ONEM2M
TECHNICAL SPECIFICATION

Document Number	TS-0009-V1.5.1
Document Name:	HTTP Protocol Binding
Date:	2016-February-29
Abstract:	HTTP Protocol Binding TS

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

Contents

2016 Scope

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

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

- Binding oneM2M Protocol primitive types to HTTP method.
- Binding oneM2M response status codes (successful/unsuccessful) to HTTP response codes.
- Binding oneM2M RESTful resources to HTTP resources.

The present document is depending on Core Protocol specification (oneM2M TS-0004) for data types.

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 reference document (including any amendments) applies.

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

[1] IETF RFC 7230 (June 2014): “Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing”.

[2] oneM2M TS-0003: Security Solutions.

[3] oneM2M TS-0004: “Service Layer Core Protocol Specification”.

[4] RFC7235: “Hypertext Transfer Protocol (HTTP/1.1): Authentication”, IETF, June 2014.

[5] RFC6750: “The Oauth 2.0 Authorization Framework: Bearer Token Usage”, October 2012.

[6] oneM2M TS-0011: Common Terminology.

[7] oneM2M TS-0001: Functional Architecture.

[8] IETF RFC 7232 (June 2014): “Hypertext Transfer Protocol (HTTP/1.1): “Conditional Requests”.

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 at http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf.

[i.2] IETF RFC 6455 (December 2011):”The WebSocket Protocol”.

3 Abbreviations

For the purposes of the present document, the following abbreviations and those given in TS-0011-Common Terminology [6] apply:

AE	Application Entity
CSE	Common Services Entity
CSE-ID	Common Service Entity Identifier
HTTP	Hyper Text Transfer Protocol
IN-CSE	Infrastructure Node – Common Services Entity
TLS	Transport Layer Security
MN-CSE	Middle Node – Common Services Entity
URI	Uniform Resource IdentifierXML eXtensible Markup Language

4 Conventions

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

5 Overview on HTTP Binding

5.1 Introduction

HTTP binding specifies the equivalence between oneM2M request and response primitives and HTTP request and response messages, respectively. This clause provides a brief overview on the mapping relationship between oneM2M and HTTP message parameters.

This clause describes how oneM2M request/response primitives can be mapped to HTTP request/response messages and vice versa.

Figure 5.1-1 illustrates an example oneM2M system configuration and its correspondence to an HTTP-based information system if HTTP binding as defined in the present document is applied. The upper diagram in Figure 5.1-1 shows with solid line arrows the flow of a request primitive originating from an AE which is registered to an MN-CSE (Registrar of AE). The request primitive is assumed to address a resource which is hosted by another MN-CSE (Host of Resource). Both MN-CSEs are registered to the same IN-CSE.

When applying HTTP binding, the oneM2M entities of the upper diagram take the roles outlined in the lower diagram of a corresponding HTTP information system as defined in [1]. The AE takes the role of an HTTP client, the MN-CSE (Registrar of AE) takes the role of a HTTP Proxy Server, and both the IN-CSE and MN-CSE (Host of Resource) take the role of a HTTP server for this particular request message.

CSEs may also issue unsolicited request messages, shown with dashed line arrows in Figure 5.1-1, and receive associated response messages. Therefore, for HTTP protocol binding, CSEs generally provides capability of both HTTP Server and HTTP Client. Aes may provide HTTP Server capability optionally in order to be able to serve Notification request messages (see TS-0004 [3] and TS-0001 [7]).

