

ETSI TS 118 120 V2.0.0 (2016-09)



**oneM2M;
WebSocket Protocol Binding
(oneM2M TS-0020 version 2.0.0 Release 2)**



Reference

DTS/oneM2M-000020

Keywords

IoT, M2M, protocol

ETSI

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

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

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

Important notice

The present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	5
3 Definitions and abbreviations.....	6
3.1 Definitions	6
3.2 Abbreviations	6
4 Conventions.....	6
5 Overview on WebSocket Binding	6
5.1 Use of WebSocket	6
5.2 Binding Overview	7
6 Protocol Binding	10
6.1 Introduction	10
6.2 WebSocket connection establishment	10
6.2.1 General.....	10
6.2.2 Client handshake.....	11
6.2.2.1 Format of request-line	11
6.2.2.2 Host header	11
6.2.2.3 Upgrade header	11
6.2.2.4 Connection header.....	11
6.2.2.5 Sec-WebSocket-Key header.....	11
6.2.2.6 Sec-WebSocket-Version header.....	11
6.2.2.7 Sec-WebSocket-Protocol header.....	12
6.2.2.8 Sec-WebSocket-Extensions header.....	12
6.2.2.9 Subprotocol names and serialization formats.....	12
6.2.3 Server handshake format	13
6.2.3.1 Format of status-line	13
6.2.3.2 Upgrade header	13
6.2.3.3 Connection header.....	13
6.2.3.4 Sec-WebSocket-Accept header.....	13
6.2.3.5 Sec-WebSocket-Protocol header.....	13
6.2.3.6 Sec-WebSocket-Extensions header.....	13
6.3 Closing WebSocket connection.....	13
6.4 Registration procedure	14
6.5 Handling of Non-Registration Request	14
6.6 Use of proxy servers.....	14
7 Security Aspects.....	14
Annex A (informative): Example Procedures	15
A.1 AE Registration and creation of a Container child resource	15
History	18

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Partnership Project oneM2M (oneM2M).

1 Scope

The present document specifies the binding of Mca and Mcc primitives onto the WebSocket binding.

It specifies:

- Procedures and message formats for operating and closing of WebSocket connections.
- How request and response primitives are mapped into the payload of the WebSocket protocol.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found at <https://docbox.etsi.org/Reference/>.

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

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

- [1] IETF RFC 6455: "The Web Socket Protocol", December 2011.
- [2] ETSI TS 118 101: "oneM2M; Functional Architecture (oneM2M TS-0001).
- [3] IETF RFC 7230: "Hypertext Transport Protocol (HTTP/1.1): Message Syntax and Routing", June 2014.
- [4] ETSI TS 118 103: "oneM2M; Security Solutions (oneM2M TS-0003)".
- [5] ETSI TS 118 104: "oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004)".
- [6] IETF RFC 7692: "Compression Extension for WebSocket", December 2015.

2.2 Informative references

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

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

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

- [i.1] oneM2M Drafting Rules.

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

oneM2M WebSocket Client (WS Client): WebSocket Client associated with an AE or a CSE capable of establishing the WebSocket connections

oneM2M WebSocket Server (WS Server): WebSocket Server associated with a CSE which accepts requests to establish WebSocket connections

3.2 Abbreviations

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

ADN	Application Dedicated Node
AE	Application Entity
ASN	Application Service Node
CBOR	Concise Binary Object Representation
CSE	Common Services Entity
FQDN	Fully Qualified Domain Name
GUID	Globally Unique Identifier
HTTP	Hypertext Transport Protocol
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IN-CSE	Infrastructure Node Common Services Entity
IP	Internet Protocol
JSON	JavaScript Object Notation
MN	Middle Node
MN-CSE	Middle Node Common Services Entity
NAT	Network Address Translator
SAEF	Security Association Establishment Framework
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URI	Uniform Resource Identifier
WS	WebSocket
XML	eXtensible Markup Language

4 Conventions

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

5 Overview on WebSocket Binding

5.1 Use of WebSocket

This binding makes use of the WebSocket protocol IETF RFC 6455 [1] to transport serialized representations of oneM2M request and response primitives over the Mca or Mcc reference points.

Establishment of a WebSocket connection shall be initiated by a WebSocket client by sending a handshake to a WebSocket server as specified in section 4 of IETF RFC 6455 [1]. Once the WebSocket connection is established, both oneM2M request and response primitives can be exchanged bi-directionally between the two endpoints of the connection. Serialized representations of the request and response primitives shall be mapped in the Payload Data field of the WebSocket base framing protocol, as defined in section 5.2 of IETF RFC 6455 [1].

A WebSocket connection employs either a TCP/IP or a TLS over TCP/IP connection. The underlying TCP and TLS connections are established as the first step of the WebSocket handshake.

