



ONEM2M TECHNICAL SPECIFICATION

Document Number	TS-0008- V-3.3.1
Document Name:	CoAP Protocol Binding
Date:	2019-02-25
Abstract:	The specification will cover the protocol specific part of communication protocol used by oneM2M compliant systems as 'CoAP binding'

This Specification is provided for future development work within oneM2M only. The Partners accept no liability for any use of this Specification.

The present document has not been subject to any approval process by the oneM2M Partners Type 1. Published oneM2M specifications and reports for implementation should be obtained via the oneM2M Partners' Publications Offices.

About oneM2M

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

More information about oneM2M may be found at: <http://www.oneM2M.org>

Copyright Notification

No part of this document may be reproduced, in an electronic retrieval system or otherwise, except as authorized by written permission.

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

© 2019, oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TSDSI, TTA, TTC).

All rights reserved.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. NO oneM2M PARTNER TYPE 1 SHALL BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY THAT PARTNER FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL oneM2M BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. oneM2M EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

Contents

1	Scope	5
2	References	5
2.1	Normative references	5
2.2	Informative references	5
3	Abbreviations and acronyms	5
4	Conventions	6
5	Overview	6
5.0	Introduction	6
5.1	Required Features	6
5.2	Introduction of CoAP	6
5.2.0	Introduction	6
5.2.1	Message Format	6
5.2.2	Caching	7
5.2.2.0	Introduction	7
5.2.2.1	Freshness	7
5.2.2.2	Validity	7
5.2.3	Blockwise Transfers	7
6	CoAP Message Mapping	7
6.1	Introduction	7
6.2	Primitive Mapping to CoAP Message	8
6.2.0	Introduction	8
6.2.1	Header	8
6.2.2	Configuration of Token and Options	9
6.2.2.0	Introduction	9
6.2.2.1	Token	9
6.2.2.2	Content Format Negotiation Options	9
6.2.2.3	URI Options	9
6.2.2.4	Definition of New Options	10
6.2.2.4.0	Introduction	10
6.2.2.4.1	From	11
6.2.2.4.2	Request Identifier	11
6.2.2.4.3	Void	11
6.2.2.4.4	Originating Timestamp	11
6.2.2.4.5	Request Expiration Timestamp	11
6.2.2.4.6	Result Expiration Timestamp	11
6.2.2.4.7	Operation Execution Time	11
6.2.2.4.8	notificationURI of Response Type	11
6.2.2.4.9	Event Category	11
6.2.2.4.10	Response Status Code	12
6.2.2.4.11	Group Request Identifier	12
6.2.2.4.12	Resource Type	12
6.2.2.4.13	Content Offset	12
6.2.2.4.14	Content Status	12
6.2.2.4.15	Assigned Token Identifiers	12
6.2.2.4.16	Release Version Indicator	12
6.2.2.4.17	Vendor Information	12
6.2.2.4.18	Group Request Target Members	12
6.2.2.4.19	Authorization Signature	12
6.2.2.4.20	Authorization Signature Request Information	13
6.2.3	Payload	13
6.2.4	Response Codes Mapping	13
6.3	Accessing Resources in CSEs	15
6.3.0	Introduction	15
6.3.1	Blocking case	15
6.3.2	Non-Blocking Asynchronous case	15

6.3.3	Non-Blocking Synchronous case	16
6.4	Mapping rules of caching	16
6.5	Usage of Blockwise Transfers	16
7	Security Consideration	16
Annex A (informative): Example Procedures.....		18
A.1	Blocking case of AE Registration	18
A.2	Non-blocking synchronous case of AE Registration.....	19
Annex B (normative): Multicast group fan out procedure.....		20
B.0	Introduction	20
B.1	Security	20
B.2	Caching	21
History		22

1 Scope

The present document will cover the protocol specific part of communication protocol used by oneM2M compliant systems as 'RESTful CoAP binding'.

The scope of the present document is (not limited to as shown below):

- Binding oneM2M primitives to CoAP messages.
- Binding oneM2M Response Status Codes to CoAP Response Codes.
- Defining behaviour of a CoAP Client and Server depending on oneM2M parameters.

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.

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

- [1] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".
- [2] oneM2M TS-0004: "Service Layer Core Protocol Specification".
- [3] IETF RFC 7959: "Block-Wise Transfers in the Constrained Application Protocol (CoAP)".
- [4] oneM2M TS-0003: "Security solutions".
- [5] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

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 reference document (including any amendments) applies.

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] oneM2M Drafting Rules.

NOTE: Available <http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf>.

3 Abbreviations and acronyms

For the purposes of the present document, the following abbreviations and acronyms apply:

ACK	Acknowledgement
AE	Application Entity
CON	Confirmable
CSE	Common Service Entity
DTLS	Datagram Transport Layer Security
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol

RST	CoAP ReSeT message
TCP	Transport Control Protocol
TLS	Transport Layer Security
TLV	Tag - Length - Value (data structure)
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
XML	eXtensible Markup Language

4 Conventions

The keywords "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

5 Overview

5.0 Introduction

The clause describes which features need to be supported in CoAP layer and introduces a message format and several features of CoAP used in this protocol binding specification.

5.1 Required Features

This clause explicitly specifies the required features of the CoAP layer for oneM2M to properly bind oneM2M primitives into CoAP messages:

- The 4-byte binary CoAP message header is defined in section 3 of IETF RFC 7252 [1].
- Confirmable (CON), Acknowledgement (ACK) and Reset (RST) messages shall be supported. The Reset message is used to send an error message in response to a malformed Confirmable message in CoAP layer.
- GET, PUT, POST and DELETE methods shall be supported. oneM2M primitives map to these methods.
- The CoAP Response Codes specified in clause 6.2.4 shall be supported for oneM2M *Response Status Code* parameter mapping.
- The Uri-Host, Uri-Port, Uri-Path, and Uri-Query shall be supported.
- The Content-Type Option shall be used to indicate the media types of the payload.
- Block-wise transfers feature may be supported to carry large payloads.
- Caching feature may be supported.