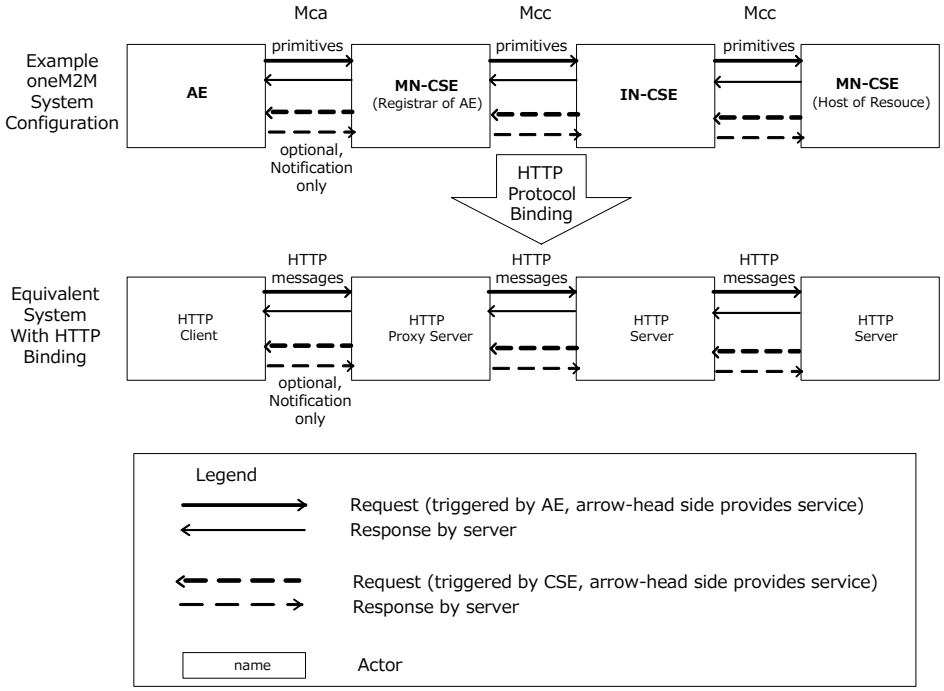

Figure 5.1-1 : Correspondence between oneM2M entities and HTTP Client and Server

Each individual request primitive will be mapped to single HTTP request message, and each individual response primitive will be mapped to a single HTTP response message, and vice-versa.

An HTTP request message consists of Request-Line, headers and message-body. An HTTP response message consists of Status-Line, headers and message-body [1]. HTTP header names are case-insensitive and a Receiver shall accept headers that are either lower or upper or any mixture thereof. This clause describes how oneM2M request/response primitives are mapped to HTTP messages at a high level. Corresponding details are specified in clause 6.

5.2 Request-Line

The HTTP method of a request message is mapped to the ***Operation*** parameter, and vice-versa.

At the message originator side the HTTP Request-Target is derived from the ***To*** parameter of the request primitive, including a query string which carries other specific primitive parameters.

HTTP-Version is specified in clause 6.

5.3 Status-Line

HTTP Version is specified in clause 6.

The Status-Code of HTTP response messages is derived from the ***Response Status Code*** parameter of the response primitive. The Reason-Phrase is not applicable to oneM2M systems and is omitted.

6 HTTP Message Mapping

6.1 Introduction

Mapping between oneM2M primitives and HTTP messages shall be applied in the following four use cases:

1. Mapping of request primitive to HTTP request message at the request originator (HTTP client)

2. Mapping of HTTP request message to request primitive at the request receiver (HTTP server)

3. Mapping of response primitive to HTTP response message at the request receiver (HTTP server)

4. Mapping of HTTP response message to response primitive at the request originator (HTTP client)

All four use cases also appear at transit CSEs.

The following clauses specify the mapping between each oneM2M primitive parameter and a corresponding HTTP message field to compose a HTTP request/response message.

6.2 Parameter Mappings on Request-Line

6.2.1 Method

The HTTP 'Method' shall be derived from the ***Operation*** request primitive parameter of the request primitive.

Table 6.2.1-1: HTTP Method Mapping

oneM2M Operation	HTTP Method
Create	POST
Retrieve	GET
Update	PUT
Delete	DELETE
Notify	POST

At the Receiver, an HTTP request message with POST method shall be mapped either to a Create or Notify ***Operation*** parameter. Discrimination between Create and Notify operations can be accomplished by inspection of the content-type header. The ***Resource Type*** parameter is present in the content-type header only when the HTTP POST request represents a Create request (see clause 6.4.3). The ***Resource Type*** parameter is not present in the content-type header when the HTTP POST request represents a Notify request.

6.2.2 Request-Target

6.2.2.1 Path component

The path component of the origin-form HTTP Request-Target shall be interpreted as the mapping of the resource identifier part of the ***To*** request primitive parameter. If the HTTP message is sent directly to the next hop CSE, the origin-form of Request-Target shall be employed (see clause 5.3.1 of [1]).

The resource identifier part of the ***To*** parameter can be represented in three different forms (see clause 6.2.3 [3] and clause 7.2 [7]):

- CSE-Relative-Resource-ID,
- SP-Relative-Resource-ID,
- Absolute-Resource-ID.

