I n t e r n a t i o n a l   T e l e c o m m u n i c a t i o n   U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4500.8

(03/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Frameworks, architectures and protocols

---

oneM2M – CoAP protocol binding

Recommendation ITU-T Y.4500.8

ITU-T

International
Telecommunication
Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	**Y.4400–Y.4549**
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4500.8

oneM2M – CoAP protocol binding

Summary

Recommendation ITU-T Y.4500.8 covers the protocol specific part of communication protocol used by oneM2M compliant systems as constrained application protocol (CoAP) bindings.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4500.8	2018-03-01	20	11.1002/1000/13503

Keywords

CoAP binding, oneM2M

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

NOTE – This Recommendation departs slightly from the usual editorial style of ITU-T Recommendations to preserve existing cross-referencing from external documents.

Table of Contents

Page

1 Scope ... 1

2 References ... 1

3 Definitions ... 1

3.1 Terms defined elsewhere ... 1

3.2 Terms defined in this Recommendation ... 2

4 Abbreviations and acronyms ... 2

5 Conventions ... 2

6 Overview ... 3

6.0 Introduction ... 3

6.1 Required features ... 3

6.2 Introduction of CoAP ... 3

7 CoAP message mapping ... 4

7.1 Introduction ... 4

7.2 Primitive mapping to CoAP message ... 5

7.3 Accessing resources in CSEs ... 11

7.4 Mapping rules of caching ... 13

7.5 Usage of blockwise transfers ... 13

8 Security consideration ... 13

Annex A – oneM2M specification update and maintenance control procedure ... 15

Appendix I – Example procedures ... 16

I.1 Blocking case of AE registration ... 16

I.2 Non-blocking synchronous case of AE registration ... 17

Bibliography ... 18

Recommendation ITU-T Y.4500.1

oneM2M – CoAP protocol binding

1 Scope

This Recommendation covers the protocol specific part of communication protocol used by oneM2M compliant systems as representational state transfer (REST) constrained application protocol (CoAP) 'RESTful CoAP bindings'.

The scope of this Recommendation is (but 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.

The Recommendation contains oneM2M Release 2 specification – oneM2M CoAP Protocol Binding V1.0.1 and is equivalent to standards of oneM2M partners including Association of Radio Industries and Businesses (ARIB), Alliance for Telecommunications Industry Solutions (ATIS) [b-ATIS.oneM2M], China Communications Standards Association (CCSA), European Telecommunications Standards Institute (ETSI) [b-ETSI TS 118 108], Telecommunications Industry Association (TIA) [b-TIA-5022.008], Telecommunications Standards Development Society India (TSDSI), Telecommunications Technology Association (TTA) [b-TTAT.MM-TS.0008] and Telecommunication Technology Committee (TTC) [b-TTC TS-M2M-0008].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.4500.1] Recommendation ITU-T Y.4500.1 (2018), *oneM2M – Functional architecture*.

[ITU-T Y.4500.4] Recommendation ITU-T Y. 4500.4 (2018), *Service layer core protocol*.

[ETSI TS 118 103] ETSI TS 118 103 V2.4.1 (2016), *oneM2M; Security solutions*.

[IETF RFC 6347] IETF RFC 6347 (2012), *Datagram Transport Layer Security Version 1.2*.

[IETF RFC 7252] IETF RFC 7252 (2014), *The Constrained Application Protocol (CoAP)*.

[IETF RFC 7959] IETF RFC 7959 (2016), *Block-Wise Transfers in the Constrained Application Protocol (CoAP).*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application entity (AE) [b-ITU-T Y.4500.11]: represents an instantiation of Application logic for end-to-end M2M solutions.

3.1.2 common services entity (CSE) [b-ITU-T Y.4500.11]: represents an instantiation of a set of Common Service Functions of the M2M environments. Such service functions are exposed to other entities through reference points.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACK	Acknowledgement
AE	Application Entity
CON	Confirmable
CSE	Common Services Entity
DTLS	Datagram Transport Layer Security
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
REST	Representational state transfer
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

5 Conventions

The keywords "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described.