5.2 Binding Overview

WebSocket binding may be employed for communication between any two endpoints which can be connected over the Mca, Mcc or Mcc' interface reference points supported by the oneM2M Architecture as shown in figure 6.1-1 of ETSI TS 118 101 [2].

When using the WebSocket protocol, one communication endpoint shall act as the WebSocket server. The WebSocket server listens for inbound handshake messages arriving from any WebSocket client to which a WebSocket connection is not yet established. Whether a communication endpoint takes the role of the client or the server shall depend on the registration relationship between the communicating entities as follows: the registree shall always use a WebSocket client, while the associated registrar shall always use a WebSocket server on the respective reference point.

This implies that ADN and ASN always take the role of a WebSocket client when WebSocket binding is employed. An MN-CSE uses a WebSocket server to communicate with its registrees and a WebSocket client to communicate with its own registrar (which can be another MN-CSE or an IN-CSE).

The IN-CSE provides a WebSocket server functionality to communicate with all its registrees, i.e. within a service provider's domain. On the Mcc' reference points, i.e. for communication between IN-CSEs of different Service Provider domains, the IN-CSE shall provide both WebSocket client and server functionality. This enables any IN-CSE to open a WebSocket connection to any IN-CSE of another Service Provider's domain.

Figure 5.2.-1 shows some applicable example system configuration.

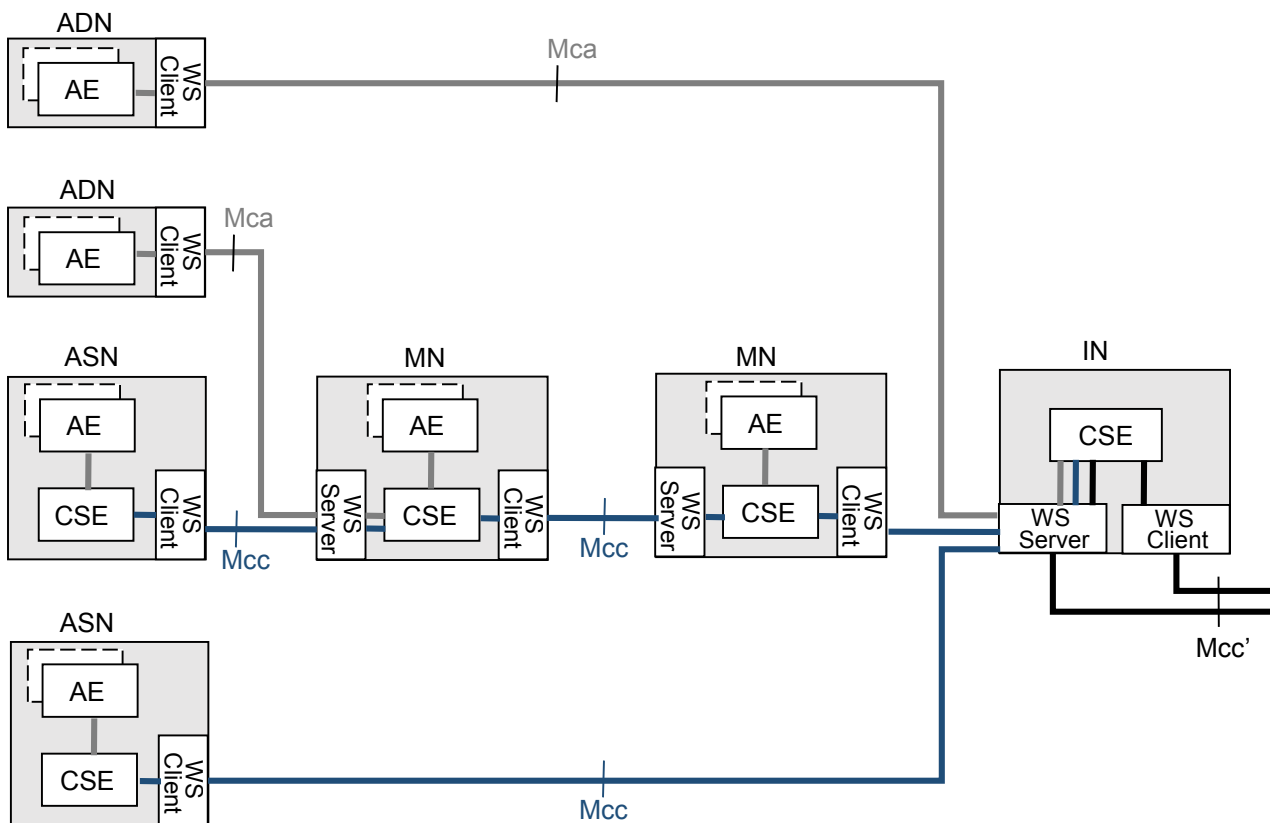


Figure 5.2-1: Example scenarios of WebSocket client and server configurations

There exists a maximum of one WebSocket connection between two nodes. A WebSocket connection is established for the first time when the initial registration procedure of an entity to its registrar is performed. On an established WebSocket connection, request and response primitives can be exchanged in both directions. Any connection may be closed by either the WebSocket client or the server, depending on the communication schedule of either entity. However, the connection can be reopened from the client side only.

