



Lightweight Machine to Machine Gateway Technical Specification

Approved Version: 1.1.1 - 2024-03-12

Open Mobile Alliance

OMA-TS-LWM2M_Gateway-V1_1_1-20240312-A

main: 20 Jun 2024 15:21:00 rev: bc871a8

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <https://www.omaspecworks.org/about/policies-and-terms-of-use/>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification.

However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <https://www.omaspecworks.org/about/intellectual-property-rights/>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

THIS DOCUMENT IS PROVIDED ON AN "AS IS" "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS.

Copyright 2024 Open Mobile Alliance.

Used with the permission of the Open Mobile Alliance under the terms set forth above.

Table of Contents

- [1. Scope](#)
- [2. Reference](#)
 - [2.1. Normative References](#)
 - [2.2. Informative References](#)
- [3. Terminology and Conventions](#)
 - [3.1. Conventions](#)
 - [3.2. Definitions](#)
- [4. Introduction](#)
- [5. Overview](#)
- [6. LwM2M Gateway Object](#)
- [7. Security Consideration](#)
- [8. LwM2M Interfaces](#)
 - [8.1. Bootstrap Interface](#)
 - [8.2. Client Registration Interface](#)
 - [8.3. Device Management And Service Enablement and Information Reporting Interfaces](#)
 - [8.3.1. Simple Operations](#)
 - [8.3.2. Composite Operations](#)
 - [8.3.3. Send Operation](#)
- [9. Data Formats](#)
- [10. Example](#)
- [Appendix A. Change History \(Informative\)](#)
 - [A.1 Approved Version History](#)

Table of Figures

[Figure: 5.-1 LwM2M Gateway Overall System Architecture](#)

Table of Tables

[Table: 2.1.-1 Normative References](#)

[Table: 2.2.-1 Informative References](#)

[Table: 3.2.-1 Definitions](#)

[Table: 6.-1 LwM2M Object: LwM2M Gateway object definition](#)

[Table: 6.-2 LwM2M Object: LwM2M Gateway Resource definitions](#)

[Table: 8.3.1.-1 Operation Parameters](#)

[Table: 10.-1 LwM2M Gateway Object Instance 0](#)

[Table: 10.-2 LwM2M Gateway Object Instance 1](#)

[Table: 10.-3 Example "Read" Operation Parameters](#)

[Table: A.1-1 Approved Version History](#)

1. Scope

This specification extends the LwM2M architecture to support the LwM2M Gateway functionality.

A LwM2M Gateway allows a LwM2M Server to manage end IoT devices "behind" the LwM2M Gateway. The protocols used between the LwM2M Gateway and its connected end IoT devices and any protocol translation carried out by the LwM2M Gateway are outside the scope of this specification.

This is version 1.1.1 of the LwM2M Gateway specification, based on Objects first introduced in the LwM2M v1.2 specification [LwM2M TS 1.2]. This specification revised the LwM2M Gateway Object for use in retrieving information about IoT devices connected to the LwM2M Gateway.

2. Reference

2.1. Normative References

[BCP 14]	"Key words for use in RFCs to Indicate Requirement Levels", B. Leiba, May 2017, URL: https://www.rfc-editor.org/info/bcp14
[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL: https://www.rfc-editor.org/rfc/rfc2119.txt
[RFC8174]	"Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", B. Leiba, May 2017, URL: https://www.rfc-editor.org/rfc/rfc8174.txt
[LwM2M TS 1.1]	"Lightweight Machine to Machine Technical Specification, Version 1.1", Open Mobile Alliance, June 2019, URL: http://www.openmobilealliance.org/
[LwM2M TS 1.2]	"Lightweight Machine to Machine Technical Specification, Version 1.2", Open Mobile Alliance, November 2020, URL: http://www.openmobilealliance.org/

Table: 2.1. -1 Normative References

2.2. Informative References

[OMADICT]	"Dictionary for OMA Specifications", Version 2.9, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_9, URL: http://www.openmobilealliance.org/
[RFC7254]	"A Uniform Resource Name Namespace for the Global System for Mobile Communications Association (GSMA) and the International Mobile station Equipment Identity (IMEI)", M. Montemurro, Ed., A. Allen, D. McDonald, P. Gosden, May 2014, URL: http://www.ietf.org/rfc/rfc7254.txt
[RFC8141]	"Uniform Resource Names (URNs)", P. Saint-Andre, J. Klensin, April 2017, URL: http://www.ietf.org/rfc/rfc8141.txt
[RFC8464]	"A URN Namespace for Device Identity and Mobile Equipment Identity (MEID)", R. Atarius, September 2018, URL: http://www.ietf.org/rfc/rfc8464.txt
[DevURN]	"Uniform Resource Names for Device Identifiers", J. Arkko, C. Jennings, Z. Shelby, (work in progress), URL: https://datatracker.ietf.org/doc/draft-ietf-core-dev-urn/

Table: 2.2. -1 Informative References

3. Terminology and Conventions

3.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

All sections and appendixes, except "Scope" and "Introduction", are normative, unless they are explicitly indicated to be informative.