Shall/Shall not:

Requirements

1) effect this Recommendation: This Recommendation needs to describe the required feature (i.e., specify a technical solution for the Requirement);
2) effect on products: every implementation (M2M Solution that complies to this Standard) must support it;
3) effect on deployments: every deployment (M2M Service based on this Standard) must use the Standardized feature where applicable – otherwise e.g., interoperability problems with other services could arise.

Should/Should not:

Recommendation

1) effect on this Recommendation: This Recommendation needs to describe a solution that allows the presence and the absence of the feature;

2) effect on products: an implementation may or may not support it, however support is recommended;

3) effect on deployments: a deployment may or may not use it, however usage is recommended.

May/Need not:

Permission/option

1) effect on this Recommendation: This Recommendation needs to describe a solution that allows the presence and the absence of the required feature;

2) effect on products: an implementation may or may not support it;

3) effect on deployments: A deployment may or may not use it.

6 Overview

6.0 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.

6.1 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].
- 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.
- A subset of response codes specified in clause 7.2.4 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.
- The token option may be used.
- Block-wise transfers feature may be supported to carry large payloads.
- Caching feature may be supported.

6.2 Introduction of CoAP

6.2.0 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.

6.2.1 Message format

This clause specifies details about the CoAP [IETF RFC 7252] message format:

- CoAP message occupies the data section of one user datagram protocol (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 type length value (TLV) format;
- CoAP options are followed by the payload part.

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

6.2.2 Caching

6.2.2.0 Introduction

CoAP [IETF RFC 7252] supports caching of responses to fulfil future equivalent requests to the same resource. Caching is supported using freshness and validity information carried with CoAP [IETF RFC 7252] responses.

6.2.2.1 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.

6.2.2.2 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.

6.2.3 Blockwise transfers

CoAP Block [IETF RFC 7959] 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.

7 CoAP message mapping

7.1 Introduction

When application entity (AE) or common services entity (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, a single oneM2M request primitive is mapped to a single CoAP request message, and a single oneM2M response primitive is mapped to a single CoAP response message. However, a single oneM2M request/response primitive is mapped to multiple CoAP request/response messages respectively when the 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 [ITU-T Y.4500.4] to a corresponding CoAP message field to compose a CoAP request/response message.

7.2 Primitive mapping to CoAP message

7.2.0 Introduction

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

7.2.1 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 7.3. 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 Table 7.2.1-1;
- 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 7.2.4;

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

Table 7.2.1-1 – oneM2M operation parameter mapping

oneM2M Operation Parameter	CoAP Method
CREATE	POST
RETRIEVE	GET
UPDATE	PUT
DELETE	DELETE
NOTIFY	POST

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.

7.2.2 Configuration of token and options

7.2.2.0 Introduction

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

7.2.2.1 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.

7.2.2.2 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);
- media types specified in clause 6.7 "oneM2M specific multipurpose Internet mail extensions (MIME) media types" of [ITU-T Y.4500.4].

Numeric values for oneM2M defined media types are listed in Table 7.2.2.2-1.

Table 7.2.2.2-1 – CoAP oneM2M specific content-formats

oneM2M Specific Media Type	ID
vnd.onem2m-res+xml	10000
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 Internet Assigned Numbers Authority (IANA) registration.	

7.2.2.3 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 7.2.2.3-1 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 7.2.2.3-1 – Mapping examples between To parameter and Uri-Path of the CoAP