5.2 Introduction of CoAP

5.2.0 Introduction

This clause describes a message format, and caching and block-wise transfers features which may be used to map oneM2M primitives to CoAP messages.

5.2.1 Message Format

This clause specifies details about the CoAP [1] message format:

- CoAP message occupies the data section of one UDP datagram.

- CoAP message format supports a 4-byte fixed-size header.
- Fixed-size header is followed by a Token value of length 0 to 8 bytes.
- The Token value is followed by a sequence of zero or more CoAP Options in TLV format.
- CoAP Options are followed by the payload part.

For more details on the CoAP message format and the supported header fields, refer to IETF RFC 7252 [1].

5.2.2 Caching

5.2.2.0 Introduction

CoAP [1] supports caching of responses to fulfil future equivalent requests to the same resource. Caching is supported using freshness and validity information carried with CoAP [1] responses.

5.2.2.1 Freshness

- CoAP server shall use Max-Age CoAP Option to specify the explicit expiration time for the CoAP Response's resource representation. This indicates that the response is not fresh after its age is greater than the specified number of seconds.
- Max-Age Option defaults to a value of 60 (seconds). In case, Max-Age Option is not present in the cacheable response, the response shall not be considered fresh after its age is greater than 60 seconds.
- The CoAP server shall set the Max-Age Option value to 0 (zero) to prevent or disable caching.
- The CoAP client, having a fresh stored response, can make new request matching the request for that stored response. In this case, the new response shall invalidate the old response.

5.2.2.2 Validity

- A CoAP endpoint with stored responses but not able to satisfy subsequent requests (for example, the response is not fresh), shall use the Etag Option to perform a conditional request to the CoAP server where the resource is hosted.
- If the cached response with the CoAP client is still valid, the server shall include the Max-Age Option in the response along with a code of 2.03 - Valid. This shall update the freshness of the cached response at the CoAP client.
- If the cached response with the CoAP client is not valid, the server shall respond with an updated representation of the resource with response code 2.05 - Content. The CoAP client shall use the updated response to satisfy request and may also replace/update the stored or cached response.

5.2.3 Blockwise Transfers

CoAP Block [3] Options may be used when CoAP endpoints need to transfer large payloads e.g. firmware, software updates. Instead of relying on IP fragmentation, CoAP Block Option should be used for transferring multiple blocks of information in multiple request-response pairs.

6 CoAP Message Mapping

6.1 Introduction

When AE or CSE binds oneM2M primitives to CoAP messages, or binds CoAP messages to oneM2M primitives, it is required that:

- AE shall host a CoAP client and should host a CoAP server; or
- CSE shall host both a CoAP client and a CoAP server.

Basically single oneM2M request primitive is mapped to single CoAP request message, and single oneM2M response primitive is mapped to single CoAP response message. However, single oneM2M request/response primitive is mapped to multiple CoAP request/response messages respectively when CoAP block-wise transfers feature is used.

Mapping between CoAP message and oneM2M primitive shall be applied in the following cases:

- when the Originator sends a request primitive;
- when the Receiver receives a CoAP message(s);
- when the Receiver sends a response primitive;
- when the Originator receives a CoAP message(s).

The following sub-clauses specify how to map each oneM2M primitive parameter defined in oneM2M TS-0004 [2] to a corresponding CoAP message field to compose a CoAP request/response message.

6.2 Primitive Mapping to CoAP Message

6.2.0 Introduction

This clause describes where to map oneM2M parameters in a primitive to header, Option and payload fields in a CoAP message.

6.2.1 Header

This clause specifies how to configure CoAP header information:

- The Version field shall be configured as 1.
- The Type field shall be configured according to clause 6.3. The Reset message is used to send a error message in response to a malformed Confirmable message in CoAP layer.
- In case of a request, the Code field indicates CoAP Method. The oneM2M *Operation* parameter shall be mapped to a CoAP Method according to the table 6.2.1-1.
- In case of a response, the Code field indicates CoAP Response Code. The oneM2M *Response Status Code* parameter shall be mapped to CoAP Response Code as specified in clause 6.2.4.

The configurations of Token Length and Message ID are left to implementation.

Table 6.2.1-1: oneM2M Operation Parameter Mapping

oneM2M Operation Parameter	CoAP Method	CoAP Method Code
CREATE	POST	0.02
RETRIEVE	GET	0.01
UPDATE	PUT	0.03
DELETE	DELETE	0.04
NOTIFY	POST	0.02

At the Receiver, CoAP request message with POST method shall be mapped to oneM2M CREATE or NOTIFY *Operation* parameter in accordance with the existence of *Resource Type* parameter. If *Resource Type* parameter exists then value of the *Operation* parameter is CREATE and if *Resource Type* parameter does not exist, the value of *Operation* parameter is NOTIFY.

6.2.2 Configuration of Token and Options

6.2.2.0 Introduction

This clause describes configuration of Token and Options based on oneM2M parameters.

6.2.2.1 Token

Due to size limitation, Request Identifier is not mapped to Token option. However, Token may be used in CoAP layer to match a CoAP request and response.

6.2.2.2 Content Format Negotiation Options

The CoAP Accept Option may be used to indicate which Content-Format is acceptable to an Originator. If a Hosting CSE supports the Content-Format specified in Accept Option of the request, the Hosting CSE shall respond with that Content-Format. If the Hosting CSE does not support the Content-Format specified in Accept Option of the request, 4.06 "Not Acceptable" shall be sent as a response, unless another error code takes precedence for this response.

Possible values for Content-Format and Accept options are listed below:

- application/xml (41);
- application/json (50);
- application/cbor (60);
- media types specified in clause 6.7 "oneM2M specific MIME media types" of oneM2M TS-0004 [2].

Numeric values for oneM2M defined media types are listed in table 6.2.2.2-1.