3.2. Definitions

Device Objects	The LwM2M Objects exposing resources of the IoT Devices.
Gateway Objects	The LwM2M Objects exposing resources of the LwM2M Gateway. Not to be confused with the LwM2M Gateway Object.
IoT Device	A device connecting to the LwM2M Gateway to be remotely managed by LwM2M Servers. Also referred to as "end IoT device" in this document.
LwM2M Gateway	A device implementing the LwM2M Client to connect IoT Devices to the LwM2M ecosystem and to enable remote management of those devices via the LwM2M protocol.
LwM2M Gateway Object	The LwM2M Object that identifies each IoT Device connected to a LwM2M Gateway with their Objects and Object Instances, that are exposed to the LwM2M Server via the LwM2M Gateway.

Table: 3.2.-1 Definitions

Kindly consult [OMADICT] for more definitions used in this document.

4. Introduction

There are a number of situations why an IoT device may be unable to directly connect to a LwM2M Server. Some IoT devices are not updated to support the LwM2M protocol or some may use a gateway to outsource processing functionality or certain protocol support capabilities. In both cases, the gateway acts on behalf of the end IoT devices and provides a "message routing" capability that enables a LwM2M Server to address these connected end IoT devices, with or without protocol translation functionality. From the point of view of this specification, the differentiation between the two cases is irrelevant.

Note: When using a LwM2M Gateway, the LwM2M messages are exchanged between the LwM2M Server and the LwM2M Gateway. The LwM2M Gateway does not forward LwM2M messages natively to the IoT Device(s). In this sense, it is different from an IP router or a CoAP proxy.

5. Overview

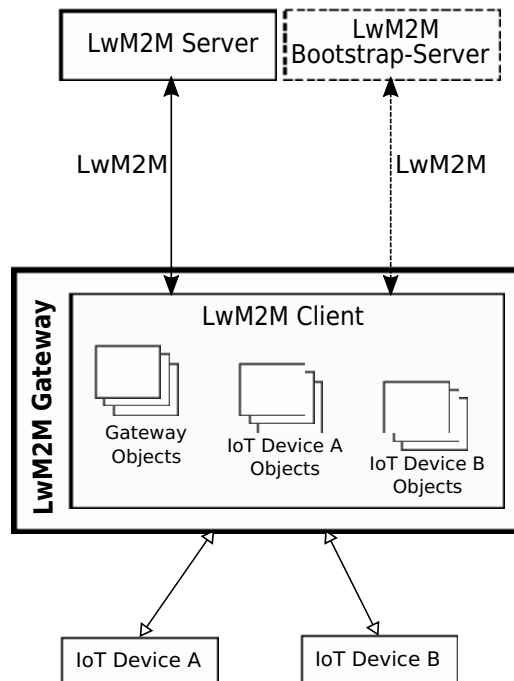


Figure: 5.-1 LwM2M Gateway Overall System Architecture

The LwM2M Gateway is acting as a LwM2M Client and registers with one or several LwM2M Servers. In the above diagram, the IoT Devices A and B are shown connected to the LwM2M Gateway. The number of IoT Devices connected to a LwM2M Gateway may vary by implementation.

Depending on the protocol technology used between the IoT Devices and the LwM2M Gateway, the LwM2M Gateway will take different steps to learn about the capabilities of the IoT Devices and how they map to LwM2M Objects, Object Instances, and Resources that can be exposed to the LwM2M Servers.

Note: Discovery of IoT Devices and their capabilities by the LwM2M Gateway is outside the scope of this specification.

To support the LwM2M Gateway functionality, a new LwM2M Object, namely the LwM2M Gateway Object, is introduced. The LwM2M Gateway Object is defined for each of the IoT Devices connected to it, and includes the Objects and Object Instances that each IoT Device presents to the LwM2M Servers through the LwM2M Gateway. The LwM2M Servers can access these LwM2M Objects under a prefix, unique per IoT Device, similar to an Alternate Path.

6. LwM2M Gateway Object

Description

This object is used by a LwM2M Gateway to maintain the IoT Devices connected to the LwM2M Gateway.