<table>
<tr><th colspan="2" rowspan="2">Method</th><th colspan="3">Request Scope</th></tr>
<tr><th>CSE-Relative</th><th>SP-Relative</th><th>Absolute</th></tr>
<tr><td rowspan="8">Structured</td><td>To</td><td>CSEBase/ae12/cont27/contInst696</td><td>/CSE178/CSEBase/ae12/cont27/contInst696</td><td>//mym2msp.org/CSE178/CSEBase/ae12/cont27/contInst696</td></tr>
<tr><td rowspan="7">Uri-Path</td><td rowspan="4">CSEBase</td><td></td><td>_</td></tr>
<tr><td>~</td><td>mym2msp.org</td></tr>
<tr><td>CSE178</td><td>CSE178</td></tr>
<tr><td>CSEBase</td><td>CSEBase</td></tr>
<tr><td>ae12</td><td>ae12</td><td>ae12</td></tr>
<tr><td>cont27</td><td>cont27</td><td>cont27</td></tr>
<tr><td>contInst696</td><td>contInst696</td><td>contInst696</td></tr>
<tr><td rowspan="5">Unstructured</td><td>To</td><td>cin00856</td><td>/CSE178/cin00856</td><td>//mym2msp.org/CSE178/cin00856</td></tr>
<tr><td rowspan="4">Uri-Path</td><td rowspan="4">cin00856</td><td></td><td>_</td></tr>
<tr><td>~</td><td>mym2msp.org</td></tr>
<tr><td>CSE178</td><td>CSE178</td></tr>
<tr><td>cin00856</td><td>cin00856</td></tr>
<tr><td colspan="5">NOTE – How to read this table: To primitive – from left to right, Uri-Path – from top to bottom.</td></tr>
</table>

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*** and ***Local Token IDs*** parameters shall be carried in Uri-Query Option in a short name form as specified in clause 8.2.2 of [ITU-T Y.oneM2M.SLCP].

7.2.2.4 Definition of new options

7.2.2.4.0 Introduction

This clause describes new CoAP options used for binding several oneM2M request/response parameters. Table 7.2.2.4.0-1 contains definitions of the new CoAP options and sub-clauses specify oneM2M parameter mapping with the newly defined CoAP options in Table 7.2.2.4.0-1.

Table 7.2.2.4.0-1 – 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)

Table 7.2.2.4.0-1 – Definition of new options

No	C	U	N	R	Name	Format	Length	Default
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)
NOTE 1 – C, U, N, R means Critical, Unsafe, NoCacheKey and Repeatable respectively [IETF RFC 7252]. Table 7.2.2.4.0-1 follows the template used in section 5.10 Option Definitions of CoAP specification [IETF RFC 7252]. NOTE 2 – CoAP option numbers specified in Table 7.2.2.4.0-1 are subject to change after review by IANA registration.								

7.2.2.4.1 From

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

7.2.2.4.2 Request Identifier

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

7.2.2.4.3 Void

[This clause is intentionally left blank.]

7.2.2.4.4 Originating Timestamp

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

7.2.2.4.5 Request Expiration Timestamp

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

7.2.2.4.6 Result Expiration Timestamp

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

7.2.2.4.7 Operation Execution Time

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

7.2.2.4.8 notificationURI of Response Type

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

7.2.2.4.9 Event Category

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

7.2.2.4.10 Response Status Code

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

7.2.2.4.11 Group Request Identifier

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

7.2.2.4.12 Resource Type

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

7.2.2.4.13 Content Offset

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

7.2.2.4.14 Content Status

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

7.2.2.4.15 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 [ITU-T Y.4500.4].

7.2.3 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 7.5 for the detail information. If ***Content*** parameter contains URI and resource representation in a response to a create request, universal resource identifier (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

7.2.4 Response code mappings

Table 7.2.4-1 defines a mapping between oneM2M ***Response Status Code*** parameter specified in [ITU-T Y.4500.4] and CoAP response code.

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

Table 7.2.4-1 – Mapping between oneM2M Response Status Code and CoAP response code

oneM2M Response Status Code	Description	Status Code of CoAP	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
4004	NOT_FOUND	4.04	Not Found
4005	OPERATION_NOT_ALLOWED	4.05	Method Not Allowed
4008	REQUEST_TIMEOUT	4.04	Not Found
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
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
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_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

Table 7.2.4-1 – Mapping between oneM2M Response Status Code and CoAP response code

oneM2M Response Status Code	Description	Status Code of CoAP	Description
5212	SPARQL_UPDATE_ERROR	5.00	Internal Server Error
6003	EXTENAL_OBJECT_NOT_REACHABLE	4.04	Not Found
6005	EXTENAL_OBJECT_NOT_FOUND	4.04	Not Found
6010	MAX_NUMBERF_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_CANCELATION_FAILED	5.00	Internal Server Error
6028	ALREADY_COMPLETE	4.00	Bad Request
6029	MGMT_COMMAND_NOT_CANCELLABLE	4.00	Bad Request

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

7.3 Accessing resources in CSEs

7.3.0 Introduction

This clause describes the behaviour of CoAP layer depending on ***Response Type*** parameter. Figure 7.3.0-1 illustrates the steps involved in each cases of interaction. See Appendix I for example procedures.