If the connection is closed temporarily, it shall be reopened when the next request primitive is sent from the client to the server side, or when the time to become reachable configured at <schedule> resource. If the WebSocket connection with the next-hop entity is not opened, and the WebSocket connection cannot be established due to lack of *pointOfAccess* address for the entity, a sending CSE may enable buffering of primitives which should be sent to the entity until the connection is reopened or their expiration time is reached. See Annex H of ETSI TS 118 104 [5] about buffering of primitives by CMDH functionality.

Figure 5.2-2 shows an example message flow for a scenario where an ADN-AE registers to its registrar MN-CSE using an unsecured TCP connection without proxy and then continues exchanging non-registration request and response primitives.

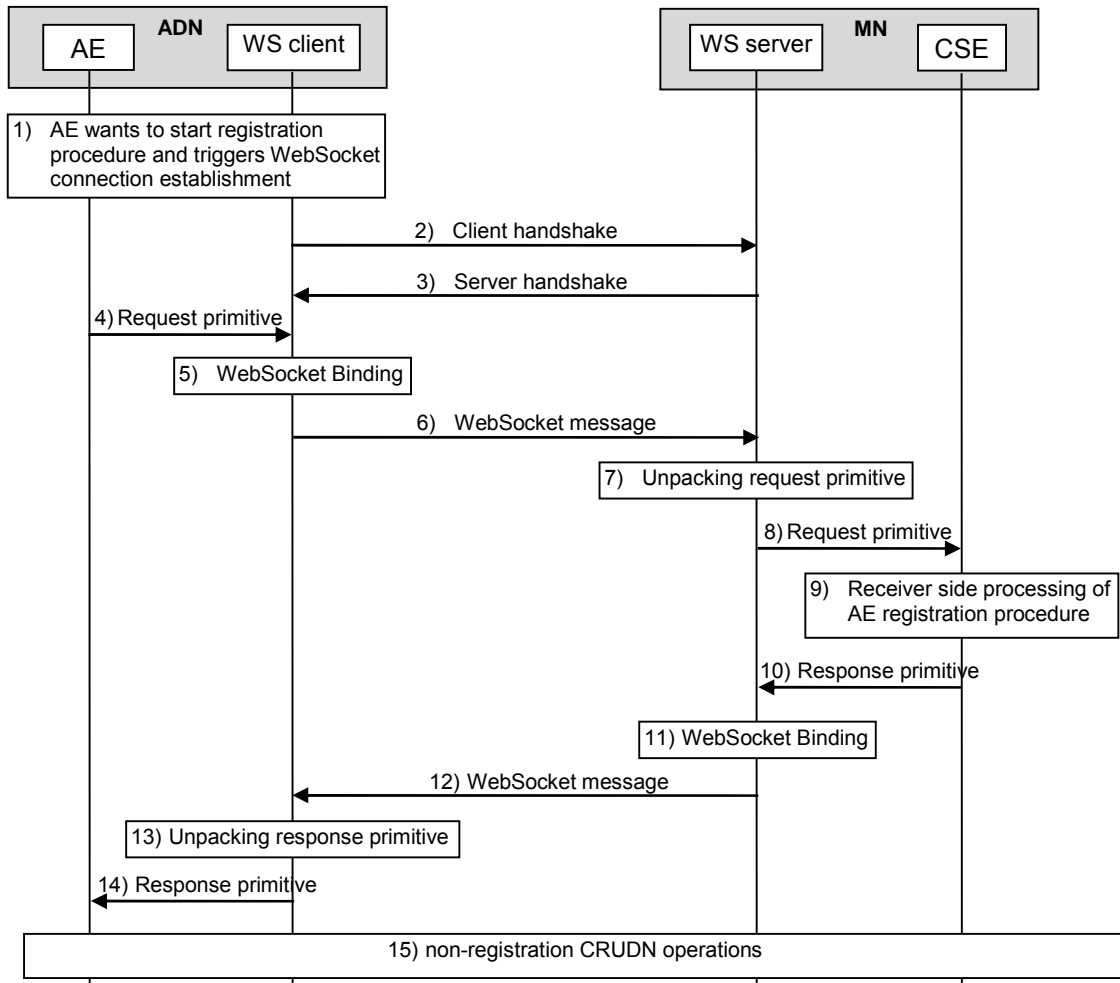


Figure 5.2-2: Example message flow with Websocket binding

1) The ADN-AE wants to register to its registrar MN-CSE. If a WebSocket connection does not exist, it is established by the following steps 2) and 3). It is assumed that the ADN-AE knows the point of access (i.e. WebSocket URI specified in IETF RFC 6455 [1]) under which the registrar CSE can be reached with WebSocket binding.