Object definition

Name	Object ID	Object Version	LWM2M Version
LwM2M Gateway	25	2.0	1.1
Object URN		Instances	Mandatory
urn:oma:lwm2m:oma:25:2.0		Multiple	Optional

Table: 6.-1 LwM2M Object: LwM2M Gateway object definition

Resource definitions

ID	Name	Operations	Instances	Mandatory	Type	Range or Enumeration	Units	Description
0	Device ID	R	Single	Mandatory	String			This resource identifies the IoT Device connected to the LwM2M Gateway.
1	Prefix	R	Single	Mandatory	String			This resource defines what prefix MUST be used for access to LwM2M Objects of this IoT Device.
3	IoT Device Objects	R	Single	Mandatory	Corelnk			This resource contains the Objects and Object Instances exposed by the LwM2M Gateway on behalf of the IoT Device. It uses the same CoreLnk format as Registration Interface.

Table: 6.-2 LwM2M Object: LwM2M Gateway Resource definitions

There is one instance of the LwM2M Gateway Object per IoT Device.

As soon as the LwM2M Gateway discovers an IoT Device and has sufficient information, it SHOULD create an instance of the LwM2M Gateway Object. The LwM2M Gateway SHOULD also create the Device Objects associated with the IoT Device. When an IoT Device is no longer manageable by the LwM2M Gateway, the LwM2M Gateway SHOULD delete the associated LwM2M Gateway Object Instance and the associated Device Objects. The LwM2M Servers are informed of the creation and deletion of the LwM2M Gateway Object Instances through the Client Registration Interface operations. As specified below, the Device Objects are not reported in the Client Registration Interface operations.

The *Device ID* Resource in the LwM2M Gateway Object contains an identifier of the IoT Device. This identifier MUST allow the LwM2M Server to uniquely identify the IoT Device. This identifier SHOULD be independent of the LwM2M Gateway used. The usage of the URN format from [RFC8141] is RECOMMENDED. The URN namespaces from [DevURN], [RFC7254], and [RFC8464] are RECOMMENDED.

The value in the *Prefix* Resource in the LwM2M Gateway Object MUST be locally unique. The LwM2M Gateway and the LwM2M Server use the Prefix to identify the targeted IoT Device as specified in the next sections.

The *IoT Device Objects* Resource in the LwM2M Gateway lists the Device Objects and their Instances exposed by the LwM2M Gateway. LwM2M Servers can use the Information Reporting interface to keep track of any changes to the LwM2M Objects and Instances associated with an IoT Device. There is no requirement for the LwM2M Gateway to expose a minimum number of Device Objects nor to expose any specific ones. Exposing LwM2M Objects that are used to control LwM2M protocol functionality, like the LwM2M Server Object or the LwM2M Security Object, are unlikely to be of value for IoT Devices that do not support LwM2M protocol.

How the LwM2M Gateway retrieves the IoT Devices information to create the Device Objects and to populate the LwM2M Gateway Object Instances depends on the technology used between the IoT Device and the LwM2M Gateway. Thus, it is out of the scope of this specification.

7. Security Consideration

As specified in [LwM2M TS 1.1] and [LwM2M TS 1.2], the LwM2M message exchanges between the LwM2M Server and the LwM2M Gateway are secured using the LwM2M-defined technologies.

The security of the message exchanges between the LwM2M Gateway and the IoT Devices is out of the scope of this specification and covered by the specifications defined by the respective communication protocols.

Consequently, the LwM2M protocol does not provide end-to-end security between the IoT Devices and the LwM2M Servers. Note that an end-to-end data security can be accomplished using encrypted values carried in dedicated LwM2M Objects.

The Access Control specified in [LwM2M TS 1.1] and [LwM2M TS 1.2] is not applicable to the Device Objects. LwM2M Servers have full access rights to the Device Objects.

8. LwM2M Interfaces

The LwM2M Gateway MUST support at least the version 1.1 of the LwM2M protocol.

The LwM2M Gateway is a LwM2M Client with the additional features described below. As such, the LwM2M Gateway MUST align with the requirements from [LwM2M TS 1.1] or [LwM2M TS 1.2], depending on the LwM2M protocol version it supports, except if explicitly specified in this document.

8.1. Bootstrap Interface

The Bootstrap Interface can only interact with the Gateway Objects. The IoT Devices can not be managed by the LwM2M Bootstrap-Server, nor be bootstrapped from the Smartcard.

The Bootstrap Information MUST NOT contain any Device Object or Device Object Instance, including when returned as a response to a "Bootstrap-Pack-Request" operation.