Each of the above three formats may include either a structured Resource ID (used for hierarchical addressing) or an unstructured Resource ID (used for non-hierarchical addressing) as defined in clause 7.2 [7].

For CSE-relative Resource ID representation, the path component of the HTTP request message shall be constructed as the concatenation of the literal "/" and the ***To*** request primitive parameter. For SP-relative Resource ID representation, the path component of the HTTP request message shall be constructed as the concatenation of the literal "/~" and the ***To*** request primitive parameter. For Absolute Resource ID representation, the path component of the HTTP request message shall be constructed by replacing the first "/" character of the ***To*** request primitive parameter with "/_".

The Table below shows valid mappings between the ***To*** request primitive parameter and the path component of the origin-form HTTP request target. In the shown examples, /myCSEID and /CSE178 represent applicable CSI-IDs,

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 6.2.2.1-1: Mapping examples between *To* parameter and path component of request-line

Resource-ID Type	*To* parameter value	path component (origin-form)
structured CSE-Relative	CSEBase/ae12/cont27/contInst696	/CSEBase/ae12/cont27/contInst696/
unstructured CSE-Relative	cin00856	/cin00856
structured SP-Relative	/CSE178/CSEBase/ae12/cont27/contInst696	/~/CSE178/CSEBase/ae12/cont27/contInst696
unstructured SP-Relative	/CSE178/cin00856	/~/CSE178/cin00856
structured Absolute	//mym2msp.org/CSE178/CSEBase/ ae12/cont27/contInst696	/_/mym2msp.org/CSE178/CSEBase/ ae12/cont27/contInst696
unstructured Absolute	//mym2msp.org/CSE178/cin00856	/_/mym2msp.org/CSE178/cin00856

At the HTTP server side, the reverse operations shall be applied to the path component of request-line to derive a replica of the original ***To*** request primitive parameter.

If the HTTP message is sent to a HTTP proxy instead directly to the next hop CSE, the absolute-form of Request-Target shall be employed (see clause 5.3.2 of [1]). The absolute-form is derived by prefixing the origin-form with the schema and the host address of the next hop CSE:

http://{host address of next hop CSE}{origin-form path-component}

6.2.2.2 Query component

The query component (e.g. query-string) may include the optional primitive parameters listed in Table 6.2.2-1 compliant with RFC 7230 [1]. Each applicable request primitive parameters and elements of ***Filter Criteria*** parameter shown in Table 6.2.2-1 shall be represented as pair of field-name and value in query-string. Multiple such pairs shall be concatenated with an ampersand '&' character used as separator between two pairs.

Table 6.2.2-1 also shows the permitted multiplicity of occurrence of field names in the query-string. Multiplicity '0..1' means that a parameter is optional and can occur at most once. Parameters with multiplicity '0..n', may occur multiple times in the query-string in the form of <query field name> = value. For example, if the resourceType element of the ***Filter Criteria*** parameter is represented by a list of 3 values '2 3 4' (see clause 6.3.4.7 in TS-0004 [3]), it would be mapped to ty=2+3+4 in the query-string. At the receiver side, this query string can be reverted back into the list type of representation. The same representation shall be applied for multiple occurrences of contentType and labels elements.

The 'attribute' element of the ***Filter Criteria*** request primitive parameter consists of two elements, name and value, which in XML notation would look for example as follows in case of multiplicity 2 (see clause 6.2.4.8 in TS-0004 [3]):

```
<attribute>
   <name>attname1</name>
   <value>attvalue1</value>
</attribute>
<attribute>
  <name>attname2</name>
  <value>attvalue2</value>
</attribute>
```

Each name (e.g. attname1 and attname2) shall represent a valid resource attribute name of the resource types indicated in the ty field of the query-string. The sequence of attribute elements as shown in the above example will be mapped into the query-string as attname1=attvalue1&attname2=attvalue2. The attribute names (i.e. attname1 and attname2 in

the above example) shall be expressed in the form of short names as defined in clause 8.2.3 of TS-0004 [3]. Note that the <attribute> tag of the XML representation is omitted in the HTTP binding.

