ETSI TS 118 113 V2.3.2 (2020-04)

oneM2M;
Interoperability Testing
(oneM2M TS-0013 version 2.3.2 Release 2A)

Reference

RTS/oneM2M-000013v2A

Keywords

interoperability, 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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

1 Scope

The present document specifies Interoperability Test Descriptions (TDs) for the oneM2M Primitives as specified in ETSI TS 118 101 [1], ETSI TS 118 104 [2], the bindings ETSI TS 118 108 [3], ETSI TS 118 109 [4] and ETSI TS 118 110 [5].

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] ETSI TS 118 101: "oneM2M; Functional Architecture (oneM2M TS-0001 Release 2)".

[2] ETSI TS 118 104: "oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004 Release 2)".

[3] ETSI TS 118 108: "oneM2M; CoAP Protocol Binding (oneM2M TS-0008 Release 2A)".

[4] ETSI TS 118 109: "oneM2M; HTTP Protocol Binding (oneM2M TS-0009 Release 2A)".

[5] ETSI TS 118 110: "oneM2M; MQTT Protocol Binding (oneM2M TS-0010 Release 2)".

[6] ETSI TS 118 115: "oneM2M; Testing Framework (oneM2M TS-0015 Release 2)".

[7] ETSI TS 118 111: "oneM2M; Common Terminology (oneM2M TS-0011 Release 2)".

[8] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[9] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[10] ETSI TS 118 105: "oneM2M; Management Enablement (OMA) (oneM2M TS-0005 Release 2A)".

[11] ETSI TS 118 106: "oneM2M; Management Enablement (BBF) (oneM2M TS-0006 Release 2A)".

[12] ETSI TS 118 103: "oneM2M; Security solutions (oneM2M TS-0003 Release 2A)".

[13] oneM2M TS-0034: "Semantics Support - Release 3".

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.

[i.2] BBF TR-069: "CPE WAN Management Protocol".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 118 111 [7] and the following apply:

NOTE: A term defined in the present document takes precedence over the definition of the same term, if any, in ETSI TS 118 111 [7].

hosting CSE: CSE where the addressed resource is hosted

M2M service provider domain: part of the M2M System that is associated with a specific M2M Service Provider

mc: interface between the management server and the management client

NOTE: This interface can be realized by the existing device management technologies such as BBF TR-069 [i.2], OMA DM [10], etc.

receiver CSE: any CSE that receives a request

registrar CSE: CSE where an Application or another CSE has registered

registree: AE or CSE that registers with another CSE

resource: uniquely addressable entity in oneM2M architecture

transit CSE: any receiver CSE that is not a Hosting CSE

3.2 Symbols

Void.

3.3 Abbreviations

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

ACP	Access Control Policy
AE	Application Entity
AE-ID	Application Entity Identifier
APP-ID	Application Identifier
BBF	BroadBand Forum
CFG	Configuration
CoAP	Constrained Application Protocol
CSE	Common Services Entity
CSE-ID	Common Service Entity Identifier
DM	Device Management
DTLS	Datagram Transport Layer Security
DUT	Device Under Test
HTTP	HyperText Transfer Protocol
IN	Infrastructure Node
IN-CSE	CSE which resides in the Infrastructure Node

IOP	Interoperability
IP	Internet Protocol
JSON	JavaScript Object Notation
LWM2M	Lightweight M2M
M2M	Machine to Machine
MA	Mandatory Announced
Mca	Reference Point for M2M Communication with AE
Mcc	Reference Point for M2M Communication with CSE
MH	Multi Hop
MO	Management Object
MQTT	Message Queuing Telemetry Transport
NB	Non-Blocking
NH	No Hop
OMA	Open Mobile Alliance
PRO	Protocol
PSK	Pre-Shared Key
RFC	Request For Comments
RP	Reference Point
RPC	Remote Procedure Calls
RQI	Request-ID
SE	Security
SH	Single Hop
SP	Service Provider
SUT	System Under Test
TCP	Transmission Control Protocol
TD	Test Description
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
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 Testing conventions

5.1 The Test Description proforma

The testing methodology used in the present document is specified in ETSI TS 118 115 [6].