Table 6.2.2.2-1: CoAP oneM2M Specific Content-Formats

oneM2M Specific Media Type	ID
vnd.onem2m-res+xml	10014
vnd.onem2m-res+json	10001
vnd.onem2m-ntfy+xml	10002
vnd.onem2m-ntfy+json	10003
vnd.onem2m-preq+xml	10006
vnd.onem2m-preq+json	10007
vnd.onem2m-prsp+xml	10008
vnd.onem2m-prsp+json	10009
vnd.onem2m-res+cbor	10010
vnd.onem2m-ntfy+cbor	10011
vnd.onem2m-preq+cbor	10012
vnd.onem2m-prsp+cbor	10013

NOTE: ID values for oneM2M specific media type are subject to change after IANA registration.

6.2.2.3 URI Options

This clause describes how to configure CoAP Uri-Host, Uri-Port, Uri-Path, and Uri-Query Options.

Host and port part of the address specified in *pointOfAccess* attribute of <remoteCSE> resource shall be mapped to Uri-Host and Uri-Port respectively.

If *To* parameter contains absolute format, then the first URI-Path Option shall contain a letter "_" and map *To* parameter removing starting "/" into next URI-Path Option(s).

If *To* parameter contains SP-relative format, then the first URI-Path Option shall contain a letter "~" and map *To* parameter removing starting "/" into next URI-Path Option(s).

If *To* parameter contains CSE-relative format, then *To* parameter shall be mapped to URI-Path Option(s).

Table 6.2.2.3-1 shows valid mappings between the **To** request primitive parameter and the Uri-Path of the CoAP.

CSEBase represents the resource name of a <CSEBase> resource, CSEBase/ae12/cont27/contInst696 represents a structured CSE-relative resource ID, and cin00856 an unstructured CSE-relative resource ID.

Table 6.2.2.3-1: Mapping examples between To parameter and Uri-Path of the CoAP

Method		Request Scope		
		CSE-Relative	SP-Relative	Absolute
Structured	To	CSEBase/ae12/cont27/contInst696	/CSE178/CSEBase/ae12/cont27/contInst696	//mym2msp.org/CSE178/CSEBase/ae12/cont27/contInst696
	Uri-Path	CSEBase		-
			~	mym2msp.org
			CSE178	CSE178
			CSEBase	CSEBase
ae12	ae12	ae12		
cont27	cont27	cont27		
contInst696	contInst696	contInst696		
Unstructured	To	cin00856	/CSE178/cin00856	//mym2msp.org/CSE178/cin00856
	Uri-Path	cin00856		-
			~	mym2msp.org
			CSE178	CSE178
			cin00856	cin00856

NOTE: How to read this table: To primitive - from left to right, Uri-Path - from top to bottom.

The *responseTypeValue* element of **Response Type**, **Result Persistence**, **Delivery Aggregation**, **Result Content**, parameters of **Filter Criteria**, **Discovery Result Type**, **Token Request Indicator**, **Tokens**, **Token IDs**, **Local Token IDs**, **Role IDs**, **Authorization Relationship Indicator**, **Authorization Signature Indicator**, **Semantic Query Indicator** parameters shall be carried in Uri-Query Option in a short name form as specified in clause 8.2.2 of oneM2M TS-0004 [2].

6.2.2.4 Definition of New Options

6.2.2.4.0 Introduction

This clause describes new CoAP Options used for binding several oneM2M request/response parameters.

Table 6.2.2.4.0-1 contains definitions of the new CoAP Options and sub-clauses specify oneM2M parameter mapping with the newly defined CoAP Options in the table 6.2.2.4.0-1.

Table 6.2.2.4.0-1: Definition of New Options

No	C	U	N	R	Name	Format	Length	Default
256					oneM2M-FR	string	0-255	(None)
257					oneM2M-RQI	string	0-255	(None)
259					oneM2M-OT	string	15	(None)
260					oneM2M-RQET	string	15	(None)
261					oneM2M-RSET	string	15	(None)
262					oneM2M-OET	string	15	(None)
263					oneM2M-RTURI	string	0-255	(None)
264					oneM2M-EC	uint	1	(None)
265					oneM2M-RSC	uint	2	(None)
266					oneM2M-GID	string	0-255	(None)
267					oneM2M-TY	uint	2	(None)
268					oneM2M-CTO	uint	2	(None)
269					oneM2M-CTS	uint	2	(None)
270					oneM2M-ATI	string	0-255	(None)
271					oneM2M-RVI	string	1	(None)
272					oneM2M-VSI	string	0-255	(None)
273					oneM2M-GTM	string	0-512	(None)
274					oneM2M-AUS	string	0-255	(None)
275					oneM2M-ASRI	string	0-255	(None)
NOTE 1: C, U, N, R means Critical, Unsafe, NoCacheKey and Repeatable respectively [1]. Table 6.2.2.4.0-1 follows the template used in clause 5.10 Option Definitions of CoAP specification [1].								
NOTE 2: CoAP Option numbers specified in table 6.2.2.4.0-1 are subject to change after review by IANA registration.								

6.2.2.4.1 From

The *From* parameter shall be mapped to the oneM2M-FR Option.

6.2.2.4.2 Request Identifier

The *Request Identifier* parameter shall be mapped to the oneM2M-RQI Option.

6.2.2.4.3 Void

6.2.2.4.4 Originating Timestamp

The *Originating Timestamp* parameter shall be mapped to the oneM2M-OT Option.

6.2.2.4.5 Request Expiration Timestamp

The *Request Expiration Timestamp* parameter shall be mapped to the oneM2M-RQET Option.

6.2.2.4.6 Result Expiration Timestamp

The *Request Expiration Timestamp* parameter shall be mapped to the oneM2M-RSET Option.

6.2.2.4.7 Operation Execution Time

The *Operation Execution Time* parameter shall be mapped to the oneM2M-OET Option.

6.2.2.4.8 notificationURI of Response Type

The notificationURI element of *Response Type* parameter shall be mapped to the oneM2M-RTURI Option.

6.2.2.4.9 Event Category

The *Event Category* parameter shall be mapped to the oneM2M-EC Option.

6.2.2.4.10 Response Status Code

The *Response Status Code* parameter shall be mapped to the oneM2M-RSC Option.

