a RESTful interface, trigger processing tasks in the underlying system that may take a long time, from minutes over hours to even days. In this case, it is inappropriate for the REST client to keep the HTTP connection open to wait for the result of the response - the connection will time out before a result is delivered. For these cases, asynchronous operations are used. The idea is that the operation immediately returns the provisional response "202 Accepted" to indicate that the request was understood, can be correctly marshalled in, and processing has started. The client can check the status of the operation by polling; additionally or alternatively, the subscribe-notify mechanism (see clause 6.12) can be used to provide the result once available. The progress of the operation is reflected by a monitor resource.

Figure 6.13.1-1 illustrates asynchronous operations with polling. After receiving an HTTP request that is to be processed asynchronously, the server responds with "202 Accepted" and includes in the payload body or in a specific "Link" HTTP header a data structure that points to a monitor resource which represents the progress of the processing operation. The client can then poll the monitor resource by using GET requests, each returning a data structure with information about the operation, including the processing status such as "processing", "success" and "failure". Initially, the status is set to "processing". Eventually, when the processing is finished, the status is set to "success" (for successful completion of the operation) or "failure" (for completion with errors). Typically, the representation of a monitor resource will include additional information, such as information about an error if the operation was not successful.

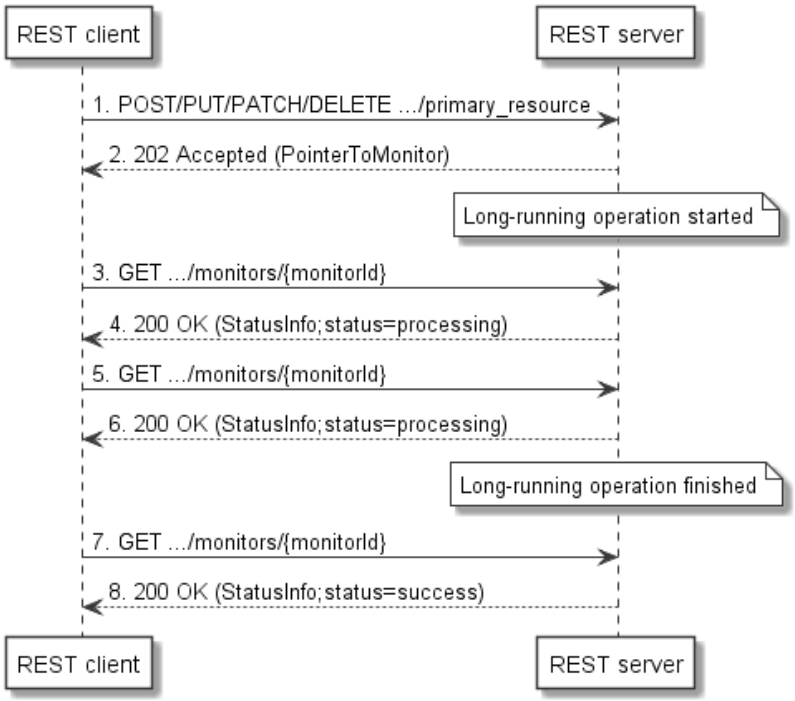


Figure 6.13.1-1: Asynchronous operation flow - with polling

Figure 6.13.1-2 illustrates asynchronous operations with subscribe/notify. Before a client issues any request that may be processed asynchronously, it subscribes for monitor change notifications. Later, after receiving an HTTP request that is to be processed asynchronously, the server responds with "202 Accepted" and includes in the payload body or in a specific "Link" HTTP header a data structure that points to a monitor resource which represents the progress of the processing operation. The client can now wait for receiving a notification about the operation finishing, which will change the status of the monitor. Once the operation is finished, the server will send to the client a notification with a structure in the payload body that typically includes the status of the operation (e.g. "success" or "failure"), a link to the actual monitor affected, and a link to the resource that is modified by the asynchronous operation, The client can then poll the monitor to obtain further information.

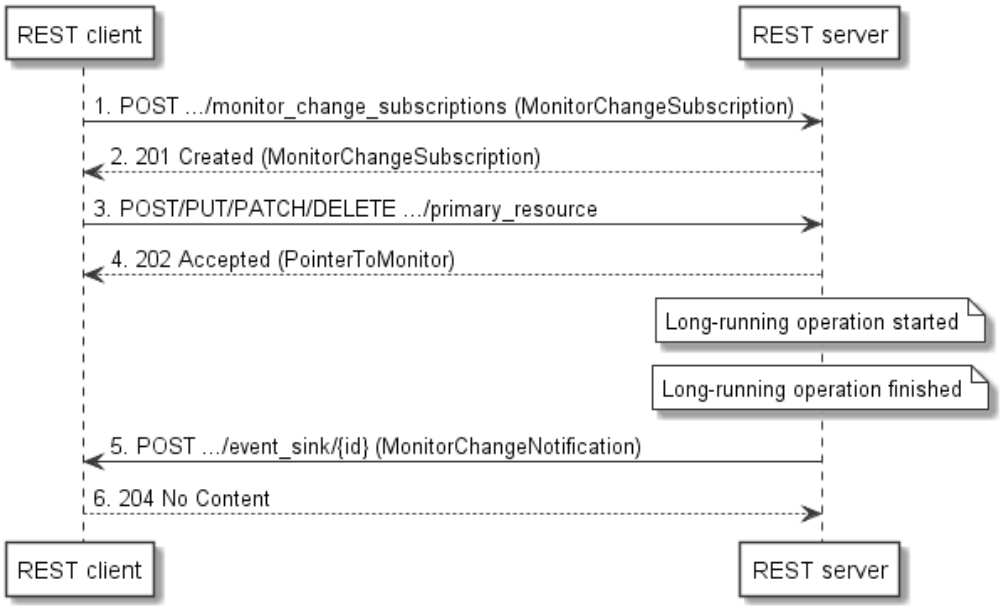


Figure 6.13.1-2: Asynchronous operation flow - with subscribe/notify

6.13.2 Resource definition(s) and HTTP methods

The following resources are involved:

1) Primary resource: The resource that is about to be created/modified/deleted by the long-running operation.

2) Monitor resource: The resource that provides information about the long-running operation.

The HTTP method applied to the primary resource can be any of POST/PUT/PATCH/DELETE.

The HTTP method applicable to read the monitor resource shall be GET.

If monitor change notifications and subscriptions to these are supported, the resources and methods described in clause 6.12 for the RESTful subscribe/notify pattern are applicable here too.

6.13.3 Resource representation(s)

If present, the structure included in the payload body of the response to the long-running operation request shall contain the resource URI of the monitor for the operation, and shall also contain the resource URI of the actual primary resource. See clause 6.14 for further information on links. If no payload body is present, the "Link" HTTP header shall be used to convey the link to the monitor.

The representation of the monitor shall contain at least the following information:

- Resource URI of the primary resource.
- Status of the operation (at least "processing", "success", "failure").
- Additional information about the result or the error(s) occurred, if applicable.
- Information about the operation (type, parameters, HTTP method used).

If subscribe/notify is supported, the monitor change notification shall include the status of the operation and the resource URI of the monitor, and shall include the resource URI of the affected primary resource.

6.13.4 HTTP headers

The link to the monitor should be provided in the "Link" HTTP header (see IETF RFC 5988 [12]), with the "rel" attribute set to "monitor". If the payload body of the message is not present, the "Link" as defined above shall be provided.

EXAMPLE: Link: <http://mecplat0815.example.com/.../monitors/mtr061070>; rel="monitor".

6.13.5 Response codes and error handling

On success, "202 Accepted" shall be returned as the response to the request that triggers the long-running operation. On failure, the appropriate error code (see annex B) shall be returned.

The GET request to the monitor resource shall use "200 OK" as the response code if the monitor could be read successfully, or the appropriate error code (see annex B) otherwise.

If subscribe/notify is supported, the provisions in clause 6.12.5 apply in addition.

