oneM2M Technical Specification
HTTP Protocol Binding

2015 年 3 月 16 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE
＜参考＞ [Remarks]

1. 英文記述の適用レベル [Application level of English description]
   適用レベル [Application level]：E2
   本標準の本文、付属資料および付録の文章および図に英文記述を含んでいる。[English description is included in the text and figures of main body, annexes and appendices.]

2. 国際勧告等の関連 [Relationship with international recommendations and standards]
   本標準は、oneM2Mで承認されたTechnical Specification 0009V1.0.1に準拠している。[This standard is standardized based on the Technical Specification 0009V1.0.1 approved by oneM2M.]

3. 上記国際勧告等に対する追加項目等 [Departures from international recommendations]
   原標準に対する変更項目 [Changes to original standard]
   原標準が参照する標準のうち、TTC標準に置き換える項目。[Standards referred to in the original standard, which are replaced by TTC standards.]
   原標準が参照する標準のうち、それらに準拠したTTC標準等が制定されている場合は自動的に最新版TTC標準等に置き換え参照するものとする。 [Standards referred to in the original standard should be replaced by derived TTC standards.]

4. 工業所有権 [IPR]
   本標準に関わる「工業所有権等の実施の権利に係る確認書」の提出状況は、TTCホームページによる。[Status of “Confirmation of IPR Licensing Condition” submitted is provided in the TTC web site.]

5. 作成専門委員会 [Working Group]
   oneM2M専門委員会 [oneM2M Working Group]
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.

© 2015, oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, 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 .............................................................................................................................................. 4  
2 References ......................................................................................................................................... 4  
  2.1 Normative references ..................................................................................................................... 4  
  2.2 Informative references .................................................................................................................... 4  
3 Abbreviations ................................................................................................................................. 5  
4 Conventions ...................................................................................................................................... 5  
5 Overview of HTTP Binding .............................................................................................................. 5  
  5.1 Introduction .................................................................................................................................. 5  
  5.2 Request-Line ................................................................................................................................. 6  
  5.3 Status-Line .................................................................................................................................... 6  
6 HTTP Message Mapping .................................................................................................................... 6  
  6.1 Introduction .................................................................................................................................. 6  
  6.2 Parameter Mappings on Request-Line .......................................................................................... 6  
    6.2.1 Method ................................................................................................................................... 6  
    6.2.2 Request-Target ........................................................................................................................ 6  
    6.2.3 HTTP-Version .......................................................................................................................... 7  
  6.3 Status-Line .................................................................................................................................... 7  
  6.3.1 HTTP-Version .......................................................................................................................... 7  
  6.3.2 Status-Code ............................................................................................................................. 7  
  6.3.3 Reason-Phrase .......................................................................................................................... 8  
6.4 Header Fields .................................................................................................................................. 8  
  6.4.1 Host .......................................................................................................................................... 8  
  6.4.2 Accept ...................................................................................................................................... 9  
  6.4.3 Content-type ............................................................................................................................. 9  
  6.4.4 Content-Location ....................................................................................................................... 9  
  6.4.5 Content-Length ........................................................................................................................ 9  
  6.4.6 Etag .......................................................................................................................................... 9  
  6.4.8 X-M2M-RI ................................................................................................................................. 9  
  6.4.12 X-M2M-OT .......................................................... 10  
  6.4.13 X-M2M-RST .................................................... 10  
  6.4.16 X-M2M-EC ........................................................... 10  
  6.4.17 X-M2M-RSC ................................................... 10  
  6.5 Message-body ............................................................................................................................ 10  
    6.6 Message Routing .......................................................................................................................... 10  
7 Security Consideration .................................................................................................................... 10  
  7.1 Authentication on HTTP Request Message .................................................................................. 10  
  7.2 Transport Layer Security ............................................................................................................. 10  
Annex A (informative): Example Procedures ....................................................................................... 11  
  A.1 <container> resource creation .................................................................................................. 11  
Annex B (informative): WebSocket ...................................................................................................... 12  
  B.1 Notification using WebSocket .................................................................................................... 12  
History .................................................................................................................................................. 13
1 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.


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://member.onem2m.org/Static_pages/Others/Rules_Pages/oneM2M-Drafting-Rules-V1_0.doc.

[i.2] IETF RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication”.

[i.3] IETF RFC 6750 (October 2012): "The OAuth 2.0 Authorization Framework: Bearer Token Usage”.