6.2.2.4.11 Group Request Identifier

The *Group Request Identifier* parameter shall be mapped to the oneM2M-GID Option.

6.2.2.4.12 Resource Type

The *Resource Type* parameter shall be mapped to the oneM2M-TY Option.

6.2.2.4.13 Content Offset

The *Content Offset* parameter shall be mapped to the oneM2M-CTO Option.

6.2.2.4.14 Content Status

The *Content Status* parameter shall be mapped to the oneM2M-CTS Option.

6.2.2.4.15 Assigned Token Identifiers

The *Assigned Token Identifiers* parameter shall be mapped to the oneM2M-ATI Option. The format of the oneM2M-ATI option shall be represented as a sequence of lti-value:tkid-value pairs separated by a colon ':' and multiple pairs appended with '+' character.

EXAMPLE: The header looks as follows:

oneM2M-ATI: lti-value1:tkid-value1 + lti-value2:tkid-value2 + ...

if the XML representation of the *Assigned Token Identifiers* parameter is given as (using short element names):

```
<ati>
  <ltia>
    <lti>lti-value1</lti>
    <tkid>tkid-value1</tkid>
  </ltia>
  <ltia>
    <lti>lti-value2</lti>
    <tkid>tkid-value2</tkid>
  </ltia>
  ...
</ati>
```

The data type m2m:dynAuthlocalTokenIdAssignments of the *Assigned Token Identifiers* parameter is defined in clause 6.3.5.43 of oneM2M TS-0004 [2].

6.2.2.4.16 Release Version Indicator

The *Release Version Indicator* parameter shall be mapped to the oneM2M-RVI Option.

6.2.2.4.17 Vendor Information

The *Vendor Information* parameter shall be mapped to the oneM2M-VSI Option.

6.2.2.4.18 Group Request Target Members

The *Group Request Target Members* parameter shall be mapped to the oneM2M-GTM Option.

6.2.2.4.19 Authorization Signature

The *Authorization Signature* parameter shall be mapped to the oneM2M-AUS Option.

6.2.2.4.20 Authorization Signature Request Information

The *Authorization Signature Request Information* parameter shall be mapped to the oneM2M-ASRI Option.

6.2.3 Payload

Content parameter shall be mapped to CoAP payload. Blockwise transfers mechanism may be used to deliver large size of *Content* parameter which is not fit into one CoAP message. Please refer to clause 6.5 for the detail information. If *Content* parameter contains URI and resource representation in a response to a create request, URI shall be mapped to Location-Path Option.

A *Token Request Information* parameter included in a response primitive shall be mapped into the payload. The Content-Format shall be set compliant with the data representation.

6.2.4 Response Codes Mapping

Table 6.2.4-1 defines a mapping between oneM2M *Response Status Code* parameter specified in [2] and CoAP Response Code.

In case of where multiple oneM2M *Response Status Code* parameters are mapped to a single CoAP Response Code, the *Response Status Code* parameter shall be specified in oneM2M-RSC Option.

Table 6.2.4-1: Mapping between oneM2M Response Status Code and CoAP Response Code

oneM2M Response Status Code	Description	CoAP Response Code	Description
1000	ACCEPTED	None	Empty Acknowledgement Message shall be used
2000	OK	2.05	Content
2001	CREATED	2.01	Created
2002	DELETED	2.02	Deleted
2004	UPDATED	2.04	Changed
4000	BAD_REQUEST	4.00	Bad Request
4001	RELEASE_VERSION_NOT_SUPPORTED	4.00	Bad Request
4004	NOT_FOUND	4.04	Not Found
4005	OPERATION_NOT_ALLOWED	4.05	Method Not Allowed
4008	REQUEST_TIMEOUT	4.04	Not Found
4015	UNSUPPORTED_MEDIA_TYPE	4.15	Unsupported Content-Format
4101	SUBSCRIPTION_CREATOR_HAS_NO_PRIVILEGE	4.03	Forbidden
4102	CONTENTS_UNACCEPTABLE	4.00	Bad Request
4103	ORIGINATOR_HAS_NO_PRIVILEGE	4.03	Forbidden
4104	GROUP_REQUEST_IDENTIFIER_EXISTS	4.00	Bad Request
4105	CONFLICT	4.03	Forbidden
4106	ORIGINATOR_HAS_NOT_REGISTERED	4.03	Forbidden
4107	SECURITY_ASSOCIATION_REQUIRED	4.03	Forbidden
4108	INVALID_CHILD_RESOURCE_TYPE	4.03	Forbidden
4109	NO_MEMBERS	4.03	Forbidden
4110	GROUP_MEMBER_TYPE_INCONSISTENT	4.00	Bad Request
4111	ESPRIM_UNSUPPORTED_OPTION	4.03	Forbidden

