|  |
| --- |
| C:\Users\grayv\Desktop\oneM2M-Logo.gif |

|  |  |
| --- | --- |
| **oneM2M**  **Technical Report** | |
| Document Number | oneM2M-TR-0053-V-0.1.0 |
| Document Name: | Lightweight oneM2M Services |
| Date: | 2018-05-02 |
| Abstract: | The document is a study of lightweight oneM2M services. Based on the result of the study, it identifies proposed optimizations and enhancements to the oneM2M system to streamline and optimize its features and services. |
| Template Version: January 2017 (Do not modify) | |

The present document is provided for future development work within oneM2M only. The Partners accept no liability for any use of this report.

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

© 2017, oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TSDSI, TTA, TTC).

All rights reserved.

The copyright and the foregoing restriction extend to reproduction in all media.

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 Definitions, symbols and abbreviations 4

3.1 Definitions 4

3.2 Symbols 5

3.3 Abbreviations 5

4 Conventions 5

5 Introduction 5

6 Analysis of Limitations of Existing oneM2M Service Functions for Constrained IoT Devices 5

6.1 Limitations of oneM2M Service Function 1 5

6.2 Limitations of oneM2M Service Function X 5

7 Potential Solutions 6

7.1 Solution A 6

7.1.1 Solution Applicability 6

7.1.2 Solution Description 6

7.2 Solution X 6

8 Conclusions 6

Annexes 6

History 7

# Scope

This document is a study of lightweight oneM2M services. Based on the result of the study, it identifies proposed optimizations and enhancements to the oneM2M system to streamline and optimize its features and services.

# References

The following text block applies.

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.

## Normative references

Normative references are not applicable in the present document.

## Informative references

Clause 2.2 shall only contain informative references which are cited in the document itself.

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>.

# Definitions, symbols and abbreviations

Delete from the above heading the word(s) which is/are not applicable.

## Definitions

Clause numbering depends on applicability.

* **A definition shall not take the form of, or contain, a requirement.**
* **The form of a definition shall be such that it can replace the term in context. Additional information shall be given only in the form of examples or notes (see below).**
* **The terms and definitions shall be presented in alphabetical order.**

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply:

Definition format

**<defined term>:** <definition>

If a definition is taken from an external source, use the format below where [N] identifies the external document which must be listed in Section 2 References.

**<defined term>**[N]: <definition>

**example 1:** text used to clarify abstract rules by applying them literally

NOTE: This may contain additional information.

## Symbols

Clause numbering depends on applicability.

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

Symbol format

<symbol> <Explanation>

<2nd symbol> <2nd Explanation>

<3rd symbol> <3rd Explanation>

## Abbreviations

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

Abbreviation format

<ABREVIATION1> <Explanation>

<ABREVIATION2> <Explanation>

<ABREVIATION3> <Explanation>

# 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].

# Introduction

*Editor’s Note: This section provides background information, including: 1) primary features of constrained IoT devices and constrained IoT access networks; 2) the challenges for supporting oneM2M service functions on constrained IoT devices; 3) the benefits of designing lightweight oneM2M services.*

# Analysis of oneM2M Functionality

*Editor’s Note: This section analyses and summarizes potential limitations and/or optimizations to the existing oneM2M functionality (e.g. subscription and notification mechanisms, access control mechanisms, addressing schemes, request/response primitives and message exchange, resource discovery mechanism, registration procedures, CSE-to-AE re-targeting mechanisms, etc.) and potential requirements.*

## Analysis of oneM2M Messages and Potential Requirement

### Introduction of oneM2M Messages

**Figure 6.1.1-1** from oneM2M TS-0001 shows the general communication flow in oneM2M that governs the information exchange over Mca, Mcc, and Mcc’ reference points (i.e. between an Application Entity (AE) and a Common Service Entity (CSE) or between two CSEs), which is based on the use of Request and Response messages. Such communications can be initiated either by the AEs or by the CSEs depending upon the operation in the Request message. For example, an AE can send a request message to a hosting CSE for application registration; then, the AE can send another request message to the hosting CSE to subscribe to certain resources; lastly, the hosting CSE may send request messages (i.e. notifications) to the AE when the status of subscribed-to resources has been changed.