A Test Description (TD) is a well detailed description of a process that aims to test one or more functionalities of an implementation. Applying to interoperability testing, these testing objectives address the interoperable functionalities between two or more vendor implementations.

In order to ensure the correct execution of an interoperability test, the following information should be provided by the test description:

- The proper configuration of the vendor implementations.
- The availability of additional equipment (protocol monitors, functional equipment, etc.) required to achieve the correct behaviour of the vendor implementations.
- The correct initial conditions.
- The correct sequence of the test events and test results.

In order to facilitate the specification of test cases an interoperability test description should include, at a minimum, the following fields as indicated table 5.1-1.

Table 5.1-1: Interoperability test description

Identifier	A unique test description ID.
Objective	A concise summary of the test which should reflect the purpose of the test and enable readers to easily distinguish this test from any other test in the document.
References	A list of references to the base specification section(s), use case(s), requirement(s) and TP(s) which are either used in the test or define the functionality being tested.
Applicability	A list of features and capabilities which are required to be supported by the SUT in order to execute this test (e.g. if this list contains an optional feature to be supported, then the test is optional).
Configuration or Architecture	A list of all required equipment for testing and possibly also including a reference to an illustration of a test architecture or test configuration.
Pre-Test Conditions	A list of test specific pre-conditions that need to be met by the SUT including information about equipment configuration, i.e. precise description of the initial state of the SUT required to start executing the test sequence.
Test Sequence	An ordered list of equipment operation and observations. The test sequence may also contain the conformance checks as part of the observations.

The test descriptions are provided in proforma tables. In order to ensure the correct execution of an interoperability test, the following information is provided in the test description:

- The configuration applied for the test.
- The need of additional equipment (protocol monitors, functional equipment, etc.) required to achieve the correct behaviour of the implementations.
- The initial conditions.
- The sequence of the test events and test results.

The following different types of test operator actions are considered during the test execution:

- A **stimulus** corresponds to an event that enforces a DUT to proceed with a specific protocol action, such as sending a message.
- A **configure** corresponds to an action to modify the DUT configuration.
- An **IOP check** consists of observing that one DUT behaves as described in the standard: i.e. resource creation, update, deletion, etc. For each IOP check in the Test Sequence, a result can be recorded. The overall **IOP Verdict** will be considered OK if all the IOP checks in the sequence are OK.
- In the context of Interoperability Testing with Conformance Checks, an additional step type, **PRO checks** can be used to verify the appropriate sequence and contents of protocol messages, this is helpful for debugging purposes. **PRO Verdict** will be PASS if all the PRO checks are PASS.

5.2 Test Description naming convention

TD/<root>/<gr>/<nn>		
<root> = root	M2M	oneM2M
<gr> = group	NH	No Hop: Testing on Mca reference point
	NB	Non-Blocking scenario
	SH	Single Hop: management of remote resources on Mca + Mcc
	MH	Multi Hop
	SE	Security
<nn> = sequential number		01 to 99

5.3 Test Settings

This clause contains some test requirements applied to the testing, some constraints, restrictions for executions or some recommendations.

In order to ease test setup and execution, the CSE and AE are requested to support the following settings:

- Security shall be disable as it is out of scope of this interoperability testing.
- Resource names are pre-provisioned, except for content instance resources that are automatically assigned by the hosting CSE.
- After each "Delete" primitive on a resource, the user shall check the resource is effectively deleted.
- Unless it is indicated in the test cases prerequisites by default, all the applications shall have the required access rights to manage resources on the CSE.

In order to address the TBDs in the oneM2M CoAP binding specification (ETSI TS 118 108 [3]), basic XML and JSON media-type numbers shall be used in the contentFormat option.

In the test descriptions specified below, the following definitions of terms used for short-hand notation apply:

Serialized Representation: refers to either an XML or a JSON representation of data in text-string format as defined in clauses 8.3 and 8.4 of ETSI TS 118 104 [2].