6.14 Pattern: Links (HATEOAS)

6.14.1 Description

The REST maturity level 3 requires the use of links between resources, allowing the REST client to traverse the resource space. ETSI MEC recommends using level 3. This is also known as "hypermedia controls" or "HATEOAS" (hyperlinks as the engine of application state). This clause describes a pattern for hyperlinks.

Hyperlinks to other resources should be embedded into the representation of resources where applicable. For each hyperlink, the target URI of the link and information about the meaning of the link shall be provided. Knowing the meaning of the link (typically conveyed by the name of the object that defines the link, or by an attribute such as "rel") allows the client to automatically traverse the links to access resources related to the actual resource, in order to perform operations on them.

6.14.2 Resource definition(s) and HTTP methods

Links can be applicable to any resource and any HTTP method.

6.14.3 Resource representation(s)

Links are communicated in the resource representation. Links that occur at the same level in the representation shall be bundled in an object (JSON) or element containing complexContent (XML schema), named "_links" which should occur as the first object/element at a particular level.

Links shall be embedded in that element (XML) or object (JSON) as child elements (XML) or contained objects (JSON). The name of each child element (XML) or contained object (JSON) defines the semantics of the particular link. The content of each link element/object shall be an attribute named "href" of type "anyURI" (XML) or an object named "href" of type string (JSON), which defines the target URI the link points to. The link to the actual resource shall be named "self" and shall be present in every resource representation if links are used in the API.

As an example, the "_links" portion of a resource representation is shown that represents paged information.

For the case of using XML, figure 6.14.3-1 illustrates the XML schema and figure 6.14.3-2 illustrates the XML instance. The XML schema language is defined in [i.5].

```
<xsd:complexType name="LinkType">
    <xsd:attribute name="href" type="xsd:anyURI"/>
</complexType>


<xsd:element name="_links">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="self" type="LinkType"/>
            <xsd:element name="next" type="LinkType" minOccurs="0"/>
            <xsd:element name="prev" type="LinkType" minOccurs="0"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
```

Figure 6.14.3-1: XML schema fragment for an example "_links" element

```
<_links>
    <self href="http://api.example.com/my_api/v1/pages/127"/>
    <next href="http://api.example.com/my_api/v1/pages/128"/>
    <prev href="http://api.example.com/my_api/v1/pages/126"/>
</_links>
```

Figure 6.14.3-2: XML instance fragment for an example "_links" element

For the case of using JSON, figure 6.14.3-3 illustrates the JSON schema and figure 6.14.3-4 illustrates the JSON object. The JSON schema language is defined in [i.4].

```
"properties": {
    "_links": {
        "required": ["self"],
        "type": "object",
        "description": "Link relations",
        "properties": {
            "self": {
                "$ref": "#/definitions/Link"
            },
            "prev": {
                "$ref": "#/definitions/Link"
            },
           "next": {
                "$ref": "#/definitions/Link"
            }
        }
    }
},
"definitions": {
    "Link" : {
        "type": "object",
        "properties": {
            "href": {"type": "string"}
        },
       "required": ["href"]
    }
}
```

Figure 6.14.3-3: JSON schema fragment for an example "_links" object

```
{
    "_links": {
        "self": { "href": "http://api.example.com/my_api/v1/pages/127" },
        "next": { "href": "http://api.example.com/my_api/v1/pages/128" },
        "prev": { "href": "http://api.example.com/my_api/v1/pages/126" }
    }
}
```

Figure 6.14.3-4: JSON fragment for an example "_links" object

6.14.4 HTTP headers

There are no specific provisions with respect to HTTP headers for this pattern.

NOTE: Specific links, such as a link to the monitor in a "202 Accepted" response, can be communicated in the "Link" HTTP header. See clause 6.13 for more details.

6.14.5 Response codes and error handling

There are no specific provisions with respect to response codes and error handling for this pattern.

6.15 Pattern: Error responses

6.15.1 Description

In RESTful interfaces, application errors are mapped to HTTP errors. Since HTTP error information is typically not enough to discover the root cause of the error, there is the need to deliver additional application specific error information.

When an error occurs that prevents the REST server from successfully fulfilling the request, the HTTP response includes a status code in the range 400..499 (client error) or 500..599 (server error) as defined by the HTTP specification (see IETF RFC 7231 [1] and IETF RFC 6585 [8]). In addition, to provide additional application-related error information, the present document recommends the response body to contain a representation of a "ProblemDetails" data structure according to IETF RFC 7807 [15] that provides additional details of the error.

6.15.2 Resource definition(s) and HTTP methods

The pattern is applicable to the responses of all HTTP methods.

6.15.3 Resource representation(s)

If an HTTP response indicates non-successful completion (error codes 400..499 or 500..599), the response body should contain a "ProblemDetails" data structure as defined below, formatted using the same format as the expected response. The response body may be omitted if the HTTP error code itself provides enough information of the error, or if there are security concerns disclosing detailed error information.

The definition of the general "ProblemDetails" data structure from IETF RFC 7807 [15] is reproduced in table 6.15.3-1. The "status" and "detail" attributes should be included, to ensure that the response contains additional textual information about an error. IETF RFC 7807 [15] foresees extensibility of the "ProblemDetails" type. It is possible that particular APIs or particular implementations define extensions to define additional attributes that provide more information about the error.

The description column only provides some explanation of the meaning to facilitate understanding of the design. For a full description, see IETF RFC 7807 [15].

Table 6.15.3-1: Definition of the ProblemDetails data type

Attribute name	Data type	Cardinality	Description
type	URI	0..1	A URI reference according to IETF RFC 3986 [9] that identifies the problem type. It is encouraged that the URI provides human-readable documentation for the problem (e.g. using HTML) when dereferenced. When this member is not present, its value is assumed to be "about:blank". See note 1.
title	String	0..1	A short, human-readable summary of the problem type. It should not change from occurrence to occurrence of the problem, except for purposes of localization. If type is given and other than "about:blank", this attribute shall also be provided.
status	Integer	0..1	The HTTP status code for this occurrence of the problem. See note 2.
detail	String	0..1	A human-readable explanation specific to this occurrence of the problem. See note 2.
instance	URI	0..1	A URI reference that identifies the specific occurrence of the problem. It may yield further information if dereferenced.
(additional attributes)	Not specified.	0..N	Any number of additional attributes, as defined in a specification or by an implementation.
NOTE 1: For the definition of specific "type" values as well as extension attributes by implementations, detailed guidance can be found in IETF RFC 7807 [15]. NOTE 2: The minimum set of information returned in ProblemDetails should consist of "status" and "detail".			

6.15.4 HTTP headers

As defined by IETF RFC 7807 [15]:

- In case of serializing the "ProblemDetails" structure using the JSON format, the "Content-Type" HTTP header shall be set to "application/problem+json".
- In case of serializing the "ProblemDetails" structure using the XML format, the "Content-Type" HTTP header shall be set to "application/problem+xml".

6.15.5 Response codes and error handling

In general, application errors should be mapped to the most similar HTTP error status code. If no such code is applicable, one of the codes 400 (Bad request, for client errors) or 500 (Internal Server Error, for server errors) should be used.

Implementations may use any valid HTTP response code as error code in the HTTP response, but shall not use any code that is not a valid HTTP response code. A list of all valid HTTP response codes and their specification documents can be obtained from the HTTP status code registry [i.8]. Annex B lists a set of error codes that is frequently used in HTTP-based RESTful APIs.

6.16 Pattern: Authorization of access to a RESTful mobile edge service API using OAuth 2.0

6.16.1 Description

This pattern defines the use of OAuth 2.0 to secure a RESTful mobile edge service API. It is used for the RESTful APIs that are defined by ETSI ISG MEC. Service-producing applications defined by third parties may use other mechanisms to secure their APIs, such as standalone use of JWT (see IETF RFC 7519 [i.13]).

The API security framework assumes an AA (authentication and authorization) entity to be available for both the REST client and the REST server. This AA entity performs the authentication for the credentials of the REST clients and the REST servers. The AA entity and the communication between the REST server and the AA entity are out of scope of the present document.