Examples of valid Request-Target representations are the following:

Example 1): Request-Target for 'nonBlockingRequestSynch'

Primitive parameters: To: /CSE1234/RCSE78/container234 (SP-Relative-Resource-ID)

Response Type: responseType = 1 (nonBlockingRequestSynch)

Result Persistence: P1Y2M3DT10H1M0S Request-Target:
/CSE1234/RCSE78/container234?rt=1&rp=P1Y2M3DT10H1M0S

Example 2): Request-Target for Discovery

When the entity wants to discover container resources where the *creator* attribute has the value 'Sam':

Primitive parameters: To: /CSE1234/RCSE78

Filter Criteria: resourceType = 3 (container)

attribute name: creator

attribute value: Sam

filterUsage = discovery

Request-Target: /CSE1234/RCSE78?ty=3&cr=Sam&fu=1

Any of the short names listed in Table 6.2.2-1, with the exception of 'atr', may be used in the query-string. The short name 'atr' itself is not used. Instead, any of the resource attribute short names as listed in Tables 8.2.3-1 to 8.2.3-5 may be used in the query-string in representations of attname=attvalue expressions, except those that shall be omitted (see clause 7.2.3.16.9 in [3]).

Table 6.2.2-1: oneM2M request parameters mapped as query-string field

Request Primitive Parameter	Query Field Name	Multiplicity	Note
Response Type	***rt***	0..1	*responseType* element of data type ***responseTypeInfo*** (cf. clause 6.3.4.29 of TS-0004 [3])
Result Persistence	***rp***	0..1	
Result Content	***rc***	0..1	
Delivery Aggregation	***da***	0..1	
createdBefore	***crb***	0..1	filterCriteria condition
createdAfter	***cra***	0..1	filterCriteria condition
modifiedSince	***ms***	0..1	filterCriteria condition
unmodifiedSince	***us***	0..1	filterCriteria condition
stateTagSmaller	***sts***	0..1	filterCriteria condition
stateTagBigger	***stb***	0..1	filterCriteria condition
expireBefore	***exb***	0..1	filterCriteria condition
expireAfter	***exa***	0..1	filterCriteria condition
labels	***lbl***	0..n	filterCriteria condition
resourceType	***ty***	0..n	filterCriteria condition
sizeAbove	***sza***	0..1	filterCriteria condition
sizeBelow	***szb***	0..1	filterCriteria condition
contentType	***cty***	0..n	filterCriteria condition
limit	***lim***	0..1	filterCriteria condition
attribute	***atr***	0..n	filterCriteria condition
filterUsage	***fu***	0..1	filterCriteria condition
Discovery Result Type	***drt***	0..1	

For partial Retrieve request primitives, the ***To*** parameter may include the name of a single attribute separated by a '#' character from the resource ID. If multiple resource attributes are to be retrieved with a partial retrieve request

primitive, these attributes are included in form of an attributeList object (as specified in clause 6.3.4.9 of TS-0004 [] with empty values) in the ***Content*** parameter.

In both cases, the short resource attribute name(s) shall be included into the fragment component of request-target, i.e. it shall follow any required query-string separated by '#' character. If more than a single attribute name is included into the fragment component, these shall be separated by a '+' character.

For example, if three resource attributes with long names resourceID, labels and requestReachability are indicated in the ***Content*** primitive parameter, the query component atrl=ri+lbl+rr is attached to the request-target. In case just a single attribute "rr" is indicated in the ***To*** parameter separated by '#' character, the query component atrl=rr is attached to the request-target. The '#' character and following attribute name shall be omitted from the path component of the request line.

At the HTTP server side, the reverse operation shall take place, when constructing the retrieve request primitive from the receive HTTP request message. Single attribute names in the query component may either be mapped back into the ***To*** parameter following a '#' character, or included into the ***Content*** parameter using the attributeList format with just a single list element included. Multiple attributes shall be included into the ***Content*** parameter as specified in [3].

6.2.3 HTTP-Version

The present document defines binding compliant with HTTP 1.1 [1]. The HTTP version field in HTTP request messages shall be set to "HTTP/1.1".

6.3 Status-Line

6.3.1 HTTP-Version

The HTTP version field in HTTP response messages shall be set to "HTTP/1.1".

6.3.2 Status-Code

The ***Response Status Code*** parameter of response primitives shall be mapped to the HTTP Status-Code. Since the ***Response Status Code*** parameter values have been defined with more detailed information than HTTP status codes, one or more ***Response Status Code*** value may be mapped to the same HTTP Status-Code. The original ***Response Status Code*** parameter value shall be carried in the X-M2M-RSC header(see clause 6.4.14).