2) The WebSocket client opens handshake to the server with subprotocol name 'oneM2M-pro-v1.0' following IETF RFC 6455 [1].
If the server can be reached under the WebSocket URI ws://example.net:9000/, the client handshake may look as follows:

```

GET / HTTP/1.1
Host: mncse1234.net:9000
Upgrade: WebSocket
Connection: Upgrade
Sec-WebSocket-Key: ud63env87LQLd4uIV20/oQ==
Sec-WebSocket-Protocol: oneM2M-pro-v1.0
Sec-WebSocket-Version: 13
  
```

3) The WebSocket server replies with a handshake to the client. In the successful case, the status-line of this HTTP response may look as follow:

```

Request-Version: HTTP/1.1
Status-Code: 101
Response-Phrase: Switching Protocols
Upgrade: WebSocket
Connection: Upgrade
Sec-WebSocket-Protocol: oneM2M-pro-v1.0
Sec-WebSocket-Accept: FuSSKAnI7C/6/FrPMt70mfBY8E=
  
```

- 4) The ADN-AE issue a registration request primitive. The request primitive may e.g. look as follows as JSON-serialized representation:

```
{ "m2m:rqpp": { "op": 1, "to": "//example.net/mncse1234", "rqi": "A1234", "pc": { "m2m:ae": { "api": "a56", "apn": "app1234" } }, "ty": 2 } }
```

NOTE: The WebSocket client associated with an ADN-AE does not need to be reachable for WebSocket Server handshake messages.

- 5) WebSocket Binding process, which transforms a single oneM2M primitive into one or more data frames of the WebSocket Framing protocol, as specified in IETF RFC 6455 [1]. When transmitting a JSON-serialized primitive in utf-8 text format, the 4-bit opcode in the WebSocket Base Framing Protocol of the first message fragment will be set to x1 ("text frame").
- 6) The WebSocket message (consisting of one or more frames) shall be sent to the WS server.
- 7) The original request primitive shall be unpacked from the WebSocket message by the WS server.
- 8) The request primitive is delivered to the MN-CSE.
- 9) The MN-CSE performs the receiver side operations of AE registration as specified in ETSI TS 118 101 [2].
- 10) The response primitive is issued to the WebSocket server.
- 11) WebSocket binding process for the response primitive is performed.
- 12) The WebSocket message (consisting of one or more frames) is sent to the client.
- 13) The response primitive is unpacked.
- 14) The response primitive is to the ADN-AE.
- 15) After successful completion of AE registration any other CRUDN requests and response primitives can be exchanged over the existing WebSocket connection in both directions. If the ADN-AE has no other requests to send, the WebSocket connection may be closed temporarily. When the WebSocket connection is closed after registration and reopened later again, the registration procedure as outlined in steps 4 to 14 is omitted. In this case any non-registration request primitives can be sent directly.

6 Protocol Binding

6.1 Introduction

The WebSocket protocol enables two-way communication between client and server even when a firewall and/or NAT are present between them. This means, once a WebSocket connection is established, request (and response) primitives can be exchanged in both directions, from the client to the server and vice versa. However, AEs may be capable of handling Notification request primitives only, or no request primitives at all.

WebSocket binding applied by oneM2M entities/nodes shall be fully compliant with IETF RFC 6455 [1]. After establishment of a WebSocket connection between two nodes, at the transmitter side each individual request and response primitive is mapped into one or several WebSocket frames.

6.2 WebSocket connection establishment

6.2.1 General

A WebSocket connection is opened by the client side as specified in section 4 of IETF RFC 6455 [1] with sending of a client handshake. The server responds with a server handshake.

The client handshake consists of an HTTP upgrade request, along with a list of required and optional header fields.

The handshake shall be a valid HTTP request as specified by IETF RFC 7230 [3]. The server handshake consists of a HTTP status-line and a list of header fields.

The applicable format of the request-line, status-line and the applicable header fields are specified in the following sub-clauses.

HTTP headers fields have case-insensitive field names.

CSEs capable to support WebSocket shall indicate the schemes ws and/or wss together with the applicable host name and port numbers in the pointOfAccess attribute of their <CSEBase> resource, i.e. as ws://host:port1 and wss://host:port2.