It is assumed that the AA entity is configured by a trusted Manager entity with the appropriate credentials and access rights information. This configuration information is exchanged between the AA entity and the REST server in an appropriate manner to allow the REST server to enforce the access rights. The trusted Manager and the actual way of performing the exchange of this information are out of scope.

The exchanges between REST client and REST server are in scope of the present document. The REST client has to authenticate towards the AA entity in order to obtain an access token. Subsequently, the client shall present the access token to the REST server with every request in order to assert that it is allowed to access the resource with the particular method it invokes. In the present version of the specification, the client credentials grant type of OAuth 2.0 (see IETF RFC 6749 [16]) shall be supported by the AA entity, and it shall be used by the REST client to obtain the access token. In any HTTP request to a resource, the access token shall be included as a bearer token according to IETF RFC 6750 [17].

Access rights are bound to access tokens, and typically configured at the granularity of methods applied to resources. This means, for any resource in the API, the use of every individual method can be allowed or disallowed. In APIs that define a REST-based subscribe-notify pattern, also the use of individual subscription types can be allowed or prohibited by access rights. Additional policies can be bound to access tokens too, such as the frequency of API calls. A token has a lifetime after which it is invalid. Depending on how the AA communicates with the REST server, it can also be possible to revoke a token before it expires.

Figure 6.16.1-1 illustrates the information flow between the three actors involved in securing the REST-based service API, the REST client, the AA entity and the REST server. Dotted lines indicate exchanges that are out of scope of the present document. It is assumed that information about the valid access tokens, such as expiry time, related client identity, client access rights, scope values, optional revocation information, need to be made available by the AA entity to the REST server by means outside the scope of the present document.

The AA entity exposes the "token endpoint" as defined by OAuth 2.0.

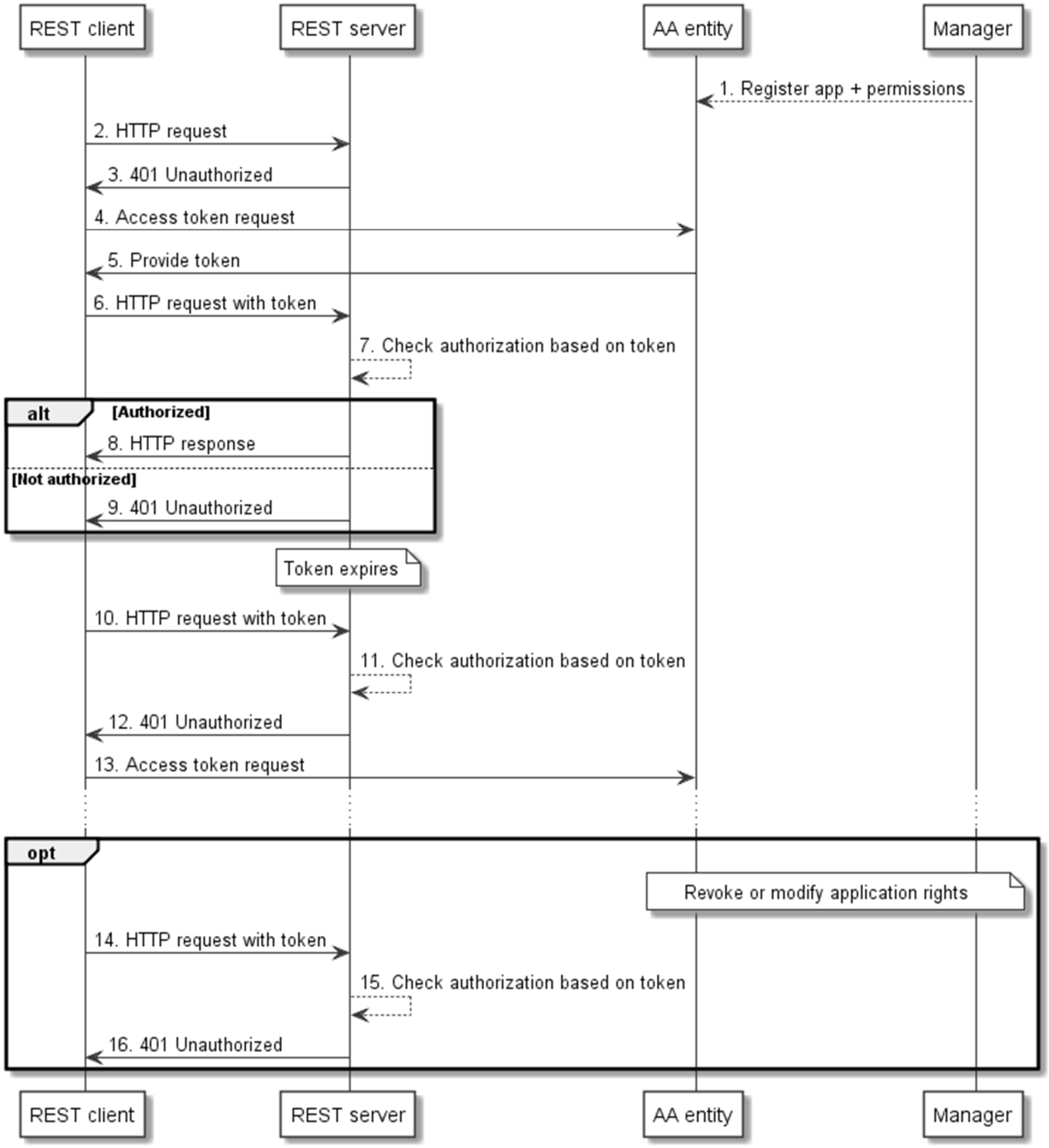


Figure 6.16.1-1: Securing a RESTful mobile edge service API with OAuth 2.0

The flow consists of the following steps:

1) The manager registers the REST client application with the AA entity and configures the permissions of the application. The method for this is out of scope of the present document.

2) The REST client sends an HTTP request to the REST server to access a resource.

3) The REST server responds with "401 Unauthorized" which indicates to the client that it has to obtain an access token for access to the resource.

4) The REST client sends an access token request to the token endpoint provided by the AA entity as specified by IETF RFC 6749 [16], and authenticates towards the AA entity with its client credentials.

5) The AA entity provides the token and additional configuration information to the REST client, as specified by IETF RFC 6749 [16].

6) The REST client repeats the request from step (2) with the access token included as a bearer token according to IETF RFC 6750 [17].

7) The REST server checks the token for validity, and determines whether the client is authorized to perform the request. This assumes that the REST server has received from the AA entity information about the valid access tokens, and additional related parameters (e.g. expiry time, client identity, client access rights, scope values). Exchange of such information is outside the scope of the present document, and is assumed to be trivial if deployments choose to include the AA entity as a component into the REST server.

8) In case the client is authorized, the REST server executes the HTTP request and returns an appropriate HTTP response rather than a "401 Unauthorized" error.

9) In case the client is not authorized, the REST server returns a "401 Unauthorized" error as defined in IETF RFC 6750 [17].

10) The REST client sends to the REST server an HTTP request with an expired token.

11) The REST server checks the token for validity, and establishes that it has expired. This assumes that the REST server has previously received information about the valid access tokens, and additional related information (in particular, the time of expiry) from the AA entity. Exchange of such information is outside the scope of the present document, and is assumed to be trivial if deployments choose to include the AA entity as a component into the REST server.

12) The REST server responds with "401 Unauthorized", and uses the format defined in IETF RFC 6750 [17] to communicate that the access token is expired.

13) The REST client sends a new access token request to the AA entity, as defined in step (4). Subsequently, steps (5) to (9) repeat.

Optionally:

14) The REST client sends to the REST server an HTTP request with a revoked token. For this optional sequence, it is assumed that the Manager has arranged to block an application from accessing a particular resource or set of resources, or has changed the application's access rights prior to that request. By means outside the scope of the present document, the Manager has further informed the AA entity about this change.

15) The REST server checks the token for validity, and establishes that it has been revoked. This assumes that the REST server has previously received information about the validity of the access token from the AA entity. Exchange of such information is outside the scope of the present document, and is assumed to be trivial if deployments choose to include the AA entity as a component into the REST server.