3 Abbreviations

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

- **CSE-ID**: Common Service Entity Identifier
- **HTTP**: Hyper Text Transfer Protocol
- **TLS**: Transport Layer Security
- **URI**: Uniform Resource Identifier

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 of HTTP Binding

This clause describes what oneM2M primitive parameters can be mapped to HTTP request/response messages.

5.1 Introduction

The present document assumes AE has the capability of HTTP Client, and CSE has the capability of both HTTP Client and Server.

![Diagram showing mapping AE/CSE to HTTP Client and Server](image)

**Figure 5.1-1 : Example of Mapping AE/CSE to HTTP Client and Server**

Single request primitive will be mapped to single HTTP request message, and single response primitive will be mapped to single HTTP response message.

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]. This clause describes how oneM2M request/response primitives are mapped to HTTP messages at a high level. Corresponding details of each sub-clause are specified in clause 6.

The Registrar CSE shall behave as 'proxy server'(see [1]).
5.2 Request-Line

Method is mapped to the oneM2M Operation parameter.

Request-URI is derived from the oneM2M To parameter, including a query string which carries specific primitive parameters.

HTTP-Version is specified in clause 6.

5.3 Status-Line

HTTP Version is specified in clause 6.

Status-Code and Reason-Phrase are derived from the oneM2M Response Status Code parameter of the response primitive.

6 HTTP Message Mapping

6.1 Introduction

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

- when the Originator sends a request primitive;
- when the Receiver receives a request primitive;
- when the Receiver sends a response primitive;
- when the Originator receives a response primitive.

The following clauses specify how to map each oneM2M primitive parameter to 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 specified according to the oneM2M Operation parameter of the request primitive.

<table>
<thead>
<tr>
<th>oneM2M Operation</th>
<th>HTTP Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>POST</td>
</tr>
<tr>
<td>Retrieve</td>
<td>GET</td>
</tr>
<tr>
<td>Update</td>
<td>PUT (full update) or POST (partial update)</td>
</tr>
<tr>
<td>Delete</td>
<td>DELETE</td>
</tr>
<tr>
<td>Notify</td>
<td>POST</td>
</tr>
</tbody>
</table>

At the Receiver, an HTTP request message with POST method shall be mapped to a oneM2M Create or Notify request primitive in accordance with the value of the Operation parameter.

6.2.2 Request-Target

The path component of HTTP Request-Target shall be interpreted as the mapping of To parameter, and the query component (e.g. query-string) shall be interpreted as other primitive parameters (see [1]).
The **To** parameter shall be mapped to in Request-Target. Only SP-Relative-Resource-ID and Absolute-Resource-ID forms (see clause 7.2 [7]) shall be applicable for **To** parameter.

If **To** parameter is SP-Relative-Resource-ID form, then ‘origin-form’ shall be used for Request-Target. If **To** parameter is Absolute-Resource-ID form, then ‘absolute-form’ shall be used for Request-Target (see clause 6.2.3 [3]).

The prefix string "http:" shall be added to the ‘absolute-form’ when the address is used in the ‘absolute-form’ in the Request-Target.

The request parameters which are not specified as oneM2M extension headers in clause 6.4 shall be specified as pair of field-name and value in query-string as shown in table 6.2.2-1.

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

<table>
<thead>
<tr>
<th>Request Parameter</th>
<th>Field Name</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result Type</td>
<td>rt</td>
<td>responseType element of the responseType parameter</td>
</tr>
<tr>
<td>Delivery Aggregation</td>
<td>da</td>
<td></td>
</tr>
<tr>
<td>createdBefore</td>
<td>crb</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>modifiedSince</td>
<td>ms</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>unmodifiedSince</td>
<td>us</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>stateTagSmaller</td>
<td>sts</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>stateTagBigger</td>
<td>stb</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>expireBefore</td>
<td>exb</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>expireAfter</td>
<td>exa</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>labels</td>
<td>lbl</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>resourceType</td>
<td>rty</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>sizeAbove</td>
<td>sza</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>sizeBelow</td>
<td>szb</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>contentType</td>
<td>cty</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>limit</td>
<td>lim</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>attribute</td>
<td>atr</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>filterUsage</td>
<td>fu</td>
<td>filterCriteria condition</td>
</tr>
<tr>
<td>Discovery Result Type</td>
<td>drt</td>
<td></td>
</tr>
</tbody>
</table>

#### 6.2.3 HTTP-Version

The present document supports binding to HTTP 1.1 [1], so the version field shall be set to “HTTP/1.1”.

#### 6.3 Status-Line

**6.3.1 HTTP-Version**

The present document supports binding to HTTP 1.1 [1], so the version field shall be set to “HTTP/1.1”.