6.2.2 Client handshake

6.2.2.1 Format of request-line

The request-line of a client handshake shall begin with the method token "GET", followed by the request target "/" and the HTTP version set to "HTTP/1.1" as follows:

```
GET / HTTP/1.1
```

If the client is configured to use a proxy when using the WebSocket Protocol, a connection to the proxy server shall be established prior to sending the above client handshake. This is described in clause 6.6.

6.2.2.2 Host header

The Host header shall be present in each client handshake.

The Host header indicates the FQDN or IP address of the Receiver CSE of the next hop. If the originator of the client handshake is an oneM2M field entity, the host header represents the registrar CSE of the originator.

When no proxy is used, the Host header shall be set as one of the pointOfAccess attribute values associated with the Receiver. Selection of the appropriate Receiver is described in ETSI TS 118 104 [5].

If the client is configured to use a proxy when using the WebSocket Protocol, then the client should connect to that proxy and ask it to open a TCP connection to the host and port rather than to the next hop CSE.

6.2.2.3 Upgrade header

The Upgrade header shall be present in each client handshake message with value WebSocket as follows:

```
Upgrade: WebSocket
```

6.2.2.4 Connection header

The Connection header shall be present in each client handshake message with value Upgrade as follows:

```
Connection: Upgrade
```

6.2.2.5 Sec-WebSocket-Key header

The Sec-WebSocket-Key header shall be present in each client handshake message. The header field includes a base64-encoded representation of a random 16 bytes pattern, for example:

```
Sec-WebSocket-Key: ud63env87LQLd4uIV20/oQ==
```

6.2.2.6 Sec-WebSocket-Version header

The Sec-WebSocket-Version header shall be present in each client handshake message with value 13 as follows:

```
Sec-WebSocket-Version: 13
```

6.2.2.7 Sec-WebSocket-Protocol header

The Sec-WebSocket-Protocol header shall be present in a client handshake message. It enables the client to indicate its supported application subprotocols on the server and be sure that the server agreed to support that subprotocol. It is used by the client to indicate the oneM2M Service Layer Protocol version and supported serialization formats to the server.

The value of the Sec-WebSocket-Protocol header shall be one or more of the registered names defined in clause 6.2.2.9. It shall also be allowed to include multiple Sec-WebSocket-Protocol headers with a value that includes one registered name each as defined in IETF RFC 6455 [1], for example:

```
Sec-WebSocket-Protocol: oneM2M.R2.0.JSON, oneM2M-R2.0_XML
```

and

```
Sec-WebSocket-Protocol: oneM2M.R2.0.XML
```

```
Sec-WebSocket-Protocol: oneM2M.R2.0.JSON
```

are equivalent headers, expressing that the WebSocket client supports both application subprotocols, oneM2M.R2.0.XML and oneM2M.R2.0.XML. The order of names indicated in the Sec-WebSocket-Protocol header specifies the client's preference.

6.2.2.8 Sec-WebSocket-Extensions header

The Sec-WebSocket-Extensions header may be used to negotiate the use of per-message compression as specified in IETF RFC 7692 [6].

If the client handshake includes the header, e.g.:

```
Sec-WebSocket-Extensions: permessage-deflate
```

it indicates to the server the client's preference to apply the compression mechanism defined in IETF RFC 7692 [6]. The header may include additional parameters as specified in IETF RFC 7692 [6].

When the server accepts use of message compression it responds with a Sec-WebSocket-Extensions header in the server handshake message as specified in clause 6.2.3.6, and in this case compression is applied in both transmission directions. If the server handshake message does not include a Sec-WebSocket-Extensions header, compression shall not be applied.

6.2.2.9 Subprotocol names and serialization formats

The Sec-WebSocket-Protocol header in the opening handshake is used to negotiate the application protocol layered on top of WebSocket. The application protocol addressed in this specification is the Release-2 version of the oneM2M Service Layer.

The oneM2M Service Layer Protocol consists of the exchange of serialized representations of request and response primitives as defined in ETSI TS 118 101 [2] and ETSI TS 118 104 [5]. This version of the specification allows use of the serialization formats listed in Table 6.2.2.9-1. Both, protocol version and serialization format are associated with a specific subprotocol name.

Table 6.2.2.9-1 lists the serialization formats, associated subprotocols names and opcode setting of the WebSocket Frame protocol applicable for the present version of this specification.