16) The REST server responds with "401 Unauthorized". Eventually, the REST client can succeed with another subsequent access token request if the revocation only affected a subset of the resources.

6.16.2 Resource definition(s) and HTTP methods

The HTTP methods follow the corresponding RESTful mobile edge service API definitions. Typically, when configuring the AA entity, access rights can be expressed separately for each resource and HTTP method. In case subscriptions are supported, separate access rights can also be defined per subscription data type.

6.16.3 Resource representation(s)

The representation of the information exchanged between the REST client and the Token endpoint of the AA entity shall follow the provisions defined in IETF RFC 6749 [16] for the client credentials grant type. The representation of information exchanged between the Manager and the AA entity, as well as between the AA entity and the REST server, are outside the scope of the present document.

6.16.4 HTTP headers

In this pattern, the access token is provided as defined by IETF RFC 6750 [17]. To protect the access token from wiretapping, HTTPS shall be used.

6.16.5 Response codes and error handling

The response codes on the API between the REST server and the REST client are defined in the corresponding RESTful mobile edge service API definitions, and shall include the provisions in IETF RFC 6750 [17]. The response codes on the token endpoint provided by the AA entity shall follow IETF RFC 6749 [16].

6.16.6 Discovery of the parameters needed for exchanges with the token endpoint

In order to be able to communicate with the token endpoint for a particular API, the REST client needs to discover its URI. The valid scope values (if supported) are part of the API documentation. The client further needs to know which set of client credentials to use to access the token endpoint. The token endpoint URI and the optional scope values will be provided as part of the security information during service discovery. The client credentials consist of the client identifier which is defined based on information in the application descriptor such as the values of the attributes "appProvider" and "appName", and the client password which is provisioned during application on-boarding, and configured into the client and the AA entity by means outside the scope of the present document.

6.16.7 Scope values

OAuth 2.0 (IETF RFC 6749 [16]) supports the concept of scope values to signal which actual access rights a token represents. The scope of the token can be requested by the client in the access token request by listing one or more scope values in the "scope" parameter. The AA entity can then potentially downscope the request, and respond with the actual scope(s) represented by an access token in the access token response in the "scope" parameter. The use of scopes is optional in OAuth 2.0. Per API, valid scopes can be defined in the API specification. Possible granularities are resources, combinations of resources and methods, or even combinations of resources and methods with actual parameter values, or values of attributes in the payload body. If no scope is defined, an access token always applies to all resources and methods of a particular API. For a REST API using OAuth 2.0, the "permission identifiers" as defined in clause 7.2 can be modelled as scope values, as illustrated in table 7.2-3. It is good practice to define one additional scope value per API that includes all individual access rights, for simplification of use.

7 Alternative transport mechanisms

7.1 Description

A mobile edge service needs a transport to be delivered to a mobile edge application. The default transport fully specified by ETSI MEC for mobile edge service APIs is HTTP-REST.

An alternative transport can also be specified for certain services that require higher throughput and lower latency than a REST-based mechanism can provide. Possible alternative transports at the time of writing are topic-based message buses (e.g. MQTT [i.9] or Apache Kafka [i.10]) and Remote Procedure Call frameworks (e.g. GRPC [i.11]). Note that not all aspects of such alternative transport mechanisms can be fully standardized, but some are left to implementation.

A transport can either be part of the mobile edge platform, or can be made available by the mobile edge application that provides the service (BYOT - bring your own transport). REST and GRPC are always BYOT as the endpoint is the piece of software that provides the service.

Service registration consists of two phases:

1) Transport discovery (only for non-BYOT)

2) Service registration including transport binding

Step 1 is performed using the "transport discovery" procedure on Mp1 (see ETSI GS MEC 011 [i.6]), to obtain a list of available transports, and only needed for a non-BYOT service. Step 2 is the "service registration" procedure on Mp1 which allows to bind a provided service to a transport. This means, a non-BYOT service registers the identifier of the platform-provided transport it intends to use, and a BYOT service registers the information of its own transport.

Transport information includes a definition of the access to the transport (e.g. URI, network address, or implementation-specific), the type of the transport (e.g. HTTP-REST, message bus, RPC, etc.), security information, metadata such as identifier, name and description, and a container for implementation-specific information. It is further specified in ETSI GS MEC 011 [i.6].

Sending data on a transport requires serialization. There are different serialization formats, for example JSON [10], XML [11] or Protocol Buffers [i.12]. Binding a service to a transport therefore also requires choosing a serialization format to be used. The data structures defined for the service can be bound to different serialization formats. The definition of the binding has to be done as part of the service definition. The JSON binding is typically fully specified for a RESTful API. Bindings to additional serializers can be provided, either in the documents defined by ETSI MEC, or in documents provided to the developer community by the mobile edge application vendors.

A further aspect of alternative transports is the mechanism how to secure a transport pipe (TLS, typically) and how a transport or the service that uses it enforces authorization. Enforcing authorization means that the endpoint that provides the service, or the transport, provides mechanisms to withhold information from unauthorized parties. REST and RPC transports can work with tokens (e.g. OAuth 2.0, see IETF RFC 6749 [16]) for authorization; here, the service endpoint is responsible for the enforcement. Message bus transports typically work by using the TLS certificates to enforce authorization; enforcement can be built into the transport mechanism. In order to realize this in an interoperable way, a service can define a list of topics to be used with transports that are topic-based, and to use these topics to scope the access of mobile edge applications to the actual information.

7.2 Relationship of topics, subscriptions and access rights

In the RESTful mobile edge service APIs defined as part of ETSI MEC, a client registers interest in particular changes by defining a subscription structure that typically contains at least one criterion against which a notification needs to match in order to be sent to the subscriber for that particular subscription. Multiple criteria can be defined, in which case all criteria need to match. Each criterion defines a particular value, or a set of values.

EXAMPLE 1: Table 7.2-1 provides a sample of the criteria part of a data type that represents subscriptions to notifications about cell changes.

Table 7.2-1: A sample of the criteria part of a data type that represents subscriptions to notifications about cell changes

Attribute name	Data type	Cardinality	Description
filterCriteria	Structure (inlined)	1	List of filtering criteria for the subscription. Any filtering criteria from below, which is included in the request, shall also be included in the response.
>appInsId	String	0..1	Unique identifier for the mobile edge application instance.
>associateId	Structure (inlined)	0..N	
>>type	Enum	1	Numeric value (0 - 255) corresponding to specified type of identifier as following: 0 = reserved 1= UE IPv4 Address 2 = UE IPv6 Address 3 = NATed IP address 4= GTP TEID.
>>value	String	1	Value for the identifier.

In topic-based message buses, subscription is done against *topics*. Each topic is a string that defines the actual event about which the client wishes to be notified. Typically, topics are organized in a hierarchical structure. Also, in such structure, often wildcards are allowed that enable to abbreviate the subscription to a complete topic sub-tree.

EXAMPLE 2: Criteria from example 1 formulated as topic, prefixed by the service name and notification type

rnis/cell_change/{applnsId}/{associateId.type}/{associateId.value}

EXAMPLE 3: Criteria from example 1 formulated as topic, with wildcard

rnis/cell_change/{applnsId}/*

If a particular mobile edge service foresees binding to a topic based message bus as an alternative transport, it is encouraged to define the list or hierarchy of topics in the specification, in order to improve interoperability. If that mobile edge service also provides REST-based subscribe-notify, it is encouraged to also define the mapping between the subscription data structures used in the RESTful API and the topic list / topic hierarchy.

In MEC, an important feature is authorization of applications. Authorization also needs to apply to subscriptions, to enable the mobile edge platform operator to restrict access of mobile edge applications to privileged information. Each separate access right is expressed by a "*permission identifier*" which identifies this right. Permission identifiers need to be unique within the scope of a particular mobile edge service. For each access right, the service specification needs to define a string to name that particular right. These strings can then be used throughout the system to identify that particular access right.