oneM2M Response Status Code	Description	CoAP Response Code	Description
4112	ESPRIM_UNKNOWN_KEY_ID	4.03	Forbidden
4113	ESPRIM_UNKNOWN_ORIG_RAND_ID	4.03	Forbidden
4114	ESPRIM_UNKNOWN_RECV_RAND_ID	4.03	Forbidden
4115	ESPRIM_BAD_MAC	4.03	Forbidden
4116	ESPRIM_IMPERSONATION_ERROR	4.03	Forbidden
4117	ORIGINATOR_HAS_ALREADY_REGISTERED	4.03	Forbidden
4118	ONTOLOGY_NOT_AVAILABLE	4.04	Not Found
4119	LINKED_SEMANTICS_NOT_AVAILABLE	4.04	Not Found
4120	INVALID_SEMANTICS	4.02	Bad Option
4121	MASHUP_MEMBER_NOT_FOUND	4.04	Not Found
4122	INVALID_TRIGGER_PURPOSE	4.02	Bad Option
5000	INTERNAL_SERVER_ERROR	5.00	Internal Server Error
5001	NOT_IMPLEMENTED	5.01	Not Implemented
5103	TARGET_NOT_REACHABLE	4.04	Not Found
5105	RECEIVER_HAS_NO_PRIVILEGE	4.03	Forbidden
5106	ALREADY_EXISTS	4.00	Bad Request
5203	TARGET_NOT_SUBSCRIBABLE	4.03	Forbidden
5204	SUBSCRIPTION_VERIFICATION_INITIATION_FAILED	5.00	Internal Server Error
5205	SUBSCRIPTION_HOST_HAS_NO_PRIVILEGE	4.03	Forbidden
5206	NON_BLOCKING_SYNCH_REQUEST_NOT_SUPPORTED	5.01	Not Implemented
5207	NOT_ACCEPTABLE	4.06	Not Acceptable
5208	DISCOVERY_DENIED_BY_IPE	4.03	Forbidden
5209	GROUP_MEMBERS_NOT_RESPONDED	5.00	Internal Server Error
5210	ESPRIM_DECRYPTION_ERROR	5.00	Internal Server Error
5211	ESPRIM_ENCRYPTION_ERROR	5.00	Internal Server Error
5212	SPARQL_UPDATE_ERROR	5.00	Internal Server Error
5213	MASH_UP_OPERATION_FAILED	5.00	Internal Server Error
5214	TARGET_HAS_NO_SESSION_CAPABILITY	4.03	Forbidden
5215	SESSION_IS_ONLINE	4.03	Forbidden
5216	JOIN_MULTICAST_GROUP_FAILED	5.00	Internal Server Error
5217	LEAVE_MULTICAST_GROUP_FAILED	5.00	Internal Server Error
5218	TRIGGERING_DISABLED_FOR_RECIPIENT	5.03	Service Unavailable
5219	UNABLE_TO_REPLACE_TRIGGER_REQUEST	5.03	Service Unavailable
5220	UNABLE_TO_RECALL_TRIGGER_REQUEST	5.03	Service Unavailable
5221	CROSS_RESOURCE_OPERATION_FAILURE	5.00	Internal Server Error
6003	EXTERNAL_OBJECT_NOT_REACHABLE	4.04	Not Found
6005	EXTERNAL_OBJECT_NOT_FOUND	4.04	Not Found
6010	MAX_NUMBER_OF_MEMBER_EXCEEDED	4.00	Bad Request
6020	MGMT_SESSION_CANNOT_BE_ESTABLISHED	5.00	Internal Server Error
6021	MGMT_SESSION_ESTABLISHMENT_TIMEOUT	5.00	Internal Server Error
6022	INVALID_CMDTYPE	4.00	Bad Request
6023	INVALID_ARGUMENTS	4.00	Bad Request
6024	INSUFFICIENT_ARGUMENTS	4.00	Bad Request
6025	MGMT_CONVERSION_ERROR	5.00	Internal Server Error
6026	MGMT_CANCELLATION_FAILED	5.00	Internal Server Error
6028	ALREADY_COMPLETE	4.00	Bad Request
6029	MGMT_COMMAND_NOT_CANCELLABLE	4.00	Bad Request
6030	EXTERNAL_OBJECT_NOT_REACHABLE_BEFORE_REQUEST_TIMEOUT	5.04	Gateway Timeout
6031	EXTERNAL_OBJECT_NOT_REACHABLE_BEFORE_OPERATION_TIMEOUT	5.04	Gateway Timeout

The Receiver decides the **Response Status Code** parameter using the combination of CoAP Response Code and oneM2M-RSC Option information.

6.3 Accessing Resources in CSEs

6.3.0 Introduction

This clause describes the behaviour of CoAP layer depending on *Response Type* parameter. Figure 6.3.0-1 illustrates the steps involved in each cases of interaction.