Host Address: refers to the authority part of a target URI as defined in IETF RFC 3986 [8] and IETF RFC 7230 [9] which can be represented as an IP literal encapsulated within square brackets, an IPv4 address in dotted decimal form, or a registered name, and optionally extended by a port identifier.

5.4 Pre-conditions

5.4.1 Registration

The AE or CSE that originates the request has been successfully registered to its corresponding CSE. The registration of the AE includes the creation of <AE> resource under the <CSEBase> of its registrar CSE. The registration of the CSE includes the creation of <remoteCSE> resource representing itself under the <CSEBase> of its registrar CSE as well as the creation of <remoteCSE> resource representing the registrar CSE under its own <CSEBase> resource. The creation of <remoteCSE> resource representing the registrar CSE can be achieved by remotely retrieving the <CSEBase> resource of the registrar CSE.

5.4.2 Security

The Originator and the receiver have successfully established security association between each other. This may involve the exchange of key and the establishment of a security connection.

The security pre-condition also assumes that the originator has the appropriate access control privilege towards the requested resource.

5.4.3 Service Subscription

Service subscription means that the originator is allowed to be connected with the oneM2M system by contract between the owner of the application and the service provider of the oneM2M system. This may require a corresponding information record in the <m2mServiceSubscriptionProfile> resource.

5.4.4 ID allocation

ID allocation means that the Originator has already acquired usable identity, either from its registrar CSE or the IN-CSE of the oneM2M system. The ID may be CSE relative or SP relative. The ID is then further used as the identity of the Originator to perform access control, charging, etc.

5.4.5 Existence of resource

Existence of resource means the resource been addressed and has already been created.

5.4.6 Management Session between Management Server and Management Client

Before the device management using external technologies is executed, it is required that a management session has already been established between the Management Server and Management Client. If there is no existing management session, the IN-CSE shall request the establishment of a management session between the Management Server and Management Client.

5.5 Binding message convention

In HTTP/CoAP/MQTT binding messages, the present document defines the convention for <variable>:

- <resourceType> represents a resource name (i.e. resourceName attribute) of a resource instance in that resourceType. For example, <CSEBase>/<AE> can represent "CSE1base/AE1" in structured resource ID format.
- <parameter> represents a value of a oneM2M request/response parameter. For example, <Request ID> can represent "0001" value of the Request ID parameter. Parameter names are case sensitive and in long names as specified in ETSI TS 118 104 [2].
- <ID> represents an AE-ID or CSE-ID in MQTT Topic names.

The value will be given at an interoperability test event.

In ETSI TS 118 110 [5], all oneM2M request/response parameters are carried in the MQTT message payload since it has no message header concept. Therefore, the MQTT message payload needs to be described more than HTTP and CoAP messages to describe those parameters in clause 8. In HTTP and CoAP binding messages, payloads are described as "empty" or "<container> resource to be created" in a very abstract way.

Since the representation can be XML or JSON, payload should be abstract to support XML and JSON. The following example is an XML representation and its abstraction for creating a <container> resource.

XML payload example for MQTT binding	<?xml version="1.0" encoding="UTF-8"?> <m2m:req xmlns:m2m="http://www.onem2m.org/xml/protocols" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.onem2m.org/xml/protocols CDT-requestPrimitive-v1_0_0.xsd"> <op>1</op> <to>CSE1Base</to> <fr>/CSE1/C_AE1</fr> <rqi>2001</rqi> <ty>3</ty> <nm>cont1</nm> <rti><rt>3</rt></rti> <pc> <cnt> <lbl>SmartMeter</lbl> <et>20141003T112033</et> </cnt> </pc> </m2m:req>
Abstracted payload example for MQTT binding	op = 1 to = CSE1Base fr = /CSE1/C_AE01 rqi = 3001 ty = 3 name = cont1 rti.rt = 3 pc.cnt.lbl = SmartMeter pc.cnt.et = 20141003T112033