For REST-based subscriptions, it is suggested that the set of subscriptions is structured such that the subscription type can be used to scope the authorization (i.e. clients can be authorized for each individual subscription type separately, and one permission identifier maps to one subscription type). If finer or coarser granularity is required, this needs to be expressed in the particular specification by suitably defining the meaning of each permission identifier. For Topic-based subscriptions, each permission identifier is suggested to map to a particular topic, or a whole sub-tree of the topics structure.

The following items are proposed to define permissions:

Permission identifier: A string that identifies the item to which access is granted or denied. It is unique within the scope of a particular mobile edge service specification.

Display name: A short human-readable string to describe the permission when represented towards human users.

Specification: A specification that defines what the actual permission means. Can be as short as just naming the resource, subscription type or topic, or can also express a condition to define authorization at finer granularity than subscription type. If multiple alternative transports are supported, can contain specifications for more than one transport.

EXAMPLE 4: Tables 7.2-2, 7.2-3 and 7.2-4 provide an example definition of permissions for two transports: REST-based and topic-based message bus. Queries only apply to the REST-based transport.

Table 7.2-2: Definition of permissions

Permission identifier	Display name	Remarks
queries	Queries	REST-based only
bearer_changes	Bearer changes	Subscribe-notify
priv_bearer_changes	Privileged bearer changes	Subscribe-notify

Table 7.2-3: Permission identifiers mapping for transport "REST"

Permission identifier	Specification
queries	Resource: …/rnis/v1/queries
bearer_changes	Resource: …/rnis/v1/subscriptions Subscription type: BearerChangeSubscription with "privileged" flag not set
priv_bearer_changes	Resource: …/rnis/v1/subscriptions Subscription type: BearerChangeSubscription with "privileged" flag set
all	All of the permissions identified by "queries", "bearer_changes" and "priv_bearer_changes".

If OAuth 2.0 is used to authorize access to a REST-based transport, the permission identifiers can be represented as OAuth 2.0 scope values.

Table 7.2-4: Permission identifiers mapping for transport "Topic-based message bus"

Permission identifier	Specification
queries	Not supported
bearer_changes	Topic: /rnis/bearer_changes/nonprivileged/*
priv_bearer_changes	Topic: /rnis/bearer_changes/privileged/*

To define the access rights that an application requests, the permission identifiers which represent the requested access rights are defined in the application descriptor.

7.3 Serializers

As indicated in clause 7.1, different serializers can be used with alternative transports for a particular service. The reason for allowing this choice is that certain serializers make more sense in combination with particular transports than others. For example, RESTful APIs nowadays typically use JSON and a large number of development tools support this combination. When using message buses or GRPC, typically high throughput and low latency is a main requirement, which can be better met using a serializer into a binary format such as protocol buffers. Specifications of a mobile edge service can define in annexes the serializer(s) that are intended to be used for the data types defined for the service. The serializer to be used with a transport needs to be signalled over Mp1 when registering a service. More details can be found in ETSI GS MEC 011 [i.6].

7.4 Authorization of access to a service over alternative transports using TLS credentials

A method to authorize access to RESTful mobile edge service APIs using OAuth 2.0 has been defined in clause 6.16. For alternative transports, as defined in clause 7, using of OAuth might not be possible or supported in all the cases, e.g. for topic-based message buses. For these cases, other mechanisms are used to authorize access to the service. Several alternative transport mechanisms already require using TLS [14] to protect the communication channels. TLS credentials can be used to authenticate the endpoints of the protected connection, and to authorize them to access the mobile edge services delivered using an alternative transport that is secured with TLS.

TLS is designed to provide three essential services: encryption, authentication, and data integrity:

- For encryption, a secure data channel is established between the peers. To set up this channel, information about the cipher suite and encryption keys is exchanged between the peers during the TLS handshake.
- As part of the TLS handshake, the procedure also allows the peers to mutually authenticate themselves based on certificates and chain of trust enabled by Certificate Authorities. In the present document, client access rights are bound to the TLS credentials related to a client identifier, which allows to authorize an authenticated client to access particular mobile edge services or parts of those.
- Besides this, integrity of the data exchanged can be ensured with the Message Authentication Code algorithm supported by the TLS protocol.

Figure 7.4-1 shows an example how TLS can be used, in case of a topic-based message bus as alternative transport, to both secure the communications between the peers, as well as to authorize the consumption of a mobile edge service by a mobile edge application.

The mobile edge application is identified by a client identifier, which may be derived from attributes such as Distinguished Name (DN) used in the client certificate, or the application name and application provider defined in the application package. In a system that is based on a topic-based message bus as alternative transport, the mobile edge service is structured into one or more topics to which the consuming application can subscribe. Permissions can be given to subscribe to individual topics. By binding these permissions to a client identifier, the mobile edge application that is identified by this client identifier can be authorized to consume the corresponding parts of the service. Likewise, a service-producing mobile edge application can be authorized to send messages to the message bus for certain topics defined for the service.

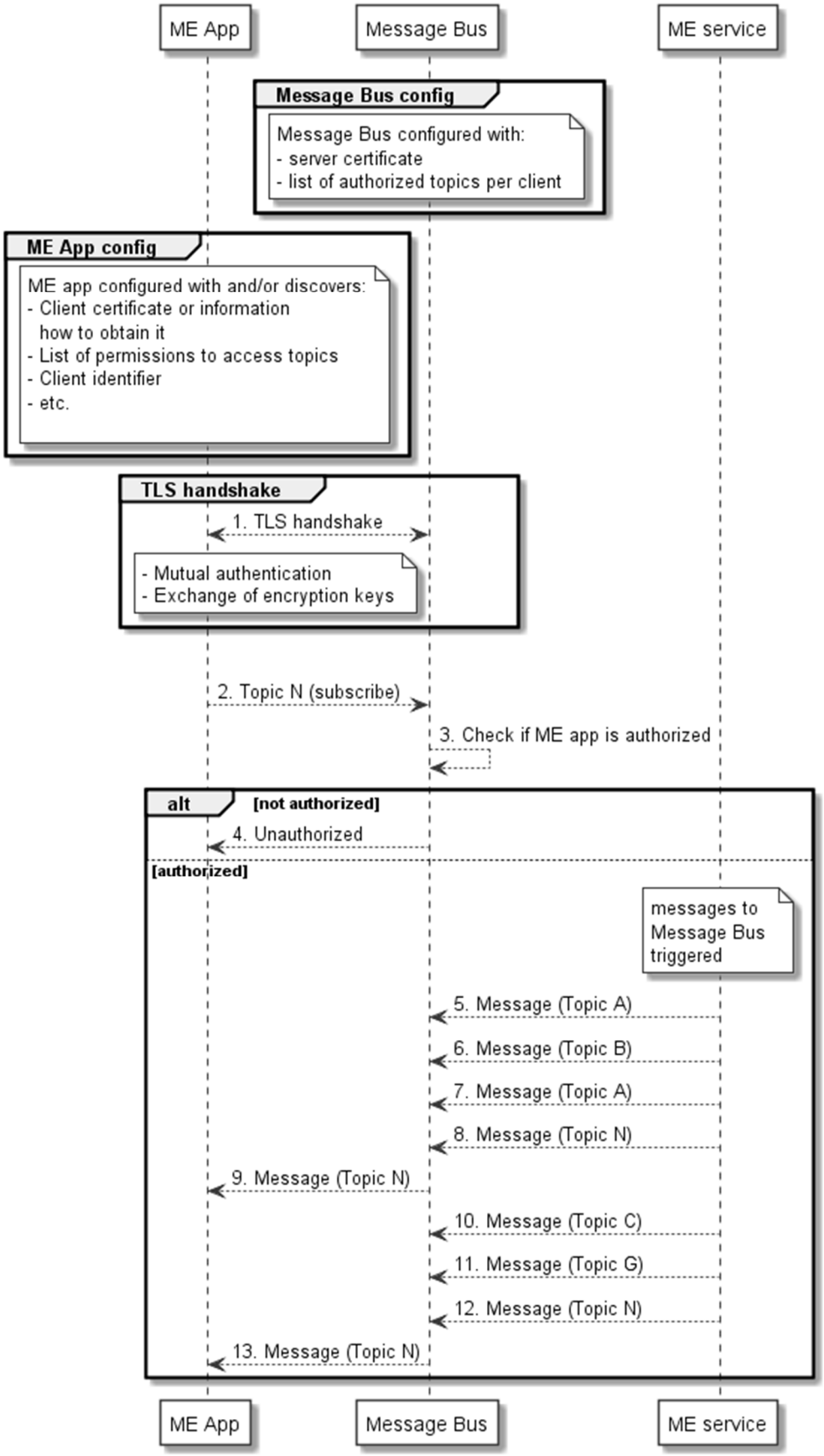


Figure 7.4-1: Using TLS for authorizing subscription to topics when using a topic-based message bus

As depicted in figure 7.4-1, there are preconditions and related procedures to provision the X.509 certificates for the message bus and for the mobile edge application. These procedures are based on the use of a Public Key Infrastructure (PKI) and they are out of scope of the present document.