Table 6.2.2.9-1: Applicable Subprotocol names

Serialization Format	Subprotocol Name	WS opcode	Notes
JSON	oneM2M.R2.0.json	x1 ("text frame")	See clause 8.4 in ETSI TS 118 104 [5]
XML	oneM2M.R2.0.xml	x1 ("text frame")	See clause 8.3 in ETSI TS 118 104 [5]
CBOR	oneM2M.R2.0.cbor	x2 ("binary frame")	See clause 8.5 in ETSI TS 118 104 [5]

6.2.3 Server handshake format

6.2.3.1 Format of status-line

The status-line of a server handshake shall begin with the HTTP version set to "HTTP/1.1", followed by the status code and reason phrase as defined in IETF RFC 6455 [1]. When the WebSocket connection is established successfully, the status-line may look as follows:

```
HTTP/1.1 101 Switching Protocols
```

For the unsuccessful connection establishment, any appropriate HTTP error status code shall be returned with optional addition of a corresponding reason phrase.

6.2.3.2 Upgrade header

The Upgrade header shall be present in each server handshake message with value WebSocket as follows:

```
Upgrade: WebSocket
```

6.2.3.3 Connection header

The Connection header shall be present in each server handshake message with value Upgrade as follows:

```
Connection: Upgrade
```

6.2.3.4 Sec-WebSocket-Accept header

The Sec-WebSocket-Accept header shall be present in each server handshake message. The header field shall be constructed from the Sec-WebSocket-Key value and the GUID as specified in section 4.2.2 of IETF RFC 6455 [1]. It may look e.g. as follows:

```
Sec-WebSocket-Accept: FuSSKANnI7C/6/FrPmt70mfBY8E=
```

6.2.3.5 Sec-WebSocket-Protocol header

The Sec-WebSocket-Protocol header shall be present in a server handshake message. It indicates to the client that the server accepts (one of) the subprotocol(s) indicated by the client.

The server compliant with this specification shall select one of the subprotocol names indicated in the Sec-WebSocket-Protocol header of the client handshake message and set the value of the Sec-WebSocket-Protocol header of the server handshake message accordingly.

6.2.3.6 Sec-WebSocket-Extensions header

If the optional Sec-WebSocket-Extensions header with value "permessage-deflate" was included in the client handshake message, the Sec-WebSocket-Extensions header with same value shall also be included into the server handshake message, if the server accepts usage of message compression, and apply message compression in the transmit direction and message decompression in the receive direction as defined in IETF RFC 7692 [6].

If the server does not accept message compression, it shall not include the Sec-WebSocket-Extensions header.

6.3 Closing WebSocket connection

Compliant with section 7 of IETF RFC 6455 [1] a WebSocket connection shall be closed by sending a Connection Close Frame (opcode x8). Both, client and server may initiate a closing handshake of an existing WebSocket connection at any time.

WebSocket connections should be kept open for as long as possible considering any given constraints due to communication policies and power saving requirements. Unless communication policies enforce the closing of network access, it is left to implementation to decide when exactly the closing of a WebSocket shall be triggered.

6.4 Registration procedure

A oneM2M entity (AE or CSE) not yet registered to its registrar CSE needs to be preconfigured with various parameters as specified in ETSI TS 118 101 [2] and ETSI TS 118 103 [4] in order to be able to send the registration request primitive (i.e. create <AE> or create <remoteCSE> request primitive). To establish a WebSocket connection, the WebSocket client shall be configured with an applicable point of access of its registrar CSE which includes FQDN or IP address and the port number.

After the Registration procedure has been successfully completed, the WebSocket Server (e.g. Registrar CSE for WebSocket Client) shall enable routing of any incoming oneM2M primitives to this registree.

Thus until the Before the Registration procedure is successfully completed, any incoming oneM2M primitives to the WebClient shall be rejected by the Receiver (e.g. registrar CSE).

Closing of the WebSocket connection after registration does not impact the registration status of an AE or CSE to its registrar, unless an explicit de-registration procedure is performed by deletion of the respective <AE> or <remoteCSE> resource instance.

6.5 Handling of Non-Registration Request

Registered entities (AE and CSE) are allowed to send and receive non-registration request primitives. A WebSocket connection should support any of the transfer modes defined in clause 8.2 of ETSI TS 118 101 [2], i.e. blocking requests, and non-blocking requests for both synchronous and asynchronous cases.

When sending blocking requests, the WebSocket connection shall not be closed before the response is received, or before any configured timeout period has expired.

When sending non-blocking requests, the WebSocket connection shall not be closed before the acknowledgment response is received, or before any configured timeout period has expired. If the entities' communication policies and power saving requirements allow, the connection should be kept open at least until an ongoing procedure has fully completed, i.e. requesting of the result in synchronous mode or completion of Notify procedure in asynchronous mode.

6.6 Use of proxy servers

The connection to a proxy shall be requested by sending a request-line with the method token "CONNECT", followed by the request target host and port of the WebSocket server and the HTTP version set to "HTTP/1.1" as follows:

```
CONNECT WSserver.example.com:80 HTTP/1.1
```

7 Security Aspects

Authentication and Transport Layer Security can be established when the oneM2M entity which hosts the WebSocket Server can be addressed with the wss URI scheme. When using the wss URI scheme, one of the Security Association Establishment Frameworks (SAEF) as defined in ETSI TS 118 103 [4] shall be applied to provide mutually authenticated Transport Layer Security between the communicating entities prior to sending the WebSocket client handshake.