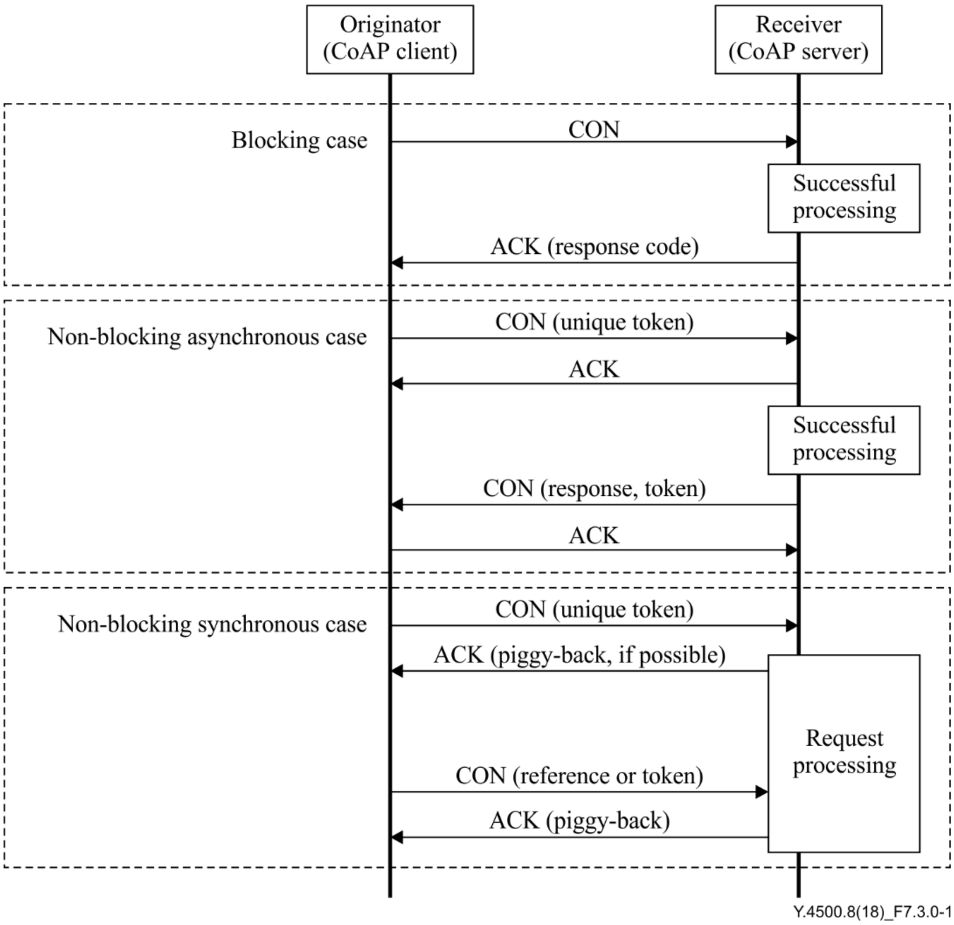

Figure 7.3.0-1 – Accessing resource cases

7.3.1 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.

7.3.2 Non-blocking qsynchronous 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.

7.3.3 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.

7.4 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.

7.5 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] for further details.

8 Security consideration

CoAP itself does not provide protocol primitives for authentication or authorization; where this is required, it shall be provided by datagram transport layer security (DTLS).

Just as hypertext transfer protocol (HTTP) is secured using transport layer security (TLS) over transmission control protocol (TCP), CoAP shall be secured using DTLS [IETF RFC 6347].