The preconditions for mobile edge applications assume that authorization-related and security-related parameters are configured as part of the runtime configuration data of the application, and/or are discovered by the mobile edge application over Mp1. These include e.g. TLS version, list of permissions and topics that can be accessed, client identifier such as Distinguished Name or application provider and application name provided in the application package, and the instructions how to obtain the client certificate.

After having obtained the valid certificate to access the specific service offered over the message bus, the mobile edge application performs the TLS handshake and subscribes to topics offered, as follows:

1) The mobile edge application and the message bus perform the TLS handshake as defined in TLS protocol [14], including mutual authentication and encryption key exchange. As a result, the mobile edge application is authenticated towards the message bus.

2) The mobile edge application subscribes to topic N with the message bus.

3) The message bus checks whether the authenticated mobile edge application is authorized to subscribe to topic N, by checking the list of authorized topics that were configured for this mobile edge application.

4) In case the mobile edge application is not authorized to subscribe to the topic, an "Unauthorized" response is returned.

Otherwise, in steps 5 through 7 the mobile edge service sends messages on topics A & B to the message bus. Since the mobile edge application has not subscribed to those topics, those messages are not forwarded to this application.

8) Message on topic N sent to the message bus by the mobile edge service.

9) The message bus forwards the message to the subscribed mobile edge application.

In steps 10 and 11 the mobile edge service sends messages on topics C & G to the message bus. Since the mobile edge application has not subscribed to those topics, those messages are not forwarded to this application.

12) Message on topic N is sent to the message bus by the mobile edge service.

13) The message bus forwards the message to the subscribed mobile edge application.

Annex A (informative): REST methods

All API operations are based on the HTTP Methods. GET and POST are not allowed to be used to tunnel other operations.

Table A-1 lists basic operations on entities and their mapping to HTTP methods.

Table A-1: Operations and HTTP methods

Operation on entities	Uniform API operation	Description
Read/Query Entity	GET Resource	GET is used to retrieve a representation of a resource.
Create Entity	POST Resource	POST is used to create a new resource as child of a collection resource (see note 1).
Create Entity	PUT Resource	If applicable, PUT can be used to create a new resource directly (see note 1).
Partial Update of an Entity	PATCH Resource	PATCH, if supported, is used to partially update a resource (see note 2).
Complete Update of an Entity	PUT Resource	PUT is used to completely update a resource identified by its resource URI.
Remove an Entity	DELETE Resource	DELETE is used to remove a resource
Execute an Action on an Entity	POST on TASK Resource	POST on a task resource is used to execute a specific task not related to Create/Read/Update/Delete (see note 3).
NOTE 1: It is not advised to mix creation by PUT and creation by POST in the same API. NOTE 2: PATCH needs to be used with care if it is intended to be idempotent. See [i.2] for general principles. The data format is defined by IETF RFC 6901 [4] / IETF RFC 6902 [6] for JSON and IETF RFC 5261 [7] for XML. NOTE 3: A task resource a resource that represents a specific operation that cannot be mapped to a combination of Create/Read/Update/Delete. Task resources are advised to be used with careful consideration.		

Annex B (informative): API response status and exception codes

The tables in this clause list HTTP error response codes typically used in the ETSI MEC REST APIs. In addition to the codes listed below, clients need to be prepared to receive any other valid HTTP error response code. A list of all valid HTTP response codes and their specification documents can be obtained from the HTTP status code registry [i.8].

Table B-1 lists the success codes which indicate that the client's request was accepted successfully.

Table B-1: 2xx - Success codes

Status Code	Description
200	OK - used to indicate nonspecific success. The response body usually contains a representation of the resource. If this code is returned, it is not allowed to communicate errors in the response body.
201	Created - used to indicate successful resource creation. The return message usually contains a resource representation and always contains a "Location" HTTP header with the created resource's URI.
202	Accepted - used to indicate successful start of an asynchronous action.
204	No Content - used to indicate success when the response body is intentionally empty.

Table B-2 lists the redirection codes which indicate that the client has to take some additional action in order to complete its request.

Table B-2: 3xx - Redirection codes

Status Code	Description
301	Moved Permanently - used to relocate resources.
302	Found - not used.
303	See Other - used to refer the client to a different URI.
304	Not Modified - used to preserve bandwidth.
307	Temporary Redirect - used to tell clients to resubmit the request to another URI.

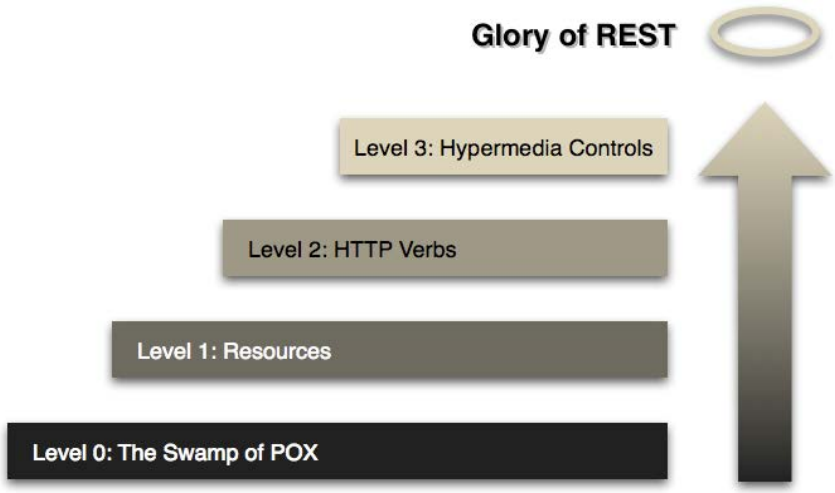
Table B-3 lists the client error codes which indicate an error related to the client's request.

Table B-3: 4xx - Client error codes

Status Code	Description
400	Bad Request - used to indicate nonspecific failure, including "catch-all" errors.
401	Unauthorized - used when the client did not submit credentials.
403	Forbidden - used to forbid access regardless of authorization state.
404	Not Found - used when a client provided a URI that cannot be mapped to a valid resource URI.
405	Method Not Allowed - used when the HTTP method is not supported for that particular resource. Typically, the response includes a list of supported methods.
406	Not Acceptable - used to indicate that the server cannot provide the any of the content formats supported by the client.
409	Conflict - used when attempting to create a resource that already exists.
410	Gone - used when a resource is accessed that has existed previously, but does not exist any longer (if that information is available).
412	Precondition failed - used when a condition has failed during conditional requests, e.g. when using ETags to avoid write conflicts when using PUT.
415	Unsupported Media Type - used to indicate that the server or the client does not support the content type of the payload body.
422	Unprocessable Entity - used to indicate that the payload body of a request contains syntactically correct data (e.g. well-formed JSON) but the data cannot be processed (e.g. because it fails validation against a schema).
429	Too many requests - used when a rate limiter has triggered.

Annex C (informative): Richardson maturity model of REST APIs

The Richardson maturity model [i.3] breaks down the principal elements of a REST approach into three steps.



NOTE: The figure is © by Martin Fowler and has been reproduced with permission from [i.3].