The SAEF is accomplished by successful completion of a TLS handshake procedure before the client sends its opening handshake message. The details of SAEF and possibly required Remote Security Provisioning Frameworks are specified in ETSI TS 118 103 [4].

In special deployment scenarios, e.g. when the communicating oneM2M entities using WebSocket binding are located in a secure environment and/or implemented on the same device, Transport Layer Security may not be required. In such scenarios unsecured WebSocket communication addressed with the ws URI scheme may be adequate.

Annex A (informative): Example Procedures

A.1 AE Registration and creation of a Container child resource

Figure A.1-1 illustrates a message flow for registration of an ADN-AE to an IN-CSE as described in clause 7.3.5.2.1 of ETSI TS 118 104 [5] with WebSocket mapping and subsequent creation of a <Container> child resource.

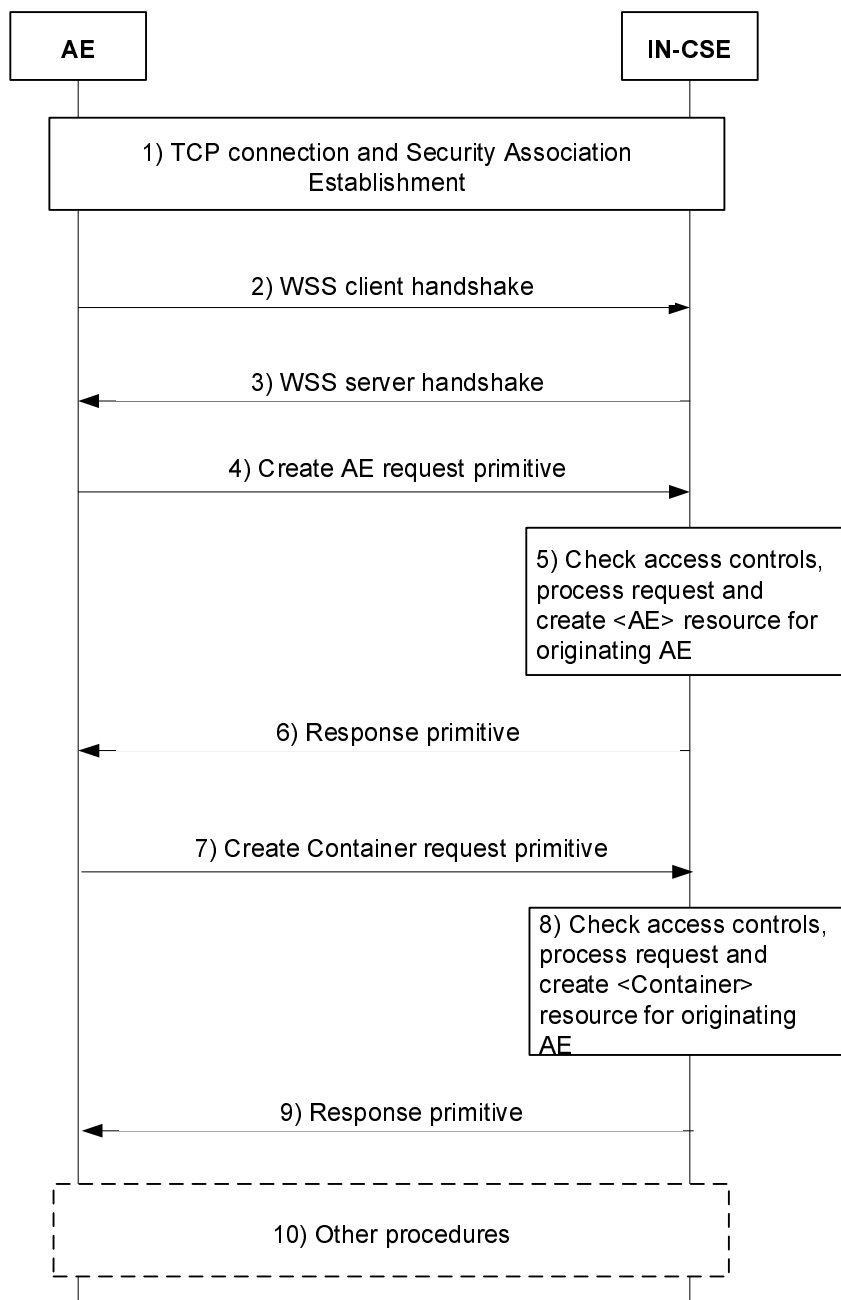


Figure A.1-1: Message flow for registration of an ADN-AE to an IN-CSE

In the considered example, the WebSocket protocol is used to send JSON serialized request and response primitives in text format.