When using the Client Initiated Bootstrap Mode or the Server Initiated Bootstrap Mode, the "Bootstrap-Discover", "Bootstrap-Read", "Bootstrap-Write", and "Bootstrap-Delete" operations MUST NOT target any Device Object or Device Object Instance.

When there is no Object ID parameter to the "Bootstrap-Delete" operation, the Device Objects MUST NOT be affected.

When there is no Object ID parameter to the "Bootstrap-Discover" operation, the LwM2M Gateway MUST NOT report the Device Objects.

Note: It is possible to use dedicated LwM2M Objects managed by the LwM2M Server to control security settings of IoT Devices. The definition of such Objects is outside the scope of this specification and likely dependent on the technology used between the IoT Devices and the LwM2M Gateway.

8.2. Client Registration Interface

The Device Objects are not reported in the Client Registration Interface. A LwM2M Server determines the Device Objects and their Instances by inspecting the Resources of the LwM2M Gateway Object Instances. When the LwM2M Gateway creates or deletes an Instance of the LwM2M Gateway Object, it performs an "Update" operation as specified in the LwM2M Protocol.

The Objects and Object Instances parameter of the "Register" and "Update" operations MUST NOT contain any Device Object or Device Object Instance.

8.3. Device Management And Service Enablement and Information Reporting Interfaces

The LwM2M Server interacts normally with the Gateway Objects. Interacting with the Device Objects requires an additional prefix indicating the targeted IoT Device.

8.3.1. Simple Operations

The "Read", "Discover", "Write", "Write-Attributes", "Execute", "Create", "Delete", and "Observe" operations accept an additional and optional parameter:

Parameter	Required	Default Value	Notes
Prefix	No	-	Prefix associated to a IoT Device
Object ID	Yes	-	Indicates the Object.
Other parameters	No	-	Other parameters depending on the operation as specified in \[LwM2M TS 1.1\] or \[LwM2M TS 1.2\]

Table: 8.3.1.-1 Operation Parameters

When the Prefix parameter is not present, the Object ID parameter MUST indicate a Gateway Object. When the Prefix parameter is present, the Object ID parameter MUST indicate an Object of the IoT Device associated with this Prefix.

If the Prefix parameter does not match any IoT Device known to the LwM2M Gateway, the LwM2M Gateway MUST return an error code indicating that the IoT Device was not found.

When the "Discover" operation contains a Prefix parameter (i.e. it targets a Device Object), the returned payload MUST NOT contain the prefix.

In the operation mapping, the Prefix parameter MUST be treated as an Alternate Path. If the LwM2M Gateway is using an Alternate Path, the LwM2M Server MUST append the Prefix parameter to the Alternate Path.

8.3.2. Composite Operations

The "Read-Composite", "Write-Composite", and "Observe-Composite" operations can target the Device Objects by prepending the name of the targeted Object, Object Instance, Resource, or Resource Instance with the Prefix associated to an IoT Device.

The "Read-Composite", "Write-Composite", and "Observe-Composite" operations MAY target Objects from several IoT Devices, and/or the LwM2M Gateway in a single request.

8.3.3. Send Operation

Resources and Resource Instances values from the Device Objects can be part of the reported values. The "Send" operation requirement from [LwM2M TS 1.1] and [LwM2M TS 1.2] is modified as follows. (The modified statement is in italics.)

The reported LwM2M Object Instances (potentially different Object types) MUST have been registered by the LwM2M Client to the LwM2M Server, *or MUST be Device Object Instances*.

9. Data Formats

When the LwM2M Gateway and a LwM2M Server are transferring resource information using one of LwM2M CBOR, SenML JSON/CBOR, or SenML-ETCH JSON/CBOR formats, the Prefix MUST be part of the name of the IoT Device Resources or Resource Instances.

The syntax of the LwM2M CBOR data format is extended as:

```
payload = CBOR_map_with_length 1*(ID, VALUE) / CBOR_infinite_map_start 1*(ID, VALUE) CBOR_break
ID = PREFIX / CBOR_unsigned_integer / CBOR_array_with_length [PREFIX] 1*(CBOR_unsigned_integer) / CBOR_infinite_array_start [PREFIX] 1*(CBOR_unsigned_integer) CBOR_break
VALUE = CBOR_value / payload
PREFIX = CBOR_string
```


10. Example

Imagine a scenario where a LwM2M Gateway has two IoT Devices connected as shown in the LwM2M Gateway Overall System Architecture (Figure 5.1-1 above). The IoT Device A exposes three LwM2M Objects via the LwM2M Gateway, namely:

- LwM2M Device (OID 3)
- LwM2M Firmware Update (OID 5)
- two instances of the IPSO Temperature Object (OID 3303)

The IoT Device B exposes 2 Objects, namely:

- LwM2M Device (OID 3)
- One instance of the IPSO Actuation Object (OID 3306)

Assuming IoT Device A and IoT Device B have device IDs "urn:dev:os:32473-101" and "urn:dev:os:32473-102" respectively, upon their discovery the LwM2M Gateway will create two instances of the LwM2M Gateway Object. It will assign locally unique prefixes, e.g. "d01" and "d02", to the two IoT Devices, and populate the two newly created LwM2M Gateway Object Instances as shown below.