Figure C-1: Step towards REST

Level 0 - the swamp of POX: it is the starting point, using HTTP as a transport system for remote interactions, but without using any web mechanisms. Essentially it is to use HTTP as a tunnelling mechanism for remote interaction.

Level 1 - resources: the first step is to introduce resources. Instead of sending all requests to a singular service endpoint, they are now addressed to individual resources.

Level 2 - HTTP methods: HTTP methods (e.g. POST, GET) may be used for interactions in level 0 and 1, but as tunnelling mechanisms only. Level 2 moves away from this, using the HTTP methods as closely as possible to how they are used in HTTP itself.

Level 3 - hypermedia controls: this is often referred to HATEOAS (Hypermedia As The Engine Of Application State). It addresses the question of how to get from a list of resources to knowing what to do.

There are several advantages by adopting hypermedia controls:

- it allows the server to change its URI scheme without breaking clients;
- it helps client developers explore the protocol;

The links give client developers a hint as to what may be possible next, e.g. a starting point as to what to think about for more information and to look for a similar URI in the protocol documentation:

- it allows the server to advertise new capabilities by putting new links in the responses.

If the client developers are implementing handling for unknown links, these links can be a trigger for further exploration.

Annex D (informative): RESTful mobile edge service API template

<Template note: This annex is a template that provides text blocks for normative specification text to be copied into other specifications. Therefore, even though this annex is informative, some of the text blocks contain modal verbs that have special meaning according to clause 3.2 of the ETSI Drafting Rules.>

4 Sequence diagrams (informative)

<Template note: This clause will be included if needed to illustrate non-trivial call flows.>

4.1 Introduction

This clause …

4.2 <Procedure 1>

<Template note: Add introductory text>
This clause …

<Template note: Add flow diagram using a tool such as PlantUML. Add a caption.)

<Template note: Start of Example>

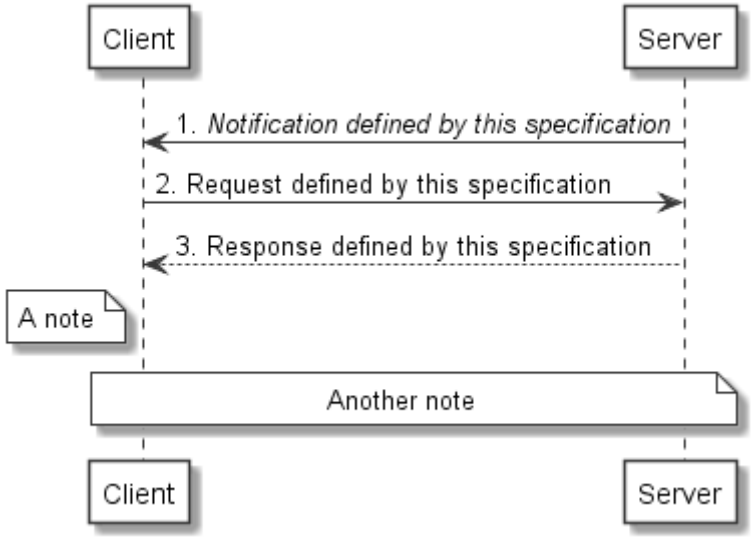


Figure 4.2-1: Flow of <Procedure 1>

<Template note: End of Example>

<Template note: Add description of the steps>
<Procedure 1>, as illustrated in figure 4.2-1, consists of the following steps:

<Template note: Start of Example>

1) The serer sends a notification to the client.
2) The client sends a request to the server.
3) The server returns a response.

<Template note: End of Example>

5 Data model (normative)

5.1 Introduction

<Template note: To be written according to the individual specification>

5.2 Resource data types

5.2.1 Introduction

This clause defines data structures to be used in resource representations.

5.2.2 Type: <TypeName1>

<Template note: TypeName1 in UpperCamel>

*<Template note: Short descriptive text of this data type, followed by a Table. Choices to be defined as follows: **"NOTE: One of "firstChoice" or at least one of "secondChoice" but not both shall be present."**>*

<Template note:

- *"Attribute name" provides the name of the attribute in lowerCamel*
- *"Data type" may provide the name of a **named data type** (structured, simple or enum) that is defined elsewhere in this document, or in a referenced document. In case of a referenced type from another document, a reference to the defining document shall be included in the "Description" column.*
- *"Data type" may also indicate the definition of an **inlined** nested **structure**. In case of inlining a structure, the "Data type" column shall contain the string "Structure (inlined)", and all attributes of the inlined structure shall be prefixed with one or more closing angular brackets ">", where the number of brackets represents the level of nesting.*
- *"Data type" may also indicate the definition of an **inlined enumeration type**. In case of inlining an enumeration type, the "Data type" column shall contain the string "Enum (inlined)", and the "Description" column shall contain the allowed values and (optionally) their meanings. There are two possible ways to define enums: just define the valid enum values (see clause 5.6.3) or to define the valid values and their mapping to integers (see clause 5.6.4). It is good practice not to mix the two patterns in the same data structure.*
- *"Cardinality" defines the allowed number of occurrence*
- *"Description" describes the meaning and use of the attribute and may contain normative statements. In case of an inlined enumeration type, the "Description" column shall define the allowed values and their meanings, as follows: "Permitted values:" on one line, followed by one paragraph of the following format for each value: "- VAL: Meaning of the value".>*

Table 5.2.2-1: Definition of type <TypeName1>

Attribute name	Data type	Cardinality	Description

<Template note: Start of Example>
This type represents a foobar indicator. Typically, this corresponds to one distinct stream signalled by foobar.

Table 5.2.2-2: Definition of type FooBar

Attribute name	Data type	Cardinality	Description
type	FooBarType	1	Indicates whether this is a foo, boo or hoo stream.
entryIdx	UnsignedInt	0..N	The index of the entry in the signaling table for correlation purposes, starting at 0.
fooBarType	Enum (inlined)	1	Signals the type of the foo bar. Permitted values: BIG_FOOBAR: Signals a big foobar. SMALL_FOOBAR: Signals a small foobar. <Template note: inlined variant of the pattern defined in clause 5.6.3.>
fooBarColor	Enum (inlined)	1	Signals the color of the foo bar. Permitted values: 1 = RED_FOOBAR: Signals a red foobar. 2 = GREEN_FOOBAR: Signals a green foobar. <Template note: inlined variant of the pattern defined in clause 5.6.4.>
firstChoice	MyChoiceOneType	0..1	First choice. See note.
secondChoice	MyChoiceTwoType	0..N	Second choice. See note.
nestedStruct	Structure (inlined)	0..1	A structure that is inlined, rather than referenced via an external type.
> someId	String	1	An identifier. The level of nesting is indicated by ">".
> myNestedStruct	Structure (inlined)	0..N	Another nested structure, one level deeper.
>> child	String	1	Child node at nesting level 2, indicated by ">>"
NOTE: One of "firstChoice" or at least one of "secondChoice" but not both shall be present.			

<Template note: End of Example>

5.3 Subscription data types

5.3.1 Introduction

This clause defines data structures for subscriptions.

5.3.2 Type: <TypeName2>

<Template note: Same structure as in clause 5.2.2>

5.4 Notification data types

5.4.1 Introduction

This clause defines data structures for notifications.

5.4.2 Type: <TypeName3>

<Template note: Same structure as in clause 5.2.2>

5.5 Referenced structured data types

5.5.1 Introduction

This clause defines data structures that can be referenced from data structures defined in the previous clauses, but can neither be resource representations nor notifications.

5.5.2 Type: <TypeName4>

<Template note: Same structure as in clause 5.2.2>

5.6 Referenced simple data types and enumerations

5.6.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

5.6.2 Simple data types

The simple data types defined in table 5.6.2-1 shall be supported.

Table 5.6.2-1: Simple data types

Type name	Description

5.6.3 Enumeration: <EnumType1>

<Template note: If the intent is to map the enum values to strings (often used in JSON), or only to define the valid values (with the intent to define their mappings to integers in a different place, specific to certain serializers), the format in this clause is suggested to be used.>

The enumeration <EnumType1> represents <something>. It shall comply with the provisions defined in table 5.6.3-1.