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 [ETSI TS 118 103].

NOTE – Some provisioning schemes of oneM2M TS-0003 [ETSI TS 118 103] enable the provisioning of end-to-end credentials, but protocols to establish security associations between non-adjacent nodes are not addressed.by oneM2M in the present release.

Annex A

oneM2M specification update and maintenance control procedure

(This annex forms an integral part of this Recommendation.)

The provisions of Annex L in [ITU-T Y.4500.1] as regards to oneM2M specification update and maintenance control procedure shall apply to this Recommendation.

Appendix I

Example procedures

(This appendix does not form an integral part of this Recommendation.)

I.1 Blocking case of AE registration

Figure I.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 [ITU-T Y.4500.4] and shows an example of blocking case which is described in clause 7.3.1.

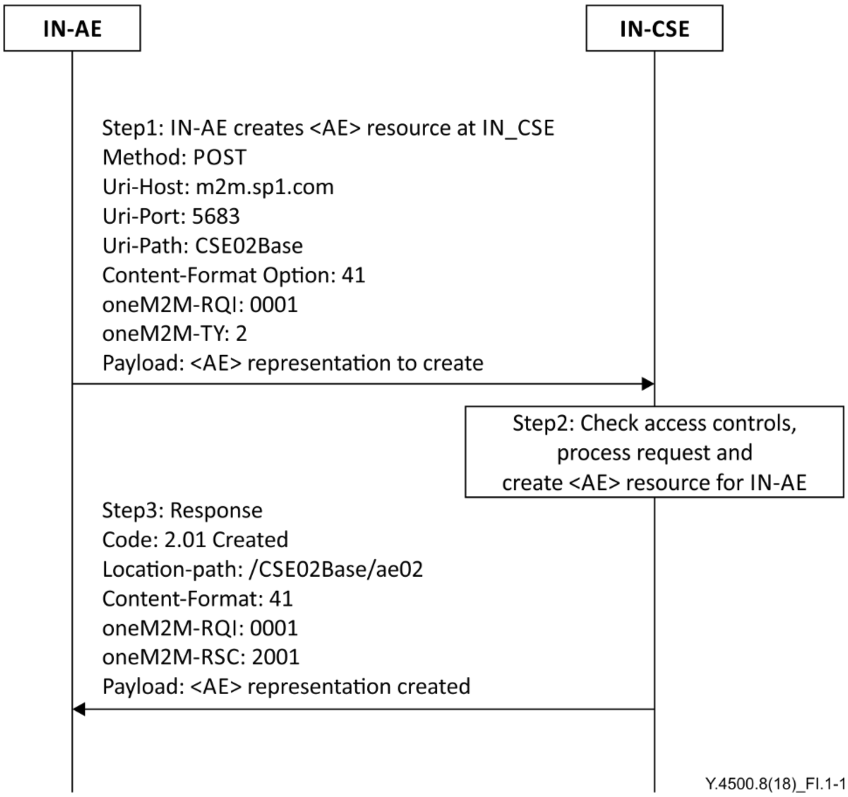

Figure I.1-1 – Binding example - blocking case of AE registration

I.2 Non-blocking synchronous case of AE registration

Figure I.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 [ITU-T Y.4500.4] and shows an example of non-blocking synchronous case which is described in clause 7.3.3.