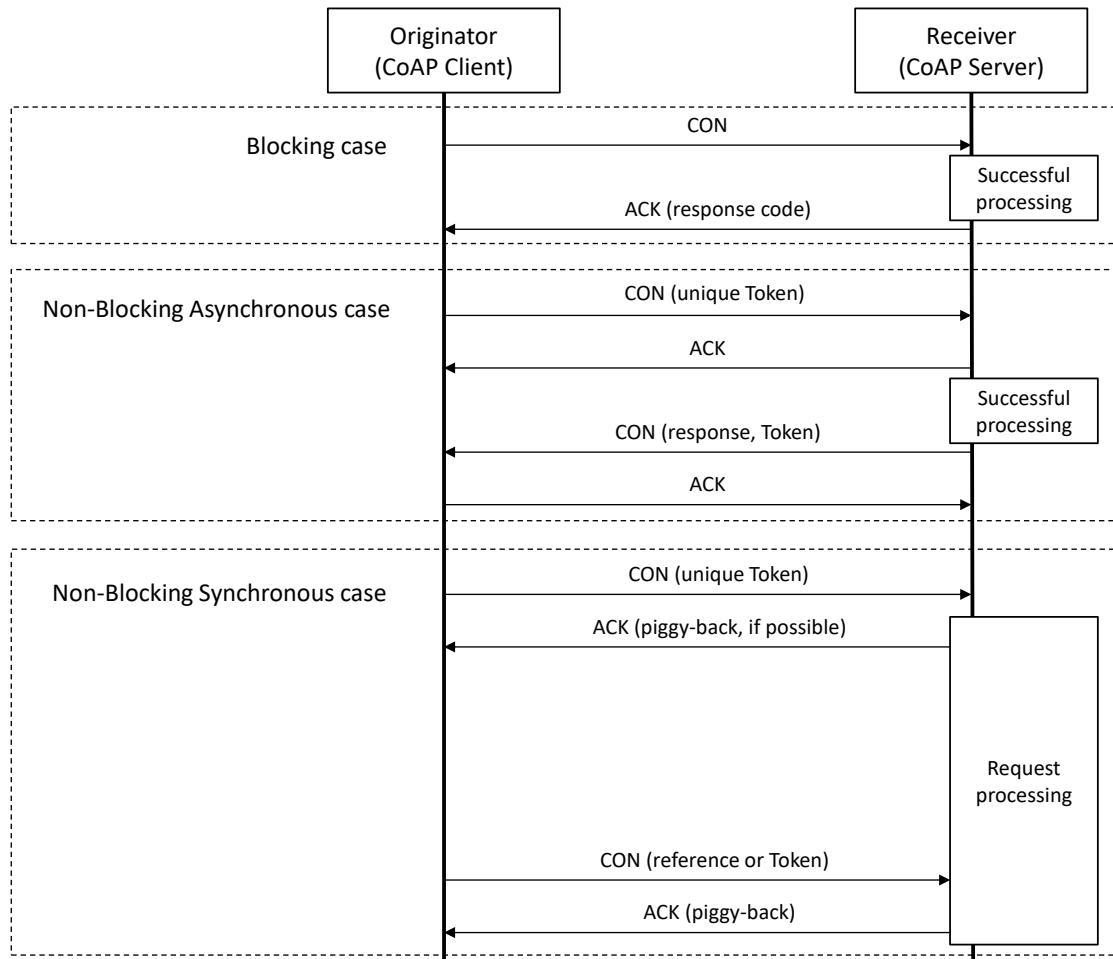


Figure 6.3.0-1: Accessing resource cases

6.3.1 Blocking case

- If *Response Type* parameter is configured as "blockingRequest" (blocking case), the Originator (CoAP client) shall use the Confirmable Method for the resource to the Receiver (CoAP server).
- In case of successful processing of the request at the Receiver, the Receiver shall piggyback the response with an appropriate response code in the Acknowledgment message that acknowledges the Confirmable request.

6.3.2 Non-Blocking Asynchronous case

- If *Response Type* parameter is configured as "nonBlockingRequestAsynch" (non-blocking asynchronous case), the Originator (CoAP client) shall use the Confirmable Method for the resource to the Receiver (CoAP server). Originator shall provide a unique Token value in the request.
- The Receiver shall provide an acknowledgment of receipt of the request using Acknowledgment message.
- The Receiver, upon successful processing of the request, shall send an appropriate response in a separate Confirmable message with the Token value. The Originator shall acknowledge the Confirmable response.

6.3.3 Non-Blocking Synchronous case

- If **Response Type** parameter is configured as "nonBlockingRequestSynch" (non-blocking synchronous case), the Originator (CoAP client) shall use the Confirmable Method for the resource to the Receiver (CoAP server). Originator shall provide a unique Token value in the request.
- The Receiver shall provide an acknowledgment of receipt of the request using Acknowledgment message. The response on the request may be piggy-backed in the Acknowledgement message if possible for the Receiver.
- The Receiver, after validating the request and before processing it fully, shall send an appropriate response including a reference in a separate Confirmable message. The Originator shall acknowledge the Confirmable response.
- The Originator can use the reference or the token to synchronously access or retrieve the resource. The Receiver, upon receipt of the request, shall respond with the current state of the resource.

NOTE: If the Receiver is a Transit CSE, the Receiver acts as CoAP client and CoAP server.

6.4 Mapping rules of caching

This clause specifies how to enable or disable CoAP caching mechanism and how to use cached information.

If the CoAP end point supports caching mechanism by freshness, the CoAP server shall:

- set the Max-Age Option value to "0" (zero) to disable caching, in order to support complete oneM2M mapping; or
- set the Max-Age option value to another value (such as the default value), in order to use CoAP caching mechanism for constrained environment.

NOTE 1: In the second case, the new request from oneM2M layer can get the stored fresh response from CoAP client, not from CoAP server.

If the CoAP end point supports caching mechanism by validity:

- the CoAP server shall not present Etag in responses to disable caching, in order to support complete oneM2M mapping; or
- the CoAP server shall present Etag in responses, in order to use CoAP caching mechanism for constrained environment.

NOTE 2: In the second case, the new request from oneM2M layer can get the stored fresh response from CoAP server, not from oneM2M layer.

6.5 Usage of Blockwise Transfers

Using Block Options, large oneM2M resource representations can be fragmented and reassembled by CoAP independently of the lower layers as well as the above application. The CoAP Block1 Option shall be used to define the size of the blocks used for oneM2M request primitives and the CoAP Block2 Option shall be used to define the size of the blocks used for oneM2M response responses. Refer to IETF RFC 7959 [3] for further details.

7 Security Consideration

This clause applies to CoAP unicast communication only. Security for multicast communication is addressed in clause B.1.

CoAP itself does not provide protocol primitives for authentication or authorization.

Just as HTTP is secured using Transport Layer Security (TLS) over TCP, CoAP can be secured using Datagram TLS (DTLS) [5].

All CoAP messages shall be sent as DTLS "application data". For matching an ACK or RST to a CON message or a RST to a NON message: The DTLS session shall be the same and the epoch shall be the same.

For matching a response to a request, the DTLS session shall be the same and the epoch shall be the same. The response to a DTLS secured request shall always be DTLS secured using the same security session and epoch.

OneM2M primitive parameters contained in CoAP messages may be protected by DTLS in a hop-by-hop manner. For the details, see oneM2M security solution specification [4].

Annex A (informative): Example Procedures

A.1 Blocking case of AE Registration

Figure A.1-1 illustrates CoAP mapping of AE Registration procedure described in clauses 7.2.2.1, 7.4.6.2.2 and E.1 of oneM2M TS-0004 [2] and shows an example of blocking case which is described in clause 6.3.1.