Figure 6.1.1-1: General Flow in oneM2M

oneM2M provides several advanced features for processing a request message and generating a corresponding response message via some new request parameters as described in **Table 6.1.1-1**. For example, the parameter “***Request Expiration Timestamp***”, if included in a request message, indicates when the request message expires. Similarly, each response message contains some response parameters as listed in **Table 6.1.1-2**. For instance, the parameter “***Result Expiration Timestamp*** ”, if contained in a response message, indicates when the response message expires. In addition, the parameter “***Content***” contains a resource representation, which can be present in a request message for creating/updating a resource or in a response message for retrieving a resource. The resource representation includes the attributes of the targeted resource.

Table 6.1.1-1: Summary of Request Parameters in oneM2M (Adapted from oneM2M TS-0001)

| Request Message Parameters | |
| --- | --- |
|
| ***Mandatory*** | ***Operation*** - operation to be executed |
| ***To*** - the address of the target resource on the target CSE |
| ***From*** - the identifier of the message Originator |
| ***Request Identifier*** - uniquely identifies a Request message |
| ***Operation dependent*** | ***Content*** - to be transferred |
| ***Resource Type*** - of resource to be created |
| ***Optional*** | ***Originating Timestamp*** - when the message was built |
| ***Request Expiration Timestamp*** - when the request message expires |
| ***Result Expiration Timestamp*** - when the result message expires |
| ***Operational Execution Time*** - the time when the specified operation is to be executed by the target CSE |
| ***Response Type*** - type of response that shall be sent to the Originator |
| ***Result Persistence*** - the duration for which the reference containing the responses is to persist |
| ***Result Content*** - the expected components of the result |
| ***Event Category*** - indicates how and when the system should deliver the message |
| ***Delivery Aggregation*** - aggregation of requests to the same target CSE is to be used |
| ***Group Request Identifier*** - Identifier added to the group request that is to be fanned out to each member of the group |
| ***Filter Criteria*** - conditions for filtered retrieve operation |
| ***Discovery Result Type*** - format of information returned for Discovery operation |
| ***Security Info*** - information about the ***Content*** if it contains security parameters |
| ***Token Request Indicator*** - indicating that the Originator may attempt Token Request procedure (for Dynamic Authorization) if initiated by the Receiver |
| ***Tokens*** - for use in dynamic authorization |
| ***Token IDs*** - for use in dynamic authorization |
| ***Role IDs*** - for use in role based access control |
| ***Local Token IDs*** - for use in dynamic authorization |

Table 6.1.1-2: Summary of Response Parameters in oneM2M (Adapted from oneM2M TS-0001)

| Response Message Parameters |
| --- |
|
| ***Response Status Code***  - successful, unsuccessful, ack |
| ***Request Identifier*** - uniquely identifies a Request message |
| ***Content*** - to be transferred |
| ***To*** **-** the identifier of the Originator or the Transit CSE that sent the corresponding non-blocking request |
| ***From*** - the identifier of the Receiver |
| ***Originating Timestamp* -** when the message was built |
| ***Result Expiration Timestamp***  - when the message expires |
| ***Event Category*** - what event category shall be used for the response message |
| ***Security Info*** - information about the ***Content*** if it contains security protocols |

### Limitations of oneM2M Messages

Request and response parameters as listed in **Table 6.1.1-1** and **Table 6.1.1-2** could make a oneM2M request or response message large. In the meantime, multiple consecutive request (or response) messages could contain the same request (or response) parameters with the same value; in another case, resource attributes contained in the “Content” parameter could be unexpected by the requestor or redundant in multiple consecutive messages. Such a large request or response message could be a burden for constrained IoT devices and/or networks with limited communication bandwidths. For example, the maximum layer-2 frame size for LoRaWAN at both US 915 MHz and EU 868 MHz band is 250 bytes, and the frame size in IEEE 802.15.4 networks is up to 127 bytes. The length of an oneM2M message if containing various request and response parameters could easily go beyond the maximum frame size which can be supported by the underlying Low-Power Wide Area Networks (LPWAN) like LoRaWAN or Low-Power Wireless Personal Area Networks (LoWPAN) such as IEEE 802.15.4.