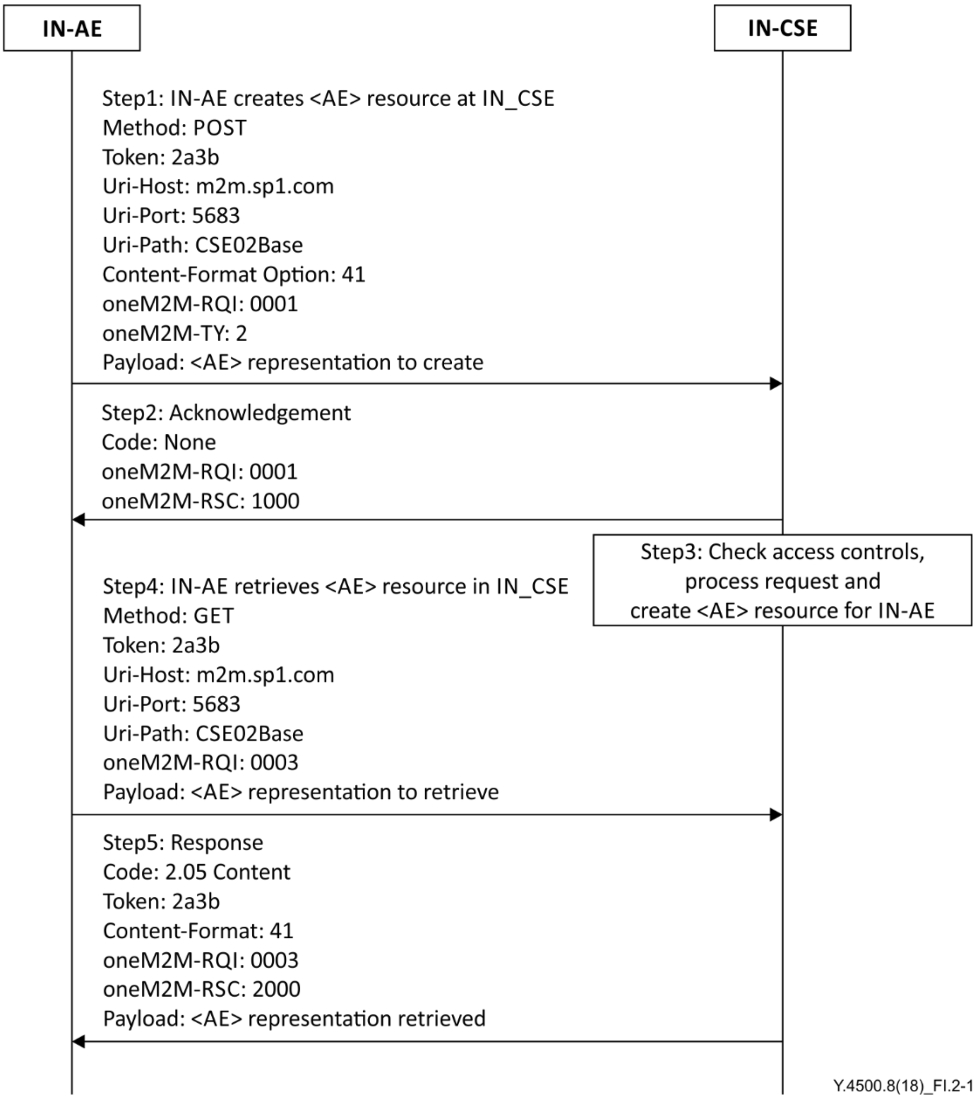

Figure I.2-1 – Binding example - non-blocking synchronous case of AE registration

Bibliography

[b-ITU-T Y.4500.11] Recommendation ITU-T Y.4500.11 (2018), *Common Terminology*.

[b-ATIS.oneM2M] Alliance for Telecommunications Industry Solutions, ATIS ONEM2M.TS0008V101-2015, *Coap Protocol Binding*.

[b-ETSI TS 118 108] European Telecommunications Standards Institute, ETSI TS 118 108 V1.0.1 (2016), *oneM2M; CoAP Protocol Binding (oneM2M TS-0008 version 1.3.2 Release 1)*.

[b-TIA-5022.008] Telecommunications Industry Association, TIA-5022.008 (2015), *CoAP Protocol Binding (oneM2M TS-0008-v1.0.1)*.

[b-TTAT.MM-TS.0008] Telecommunications Technology Association, TTAT.MM-TS.0008 v1.0.1 (2015), *oneM2M - CoAP Protocol Binding v1.0.1*.

[b-TTC TS-M2M-0008] Telecommunication Technology Committee, TTC TS-M2M-0008 v1.0.1 (2015), *oneM2M Technical Specification CoAP Protocol Binding*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018