The message flow may look as follows:

- 1) TCP connection establishment and Security Association Establishment as defined in ETSI TS 118 103 [4] based on TLS handshake procedure is accomplished.

The WSS client sends e.g. the following opening handshake message, offering to use either JSON or XML serialization of primitives:

```
GET / HTTP/1.1
```

```
Host: mncsel234.net:9000
```

```
Upgrade: WebSocket
```

```
Connection: Upgrade
```

```
Sec-WebSocket-Key: ud63env87LQLd4uIV20/oQ==
```

```
Sec-WebSocket-Protocol: oneM2M.R2.0.json, oneM2M.R2.0.xml
```

```
Sec-WebSocket-Version: 13
```

- 2) The WSS server selects use of JSON serialization and responds the following handshake message:

```
Request-Version: HTTP/1.1
```

```
Status-Code: 101
```

```
Response-Phrase: Switching Protocols
```

```
Upgrade: WebSocket
```

```
Connection: Upgrade
```

```
Sec-WebSocket-Protocol: oneM2M.R2.0.json
```

```
Sec-WebSocket-Accept: FuSSKANnI7C/6/FrPMT70mfBY8E=
```

- 3) The AE sends the following request primitive in textual JSON serialized format:

```
{ "m2m:rqp": { "op": 1, "to": "//example.net/mncsel234", "rqi": "A1000",
"rcn": 7, "pc": { "m2m:ae": { "rn": "SmartHomeApplication", "api": "Na56",
"apn": "app1234" } }, "ty": 2 } }
```

The above JSON object is mapped by the WS client into a data frame of the WebSocket Framing protocol in utf-8 text format, the 4-bit opcode in the WebSocket Base Framing Protocol of the first message fragment is set to x1 ("text frame").

- 4) The IN-CSE validates the privilege of the originator to create an <AE> resource, and accepts the request to create the resource.
- 5) The IN-CSE acknowledges the success of the request by responding the following JSON serialized response primitive. The response primitive includes all attributes of <AE> instance created in Step 5.

```
{ "m2m:rsp": { "rsc": 2001, "rqi": "A1000", "pc": { "m2m:ae": { "rn": "SmartHomeApplic
ation", "ty": 2, "ri": "ae1", "api": "Na56", "apn": "app1234", "pi": "cb1", "ct": "201
60506T153208",
"lt": "20160506T153208", "acpi": [ "acp1", "acp2" ], "et": "20180506T153208",
"aei": "S_SAH25" } } } }
```

The above JSON object is mapped by the WS server into a data frame of the WebSocket Framing protocol in utf-8 text format, the 4-bit opcode in the WebSocket Base Framing Protocol of the first message fragment is set to x1 ("text frame").

- 6) The AE sends in textual JSON serialized format the following request primitive to create a <Container> resource as child resource of the <AE> created in Step 5:

```
{ "m2m:rqp": { "op": 1, "to": "//example.net/mncse1234/SmartHomeApplication",  
  "rqi": "A1001", "rcn": 7, "pc": { "m2m:cnt": { "rn": "SmartHomeContainer", "mbs": 100000, "mni": 500 } }, "ty": 3 } }
```

The above JSON object is mapped by the WS client into a data frame of the WebSocket Framing protocol in utf-8 text format, the 4-bit opcode in the WebSocket Base Framing Protocol of the first message fragment is set to x1 ("text frame").

- 7) The IN-CSE validates the privilege of the originator to create an <Container> resource under the <AE> resource created in step 5, and accepts the request to create the resource.
- 8) The IN-CSE acknowledges the success of the request by responding the following JSON serialized response primitive:

```
{ "m2m:rsp": { "rsc": 2001, "rqi": "A1001", "pc": { "m2m:cnt": { "rn": "SmartHomeContainer", "ty": 3, "ri": "cnt1", "pi": "ae1", "ct": "20160506T154048",  
  "lt": "20160506T154048", "acpi": [ "acp1" ], "et": "20180506T154048", "cr": "S_SAH25", "st": 0, "mni": 500, "mbs": 100000, "cni": 0, "cbs": 0, "mia": 3600 } } } }
```

The above JSON object is mapped by the WS server into a data frame of the WebSocket Framing protocol in utf-8 text format, the 4-bit opcode in the WebSocket Base Framing Protocol of the first message fragment is set to x1 ("text frame").

- 9) Primitives of further subsequent CRUDN procedures may be transferred on the existing WebSocket connection.

History

Document history		
V2.0.0	September 2016	Publication