Resource ID	Resource Name	Resource Value
0	Device ID	urn:dev:os:32473-101
1	Prefix	d01
3	End IoT Device Objects	</3/0>;ver=1.2,</5/0>;ver1.1,</3303/0>,</3303/1>

Table: 10.-1 LwM2M Gateway Object Instance 0

Resource ID	Resource Name	Resource Value
0	Device ID	urn:dev:os:32473-102
1	Prefix	d02
3	End IoT Device Objects	</3/0>;ver=1.1,</3306/0>

Table: 10.-2 LwM2M Gateway Object Instance 1

Assuming the LwM2M Gateway is provisioned with a single LwM2M Server Account and supports the Firmware Update Object, when registering, or updating its registration to the LwM2M Server, the LwM2M Gateway presents the following list of Objects and Object Instances:

```
</1/0>,</3/0>,</5/0>,</25/0>,</25/1>
```

The two LwM2M Gateway Object Instances inform the LwM2M Server that two IoT Devices are connected to the LwM2M Gateway. The LwM2M Server need to perform a "Read" operation on the LwM2M Gateway Object Instances to determine:

- the IDs of the IoT Devices connected to the LwM2M Gateway,
- the Prefix to access the LwM2M Objects exposed by each IoT Device through the LwM2M Gateway, and
- the list of Objects and Object Instances exposed by the IoT Devices.

The LwM2M Server can retrieve the values of the first Instance of the IPSO Temperature Object of the IoT Device A by sending to the LwM2M Gateway a "Read" operation with the following parameters:

Parameter	Value
Prefix	d01
Object ID	3303
Object Instance ID	0

Table: 10.-3 Example "Read" Operation Parameters

Using the CoAP mapping, this operation is mapped to a `GET /d01/3303/0`.

Here the LwM2M Gateway relies on the Prefix to determine which IoT Device is targeted by the "Read" operation. Retrieving the values from the IoT Device depends on the protocol technology used between the IoT Device and the LwM2M Gateway, and is out of the scope of this specification.

The LwM2M Gateway will then return the values to the LwM2M Server. A possible response, encoded in SenML JSON, is:

```
[
  {"bn":"/d01/3303/0/", "n":"5700", "v":22.1},
  {"n":"5601", "v":17.5},
  {"n":"5602", "v":23.9},
  {"n":"5701", "vs":"Cel"}
]
```

Likewise, the LwM2M Server can read the manufacturer name and the battery level of both IoT Devices by sending to the LwM2M Gateway a "Read-Composite" operation with the following parameter:

```
[
  {"bn":"/d01/3/0/","n":""},
  {"n":"/9"},
  {"bn":"/d02/3/0/","n":""},
  {"n":"/9"}
]
```

A possible response, encoded in LwM2M CBOR, is:

```
A2      # map(2)
  83     # array(3)
    63   # text(3)
      643031 # "d01"
    03   # unsigned(3)
    00   # unsigned(0)
  A2     # map(2)
    00   # unsigned(0)
    69   # text(9)
      436F6D70616E792041 # "Company A"
```

```
09      # unsigned(9)
18 64   # unsigned(100)
83      # array(3)
63      # text(3)
  643032 # "d02"
03      # unsigned(3)
00      # unsigned(0)
A2      # map(2)
  00     # unsigned(0)
  69     # text(9)
    436F6D70616E792042 # "Company B"
09      # unsigned(9)
18 41   # unsigned(65)
```

interpreted as the CBOR diagnostic notation as:

```
{
["d01", 3, 0]: {0: "Company A",
               9: 100},
["d02", 3, 0]: {0: "Company B",
               9: 65}
}
```

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-LWM2M_Gateway-V1_1-20210518-A	18 May 2021	Status changed to Approved by DMSE WG on 18 May 2021.
OMA-TS-LWM2M_Gateway-V1_1_1-20240312-A	12 Mar 2024	Status changed to Approved by DMSE WG on 12 Mar 2024.

Table: A.1-1 Approved Version History