Table 5.6.3-1: Enumeration <EnumType1>

Enumeration value	Description
A_VALUE	The description of this enum value
ANOTHER_VALUE	The description of this other enum value

5.6.4 Enumeration: <EnumType2>

<Template note: If the intent is to map the enum values to integers independent of the serializer, the format in this clause is suggested to be used. "<int>" in the table below to be replaced by an actual integer value.>

The enumeration <EnumType2> represents <something>. It shall comply with the provisions defined in table 5.6.4-1.

Table 5.6.4-1: Enumeration <EnumType2>

Enumeration value	Description
<int> = A_VALUE	The description of this enum value
<int> = ANOTHER_VALUE	The description of this other enum value

6 RESTful API definition (Normative)

6.1 Introduction

This clause defines the resources and operations of the <Name of the API here> API.

6.2 Global definitions and resource structure

All resource URIs of this API shall have the following root:

- **{apiRoot}/{apiName}/{apiVersion}/**

"ApiRoot" and "apiName" are discovered using the service registry. It includes the scheme ("https"), host and optional port, and an optional prefix string. The API shall support HTTP over TLS (also known as HTTPS [13]) (see IETF RFC 2818 [13]). TLS version 1.2 as defined by IETF RFC 5246 [14] shall be supported. HTTP is not recommended. The "apiVersion" shall be set to "v1" for the current version of the specification. All resource URIs in the sub-clauses below are defined relative to the above root URI.

<Template note: Adapt the sentence below as appropriate for the particular API>

The content formats XML and JSON shall be supported.

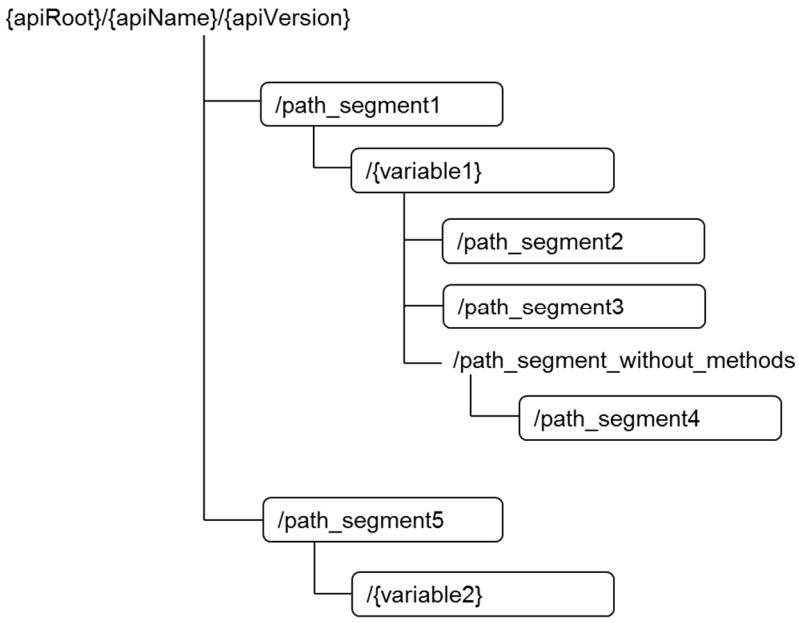
<Template note: Certain APIs may also want to introduce their own content type and register with IANA >

The JSON format is signalled by the content type "application/json" and the XML format is signalled by the content type "application/xml".

Figure 6.2-1 illustrates the resource URI structure of this API. Table 6.2-1 provides an overview of the resources defined by the present document, and the applicable HTTP methods.

<Template note: Start of Example>

<Template note: a filled node represents a sub-URI that has at least one supported operation associated. All node names are examples only>



<Template note: End of Example>

Figure 6.2-1: Resource URI structure of the <xyz> API

<Template note: Overview table of resources and operations>

Table 6.2-1: Resources and methods overview

Resource name	Resource URI	HTTP method	Meaning
<Resource name>	<relative URI below root>	GET	<Operation executed by GET>
		PUT	<Operation executed by PUT>
		PATCH	<Operation executed by PATCH>
		POST	<Operation executed by POST>
		DELETE	<Operation executed by DELETE>

<Template note: Start of Example>

Table 6.2-2: Resources and methods overview

Resource name	Resource URI	HTTP method	Meaning
All foobar sessions	/{userId}/sessions	GET	Retrieve a list of foobar sessions
		POST	Create a new foobar session
Individual foobar session	/{userId}/sessions/{sessionId}	GET	Retrieve a foobar session
		DELETE	Terminate a foobar session

<Template note: End of Example>

<Template note: Repeat the following level 2 clause as often as needed, once per resource>

6.3 Resource: <Meaning>

6.3.1 Description

This resource is used to …/ This resource represents …/ <or similar text as applicable>

6.3.2 Resource definition

Resource URI: **{apiRoot}/{apiName}/v1/<name>**

This resource shall support the resource URI variables defined in table 6.3.2-1.

Table 6.3.2-1: Resource URI variables for resource "<Meaning>"

Name	Definition
apiRoot	See clause 6.2
apiName	See clause 6.2
<name>	<definition>

6.3.3 Resource methods

6.3.3.1 GET

The <GET> method … <Meaning(s) of the operation in API space> or <Not supported>

<Template note: Start of Example>

The GET method retrieves information about a fooBar object.

<Template note: End of Example>

This method shall support the URI query parameters, request and response data structures, and response codes, as specified in the tables 6.3.3.1-1 and 6.3.3.1-2.

Table 6.3.3.1-1: URI query parameters supported by the <GET> method on this resource

Name	Data type	Cardinality	Remarks
<name> or n/a	<type> or <leave empty>	0..1 or 1 or 0..N <leave empty>	<only if applicable>

Table 6.3.3.1-2: Data structures supported by the <GET> request/response on this resource

	Data type	Cardinality	Response codes	Remarks
Request body	<type> or n/a	<1 (i.e. object)> or <0..N, 1..N, m..n (i.e. array)> or <leave empty>	<only if applicable>	
Response body	<type> or n/a	<1 (i.e. object)> or <0..N, 1..N, m..n (i.e. array)> or <leave empty>	<list applicable codes with name from IETF RFC 7231, etc.>	<Meaning of the success case> or <Meaning of the error case with additional statement regarding error handling>

<Template note: If a statement in the "Remarks" column repeats too often, it can be represented as a NOTE at the bottom of the table>

<Template note: Start of Example>

Table 6.3.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	Cardinality	Remarks
foo_bar	String	0..1	The foo bar

Table 6.3.3.1-2: Data structures supported by the GET request/response on this resource

Request body	Data type	Cardinality	Remarks	
	n/a			
Response body	Data type	Cardinality	Response codes	Remarks
	FooBarInstance	1	201 Created	The foobar session was created successfully.
	ProblemDetails	0..1	400 Bad Request	Incorrect parameters were passed to the request. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	404 Not Found	The resource URI was incorrect. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	1	403 Forbidden	The operation is not allowed given the current status of the resource. More information shall be provided in the "detail" attribute of the "ProblemDetails" structure.

<Template note: Note that the cardinality of the "ProblemDetails" structure may differ between different error codes. Some may require the provision of application specific details, for some it may be merely optional or recommended. >

<Template note: End of Example>

<Template note: If applicable, add a statement on HTTP headers specific to the operation>

On success, the HTTP response shall/should/may include a <name> HTTP header that…

<Template note: Start of Example>
On success, the HTTP response shall include a "Location" HTTP header that contains the URI of the newly-created resource.

<Template note: End of Example>

<Template note: If necessary, describe error handling in text>

Error handling: text text text

6.3.3.2 PUT

<same structure as for GET>

6.3.3.3 PATCH

<same structure as for GET>
<Template note: The data type in the request body should be defined carefully in a particular format, refer to pattern 6.9 for detail>

6.3.3.4 POST

<same structure as for GET>

6.3.3.5 DELETE

<same structure as for GET>

History

Document history		
V1.1.1	July 2017	Publication