oneM2M Technical Report	oneM2M Technical Report
Document Number	TR-0063-V-0.0.2
Document Name:	Effective IoT Communication to Protect 3GPP Networks\
Date:	<2024-04-24>
Abstract:	< An abstract of the document and information that may be used in subsequent electronic searches>
Template Version: January 2020 (do not modify)	

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

Contents

1 Scope

Mass deployment of IoT devices, is causing an increased risk of signalling floods e.g. by concurrently transmitting IoT devices and hence causing a risk for the stability- and the efficient use of their mobile networks. One of the reasons is that IoT customers or integrators, often do not considering the specifics of mobile networks in their IoT device application design, subsequently causing inefficient communication or even loss of reachability. Operators are increasingly reporting problems from their live networks, like masses of concurrently resetting and reattaching devices within a small geographical region. Such events may cause their networks to collapse. GSMA has already flagged such events and has started to address the subject of badly behaving IoT devices / Applications. To avoid such scenarios upfront, GSMA released TS.34, “IoT Device Connection

Efficiency Guideline" [1] . GSMA TS. 34 [1] gives guidance, which IoT device applications need to consider, to safely- and efficiently cooperate with cellular networks. However, the drawback of guidelines is the fact that the target audience: a.) needs to be aware of the existence of such guidelines and b.) needs to read, understand and follow such guidelines. This work aims to check and enhance oneM2M as an Embedded Service Layer in a way that the requirements formulated in GSMA TS.34 [1] are taken into account and Applications developed not considering requirements in GSMA TS.34 [1] , do not create adverse effects in the network, because the oneM2M as Embedded Service Layer is shielding the network from badly behaving applications. GSMA TS. 34 [1] is already referring towards an evolution of an IoT Service Architecture, where the IoT Device Applications are becoming disaggregated from an Embedded Service Layer. Such an Embedded Service Layer is providing several generic IoT functionalities (e.g. device management, security, location, application framework. . .). The common service layer specified by oneM2M complies to this IoT Service Architecture.

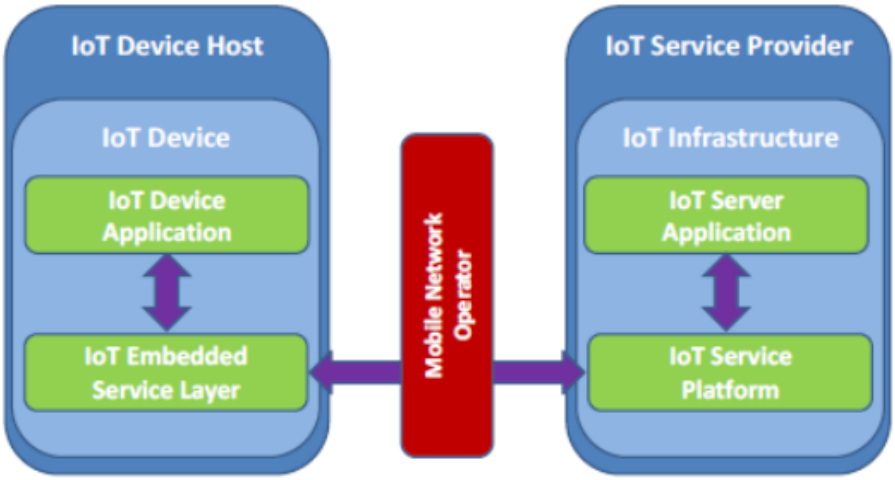

Figure 1: Figure 1-1: Generalised "Layered" IoT Service Architecture, as depicted GSMA TS 34 Figure 3

Applications being deployed on top of a common service layer are less critical to the network, because the common service layer takes over a protection role for the network. Inefficient or even harmful activities of applications would be prevented upfront and can't hit the network. On the other hand, oneM2M provides functionality for the applications, e.g. scheduling transmissions according to the service needs. The recommended evolved architecture in GSMA TS.34 [1] (refer Figure 1X) aligns well with the oneM2M architecture shown in Fig 1-1.