**Figure 6.1.2-1** illustrates a smart metering use case, where each cellular UE smart meter uses low-power wide-area access technologies such as 3GPP Narrow-Band Internet of Things (NB-IoT) to communicate with a Server where an IoT service layer resides for storing and managing meter data from various UEs; the Server could be deployed by an electricity company. Basically, there could be a smart meter application running on each UE to periodically send meter readings to the Server. In addition, multiple smart meters (e.g. deployed in the same community) may report their readings to the Server in the same way (e.g. reporting frequency, how request messages shall be processed by the Server, etc.). As such, each smart meter may repeatedly send similar request messages to the Server, and multiple meters may also send similar request messages to the Server at different times. These two aspects are abstracted and discussed furthermore in **Figure 6.1.2-2** and **Figure 6.1.2-3**.



Figure 6.1.2-1: Smart Metering Use Case based on Cellular IoT

**Figure 6.1.2-2** illustrates interactions between an application and a service layer. In this example, the application (e.g. smart meter application on a smart meter in **Figure 6.1.2-1**) repeatedly sends request messages to the service layer. Each request message contains a set of request parameters; likewise, the corresponding response message contains response parameters. In addition, the application may request the same services/resources from the service layer during certain time durations; thus, each repeated request message includes the same set of request parameters.

**Figure 6.1.2-3** shows another example, where multiple applications (e.g. smart meter applications on smart meters in **Figure 6.1.2-1**) interact with the same service layer. In this scenario, although three (or more) applications could access different service/resources, they may instruct the service layer to process their request messages in the same way. For example, they may indicate to the service layer: the same request message expiration time, the same result expiration time, etc. Therefore, the request message from each application may contain the same set of request parameters.



Figure 6.1.2-2: Interactions between an Application and a Service Layer



Figure 6.1.2-3: Interactions between Multiple Applications and a Service Layer

The following limitations of oneM2M communication flow for constrained IoT devices are identified:

1. If a oneM2M request (or response) message contains too many request (or response) parameters, it cannot be sent in one layer-2 frame, which causes high message overhead and increases message transmission latency.
2. If a oneM2M request (or response) message is contained in multiple layer-2 frames, the loss of one layer-2 frame will results in the failure of oneM2M message delivery.
3. Even if a oneM2M request (or response) message can be completely contained in one layer-2 frame, the large size of the oneM2M message increases the message loss probability over the wireless channel.
4. Parameters contained in multiple consecutive oneM2M request (or response) messages could be the same and redundant, which increases message overhead unnecessarily.
5. The resource representation in the “Content” parameter may contain some extra attributes which are not expected or required by the requestor.
6. The resource representation in the “Content” parameter from multiple consecutive oneM2M request (or response) messages may contain the same or redundant attributes, which causes extra message overhead unnecessarily.
7. The oneM2M service layer does not currently support any compression mechanisms and is unable to leverage existing header compression protocols (e.g. IETF RFC 3095 for robust header compression) which have been designed for network layer, transport layer, and application protocol layer. None of these are directly applicable to the oneM2M service layer.

### Potential Requirements

1. The oneM2M System shall support suitable request/response message interaction between a service layer and a constrained IoT device with low latency.
2. The oneM2M System shall support suitable request/response message interaction between a service layer and a constrained IoT device with low communication overhead.
3. The oneM2M System shall support suitable approaches for constrained IoT device to minimize request message size.
4. The oneM2M System shall support suitable approaches for constrained IoT device to minimize response message size.
5. The oneM2M System shall support suitable approaches for constrained IoT device to remove unrequired or redundant attributes from the resource representation as contained in the “Content” parameter.

### Potential Solutions

*Editor’s Note: The section describes potential solutions related to optimizing/enhancing the oneM2M function to address the identified limitations and requirements.*

## Limitations of oneM2M Function X

# Conclusions

*Editor’s Note: This clause provides a summary of the conclusions drawn during the study*

# Annexes

Each annex **shall** start on a new page (insert a page break between annexes A and B, annexes B and C, etc.).

Use the **Heading 9** style for the title and the Normal style for the text.

Annex <A>:  
Title of annex *(style H9)*

<Text>

<PAGE BREAK>

# History

|  |  |  |
| --- | --- | --- |
| **Publication history** | | |
| V.1.1.1 | <dd Mmm yyyy> | <Milestone> |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

| **Draft history** (to be removed on publication) | | |
| --- | --- | --- |
| V0.0.1 | 2018-03-01 | Skeleton of the TR |
| V0.1.0 | 2018-05-02 | Update to include ARC-2018-0052R02-Limitations\_of\_oneM2M\_Messages which was agreed at ARC34 |