The mapping of ***Response Status Code*** parameter value of oneM2M request primitive to Status-Code of HTTP request messages is specified in Table 6.3.2-1.

Table 6.3.2-1: Status Code Mapping

oneM2M Response Status Codes	HTTP Status Codes
1000 (ACCEPTED)	202 (Accepted)
2000 (OK)	200 (OK)
2001 (CREATED)	201 (Created)
4000 (BAD_REQUEST)	400 (Bad Request)
4004 (NOT_FOUND)	404 (Not Found)
4005 (OPERATION_NOT_ALLOWED)	405 (Method Not Allowed)
4008 (REQUEST_TIMEOUT)	408 (Request Timeout)
4101 (SUBSCRIPTION_CREATOR_HAS_NO_PRIVILEGE)	403 (Forbidden)
4102 (CONTENTS_UNACCEPTABLE)	400 (Bad Request)
4103 (ACCESS_DENIED)	403 (Forbidden)
4104 (GROUP_REQUEST_IDENTIFIER_EXISTS)	409 (Conflict)
4105 (CONFLICT)	409 (Conflict)
5000 (INTERNAL_SERVER_ERROR)	500 (Internal Server Error)
5001 (NOT_IMPLEMENTED)	501 (Not Implemented)
5103 (TARGET_NOT_REACHABLE)	404 (Not Found)
5105 (NO_PRIVILEGE)	403 (Forbidden)
5106 (ALREADY_EXISTS)	403 (Forbidden)
5203 (TARGET_NOT_SUBSCRIBABLE)	403 (Forbidden)
5204 (SUBSCRIPTION_VERIFICATION_INITIATION_FAILED)	500 (Internal Server Error)
5205 (SUBSCRIPTION_HOST_HAS_NO_PRIVILEGE)	403 (Forbidden)
5206 (NON_BLOCKING_REQUEST_NOT_SUPPORTED)	501 (Not Implemented)
5207 (NOT_ACCEPTABLE)	406 (Not Acceptable)
6003 (EXTERNAL_OBJECT_NOT_REACHABLE)	404 (Not Found)
6005 (EXTERNAL_OBJECT_NOT_FOUND)	404 (Not Found)
6010 (MAX_NUMBER_OF_MEMBER_EXCEEDED)	400 (Bad Request)
6011 (MEMBER_TYPE_INCONSISTENT)	400 (Bad Request)
6020 (MANAGEMENT_SESSION_CANNOT_BE_ESTABLISHED)	500 (Internal Server Error)
6021 (MANAGEMENT_SESSION_ESTABLISHMENT_TIMEOUT)	500 (Internal Server Error)
6022 (INVALID_CMDTYPE)	400 (Bad Request)
6023 (INVALID_ARGUMENTS)	400 (Bad Request)
6024 (INSUFFICIENT_ARGUMENT)	400 (Bad Request)
6025 (MGMT_CONVERSION_ERROR)	500 (Internal Server Error)
6026 (CANCELLATION_FAILED)	500 (Internal Server Error)
6028 (ALREADY_COMPLETE)	400 (Bad Request)
6029 (COMMAND_NOT_CANCELLABLE)	400 (Bad Request)

6.3.3 Reason-Phrase

The Reason-Phrase shall be omitted in HTTP response messages.

6.4 Header Fields

6.4.0 Introduction

The header fields listed in this clause shall be supported by all entities of the oneM2M system when using HTTP binding. Any other unrecognized HTTP headers shall be ignored by the HTTP client and server.

6.4.1 Host

The Host header shall be present in each HTTP request message.

While the Request-Target indicates a target resource on the Hosting CSE, the Host header indicates the FQDN or IP address of the Receiver CSE of the next hop in multi-hop communication scenarios. Therefore, the Request-Target is not changed but the Host header is changed each time when a request is forwarded to the next hop CSE.

When no HTTP proxy is used, the Host header shall be set as one of the pointOfAccess attribute values of the Receiver(i.e. pointOfAccess attribute of the corresponding <remoteCSE> resource). Selection of the appropriate

Receiver is described in oneM2M TS-0004 [3]. In this case the origin-form of target URI shall be used (see clause 6.2.2).