oneM2M with the CSE functionality in between the IoT Application and the network connectivity, is well suited to enforce the requirements being addressed

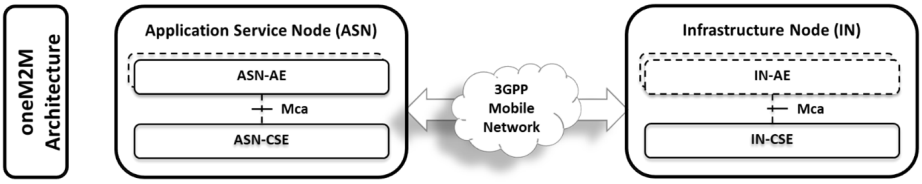

Figure 2: Figure 1 2: oneM2M architecture for CIoT devices

in GSMA TS.34 [1] , and hence protect the network from unwanted signalling floods and enforces an efficient communication, even if the Application (AE) has been created without GSMA TS.34 [1] knowledge or compliance. This TR is analysing which functionalities recommended by GSMA TS.34 [1] being in scope of an Embedded Service Layer are already covered by oneM2M functionality (e.g. like in CDMH), and which GSMA TS.34 [1] functionality is missing from oneM2M, to identify it and enhance oneM2M accordingly to meet the GSMA TS.34 [1] recommendations.

2 References

The following text block applies.

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

2.1 Normative references

As a Technical Report (TR) is entirely informative it shall not list normative references.

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

Not applicable.

2.2 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.

- [1] GSM Association Official Document TS.34 “IoT Device Connection Efficiency Guidelines”

- [i.2] oneM2M Drafting Rules https://member.onem2m.org/static_Pages/others/Rules_Pages/oneM2M-Drafting-Rules-V1%202%202.doc
- [i.3] oneM2M TS-0001: "Functional Architecture"
- [i.4] oneM2M TS-0018: "Test Suite Structure & Test Purposes"
- [i.5] oneM2M TS-0025: "Definition of Product Profiles"
- [i.6] oneM2M TS-0026: "3GPP Interworking"

3 Definition of terms, symbols and abbreviations

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

3.1 Terms

IoT Device : The combination of both the IoT Device Application and the Communications Module.

Well-known location: a target URI in the oneM2M CSE resource tree that is a place where you should store information that is expected to be at the same location on every oneM2M CSE.

3.2 Symbols

Clause numbering depends on applicability.

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

Symbol format

```
&lt;symbol>    &lt;Explanation>
&lt;2nd symbol>    &lt;2nd Explanation>
&lt;3rd symbol>    &lt;3rd Explanation>
```

3.3 Abbreviations

Abbreviations should be ordered alphabetically.

Clause numbering depends on applicability.

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

Abbreviation format

```
&lt;ABBREVIATION1>    &lt;Explanation>
&lt;ABBREVIATION2>    &lt;Explanation>
&lt;ABBREVIATION3>    &lt;Explanation>
```

4 Conventions

The key words “Shall”, “Shall not”, “May”, “Need not”, “Should”, “Should not” in this document are to be interpreted as described in the oneM2M Drafting Rules [i.2]

5 Analysis of GSMA TS.34 Requirements

<Text>

5.1 Introduction

GSMA TS.34 [1] represents a guideline and giving requirements for whole IoT Device, as defined in Figure X to ensure an efficient connection.

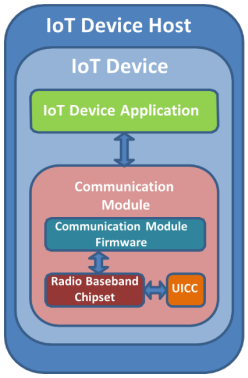

Figure 3: Figure 5.1-1: Generalised IoT Device Architecture according to GSMA TS.34[1]

Requirements with regards to an efficient communication are grouped and categorized in TS.34 [1] . E.g. requirements are formulated for the following areas:

- IoT Device Application Requirements
- Communication Module Requirements
- IoT Service Provider Requirements
- Policy-based Connection Efficiency Requirements
- Radio Policy Manager Requirements
- 3GPP Connection Efficiency Features

oneM2M is most beneficially able to support an efficient communication in the area of the IoT Device Application, while other areas, like required support of “3GPP Connection Efficiency Features” can be considered out of scope of oneM2M, and hence out of scope of this WI. With regards to “IoT Device Application Requirements”, GSMA TS.34 [1] differentiates further between:

1. Monolithic IoT Device Application Requirements: Those requirements are applicable for devices without an embedded Service layer and hence are out of scope oneM2M anyway.
2. Tiered IoT Device Applications Requirements: Those requirements are applicable for applications providing the required functionality according to GSMA TS.34 [1] , cooperatively together with the embedded Service layer.
3. IoT Embedded Service Layer Requirements: Those requirements are applicable for the embedded Service layer, providing the required functionality according to GSMA TS.34 [i.1]

While the main focus of this work is primarily on 2) and 3) further requirements in GSMA TS.34 [1] have been screened, analysed and used to inspire functionality to be taken for oneM2M to ensure an efficient IoT communication.

The considered Requirements out of GSMA TS.34 [1] in the context of oneM2M are listed in the subsequent sections, with the respective numbering schema kept as used in TS.34 [1] , for your reference.

5.2 IoT Device Requirements

Table 2: Table 5.2-1: GSMA defined requirements from GSMA TS 34 [1]

Requirement ID	Description from GSMA TS 34 [1]	Reference clause
TS.34_3.0_REQ_001	The IoT Device SHOULD conform to all IoT Device Application requirements defined in TS.34, section 4.	5.4
TS.34_3.0_REQ_002	The IoT Device SHALL conform to all Communication Module requirements defined in TS.34, section 5.	Not within the scope of oneM2M
TS.34_3.0_REQ_003	The IoT Device SHOULD conform to GSMA TS.24 “Operator Minimum Acceptance Values for Device Antenna Performance” [x].	Not within the scope of oneM2M

Requirement ID	Description from GSMA TS 34 [1]	Reference clause
TS.34_3.0_REQ_004	When required by the Mobile Network Operator, the IoT Device SHALL be certified by the GCF and/or the PTCRB.	Recommended by oneM2M. Conformance test cases are defined in TS-0018 [i.4]. Profiles are defined in TS-0025 [i.5]

5.3 IOT Device Application Requirements

This clause is derived from GSMA TS.34 [1] , clause 4. Two architectures are described in GSMA TS.34 [1] , where the IoT Device application can be a monolithic application that meets all the requirements in clause 4.0 or an evolved architecture that separates the device application requirements into clause 4.1 and the IoT embedded service layer requirements into clause 4.2. This technical report addresses the evolved architecture. The remainder of this section is organized by the components shown in figure 5.3-1.

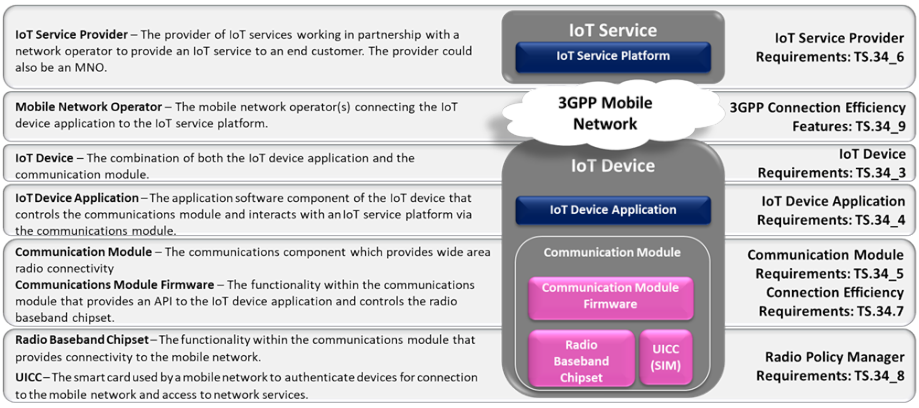

Figure 4: Figure 5.3-1: Requirements for CIoT solutions

5.4 Tiered IoT Device Application Requirements

In the GSMA evolved architecture the Tiered IoT Device Application performs the business logic of the IoT solution. The GSMA requirements for such an application are captured in table 5.4-1.