**6.3.2 Status-Code**

The **Response Status Code** parameter shall be mapped to HTTP Status-Code. Since the **Response Status Code** parameter have been defined more specifically than HTTP status codes, one or more **Response Status Code** may be mapped to one Status-Code. The original **Response Status Code** parameter shall be carried in X-M2M-RSC (see clause 6.4.14).

N:1 status code mapping from the oneM2M request primitive to HTTP request message shall be:
Table 6.3.2-1: Status Code Mapping

<table>
<thead>
<tr>
<th>oneM2M Response Status Codes</th>
<th>HTTP Status Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 (ACCEPTED)</td>
<td>202 (Accepted)</td>
</tr>
<tr>
<td>2001 (CREATED)</td>
<td>201 (Created)</td>
</tr>
<tr>
<td>2101 (?) (CONFLICT)</td>
<td>409 (Conflict)</td>
</tr>
<tr>
<td>4000 (BAD_REQUEST)</td>
<td>400 (Bad Request)</td>
</tr>
<tr>
<td>4004 (NOT_FOUND)</td>
<td>404 (Not Found)</td>
</tr>
<tr>
<td>4005 (OPERATION_NOT_ALLOWED)</td>
<td>405 (Method Not Allowed)</td>
</tr>
<tr>
<td>4008 (REQUEST_TIMEOUT)</td>
<td>408 (Request Timeout)</td>
</tr>
<tr>
<td>4101 (SUBSCRIPTION_CREATOR_HAS_NO_PRIVILEGE)</td>
<td>403 (Forbidden)</td>
</tr>
<tr>
<td>4102 (CONTENTS_UNACCEPTABLE)</td>
<td>400 (Bad Request)</td>
</tr>
<tr>
<td>4103 (ACCESS_DENIED)</td>
<td>403 (Forbidden)</td>
</tr>
<tr>
<td>4104 (GROUP_REQUEST_IDENTIFIER_EXISTS)</td>
<td>409 (Conflict)</td>
</tr>
<tr>
<td>5000 (INTERNAL_SERVER_ERROR)</td>
<td>500 (Internal Server Error)</td>
</tr>
<tr>
<td>5001 (NOT_IMPLEMENTED)</td>
<td>501 (Not Implemented)</td>
</tr>
<tr>
<td>5103 (TARGET_NOT_REACHABLE)</td>
<td>404 (Not Found)</td>
</tr>
<tr>
<td>5105 (NO_PRIVILEGE)</td>
<td>403 (Forbidden)</td>
</tr>
<tr>
<td>5106 (ALREADY_EXISTS)</td>
<td>403 (Forbidden)</td>
</tr>
<tr>
<td>5203 (TARGET_NOT_SUBSCRIBABLE)</td>
<td>403 (Forbidden)</td>
</tr>
<tr>
<td>5204 (SUBSCRIPTION_VERIFICATION_INITIATION_FAILED)</td>
<td>500 (Internal Server Error)</td>
</tr>
<tr>
<td>5205 (SUBSCRIPTION_HOST_HAS_NO_PRIVILEGE)</td>
<td>403 (Forbidden)</td>
</tr>
<tr>
<td>5206 (NON_BLOCKING_REQUEST_NOT_SUPPORTED)</td>
<td>501 (Not Implemented)</td>
</tr>
<tr>
<td>6003 (EXTERNAL_OBJECT_NOT_REACHABLE)</td>
<td>404 (Not Found)</td>
</tr>
<tr>
<td>6005 (EXTERNAL_OBJECT_NOT_FOUND)</td>
<td>404 (Not Found)</td>
</tr>
<tr>
<td>6010 (MAX_NUMBER_OF_MEMBER_EXCEEDED)</td>
<td>400 (Bad Request)</td>
</tr>
<tr>
<td>6011 (MEMBER_TYPE_INCONSISTENT)</td>
<td>400 (Bad Request)</td>
</tr>
<tr>
<td>6020 (MANAGEMENT_SESSION_CANNOT_BE_ESTABLISHED)</td>
<td>500 (Internal Server Error)</td>
</tr>
<tr>
<td>6021 (MANAGEMENT_SESSION_ESTABLISHMENT_TIMEOUT)</td>
<td>500 (Internal Server Error)</td>
</tr>
<tr>
<td>6022 (INVALID_CMDTYPE)</td>
<td>400 (Bad Request)</td>
</tr>
<tr>
<td>6023 (INVALID_ARGUMENTS)</td>
<td>400 (Bad Request)</td>
</tr>
<tr>
<td>6024 (INSUFFICIENT_ARGUMENT)</td>
<td>400 (Bad Request)</td>
</tr>
<tr>
<td>6025 (MGMT_CONVERSION_ERROR)</td>
<td>500 (Internal Server Error)</td>
</tr>
<tr>
<td>6026 (CANCELLATION_FAILED)</td>
<td>500 (Internal Server Error)</td>
</tr>
<tr>
<td>6028 (ALREADY_COMPLETE)</td>
<td>400 (Bad Request)</td>
</tr>
<tr>
<td>6029 (COMMAND_NOT_CANCELLABLE)</td>
<td>400 (Bad Request)</td>
</tr>
</tbody>
</table>