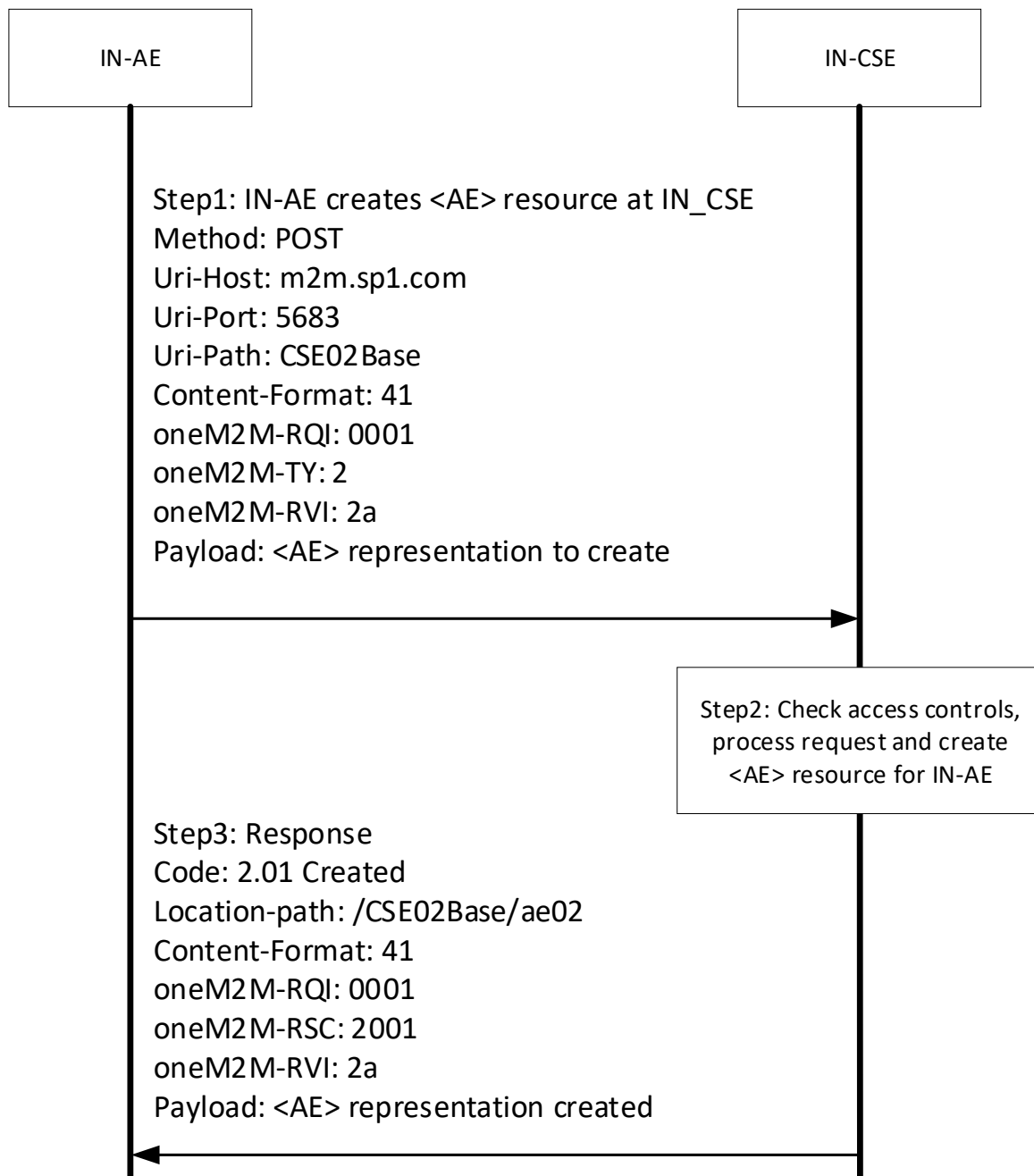


Figure A.1-1: Binding Example - Blocking case of AE Registration

A.2 Non-blocking synchronous case of AE Registration

Figure A.2-1 illustrates CoAP mapping of AE Registration procedure described in clauses 7.2.2.1, 7.4.6.2.2 and E.2 of oneM2M TS-0004 [2] and shows an example of non-blocking synchronous case which is described in clause 6.3.3.