Table 3: Table 5.4 1: Tiered IoT Device Requirements

Requirement ID	Description from GSMA TS 34 [1]	Reference clause
TS.34_4.1_REQ_001	If data speed and latency is critical to the IoT Service the IoT Device Application should be able to retrieve mobile network speed and connection quality information from the IoT Embedded Service Layer in order to request the appropriate quality of content from the IoT Service Platform.	See clause 6.1
TS.34_4.1_REQ_002	The IoT Device Application should always be prepared to handle situations when communication requests fail, when such failure is reported by the IoT Embedded Service Layer.	See clause 6.2

Requirement ID	Description from GSMA TS 34 [1]	Reference clause
TS.34_4.1_REQ_003	Each time there is a need to send data over the mobile network the IoT Device Application should classify the priority of each communication. For example, the IoT Device Application should distinguish between data that requires instantaneous transmission and delay tolerant data that could be aggregated and/or sent during non-peak hours. Such information about the priority of the communication should be communicated to the IoT Embedded Service Layer.	See below [UPDATE THIS]
TS.34_4.1_REQ_004	When an IoT Device Application does not need to perform regular data transmissions and it can tolerate some latency for its IoT Service, it should communicate this information to the IoT Embedded Service Layer so that it can use this information in its interactions with the network.	See below [UPDATE THIS]

6 oneM2M Solutions for for Efficient Communications over 3GPP networks

6.1 Use Case / Solution 1

Editor's Note: To define call flows that implement the requirements described in clause 5.

7 Example scenarios to protect 3GPP networks

7.1 Introduction

Editor's Note: This clause proposes examples that are used to describe solutions in clause 6

7.2 Scenario 1

8 Proposed oneM2M Enhancements

8.1 Introduction

Editor's Note: This clause proposes enhancements to existing specifications if any that are identified in Clause 6

8.2 Enhancement 1 Description

Editor's Note: This clause describes a specific change

9 Conclusion

9.1 Introduction

Editor's Note: This clause describes the coverage of GSMA TS.34 requirements. Identifies possible feedback to GSMA for further work on this topic.

Proforma copyright release text block

This text box shall immediately follow after the heading of an element (i.e. clause or annex) containing a proforma or template which is intended to be copied by the user. Such an element shall always start on a new page.

Notwithstanding the provisions of the copyright clause related to the text of the present document, oneM2M grants that users of the present document may freely reproduce the <proformatype> proforma in this {clause|annex} so that it

can be used for its intended purposes and may further publish the completed <proformatype>.

<PAGE BREAK>

Annexes

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

Annex <A>:

Title of annex

<Text>

<PAGE BREAK>

Annex <B>:

Title of annex

<Text>

First clause of the annex

<Text>

B.1.1 First subdivided clause of the annex

<Text>

<PAGE BREAK>

Annex <y>:

Bibliography The annex entitled “Bibliography” is optional.

It shall contain a list of standards, books, articles, or other sources on a particular subject which are not mentioned in the document itself.

It shall not include references mentioned in the document.

- <Publication>: “<Title>”.

OR

<Publication>: “<Title>”.

<PAGE BREAK>

History

This clause shall be the last one in the document and list the main phases (all additional information will be removed at the publication stage).

Publication history	Publication history	Publication history
V1.1.1	<yyyy-mm-dd>	<Milestone>

Draft history (to be removed on publication)	Draft history (to be removed on publication)	Draft history (to be removed on publication)
V0.0.2	<2024-04-25>	SDS-2021-0085R04-protect_the_network_intro SDS-2024-0053-Initial_conversion_to_markdown