6.3.3 Reason-Phrase

Reason-Phrase shall be omitted.

6.4 Header Fields

6.4.1 Host

The Host header shall be included in a HTTP request message.

While the Request-Target indicates a target resource on the Hosting CSE, the Host header indicates a Receiver CSE in multi-hop communication. Therefore, the Request-Target is not changed but the Host header is changed each time when a request is forwarded.

The Host header shall be set as one of pointOfAccess attribute values of the Receiver (i.e. pointOfAccess attribute of the corresponding <remoteCSE> resource). Selection of the proper Receiver is described in oneM2M TS-0004 [3].
6.4.2 Accept

The Originator may use the Accept header to indicate which content-type is supported by the Originator. The Accept header shall be mapped to a set of media types among "application/xml", "application/json", "application/vnd.onem2m-prsp+xml", "application/vnd.onem2m-prsp+json".

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", "application/vnd.onem2m-res+xml", "application/vnd.onem2m-res+json", "application/vnd.onem2m-ntfy+xml", "application/vnd.onem2m-ntfy+json", "application/vnd.onem2m-attrs+xml", "application/vnd.onem2m-attrs+json".

Content-type of the HTTP response should be chosen by the Hosting CSE considering Accept header given in the HTTP request. For example, if the Accept header in a request is set to "application/vnd.onem2m-prsp+xml", then the response should use one of the oneM2M defined media types in XML serialization (see clause 6.7 [3]).

6.4.4 Content-Location

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

6.4.5 Content-Length

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

6.4.6 Etag

A retrieve response primitive corresponding to a resource retrieval request primitive should include an Etag header together with the resource representation [1].

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

If a CSE supports the Etag header, then the CSE shall support conditional requests.

6.4.7 X-M2M-Origin

The X-M2M-Origin header shall be mapped to the From parameter of the request/response primitive.

The X-M2M-Origin header value shall be specified by the composer 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.

6.4.9 X-M2M-NM

The X-M2M-NM header shall be mapped to the Name parameter if applicable.

6.4.10 X-M2M-GID

The X-M2M-NM header shall be mapped to the Group Request Identifier parameter 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 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 if applicable.

6.4.13 X-M2M-RST

The X-M2M-RST header shall be mapped to the Result Expiration Timestamp parameter if applicable.

6.4.14 X-M2M-RET

The X-M2M-FC header shall be mapped to the Request Expiration Timestamp parameter if applicable.

6.4.15 X-M2M-OET

The X-M2M-FC header shall be mapped to the Operation Execution Time parameter if applicable.

6.4.16 X-M2M-EC

The X-M2M-ECT header shall be mapped to the Event Category parameter if applicable.

6.4.17 X-M2M-RSC

The X-M2M-RSC header shall be mapped to the Response Status Code parameter in a HTTP response message.

6.5 Message-body

Message-body shall be mapped to the Content parameter if applicable.

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 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.

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 the token.

7.2 Transport Layer Security

oneM2M primitive parameters contained in HTTP messages may be protected by TLS as 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 7.3.7.2.1.

```
Step 1: AE requests to create a <container> resource at ASN-CSE
POST /CSE1?rc=0 HTTP/1.1
Host: 192.168.0.2
X-M2M-Origin: CAE1
X-M2M-NM: cont1
X-M2M-RI: 0001
Content-Type: application/vnd.onem2m-res+xml; ty=3
Content-Length: 52

<cnt>
  <mni>10</mni>
</cnt>
```

Step 2: Local Processing
Process the request and create "cont1" resource

```
Step 3: CSE responses OK
HTTP/1.1 201
X-M2M-RI: 0001
Content-Location: /CSE1/cnt1
Content-Length: 0
```

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.
## Publication history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0.1</td>
<td>30 Jan 2015</td>
<td>Release 1 - Publication</td>
</tr>
</tbody>
</table>