If the HTTP request message is sent to a HTTP proxy rather than to the next hop CSE, the Host header shall be set to the FQDN or IP address of the proxy. In this case the absolute-form of target URI shall be used (see clause 6.2.2).

6.4.2 Accept

The Originator may use the Accept header to indicate which media types are acceptable for the response. The Accept header shall be mapped to a set of media types among “application/xml”, “application/json”, or the oneM2M defined media types defined in clause 6.7 of [3]. Note that some of the oneM2M defined media types defined in clause 6.7 of [3] are not applicable for the response. Note that this information is not included in a request primitive.

6.4.3 Content-Type

Any HTTP request or response containing message-body shall include the Content-type header set to one of “application/xml”, “application/json”, or the oneM2M defined media types defined in clause 6.7 of [3]..

Content-Type of the HTTP response should be chosen by the Hosting CSE considering the Accept header given in the HTTP request.

The value of the Resource Type primitive parameter, which is present in Create request primitives only, shall be appended to the Content-type of the corresponding HTTP request message in the form ty=value, separated by a semicolon character. A valid Content-Type header in this case looks e.g. as follows:

Content-Type: application/vnd.onem2m-res+xml; ty=3

6.4.4 Content-Location

The Content-Location header of HTTP response messages shall be set to the URI of the created resource, when responding to a Create request primitive. The URI shall be retrieved from the ***Content*** parameter of the response primitive. See clause 7.2.3.11 “Create a success response” in [3].

6.4.5 Content-Length

If message-body is included into HTTP request or response messages, the Content-Length header shall be included indicating the length of the message-body in octets (8-bit bytes).

6.4.6 Etag

A response primitive sent in reply to a resource retrieval request primitive should include an Etag header [8] in combination with the resource representation in the HTTP message body.

Etag facilitates the use of conditional requests (i.e. using the if-match and if-none-match HTTP headers) [8].

If a CSE supports the Etag header, then the CSE shall support conditional requests compliant with [8].

6.4.7 X-M2M-Origin

The X-M2M-Origin header shall be mapped to the ***From*** parameter of request and response primitives and vice versa, if applicable.

The X-M2M-Origin header value shall be assigned by the Originator of the request (e.g. AE or CSE).

6.4.8 X-M2M-RI

The X-M2M-RI header shall be mapped to the ***Request Identifier*** parameter of request and response primitives and vice versa.

6.4.9 Void

6.4.10 X-M2M-GID

The X-M2M-GID header shall be mapped to the ***Group Request Identifier*** parameter of request primitives and vice versa, if applicable.

6.4.11 X-M2M-RTU

The X-M2M-RTU header shall be mapped to the *notificationURI* element of the ***Response Type*** parameter of request primitives and vice versa, if applicable. If there are more than one value in the element, then the values shall be combined with "&" character.

6.4.12 X-M2M-OT

The X-M2M-OT header shall be mapped to the ***Originating Timestamp*** parameter of request and response primitives, and vice versa, if applicable.

6.4.13 X-M2M-RST

The X-M2M-RST header shall be mapped to the ***Result Expiration Timestamp*** parameter of request and response primitives, and vice versa, if applicable.

6.4.14 X-M2M-RET

The X-M2M-RET header shall be mapped to the ***Request Expiration Timestamp*** parameter of request primitives and vice versa, if applicable.

6.4.15 X-M2M-OET

The X-M2M-OET header shall be mapped to the ***Operation Execution Time*** parameter of request primitives and vice versa, if applicable.

6.4.16 X-M2M-EC

The X-M2M-EC header shall be mapped to the ***Event Category*** parameter of request and response primitives, and vice versa, if applicable.

6.4.17 X-M2M-RSC

The X-M2M-RSC header in a HTTP response message shall be mapped to the ***Response Status Code*** parameter of response primitives and vice versa.

6.5 Message-body

Message-body shall be mapped to the ***Content*** parameter of request and response primitives, and vice versa, if applicable. This applies to the ***Content*** parameter of all primitives, except for partial Retrieve request primitives. Attributes contained in a Retrieve request primitive shall be mapped to the fragment component of request-target, as specified in clause 6.2.2.3, and vice versa.

6.6 Message Routing

HTTP request and response message routing shall be performed as described in HTTP/1.1 [1].

7 Security Consideration

7.1 Authentication on HTTP Request Message

When sending the credential to be checked by the Registrar CSE, Proxy-Authorization header should be used as specified in HTTP/1.1 (see [4]).