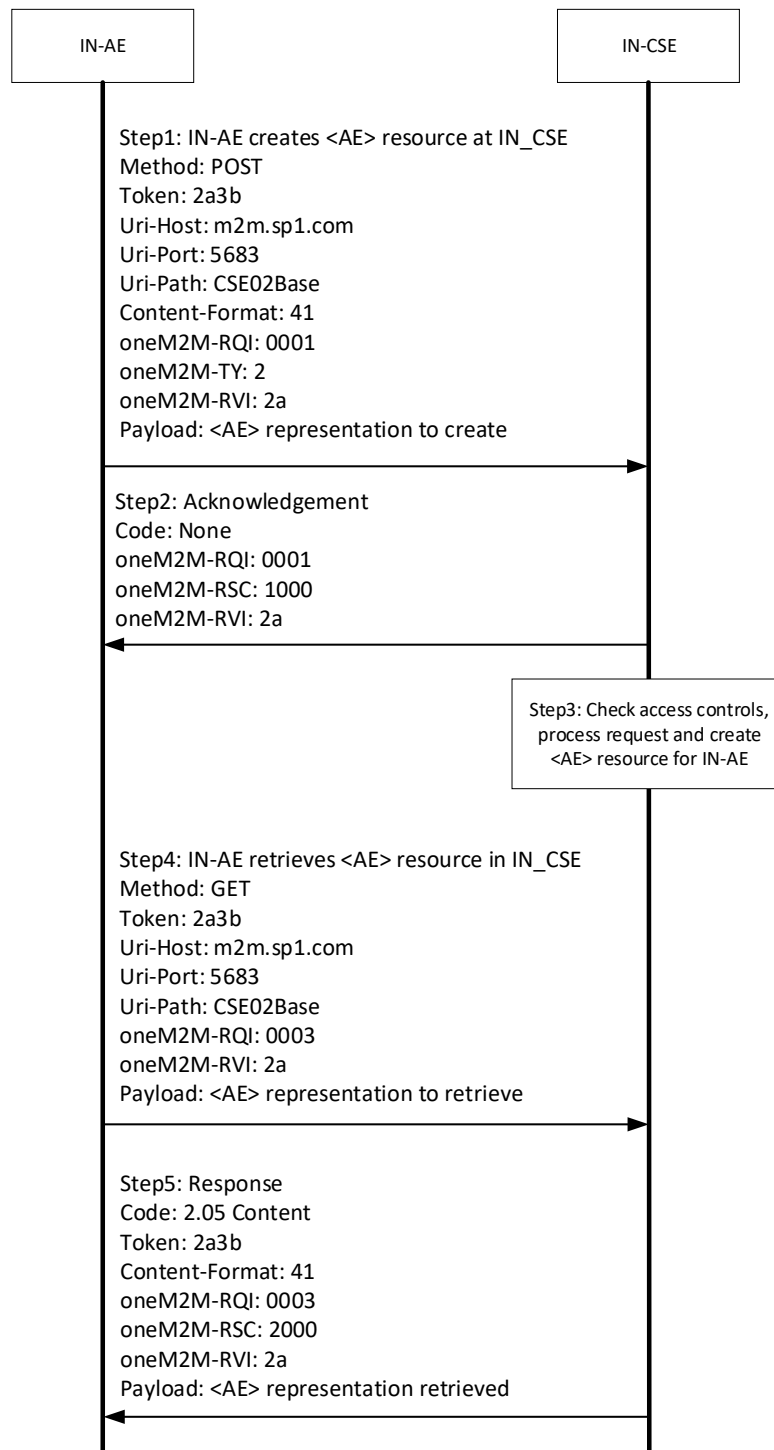


Figure A.2-1: Binding Example - Non-blocking synchronous case of AE Registration

Annex B (normative): Multicast group fan out procedure

B.0 Introduction

This clause describes the behaviour of CoAP layer for multicast group fan out procedure. Figure B.0-1 illustrates the steps involved in the interaction.

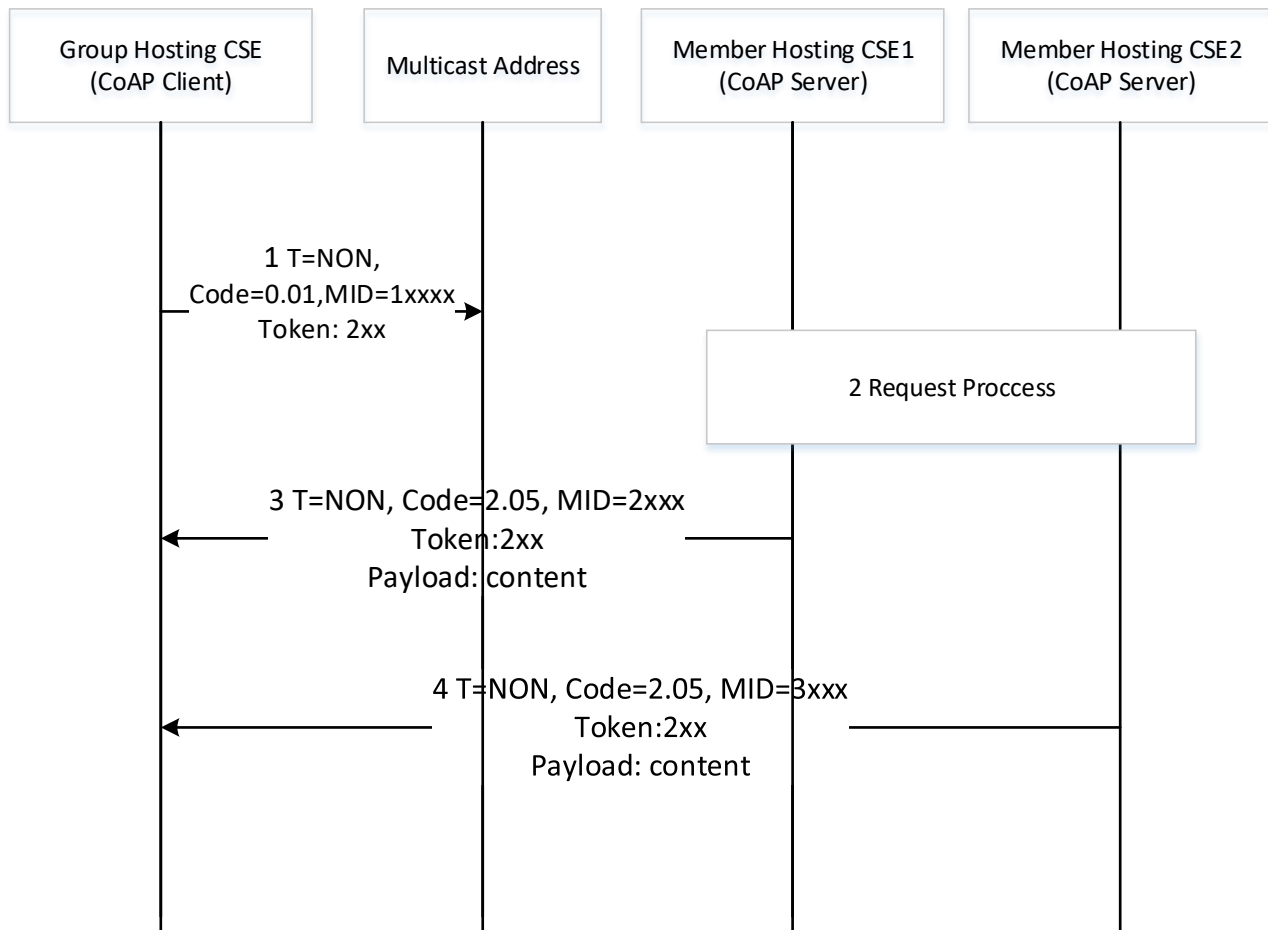


Figure B.0-1: Multicast group fan out procedure

- The Group Hosting CSE (CoAP client) shall use the Non-confirmable Method for the resource to the Member Hosting CSEs (CoAP server). The Group Hosting CSE shall provide a unique Token value in the request.
- The Member Hosting CSE, upon successful processing of the request, shall send an appropriate response in a separate Non-confirmable message with the same Token value.

B.1 Security

DTLS is not applicable to multicast group fan out messages. Security for multicast group fan out is addressed in clause 6.1.2.2.3 of oneM2M TS-0003 [4].

B.2 Caching

A GET request to a multicast group fan out shall not contain an ETag option.

History

Publication history		
V3.3.1	February 2019	Release 3 - Publication