When sending the credential to be checked by Hosting CSE, Authorization header should be used as specified in HTTP/1.1 [4].

When the credential to be checked by Hosting CSE is an Access Token which is compatible with Oauth 2.0 framework (see [5]), the Bearer authentication scheme shall be used as specified in Oauth 2.0 framework.

NOTE: The oneM2M Security Solutions [2] does not provide any details on usage or provisioning of the token.

7.2 Transport Layer Security

oneM2M primitive parameters contained in HTTP messages may be protected by TLS in a hop-by-hop manner. For the details, see the oneM2M Security Solutions specification [2]

NOTE: Some provisioning schemes of oneM2M TS-0003 [2] 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 (informative): Example Procedures

A.1 <container> resource creation

Figure A.1-1 is HTTP mapping of procedure described in clause 7.4.7.2.1 [3]. Note the example shown in the figure applies under the following assumptions:

- "CSE1" is the name (i.e. value of the resourceName attribute) of the <CSEBase> resource of the registrar CSE
- "cont1" is the name of the created <container> resource chosen by the registrar CSE

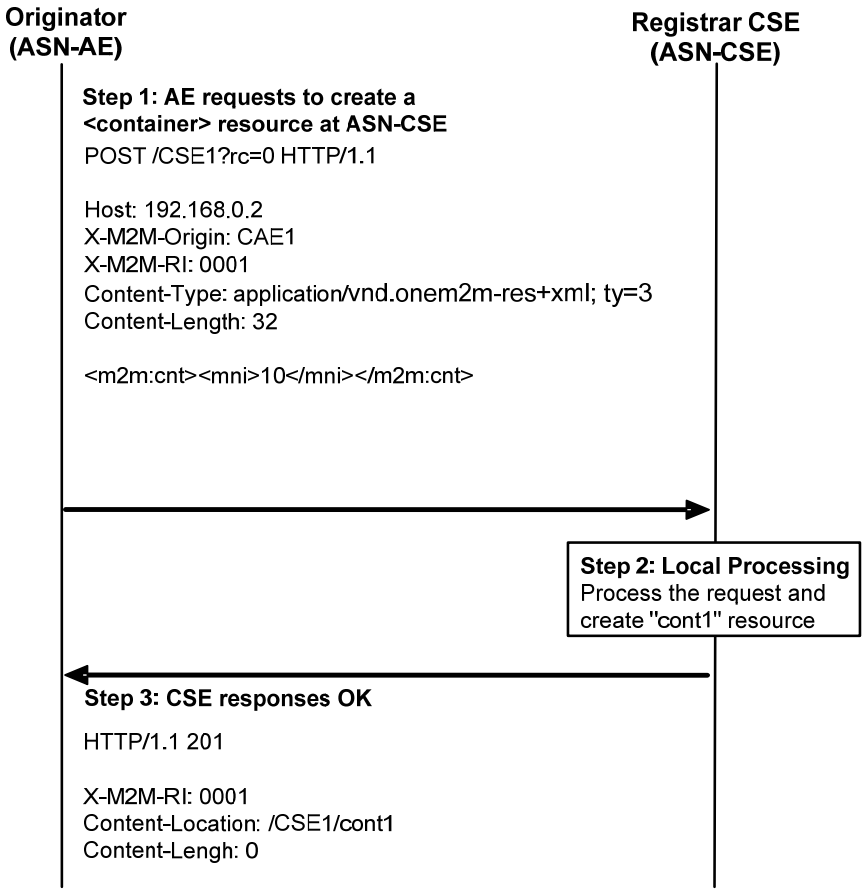

Figure A.1-1: oneM2M HTTP Binding Example – container creation

Annex B (informative): WebSocket

B.1 Notification using WebSocket

WebSocket [i.4] can be used for transporting notifications to an AE/CSE. This can be useful for an AE/CSE which is not server-capable or cannot be reachable for delivery of unsolicited requests.

For example, when an AE needs to receive a notification message from the CSE, the AE establishes a WebSocket connection to a CSE. When a new notification message is generated, the notification will be sent to the AE as the data frame of the WebSocket.

History

Publication history		
V1.0.1	30 Jan 2015	Release 1 – Publication
V1.5.1	29 Feb 2016	Updated Release 1 - Publication